ZETES TSP QUALIFIED CA

CERTIFICATION PRACTICE STATEMENT

Certification Practice Statement

for the

ZETES TSP Qualified CA

Publication date :	**27/07/2016**		
Effective date :	**29/06/2016**		
Document OID :	**1.3.6.1.4.1.47718.2.1.1.2**		
Version :	**1.0**	**27/06/2016**	**approved by PMA**

Table of Content

Figures

Tables

ABOUT THIS DOCUMENT

The present document is the Certification Practice Statement (CPS) for the ZETES TSP Qualified CA.

Intellectual Property Rights

Document Version History

Version	Publication Date	Effective Date	Information about this Version
1.0	27/06/2016	29/06/2016	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 smart cards. 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 1130 Brussel België BTW BE 0408 425 626	Rue de Strasbourg 3 1130 Bruxelles Belgique TVA BE 0408 425 626	Rue de Strasbourg 3 1130 Brussels Belgium 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

Within Zetes SA the business unit Zetes CardS provides card personalisation services and fulfilment services to governments, the financial sector and private organisations.

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 Certification Service Provider (CSP) as defined in the Belgian Law of 9 July 2001 which implements the European Directive 1999/93/EC on a Community framework for electronic signatures.

The ZETES TSP hierarchy of CAs consist of a root CA which issues certificates to sub-CAs operated by ZETES TSP.

The ZETES TSP Qualified CA issues Qualified Certificates and non-Qualified Certificates to natural persons. The present document is the Certification Practice Statement for this CA.

1 INTRODUCTION

1.1 Overview

This Certification Practice Statement applies to the issuance of Normalized Certificates and Qualified Certificates as defined in the EU Directive 1999/93/EC on a Community framework for electronic signatures.

These certificates are issued by the ZETES TSP Qualified CA. Every certificate issued by the ZETES TSP Qualified CA will carry a Certificate Policy OID corresponding to the assurance level of that Certificate as stated in the applicable ZETES TSP (Qualified) Certificates Certificate Policy.

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

- the present ZETES TSP Certification Practice Statement (CPS),
- the ZETES TSP (Qualified) Certificates Certificate Policies (CP),
- and the ZETES TSP (Qualified) Certificates Terms and Conditions (CTC).

Conformity with RFC 3647

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

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

This CPS is in accordance with requirements laid down in the Directive 1999/93/EC of the European Parliament and Council on a Community framework for electronic signatures and with the requirements laid down in the Regulation 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. Also, this CPS conforms to the 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.

Non-disclosure

Section 3.6 of the RFC 3647 and clause 5.2 of the ETSI EN 319 411-2 provide for the use of references to divide disclosures between public information and security sensitive confidential information. For reasons of confidentiality, ZETES cannot disclose all details on controls in this CPS, but instead included references to internal detailed documents. These documents will only be made available to duly authorised auditors.

1.2 Document name and identification

This document is called the 'ZETES TSP (Qualified) Certificates – Certification Practice Statement'.

The unique OID for this Certification Practice Statement is:

dotted notation	1.3.6.1.4.1.47718.2.1.1.2
full notation	{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) zetes(47718) zetes-tsp(2) cs(1) cert practice-statement(1) qca(2) }

1.3 PKI participants

In the context of issuing (Qualified) Certificates, ZETES TSP is acting as the Certification Service Provider (CSP). ZETES TSP has final and overall responsibility for the provision of the ZETES (Qualified) Certificates offering, namely:

- the provision service for the Secure Subject,
- the personalisation and delivery service for the Secure Subject Device,
- the Certificate generation services through the ZETES TSP Certification Authority,
- 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),
- the Dissemination Services.

ZETES TSP is only one of several PKI participants. The PKI participants are all the legal entities who are involved in any of the processes and activities of ZETES TSP as a 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 Certificate Practice Statements and Certificate Policies that are maintained by ZETES TSP.

PKI participants are defined as follows:

Subscribers	An organization that enters into a contractual agreement with ZETES TSP on behalf of Subjects
Subjects	Natural persons whose identity or identifier is encoded in the end user certificate issued by a CA. A Subject adheres to a Subscriber.
Relying Parties	Third parties who rely on the validity of the certificate issue by the CA for authentication or for validation of a transaction or document
CA - Certification Authorities	Certification Authority which issues 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 Subject device/card personalisation services for Secure Subject Devices/Cards and the CA. It is the only part of the RA that is in direct contact with the CA or with the card personalisation infrastructure.
SUB-RA - Subordinate Registration Authorities	The 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	A 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.
L-SRA - Suspension and Revocation Authority	A local representative of the SUB-SRA, who performs the front-office request procedure and vetting procedure for a Subject requesting suspension or revocation of the Subject's certificate.
Publication and Repository Services	Online publication of documents such as Certificate Practice Statements, Certificate Policies, Certificates Terms and Conditions, certificate validation data such as root certificates, certificate revocation lists, etc.
Subject Device Provisioning Services more commonly referred to as Card Provisioning Services	The Subject Device is also referred to as "card" or as "SSCD" for Secure Signature Creation Device or "QSCD" for Qualified Signature Creation Device. ZETES TSP supplies the device to the Subscribers and Subjects. The device is usually a PKI smartcard but can also be another form factor such as a USB PKI device.

Subject Device Personalisation and Delivery Services more commonly referred to as Card Personalisation and Delivery Services	Card personalisation services by Zetes CardS, i.e. the process of printing the card body, encoding the chip and generating the cryptographic keys on the chip, printing the PIN/PUK letter, etc. Card Delivery Services i.e. the process of distributing the cards and PIN/PUK letters to the Subjects and/or card issuing points.

This CPS covers the following combination of roles and organization of PKI participants:

- The role of Registration Authority and the role of Suspension & Revocation Authority are combined. Any further references to Registration Authority entities in the CPS and in the CP implicitly refer to the equivalent Suspension & Revocation Authority entities.
- The Subordinate RA and Local RA always belong to or depend on the Subscriber

This is illustrated by the following diagram:

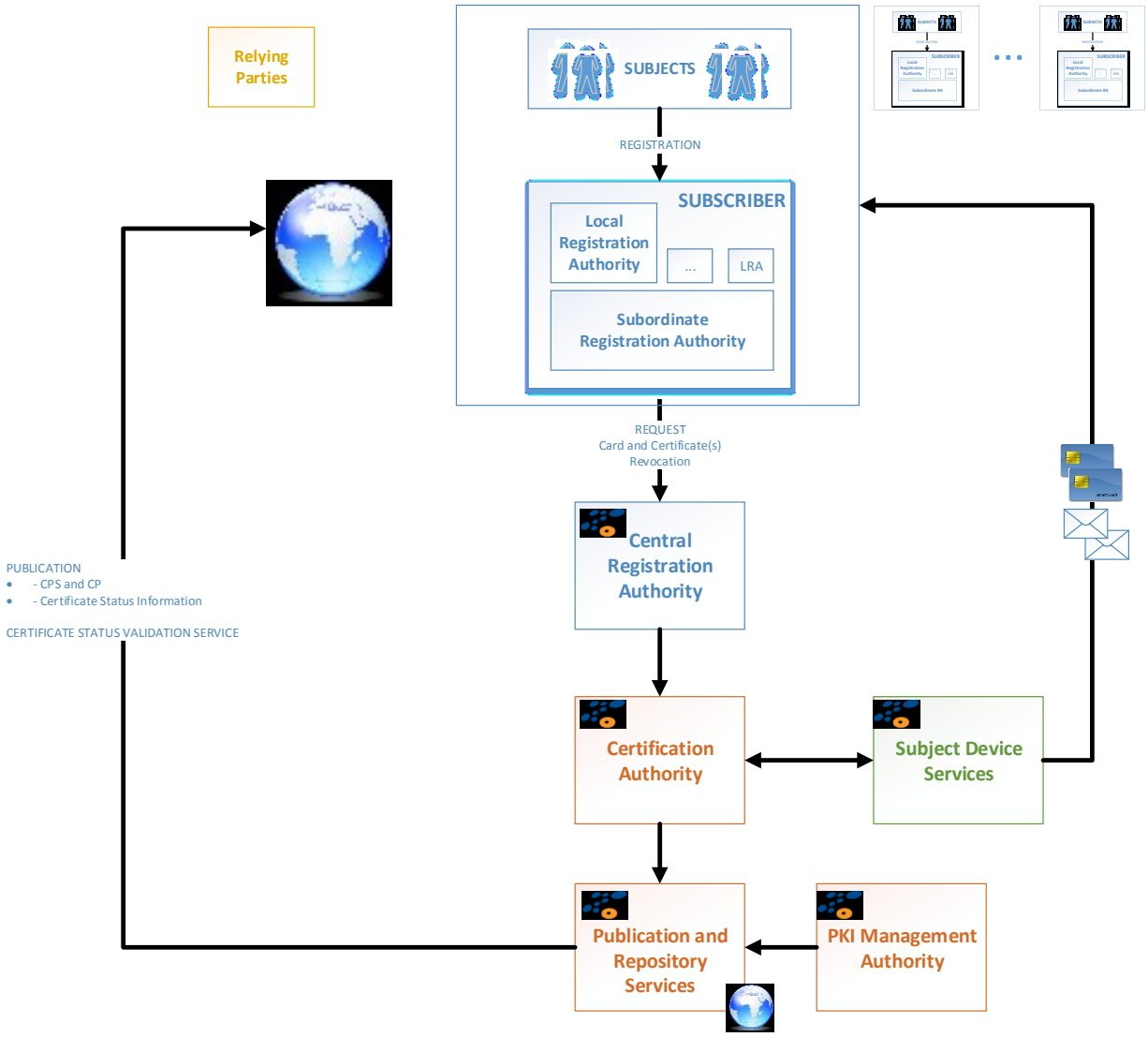


Figure 1 Diagram of the PKI participants

1.3.1 Certification Authorities (CA)

CAs are responsible for:

- Issuing certificates;
- Issuing CRLs (Certificate Revocation List) on a regular basis or when a certificate status change occurs;
- Providing OCSP (On-line Certificate Status Protocol) services

ZETES TSP operates a 2-level CA hierarchy for issuing Normalized Certificates and Qualified Certificates to Subjects.

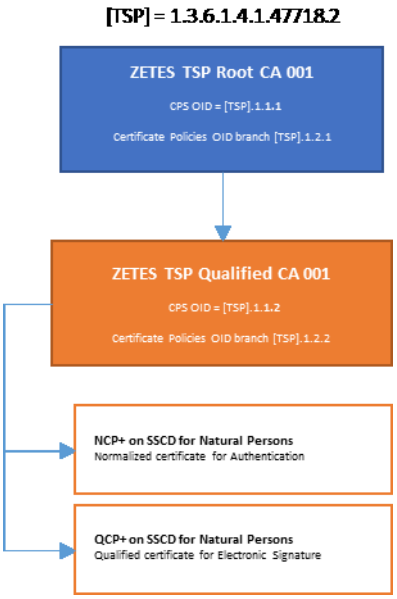


Figure 2 CA hierarchy

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;
- 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:

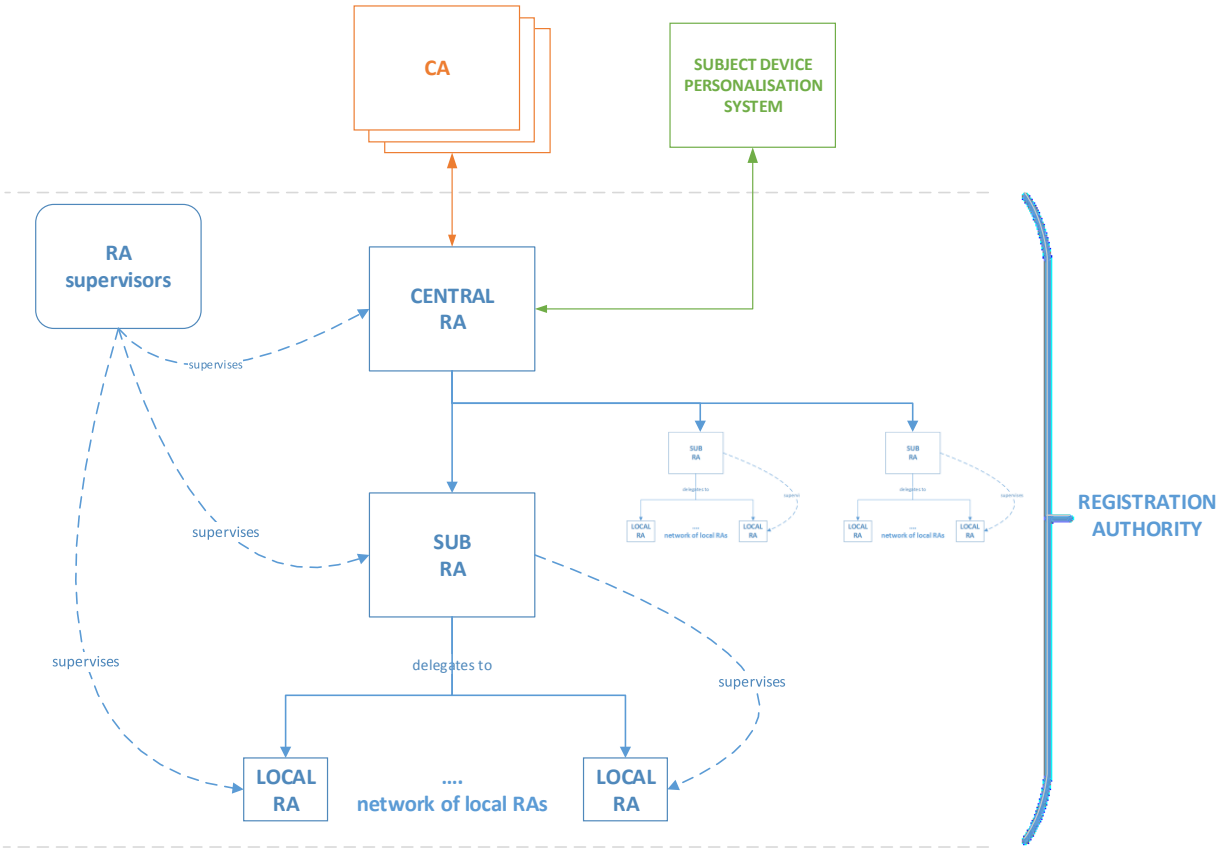


Figure 3 Registration Authority entities

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 Subject 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)

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

A Subordinate RA delegates the actual registration process of natural persons to one or more Local Registration Authorities.

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

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

- ZETES TSP
- the Subscriber
- the Subordinate RA
- a third party

1.3.2.4 Local Registration Authorities (L-RA)

The Local RA is the organization that is responsible for the actual registration of the Subject for who the certificates are intended. The registration process depends on the requirements laid down in the Certificate Policy.

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

The tasks, responsibilities and identity of the LRA is defined in the certificate policy.

The role of Local RA can be performed by various parties:

- ZETES TSP
- the Subscriber
- the Subordinate RA
- a third party

1.3.3 Subscribers and Subjects

1.3.3.1 Subscribers (organizations)

Subscribers are organizations who enter 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.

In addition, the present CPS, applicable CPs and CTC are an integral part of the Subscriber agreement.

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

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;

1.3.3.2 Subjects (natural persons)

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

Subject 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 present CPS, the relevant CPs, 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 Subject Device Provisioning Services

The Secure Subject Devices required to contain the private key corresponding to 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 Subject Device personalisation process. The private key is generated in the Subject Device and cannot be exported in clear text form.

1.3.5.2 Dissemination and Repository Services

ZETES is operating the Dissemination Services (publication of Certification Practice Statement, Certificate Policy, Certificates 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, Certificates 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 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 has overall responsibility for the TSP Services.

The PMA is the high-level management body with final authority and responsibility for:

(a) Specifying and approving the PKI infrastructure and practices.
(b) Approving the Certification Practice Statement and the related certificate policies, as well as other declarations of practices and policies for other TSP services when applicable (e.g. time stamping Practice Statement and policies).
(c) Defining the review process for, including responsibilities for maintaining, the Certification Practice Statement and the related certificate policies, as well as other declarations of practices and policies for other PKI services when applicable (e.g. time stamping Practice Statement and policies).
(d) Defining the review process that ensures that applicable certificate policies, and other relevant policies when applicable, are supported by the Practice Statement(s).
(e) Defining the review process that ensures that the PKI authorities, including certification authorities (CAs) and other authorities when applicable (e.g. time stamping authorities – TSAs), as well as all component service of the PKI, properly implements the applicable practices, policies and procedures.
(f) When applicable, authorising part or all component service of the PKI to be provided and/or operated by third parties and the applicable terms and conditions.
(g) Publication to the Subscribers and Relying Parties of the relevant declaration of practices and of policies.
(h) Continually and effectively managing PKI related risks. This includes a responsibility to periodically re-evaluate risks to ensure that the controls that have been defined remain appropriate, and a responsibility to periodically review the controls as implemented, to ensure that they continue to be effective.
(i) Specifying cross-certification or mutual recognition procedures and handling related requests.
(j) Defining internal and external auditing processes with the aim to ensure the proper implementation of the applicable practices, policies and procedures.
(k) Initiating and supervising internal and external audits.
(l) Executing the audit recommendations.
(m) Undertaking any action it considers necessary to ensure the proper execution of the above areas of responsibility.
(n) Defining the scope of the PKI related service offering, among others by:
    1) Defining the certificate classes to be supported by the PKI;
    2) Defining the PKI related entities that will be registered by or under the responsibility of the RA.
    3) Defining the needs for policies that are to be followed for each of the certificate classes;
(o) Ensuring that practices for each of the above mentioned entities are defined and implemented in a manner that is consistent with this document;
(p) Mediating in disputes involving Subscribers and/or entities that have been registered by the RA and the entities that have been implemented by or under the responsibility of the CSP.
(q) Initiating when appropriate highly sensitive PKI operations such as CA root key revocation and renewal or termination of the PKI service.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The appropriate certificate usage is described in the CPS for the PKI components certificates and in the Certificate Policy for the subject's certificate.

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.

1.4.2 Prohibited certificate uses

Any usage of a certificate other than the usage explicitly allowed in the CPS and the 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).

The PMA includes senior members of management as well as staff responsible for the operational management of the ZETES TSP PKI environment.

1.5.2 Contact person

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

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

1.5.3 Person determining CPS suitability for the policy

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

1.5.4 CPS approval procedures

The PMA is responsible for the approval of the CPS. 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
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.
Qualified Certificate	A Certificate which meets the requirements laid down in Annex I of EU Directive 1999/93/EC and is provided by a Certification Service Provider who fulfils the requirements laid down in Annex II of that Directive.
Relying party	Person or organisation acting upon a Certificate, typically to verify signatures by the Subscriber or to perform encryption towards the Subscriber. The Relying Party relies upon the accuracy of the binding between the Subscriber public key distributed via that Certificate and the identity and/or other attributes of the Subscriber contained in that Certificate. In the context of this *Certification Practice Statement*, Relying Parties are as further defined in section 1.3.4.
Subscriber	Person or organisation contracting with the Certification Authority, for being issued one or more Certificates. In the context of this *Certification Practice Statement*, the Subscribers are as further defined in section 1.3.3.1.

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) Certificate 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 **https://tsp.zetes.com**	This URL refers to the welcome page of the web site for ZETES TSP. This web site provides: • general information about Zetes SA and the ZETES TSP business unit • announcements and notifications • a section with technical support and documentation and software downloads for users of the cards and/or certificates that are issued by ZETES TSP • a section with user friendly web pages for downloading documents such as the terms and conditions, certificate policies, etc. • 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) • a contact page
https://repository.tsp.zetes.com	This URL refers directly to the page for downloading documents such as the • Certificates Terms and Conditions, , • Certificate Practice Statements, • Certificate Policies, • etc.
http://crt.tsp.zetes.com	This URL refers to 1. a web page for manual interactive download of CA certificates 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 1. a web page for manual interactive download of ARL and CRL 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 and the combined CRL 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 Subject Secure 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 are 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. Expired certificates that were revoked before their expiration dates are removed from the certificate revocation lists. CRLs are updated until all certificates that that were issued by the respective CA key have expired.

Expired certificates that were revoked before their expiration dates are removed from the certificate revocation lists.

The OCSP service is synchronised with the latest CRL. 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, Certificates Terms and Conditions, and other public documents are published whenever a change occurs, ensuring a period of minimum four (4) 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

End-entities certificates bear Distinguished Name (DN) as defined in applicable CPs.

The DN for the ZETES TSP Qualified CA is:

CN= ZETES TSP QUALIFIED CA 001

SN= 001

O= ZETES SA (VATBE-0408425626)

C= BE

In the above *001* is the 3-digit serial number assigned by the RA to as part of the name of the CA entity. This serial number should not to be confused with the certificate serial number which is automatically generated.

3.1.2 Need for names to be meaningful

Names are meaningful. Refer to clause 3.1.1.

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**).

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).

serialNumber	Unique official identifier *as assigned by the RA/C-RA/SUB-RA/L-RA* *This can be a numbering scheme which is unique to the Subscriber or which is derived from the breeder document that was used to register the Subject e.g. the National Register Number on an identity card, f*ormatted as specified in ETSI EN 319 412-1, e.g. PASBE-EI383940, IDCBE-5920565758-43, TINBE-0123456789, etc. together with a semantic identifier
title	**official title of the Subject** *as assigned by the RA/C-RA/SUB-RA/L-RA/Subscriber*
givenName	**official given name(s) of the Subject** 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	**official surname(s) of the Subject** 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	**official name of the Subject + indication of the intended purpose for this**

	certificate space (“ “) separated short-form concatenation of given name(s) and surname(s) followed by a label (text enclosed in brackets) identifying the purpose or use context of the certificates e.g. Firstname Lastname (Authentication)
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** As formatted in ETSI EN 319 412-1 (e.g. VATBE-0123456789) together with a semantic identifier. It is representing the registration number of the organization as stated in the official records.

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 rules for interpreting the names are provided in clauses 3.1 of the present document and in the Certificate Policies.

3.1.5 Uniqueness of names

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

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 Subject Devices

Unless otherwise specified in the applicable Certificate Policy, the keys for Secure Subject Devices/Smartcards are generated inside the embedded chip of the Secure Subject Device/Smartcard.

The Secure Subject Device/Smartcard is selected by Zetes. The Secure Subject Device/Smartcard used for certificates for natural persons complies with the technical standards and certification requirements as defined in CEN CWA 14169 for a Secure Signature Creation Device of Type 3 (SSCD Type 3).

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

- the 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, on other cases only immediately following the key generation process and within the same session
- the card 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

The key generation process for the Secure Subject Device/Smartcard as well as the certificate request generation process are an integral part of the personalisation process of the Secure Subject Device/Smartcard. The personalisation process for the device is performed for ZETES TSP in the central personalisation facility of Zetes CardS.

The keys are generated in controlled conditions, in a secure environment on premise at Zetes and under the supervision of authorized Zetes personnel. The CA only accepts authenticated certificate requests that originate from inside this controlled environment.

This key generation process complies with the relevant technical standards ETSI TS 102 042 and ETSI TS 101 456.

The combination of the choice of device and the key generation process guarantees that possession of the private key is guaranteed and that the origin of this key is known.

This applies to Secure Subject Devices that are issued to:

- Subjects
- CA administrators and operators
- RA administrators and operators
- SRA administrators and operators

Proof of Possession of Private Key for PKI Components

The methods to prove the possession of private key for CAs (i.e. Root CA and Issuing CAs), are detailed in internal confidential documentation.

Methods to prove the possession of private key for PKI component services (e.g., RA, CRLs signers, OCSP responders, SRAs, etc.) are detailed in internal confidential documentation.

3.2.2 Authentication of organization identity

The ZETES TSP Qualified CA only issues Subject certificates for natural persons (the Subjects). The ZETES TSP Qualified CA does not issue certificates to organizations, although organizations can be a PKI participant, as described in section 0.

For this reason the organization identity of certain PKI participants must be authenticated. The authentication procedure to verify the link between a Subscriber as an organization and a Subject, is based on ETSI EN 319 411-1.

Organisational entities other than ZETES that are PKI Participants

As PKI Participant, an organization has a role and responsibilities e.g. as a Subscriber, as a Subordinate RA, as a Local RA, etc.

Organizations who are a PKI Participant 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. ZETES TSP will also verify the organization's mandate (as Subscriber) to represent a well-defined group of natural persons (as Subjects).

Belgian organizations are authenticated based on recent documents and attestations which are valid in Belgium, organizations from other EU countries are authenticated based on the equivalent documents and attestations as applicable for the country in question.

The list of documents and attestations is as follows

- an extract from the Commercial Register
- a constitutive act
- an official document or original certified mandate stating the responsibilities or disposition powers of the organization, such as CEO, CFO, delegated administrator, board of directors, etc.
- for the natural person who is the legal representative of the organization
    - a copy of the identity documents (identity card, passport, residency card)
    - physical presence of this person to present the identity documents to ZETES TSP
    - proof of the legal address, civil state and profession
    -
- an explanatory description of the structure of the organization

In case the organization is acting as a Subscriber and therefor represents Subjects, ZETES TSP will require a verifiable proof and description of the Subscriber's mandate and relationship with the Subscribers.

Organisational entities that are internal to Zetes

All internal organisation entities are part of the same legal entity Zetes SA.

Identification and authentication procedures for the registration of the PKI component services (e.g. Root CA, CAs, RAs, CRLs signers, OCSP responders, SRAs, etc.) are detailed in internal confidential documentation.

3.2.3 Authentication of individual identity

Authentication of Identity

The ZETES TSP Qualified CA only issues certificates for natural persons (the Subjects). The ZETES TSP Qualified CA does not issue certificates to organizations or individuals in the role of Subscriber.

The registration of an individual for obtaining a Subject certificate as a natural person, requires in-person registration with a Local RA of the designated Subordinate RA.

The authentication process includes the following:

- The individual (Subject) must appear in person before an authorized operator of the Local RA
- The individual (Subject) must present a valid and authentic identity document (national identity card, residence permit, passport, etc.) to the Local RA operator. The presented identity document must be valid for at least 6 full months starting from the 1st of the month following the registration date.
- 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
- If the individual was already registered by the Subscriber or the Subordinate RA and if this registration process is equivalent to the registration process described above, then the existing registration data may be used instead of doing a new registration in person

The identity of a Subject must be authenticated. The authentication procedure to verify the identity of a Subject, the link between a Subscriber as an organization and a Subject, is based on ETSI EN 319 411-1.

Optionally the authentication process may include the capture of biometric data such as fingerprints that can be used

- for devices with biometric Match on Card, the fingerprint replaces the PIN
- to verify the Subject's identity e.g.
    - for the handover of the Secure Subject Device
    - when the Subject returns to request a new Secure Subject Device
    - when the Subject returns to request revocation of his/her certificates

Authentication of Professional Attributes or Membership Attributes

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

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

The Subscriber may attest to a Subject's membership of the organization such as member, employee, associate, role, department, etc.

Authentication of Individuals that are internal to the operations of the PKI

Identification and authentication procedures for the registration of the trusted persons/roles operating the PKI component services are detailed in internal confidential documentation.

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. The CA or RA do not verify the existence or correctness of the e-mail address.

3.2.5 Validation of authority

The Subscriber, in the role of Subordinate RA, defines and controls which Subjects are entitled to a certificate. The definition of the validation of authority may be detailed in the Subscriber Agreement.

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-keying of an existing Secure Subject Device is not supported.

If the key e.g. because the key length is no longer considered adequate or if the certificate must be renewed e.g. because the Subjects name or attributes have changed, then the Subject must request a new Secure Subject Device, which implicitly includes new certificates.

Re-key requests are processed as new certificate requests. Before such new certificates are issued, the identity and attributes of the applicant will be verified again following the same procedure as described in section 3.2 on Initial Identity Validation.

3.3.2 Identification and authentication for re-key after revocation

The procedures are the same as for Initial Identity Validation (see section 3.2).

If a revoked certificate must be renewed, the Subject must request a new Secure Subject Device, which implicitly includes new certificates.

Re-key requests are processed as new certificate requests. Before such new certificates are issued, the identity and attributes of the applicant will be verified again following the same procedure as described for Initial Identity Validation.

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
- the Subordinate RA
- the Subscriber
- the Subject

The procedures and conditions for requesting and executing a certificate revocation are described in this CPS and in the 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 in the Subordinate RA.

Revocation Requests for other certificates that are internal to the operations of the PKI

PKI component services (e.g. Root CA, CAs, RAs, CRLs signers, OCSP responders, SRAs, etc.) and certificates issued to the trusted persons/roles operating them, are detailed in internal confidential documents, a.o. the CAs key ceremony and the disaster recovery plan.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The following sections describe procedures that are common to all types of Subject certificates. For details pertaining to a specific type of certificate, please refer to the applicable Certificate Policy.

The procedures relating to PKI component services (e.g. CAs, RAs, CRLs signers, OCSP responders, SRAs, etc.) and the related persons/roles operating them are described in internal confidential documentation.

The following sections only present the elements of these documents that can be publicly disclosed.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate Application by Natural Persons

The ZETES TSP Qualified CA does not issue certificates to natural persons on an individual basis. The ZETES TSP Qualified CA only issues certificates to natural persons (the Subjects) who are entitled to a certificate through explicit approval by and intervention of an organization (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 or the Subject Agreement that incorporate this CPS, the specific Certificate Policies and the Certificates 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 an authorized and authenticated Subordinate RA. The Subordinate RA and the Subscriber can be one and the same legal entity.

Certificate Application by Legal Persons / Organizations

The ZETES TSP Qualified CA does not issue certificates to organisations or to individuals representing an organisation.

Certificate Application for internal PKI Participants

Internal certificate applications to issuing CAs or certificate applications to the Root CA:

- PKI components services certificates and/or associated trusted persons/roles certificates can be submitted by authorised representative of the PKI on behalf of the PMA, as described in internal confidential documents.
- CA certificates: the Root-CA and the Issuing (Qualified) CA(s) are the sole admitted candidates for CA certificates.

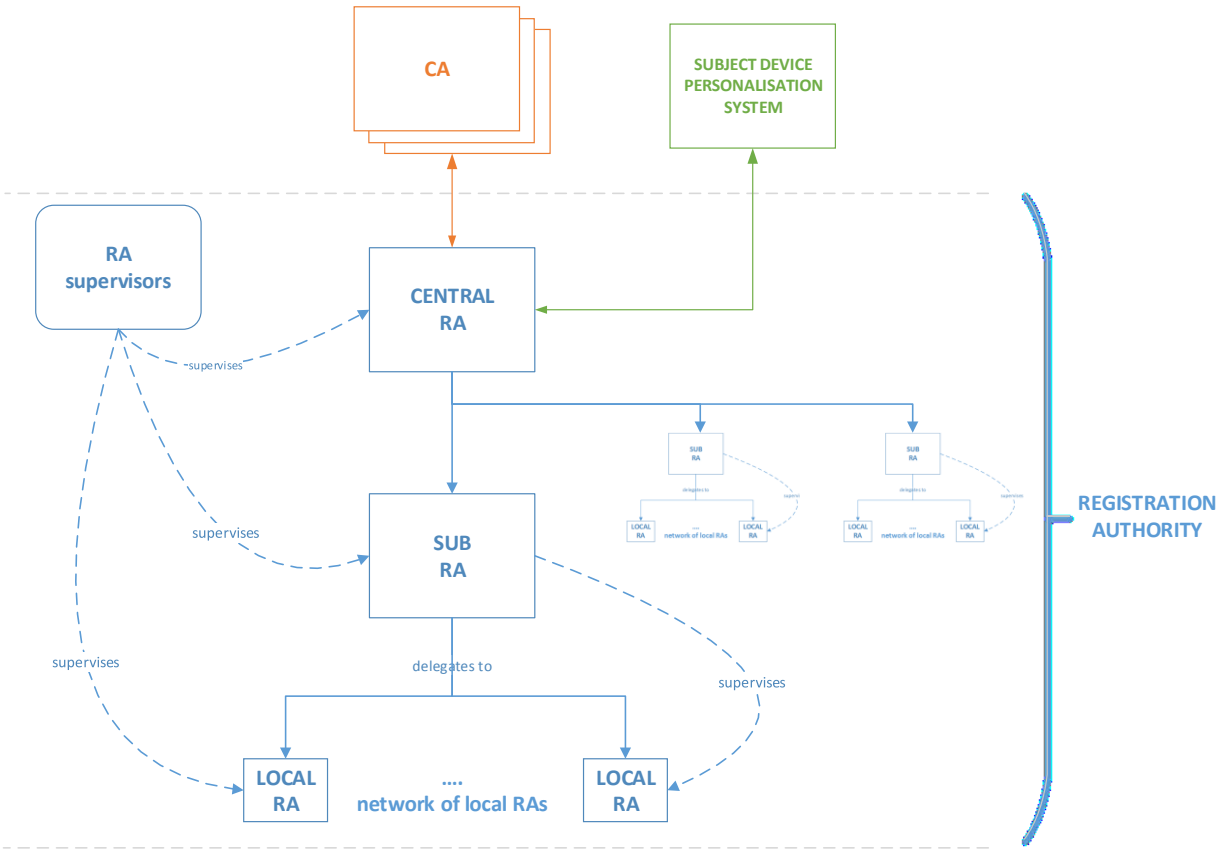
4.1.2 Enrolment process and responsibilities

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, please see sections 0 and 1.3.2. The relationship between these entities is illustrated below.

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 Subscribers.

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



The Central RA relies on the enrolment process performed by a Subordinate RA. The Subordinate RA delegates the enrolment process to one or more of its 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 CPS, in the 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 locations or on a secure system according to the requirements defined in the CPS, the applicable CP and applicable national laws.

4.1.2.2 Enrolment of Subjects

The Subject Agreement

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

- the registration form
- reference where to download the Certificates Terms and Conditions and access to a printed copy
- reference where to download the CSP and the CP and access to a printed copy
- bylaws, notices or other documents provided by the Subscriber (to be defined in the Subscriber Agreement)

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

The signed enrolment form is considered the formal acceptance by the Subject of the Subject Agreement and that the Subject

- accepts responsibility that the information provided by the Subject to the RA is correct, complete, valid and up to date,
- that the Subordinate RA and ZETES TSP as CSP maintain a retention period of 30 years counting from the date of the issued certificate of all the information pertaining to the registration and enrolment, the certificate request, the revision of a Secure Subject Device, 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

Pre-enrolment for Subjects

Depending on the organisation of the Subordinate RA and/or the Subscriber, the Subject can do a pre-enrolment via an online application (e.g. web site or app) to speed up the actual enrolment process.

Enrolment Process for Subjects

The actual enrolment process begins at the Local RA or L-RA. The L-RA is responsible for the face to face enrolment of each applicant. Its duties are to collect the required documents and attestations for the subsequent validation of the applicant's identity and attributes. The L-RA operator 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 SUB-RA checks and completes the enrolment data. 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 Central RA or C-RA is responsible for the correct authentication of Subscribers 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 Subject Device (smartcard), for the key generation process on the Secure Subject 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 Subject Device (e.g. a smartcard) 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 Subject Device (smartcard) to the Subjects

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

The Secure Subject 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 of a smartcard) is delivered to the Subject

- in a closed container
- via a different distribution channel
- separate from the Secure Subject Device
- at a different point in time

Compliance with Standards

Unless explicitly stated otherwise, the processes are compliant with the relevant technical standards ETSI TS 101 456 for QCP+ certificates or ETSI TS 101 042 for NCP+ 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.

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 **30** 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 Subject 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

4.1.2.4 Enrolment of administrators and operators for Subordinate RAs and their Local RAs

ZETES TSP RA may delegate tasks to organizations that are not part of Zetes SA. Typically, the Subordinate RA and its local RA have their own legal entity. These external organizations are bound by a contractual agreement, the Registration Authority Agreement. This agreement defines the rights and obligations of the RA participants that are not part of the Zetes SA legal entity.

For the enrolment of administrators and operators for Subordinate RAs (and their Local RAs) the following conditions apply:

- the Subordinate RA must pass the qualification criteria laid down by ZETES TSP
- the Subordinate RA must be operational
- the Registration Authority Agreement must be in effect
- each operator or administrator must successfully complete a training course
- each operator or administrator must be a duly mandated employee, delegate, representative, etc. of the Subordinate RA

The operators of a Subordinate RA and its Local RAs are enrolled by the ZETES TSP Central RA according to a procedure defined in the Registration Authority Agreement for that Subordinate RA.

4.1.2.5 CA certificate applications to the Root CA

The processes and procedures used to enrol the PKI component services (e.g. CAs, RAs, CRLs signers, OCSP responders, SRAs, etc.) and to enrol the trusted persons/roles operating them are further described in internal confidential documentation.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Identification and Authentication for a Subject certificate

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

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

See also 4.1.2.

Identification and Authentication for CA certificate or PKI components certificate

ZETES TSP, acting as Certification Service Provider, is the owner and custodian of the keys and certificates of the CA hierarchy for the ZETES TSP Qualified CA.

All certificate requests for CAs and for PKI components are created by and processed by personnel of ZETES TSP on systems that are internal to the ZETES TSP PKI infrastructure.

The PMA defines and assigns the trusted roles concerning the management of the CA keys and certificates, to trusted employees, as defined in internal confidential documents such as the custodian list and the CA Key Ceremony documentation. The trusted employees have been vetted and have appropriate security clearance for their respective duties.

For the Root CA these trusted employees are part of the quorum in charge of the Root CA key self-certification ceremony.

Only a selected group of authorized trusted employees, entitled by the PMA, are in charge generating keys and issuing a certificate request for a CA or a PKI components that is internal to the ZETES TSP PKI infrastructure.

Only a selected group of authorized trusted employees, entitled by the PMA, are in charge of processing a certificate request for a CA or a PKI components that is internal to the ZETES TSP PKI infrastructure.

Such requests are validated by the appropriate CA RA officer in addition to additional checks performed by other trusted roles that are involved in the process.

4.2.2 Approval or rejection of certificate applications

Approval or Rejection for a Subject certificate

Approval or rejection of certificate applications are 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 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.

Approval or Rejection for a CA certificate or PKI components certificate

ZETES TSP, acting as Certification Service Provider, is the owner and custodian of the keys and certificates of the CA hierarchy for the ZETES TSP Qualified CA.

All certificate requests for CAs and for PKI components are created by and processed by personnel of ZETES TSP on systems that are internal to the ZETES TSP PKI infrastructure.

ZETES TSP as CSP is responsible for the validation and vetting of certificate requests for CAs and internal PKI components.

4.2.3 Time to process certificate applications

Time to process certificate applications for Subjects

Not relevant because the ZETES TSP Qualified CA does not issue certificate immediately upon registration and because the certificates are not immediately available to the Subject when the certificates are created by the CA.

The certificates are stored on a Secure Subject Device which is delivered to the Subject in person. The personalisation of a Secure Subject Device is subject to the schedule of the personalisation system. The delivery process may take several hours or several days and depends on the availability of the Subject to receive or collect the Secure Subject Device.

Time to process certificate applications for CAs, other PKI components and PKI administrators and operators

As specified in internal confidential documentation pertaining to the specific procedure or ceremony.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Issuance of a certificate for a Secure Subject Device for a Subject

The certificate is issued as part of the personalisation process of the Secure Subject Device. The CA will only receive certificate requests from the Central RA in conjunction with the personalisation system for the Secure Subject Devices. The CA, the Central RA and the personalisation system are integrated systems and communicate over closed network connections. The network connections between the CA and the other components all use certificate based authentication and encryption. The CA will only process requests that originate from a properly authenticated 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 an authenticated 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.

Issuance of a certificate for a Secure Subject Device for a Operators and Administrators

Same as for the issuance of a certificate for a Secure Subject Device for a Subject.

Issuance of a certificate for a PKI Component

The ZETES TSP Qualified CA only issues PKI Component certificates for the ZETES TSP Certificate Validation Service (i.e. the OCSP service). Key and certificate renewal of the OCSP services and the issuance of the new OCSP certificate are as specified in the internal documentation pertaining to the specific procedure or ceremony.

4.3.2 Notification of issuance of certificate

Notification of issuance of a certificate for a Secure Subject Device for a Subject

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

Notification of issuance of a certificate for a Secure Subject Device for Operators and Administrators

Same as for the issuance of a certificate for a Secure Subject Device for a Subject.

Notification of issuance of a certificate for a PKI Component

As specified in the internal documentation pertaining to the specific procedure or ceremony.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is accepted by the Subscriber and the Subject upon completion of the handover procedure or delivery procedure of the Secure Subject Device to the Subject.

The Subscriber and the Subject both have the right to reject the certificate and return the Secure Subject Device, provided at least one of the following objections apply:

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

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

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

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

- the Secure Subject 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 RA 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

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

If explicitly stipulated in the Subject Agreement, the CA will notify the Subject of the issuance of the certificate, by means of notification method stipulated in said Subject Agreement.

4.5 Key pair and certificate usage

4.5.1 Subject private key and certificate usage

The ZETES TSP Qualified CA issues certificates for keys stored on Secure Subject Devices that comply with the requirements and specifications for a Secure Signature Creation Device of Type 3 as define in CEN CWA 14169.

This compliance guarantees that:

- the private key cannot be extracted from the Secure Subject 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 key and certificate have associated Activation Data that is used for activation of the Secure Subject Device.

This secret information can be

- set by ZETES TSP but changed by the Subject (e.g. the PIN code of a card)
- set by ZETES TSP (e.g. cryptographic keys for post-issuance card management tasks)
- set by the Subject (e.g. a fingerprint for Match on Card)

The ZETES TSP Qualified CA is responsible for

- providing a Secure Subject Device that complies with CEN CWA 14169
- initializing the Secure Subject Device and its initial associated Activation Data
- secure distribution of the Secure Subject Device to the Subject
- secure distribution of the initial associated Activation Data to the Subject

The Subject is bound by the conditions and obligations mentioned the Subject Agreement, which includes this CPS. The Subject must protect the Secure Subject Device and any associated Activation Data or other information against loss, theft, disclosure, compromise or modification.

Once the Secure Subject 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 defined in the Certificate Policy and 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 Subject Device
- not sharing the Secure Subject Device with another person
- setting Activation Data that is unique and that comply with the guidelines given in the Certificate Policy
- keeping these secret information confidential
- safe storage any document or medium containing transcripts of part or all of the associated Activation Data
- separation of storage for the Secure Subject Device and the associated Activation Data
- not disclosing the Secure Subject Device to another person

See the applicable Certificate Policy for more details.

4.5.2 Relying party public key and certificate usage

Relying Parties should not rely on a (Qualified) Certificates unless they have performed the following actions:

- Evaluate whether the certificate is appropriate for the intended usage
- Restrictively use 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 Certificate 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 Certificate Practice Statement and the Certificate Policy,
- only rely on a Certificate as may be reasonable under the circumstances.

4.6 Certificate renewal

Not applicable. The ZETES TSP Qualified CA does not renew certificates, i.e. does not issue new certificates for existing keys on already issued Secure Subject Devices. Situations that may require certificate renewal are handled as a request for replacement of the Secure Subject Device, which involves:

- revocation of the previous certificates
- personalisation of a new Secure Subject Device with new key pairs
- new certificates

4.7 Certificate re-key

Not applicable. The ZETES TSP Qualified CA does not support re-key, i.e. does not issue certificates for new keys on already issued Secure Subject Devices. Situations that may require re-key are handled as a request for replacement of the Secure Subject Device, which involves:

- revocation of the previous certificates
- personalisation of a new Secure Subject Device with new key pairs
- new certificates

4.8 Certificate modification

Not applicable. The ZETES TSP Qualified CA does not modify certificates, i.e. does not issue modified certificates for existing keys on already issued Secure Subject Devices. Situations that may require certificate modification are handled as a request for replacement of the Secure Subject Device, which involves:

- revocation of the previous certificates
- personalisation of a new Secure Subject Device with new key pairs
- new certificates

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Circumstances for Revocation of a Subject certificate

Revocation is needed for the following reasons:

- The Subject has not collected the Secure Subject Device in due time, as specified in the applicable Certificate Policy or Certificates 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 Subject 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 CPs have been violated);
- The Secure Subject 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.
- 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 .

Circumstances for Revocation of a CA certificate

A CA certificate may be revoked for security reasons in emergency if:

- The PMA has reason to believe or suspect that the CA's private key has been compromised,
- The PMA has reason to believe or suspect that the activation secret has been compromised.

A CA certificate may be revoked in a non-urgent circumstance:

- for prevention of risk, if the PMA has reason to believe or suspect that the CA's private key might be compromised in the middle term; this includes cryptography obsolescence in particular with regard to ENISA's prescriptions, new vulnerabilities in cryptography, etc.,
- if a certified data is modified.

Circumstances for Revocation of a PKI components certificate

As specified in the internal procedures of the ZETES TSP PKI environment.

4.9.2 Parties that can request revocation

Parties that can request Revocation of a Subject certificate

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 Certificate Policy.

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

Parties that can request Revocation of a CA certificate

A Revocation Request of CA certificate can only originate from the PMA.

Parties that can request Revocation of a PKI component certificate.

A Revocation Request of PKI components certificate can originate from the PMA or under the authority of the PMA through the operational procedures for the PKI component in question.

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 and may vary with the Subscriber under whose authority the Subject obtained the certificate.

CHANNEL	SUBJECT AUTHENTICATION MECHANISMS
LOCAL RA/SRA	**identification** • a combination of name, date of birth, member number, card number, etc **authentication mechanisms (in person)** • an official identification document such as a national ID card or a passport • biometric authentication • a pre-defined revocation authentication code
CALL CENTER	**identification** • a combination of name, date of birth, member number, card number, etc **authentication mechanisms** • control questions (personal information other than the identifiers) • a pre-defined revocation authentication code
E-MAIL	**identification** • a combination of e-mail address, name, date of birth, member number, card number, etc. **authentication mechanisms** • e-mail address of the sender • signed e-mail using national electronic ID card • signed e-mail using a valid ZETES TSP certificate for authentication • a pre-defined revocation authentication code
WEB SITE	**identification** • a combination of e-mail address, name, date of birth, member number, card number, etc. **authentication mechanisms** • a pre-defined revocation authentication code • logon to web site using a national electronic ID card • logon to web site using a valid ZETES TSP certificate for authentication

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 as defined in the Subscriber Agreement or in the applicable law

Procedure for revocation of Subject certificates - request by the Subscriber

A Subscriber, in its role a 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
E-MAIL	**identification** • a combination of e-mail address, name, organization and role **authentication mechanisms** • signed e-mail using a valid ZETES TSP certificate for authentication
EXTRANET	**identification** • a combination of e-mail address, name, organization and role **authentication mechanisms** • logon to extranet using a valid ZETES TSP certificate for authentication

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

Procedure for revocation of Subject certificates - request by an RA/SRA entity

A Local RA/SRA can only request revocation through its supervising Subordinate RA/SRA and upon explicit request of the Subject.

The Subordinate RA/SRA entity 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 RA/SRA Agreement.

The Central RA/SRA entity can decide to revoke a Subject's certificate(s). The procedures are described in the Subscriber Agreement and in the RA/SRA Agreement.

Procedure for revocation of CA certificates

The revocation of a CA key for security reason is a critical process that must be performed in emergency, as defined by the internal procedures of ZETES TSP. Revocation of a CA certificate requires approval of the PMA.

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

Process time for revocation of Subject certificates

Revocation requests are processed within 1 business day following receipt of the revocation request.

Process time for revocation of CA certificates or PKI component certificates

Under normal operational conditions an OCSP key and certificate is replaced before it is revoked, to guarantee continuity of the OCSP service towards the Relying Parties.

In case of a key compromise ZETES TSP undertakes best effort to revoke the certificate without delay within 24 hours. The process time for revocation of a CA certificate or a PKI component certificate for any other reason will be determined on a case by case basis.

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)

Latency for CRLs after revocation of Subject certificates

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

Latency for CRLs after revocation of CA certificates or PKI component certificates

ZETES TSP will make best effort to update the certificate status information to Relying Parties within 3 hours from 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 0 for information on Access Control and Restrictions regarding the use of the OCSP service.

4.9.11 Other forms of revocation advertisements available

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

OCSP service availability 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.

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 tems 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

The key usage of the certificates issued by the ZETES TSP Qualified CA are set to authentication and 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 Subject Device compliant with SSCD Type 3 as defined in CWA 14169 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

5.1 Physical controls

ZETES TSP has established physical security measures and environmental controls commensurate with the value and critical nature of the assets they apply to. Physical and environmental security is aimed to prevent, deter, detect and delay unauthorized access, loss, theft, damage, compromise, interferences and interruption to business activities.

5.1.1 Site location and construction

ZETES TSP facilities are organized, partitioned and segregated into distinct areas with specific physical security measures according the type and sensitivity of assets and the operations conducted.

Physical security measures regarding the facilities include but are not limited to reinforced material and construction technics, locked rooms and vaults.

5.1.2 Physical access

The sites hosting the CA implement proper security controls, including access control, intrusion detection and CCTV. Access to the sites is limited to authorized personnel.

The CA‘s secure premises within these sites are located in an area appropriate for high-security operations. These premises feature numbered zones and locked rooms, cages, safes, and cabinets.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones such as locating CA operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

5.1.3 Power and air conditioning

Power and air conditioning operate with a high degree of redundancy.

5.1.4 Water exposures

Premises are protected from any water damages.

5.1.5 Fire prevention and protection

Prevention and protection as well as measures against fire exposures are implemented.

5.1.6 Media storage

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

5.1.7 Waste disposal

To prevent unwanted disclosure of sensitive data, waste is disposed of in a secure manner.

5.1.8 Off-site backup

ZETES TSP has a backup and disaster recovery site located in separate premise with similar protection measures. In case of adverse situation as a natural disaster, fire or act of terrorism, ZETES TSP implements the necessary measure to recover its services according the legal and contractual requirements.

5.2 Procedural controls

5.2.1 Trusted roles

ZETES TSP follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of the members of the staff and of the satisfactory performance of their duties in the fields of electronic signature-related technologies.

All members of the staff operating the key management operations, administrators, security officers, and system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

Trusted roles within ZETES TSP are activities conducted to operate, maintain, monitor, review and communicate about TSP activities. Trusted roles are allocated to duly identified persons by the PMA.

Trusted roles are listed and defined within ZETS TSP competences management system and include:

- Plant Manager
- PKI manager
- IT Manager
- Security Officer
- PKI administrator
- PKI operator
- System administrator
- System auditor
- System operator
- PKI operator
- Registration officer
- Revocation officer
- Key custodians

Zetes conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make due diligence attempt to determine their trustworthiness and competence.

5.2.2 Number of persons required per task

Where dual or multiple control is required at least two trusted roles need to bring their respective and split knowledge in order to be able to proceed with the ongoing operation.

Circumstances requiring dual or multiple control are detailed in the PKI system and documented in the CA key ceremonies reports and related records.

5.2.3 Identification and authentication for each role

Each member of ZETES TSP acting in a trusted role is identified and authenticated to access the infrastructure to conduct his role by means of at least 2 factors authentication credentials or under dual control.

5.2.4 Roles requiring separation of duties

All actions with respect to the CA can be attributed to the components of the CA and the member of the CA staff that has performed the action.

Zetes ensures separation among the following discreet work groups documented in internal documents “ZETES TSP – Organisation”

- PKI administration personnel
- System and network administration personnel
- Security personnel to enforce security measures, including registration and revocation officers
- Audit personnel.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Zetes implements practices that provides reasonable assurance regarding trustworthiness and competence of the member of its staff. Learning and training certificates, professional experience, feedback from previous employers, trusted employee’s recommendations, certificates delivered by the authority are some common practices used in this perspective.

5.3.2 Background check procedures

Zetes with regards to the CA activities makes the relevant checks on prospective employees by means of status reports issued by a competent authority or third-party statements.

5.3.3 Training requirements

Zetes with regards to the CA activities makes available relevant technical training for their personnel to perform their CA functions.

5.3.4 Retraining frequency and requirements

Periodic training updates will be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job rotation frequency and sequence

Zetes does not impose job rotation as a principle. Changes in roles are managed through training and competences management with respect of segregation of roles where applicable.

5.3.6 Sanctions for unauthorized actions

Zetes with regards to the CA activities sanctions personnel for unauthorized actions or violation of security procedures. Sanctions may include – but are not limited to – disciplinary action, revocation of privileges, dismissal, civil or criminal proceedings.

The severity of a particular violation is evaluated by the PMA. The PMA ensure that the sanction taken is both appropriate and proportional to the violation.

5.3.7 Independent contractor requirements

Independent CA component services subcontractors and their personnel are subject to the same background checks as the CA personnel with regards to the CA activities. The background checks include:

- Criminal convictions for serious crimes.
- Misrepresentations by the candidate.
- Appropriateness of references.
- Any clearances as deemed appropriate.
- Privacy protection.
- Confidentiality conditions.

5.3.8 Documentation supplied to personnel

Zetes with regards to the CA activities makes available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit logging procedures

5.4.1 Types of events recorded

For all events related to the CA key operations, records will be kept that include all information related to that event that can be useful for auditing purposes.

Extensive security logging and monitoring is performed at various levels including (non-exhaustive):

- the physical level (including equipment cabinet access)
- the network level
- the operating system level
- the application level

The PKI software and associated routines record events that include but are not limited to:

- Issuance of a certificate: request, approval or rejection (with reason) of request, registration information, Identification of the RA approving or processing the request, certificate generation/activation.
- Revocation of a certificate: revocation request, approval or rejection (with reason) of request, Identification of the RA approving or processing the request, Identification of the requestor.
- Publishing of a CRL
- Request to and answers from the OCSP services (responders)
- personalisation of SSCD

The audit logs records contain:

- The identification of the operation.
- The date and time of the operation.
- The identification of the certificate, involved in the operation.
- The identity of the transaction requestor (e.g. the RA security officer in the event of certificate issuance or revocation, or more than one member of the PMA for the events other than certificate issuance).

In addition, audit logs of relevant operational events in the infrastructure are maintained, including, but not limited to:

- Log in and log out of PKI components administrative interfaces.
- Start and stop of servers.
- Outages and major problems.
- Physical access of personnel and other persons to sensitive parts of the PKI site.
- Backup and restore.
- Report of disaster recovery tests.
- Audit inspections.
- Upgrades and changes to systems, software and infrastructure.
- Security intrusions and attempts at intrusion.

Auditing events are not given log notice.

5.4.2 Frequency of processing log

The PKI operations staffs regularly monitor security related events. Information about critical events is forwarded to the appropriate department for immediate attention. Reports that are generated from the audit logs are reviewed at least every 8 days by internal auditors.

5.4.3 Retention period for audit log

System logs are retained for 18 months. For audit logs for the CA and PKI components, see section 5.5.2.

5.4.4 Protection of audit log

The audit logs of the CA application software and PKI components application software are digitally signed and time stamped. The signature key is protected by an HSM. Consolidated logs are stored on secure backup media and stored in a safe storage location.

5.4.5 Audit log backup procedures

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by PKI RA and CA Officers. For key ceremonies a relevant extract of the audit log is made stored separately.

5.4.6 Audit collection system (internal vs. external)

The PKI audit collection system is internal.

5.4.7 Notification to event-causing Subject

There are no requirement for ZETES TSP to notify the Subject who caused an audit event.

5.4.8 Vulnerability assessments

The entire infrastructure is subject of a vulnerability assessment at least once a year and whenever a critical part of the infrastructure is affected. The assessment covers the ICT infrastructure, the special cryptographic equipment, the physical environment, data storage, software, personnel, processes and procedures and communication.

Vulnerability assessment of the audit log is part of the ZETES TSP risk assessment and risk management program documented internally.

5.5 Records archival

5.5.1 Types of records archived

See section 5.4.1 and 5.5.2.

5.5.2 Retention period for archive

The archive retention periods for the various types of records are:

- issued certificates for a period of 30 years after expiration of a certificate,
- audit trails on the issuance of certificates for a period of at least 30 years after expiration of a certificate,
- copies of identification documents are retained for at least 30 years after expiration of the certificate,
- audit trail of the revocation of a certificate for a period of at least 30 years after revocation of a certificate,
- CRLs for at least 30 years after creation of the CRL,
- documentation supporting the issuance and use of the certificate is kept for a period of at least 30 years after the expiration of the last certificate supported by the documentation.

5.5.3 Protection of archives

The archives are protected against manipulation or wilful destruction. As far as possible archive will be retained and protected in electronic form.

Paper-based records are archived and under control of the respective roles that process them. Paper-based archive may be stored on multiple location according the requirements laid down in the applicable CP. In particular, registration information will be securely stored to provide reasonable assurance regarding secrecy, integrity and availability.

5.5.4 Archive backup procedures

Backup copies of the relevant electronic system logs and electronic audit logs are stored in multiple locations.

5.5.5 Requirements for time-stamping of records

The audit logs created by the CA and OCSP service are signed and time stamped, the signature key is protected by an HSM and the time source is the same as for the CA or OCSP service.

5.5.6 Archive collection system (internal or external)

The archive collection system for the CA and PKI components operated by ZETES TSP is internal infrastructure of ZETES TSP. The archive collection system for Subordinate RA and their Local RA is done by the respective parties. ZETES TSP as RA supervisor will assist these RA entities to create and maintain an archive for their activities.

5.5.7 Procedures to obtain and verify archive information

The contents of the archive are not accessible except for authorized personnel of ZETES TSP and with exception of obligations by law or by court order.

Access to archive by authorized personnel must be motivated (e.g. in case of incident investigation, to test the “retrieval" procedure, etc.).

The Certificate Subject may access information related to his personal information and registration form by written request addressed to the ZETES TSP Central RA Officer.

Disclosure of information from the archive upon request by an implicated party other than the Certificate Subject is at the discretion of ZETES TSP and requires approval by the PMA. ZETES TSP reserves the right to charge a compensation to cover the expenses of the retrieval of the information from the archives.

5.6 Key changeover

Key changeover is not applicable, as end-entity certificates will be issued with a validity time within the validity time of the CA certificates.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Zetes TSP defined an incident management procedure including incident reporting and handling procedure.

These procedures are established to ensure a quick, effective and orderly response to (information) security incidents providing knowledge to reduce the likelihood and impact of recurring incident. Incident records and gained knowledge are reviewed during the risk assessment exercise and participate from the risk management procedure.

The specific cases of key compromises are dealt in section 5.7.3.

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

Zetes TSP establishes the necessary measures to ensure full and highly automated recovery of CA services in case of a disaster, corrupted servers, software or data.

Computing resources, software and data are replicated in a second location. Backup copies of software and data are kept on regular base and available on both sites according the ZETES TSP backup procedure.

Distance between both locations supporting ZETES TSP activities is sufficient to support a natural local disaster. Sufficient fast and secure communication infrastructure and services between the two sites ensures data integrity and effective recovery point.

Disaster recovery infrastructure and procedures are be fully tested at least once a year and the report is reviewed by the PMA.

5.7.3 Entity private key compromise procedures

In case of a CA compromise, ZETES TSP will

- decommission the compromised key
- Notify impacted PKI participants
- revoke the certificates impacted by the corrupted CA
- assess the relevance to revoke all certificates (this depends amongst other on the time of compromise)

By decision of the PMA and providing that the cause of compromise has been discarded, ZETES TSP will generate a new CA key and destroyed certificates can be re-issued.

In case of end-entity certificates compromise, revocation shall be performed and a new certificate shall be issued provided that the cause of compromise has been discarded. The end-entity (or the subscriber) has to notify ZETES TSP of any compromise or suspicion of compromise of their private key. PKI participants' obligations are detailed in the applicable sections of the CPS and the CP.

5.7.4 Business continuity capabilities after a disaster

Zetes TSP establishes the necessary measures to full and automatic recovery of the on-line services in case of a disaster, corrupted servers, software or data.

Recovery of the Root CA off-line services is ensured by the activation of the Root CA backup at the secondary site. As principle for the root CA key ceremony, all needed resources and secrets to pursuit the ZETES TSP activities will still be available in case one site should completely and definitely be destroyed.

Depending on the cause of the disaster and their effects, the PMA will assess the measures to be taken regarding

- the protection of sensitive resources and information on the disabled site
- the need to revoke the CA's impacted by the disaster (as the protection of disabled site cannot be ensured)
- the setup of a third site

A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

5.8 CA or RA termination

Terminating a certification service and as a result terminating, when applicable, the CA(s) and other PKI component services is an event as important as their initiation. Both require planning physical, logical, operational, procedural and human aspects. Security of information and reputation is at risk. Furthermore, legal requirements apply.

For clarification, the cessation of the issuance of new Qualified Certificates by the ZETES TSP Qualified CA while all other component services are kept under full normal operations, including the provision of certificate validity status information services (e.g. CRLs, OCSP services), is not in scope. Also the controlled transfer of services and components from ZETES TSP to another organization or transfer from an old CA to a new CA are not in scope.

This section describes the minimum procedures to be completed in a situation where all services provided by ZETES TSP associated with qualified certificates are terminated:

In the context of a scheduled termination:

- Cessation of the issuance of any new qualified certificate
- Termination notification to the Belgian Supervisory Body, the Subjects, The Subscribers and the Relying Parties within 3 months and no later than 2 months before the effective termination
- Dissemination of relevant information
- Preservation and transfer of auditing and archival records to the arranged custodian
- Revocation of unexpired and unrevoked Subjects' Qualified Certificates
- Creation of a last CRL
- When applicable, decommissioning of the CA keys

In the context of an unscheduled termination :

As far as it is possible, the plan for expected termination as described in section above will be followed with the following potential significant differences:

- Shorter or even no delay for the notification of the interested parties
- Shorter or no delay for the revocation of Subjects' Qualified Certificates

6 TECHNICAL SECURITY CONTROLS

Private keys for the ZETES TSP PKI infrastructure are protected by means of Hardware Security Modules that have the relevant security certification labels such as FIPS 140-2 level 3 and/or Common Criteria EAL4 or higher.

Physical access to the HSM is limited to authorised personnel only. The HSM equipment is installed in a secure environment.

Operational use of the HSM equipment is controlled by a combination of activation assets (e.g. smartcards) and activation data (e.g. PIN codes, passphrases, etc.). Activation assets and activation data are assigned to multiple custodians and are stored in a secure location, separate from the HSM equipment. Activation, backup and restore operations always requires involvement of multiple custodians. The separation of activation assets/data is organized such that no single custodian can exercise control over the protected key material.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation for CAs

The key pairs for any CA are generated on-board an HSM, under the authority of and with explicit consent of the PMA, under supervision of a Security Officer, under at least dual control and as part of a formal key ceremony in the presence of witnesses.

Key pair generation for the OCSP service

The key pairs for the OCSP service components are generated on-board an HSM, under the authority of and with explicit consent of the PMA, under supervision of a Security Officer, under dual control and as part of a formal key ceremony in the presence of witnesses.

Key pair generation for the other PKI components

The key pairs for other PKI components are generated on-board an HSM, under the authority of and with explicit consent of the PMA, under supervision of a Security Officer and under dual control.

Key pair generation for RA and SRA operators

The key pairs for RA operators and SRA operators are generated on-board an SSCD Type 3 Secure Subject Device, under the authority of and with explicit consent of the PMA, under supervision of a Security Officer and under dual control.

Key pair generation for Subjects

The key pairs for Subjects operators are generated on-board an SSCD Type 3 Secure Subject Device, under the authority of and with explicit consent of the PMA, as an integrated part of the Secure Subject Device personalisation service.

6.1.2 Private key delivery to Subscriber or Subject

Not applicable.

For the ZETES TSP Qualified CA the Subscriber is an organization. There are no private keys issued for the Subscriber. The ZETES TSP Qualified CA does issue certificates for a Subscriber's Subjects. The key generation process for a Subject is described in section 6.1.1.

6.1.3 Public key delivery to certificate issuer

Public Key delivery to the offline Root CA

The ZETES TSP Root CA is an offline CA. Certificate requests (that include the public key of the requester) are transferred by means of a secure storage medium. The storage medium's technical characteristic protects the data content against unauthorized manipulation. The transfer is done in a single key ceremony, in the presence of witnesses, and with a direct transfer of the public key immediately following the generation of the key pair.

This applies for public keys for subordinate CAs (such as the ZETES TSP Qualifying CA) and for public keys for OCSP services that act on behalf of the ZETES TSP Root CA.

The procedures, the ceremony, the tools used and the environment in which the key pair is generated and the public key extracted, ensure the requester is in possession of the private key for which the certificate is requested.

Public Key delivery to the issuing Qualified CA

The ZETES TSP Qualified CA has a network connection to internal systems of ZETES TSP for certificate revocation and for generating certificates for Secure Subject Devices that are personalised by Zetes CardS on behalf of ZETES TSP. Certificate requests (that include the public key of the requester) are transferred by means of a secure and authenticated internal network connection between the environment for the personalisation of Secure Subject Devices and the environment for the CA. The transfer is done just in time, in synchronisation with the personalisation process for the Secure Subject Device.

This applies to public keys for all Secure Subject Devices, and for public keys for OCSP services that act on behalf of the ZETES TSP Qualified CA.

The procedures, the ceremony, the tools used and the environment in which the key pair is generated and the public key extracted, ensure the requester is in possession of the private key for which the certificate is requested.

6.1.4 CA public key delivery to Relying Parties

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:

CA	RSA4096	generated and used on HSM
OCSP service	RSA2048	generated and used on HSM
Internally signed audit logs	RSA2048	generated and used on HSM
SSCD Type 3 *	RSA2048	generated and used on SSCD Type 3

** used as Secure Subject Device for Subjects but also authentication device 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 ensure 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’

ECDSA, ECDH:

- 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,
- only elliptic curves P-192, P-224, P-256, P-384, P-521, K-163, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-409 or B-571 as specified in FIPS 186-2 Appendix 6 are used

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 this Certificate Practice Statement and in the applicable Certificate Policies.

For details about the encoded key usage see the document Certificate Profiles, below is an overview:

Key usage for CA certificates:	KeyCert signing
	CRL signing

Key usage for OCSP certificates:	digitalSignature - OCSP signing
Key usage for user certificates for authentication purposes:	digitalSignature - keyEncipherment
Key usage for user certificates for authentication purposes:	nonRepudiation - keyEncipherment

An additional restriction on key usage applies to all the keys that are used for internal purposes by CA/RA/SRA operators and systems. These keys may only be used within the context and restrictions of the operator's role or system's role within the Zetes PKI environment.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Private keys for CA and OCSP

To protect the private keys used by the CA and the OCSP service, the ZETES TSP Qualified CA uses state of the art cryptographic modules. In this document these will be referred to as HSM (for Hardware Security Module).

The HSM are prepared, initialized and managed in compliance with:

- ETSI TS 102 042
- ETSI TS 101 456
- CWA 14167-1 :2003

Private keys for Secure Subject Devices

To protect the private keys used by the Subject or the operators of the CA and RA, the ZETES TSP Qualified CA uses cryptographic modules In this document these will be referred to as Secure Subject Devices, SSCD (for Secure Signature Creation Device) or smartcards, depending on the context.

These SSCD may come in different form such as an ID-1 size smartcard, a SIM- size smartcard or a USB device (similar in shape to a USB memory stick).

The Secure Subject Device contains an embedded security controller (the chip) that meets the following requirements:

- the device allows to generate electronic signatures over previously externally calculated hash values.
- the device generates the signature key pair
- the device is able to protect the secrecy of the internally generated and stored private key
- the device and restricts the usage access to the authorised Subject only by means of a PIN code or an equivalent such as biometric Match on Card
- the device complies with the requirements for a SSCD Type 3 as reference in or specified by:
    - European Directive (1999/93/EC) on a Community framework for electronic signatures,
    - the Belgian law of 9 July 2001 regarding the determination of the rules for the legal framework for electronic signatures and certificate services,
    - CWA 14169 Secure Signature Creation Devices "EAL4+"

- CWA 14355 Guidelines for the Implementation of Secure Signature Creation Devices
- the device achieved Common Criteria certification
  - to an evaluation assurance level “CC EAL4+ SOF-high” or better
  - internationally accepted under European Recognition of ITSEC/CC certificates (SOGIS-MRA) or International Recognition of CC - certificates (CCRA)
  - according to the appropriate Protection Profile as defined in CEN CWA 14169

6.2.2 Private key multi-person control

Private keys for CA and OCSP

The activation and/or use of the private keys in the HSM infrastructure that hold the private keys for the CA and OCSP service is protected by access control and activation mechanisms that require 2 or more custodians to be involved in the process. The activation assets or activation data needed for the activation and/or use of the HSMs is under control of yet more trusted roles and are not directly accessible to the custodians. Custodians require prior approvial by the authorized Security Officer to be allowed access to the activation assets or activation data under their care.

Private keys for Secure Subject Devices

Not applicable.

6.2.3 Private key escrow

Private keys cannot and are never extracted from the HSM or SSCD on which they are generated. Private keys are never put in escrow.

6.2.4 Private key backup

Private keys for CA and OCSP

Private keys on an HSM for the CA or OCSP infrastructure are generated on-board the HSM and are backed up.

The backups are exclusively used for :

- restore for recovery in case of failure of the infrastructure
- restore in case of replacement of an existing HSM
- iniitializing additional HSMs to expand the infrastructure’s capacity

The backup of the keys is also created inside the HSM. The encrypted backup is exported from the HSM into a file. The backup encryption key is itself is generated inside the HSM during the installation and initialization of HSM and is split into key shares which are stored on a set of HSM backup cards.

Backup and restore or transfer of private keys requires a quorum of n-of-m HSM backup cards. Each card has an activation code which is independent from the other cards.

Private keys and other security critical data is always encrypted (backup operation) or decrypted (restore operation) inside the HSM itself. The encryption key is split over a set of m HSM backup cards. A restore operation requires a pre-defined quorum of n-of-m HSM backup cards.

The backup, the activation assets and the activation data are assigned to multiple custodians and are stored in separate locations.

Private keys for Secure Subject Devices

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

6.2.5 Private key archival

Private keys for CA and OCSP

Private keys are on an HSM are not archived as such but are backed up and stored for other reasons. See section 6.2.4.

Private keys for Secure Subject Devices

Private keys on a Secure Subject 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 for CA and OCSP

Private keys on an HSM for the CA or OCSP infrastructure are generated on-board the HSM and can be transferred to another HSM. Transfer of private keys to another HSM requires multi-person control in the form of a quorum of *n-of-m* HSM cards. Transfer of private keys into another HSM requires approval of the PMA. See section 6.2.4 for information on the segregation of cards and codes.

Private keys for Secure Subject Devices

Private keys on a Secure Subject Device cannot be transferred.

6.2.7 Private key storage on cryptographic module

Private keys for CA and OCSP

All keys inside the HSM are stored inside the HSM in encrypted form, the key encryption key cannot be extracted from the HSM or used for any other purpose.

The key encryption key stored in a special memory area of the HSM which is connected to the sensory controller of the HSM. The sensory controller can, in a case of an alarm, delete or render useless the key material in the HSM.

Private keys for Secure Subject Devices

Private keys on a Secure Subject Device are stored in secure memory. The Secure Subject Device is an SSCD of Type 3. The embedded microchip provides protects private keys and other security related information against hacks.

6.2.8 Method of activating private key

Private keys for CA

Private keys on the dedicated HSM for the CA are grouped per CA entity (i.e. per logical CA, not physical CA).

Access to the control interface for activating or deactivating a group is restricted by a dual control mechanism.

Deactivation of the private key for the ZETES TSP Qualified CA requires at least two authorized administrators and operators.

Activation of the private key for the ZETES TSP Qualified CA requires at least 4 authorized administrators and operators. Two for accessing the control interface and two more for entering the group's activation passphrase.

Private keys for OCSP service

The HSM for the OCSP service is not used for CA functions.

Private keys on the dedicated HSM for the OCSP service are automatically activated upon power on without requiring further intervention.

Private keys on the dedicated HSM for the OCSP service are organized in groups.

Access to the control interface for activating or deactivating a group is restricted by a dual control mechanism.

Deactivation of the private key for the ZETES TSP Qualified CA requires at least two authorized administrators and operators.

Activation of the private key for the ZETES TSP Qualified CA requires at least two authorized administrators and operators.

Private keys for Secure Subject Devices

The Secure Subject Device is a device under the sole control of one person: the Subject. The private key is activated by means of a PIN code or an equivalent mechanism such as biometric Match-on-Card.

The Subject can deactivate the private key by repeatedly providing an incorrect PIN code or incorrect biometric authentication.

6.2.9 Method of deactivating private key

See section 6.2.8.

6.2.10 Method of destroying private key

CA and PKI components - automatic destruction of all Private Keys in the HSM for alarm situations

See section 6.2.7

.

CA and PKI components - planned destruction of all Private Keys in the HSM

The External Erase circuit of the HSM is used to immediately zeroize and render useless all keys stored in the HSM and thus effectively destroying all the private keys in that HSM. This procedure is applied when an HSM is to be removed for repair, replacement or decommissioning or when the HSM needs to be re-initialized.

CA and PKI components - selective destruction of a Private Key in the HSM

Private keys are selectively destroyed if the key assignment is deleted in the configuration of the CA or PKI component. When a key in the HSM is deleted, the relevant record in the HSM's internal key database is marked as deleted which immediately deactivates the key and makes it unavailable. The key will also be zeroized and deleted from the HSM memory.

Private keys for Secure Subject Devices

The Secure Subject Device is a device under the sole control of one person: the Subject. The private key is activated by means of a PIN code or an equivalent mechanism such as biometric Match-on-Card.

The Subject can deactivate the private key by repeatedly providing an incorrect PIN code or incorrect biometric authentication.

6.2.11Capabilities and Rating of the Cryptographic Module

The HSM complies with the technical requirement CEN EN 319 411 part 1 under the European Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (referred to as the eIDAS - electronic IDentification and Authentication Services) was published as Regulation (EU) No 910/2014 o 28 August 2014.

The HSM is certified FIPS 140-2 level 3 and meets the overall requirement applicable to this level:

FIPS 140-2 Security Requirements Section	**FIPS 140-2 Level**
Cryptographic Module specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	not applicable
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

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

Activation data for the CA and for OCSP:

All activation data such as PIN codes, passwords and passphrases and activation assets such as smartcards are securely stored in multiple locations in locked compartments of safes in a secure vault.

Activation data and the associated activation assets are segregated, i.e. are assigned to different custodians, and are stored in separate storage compartments for each custodian.

Where relevant, activation data such as passwords and passphrases are split in parts and each part is assigned to a different custodian.

Strict rules for the length, syntax, structure and content of the activation data ensure that the activation data for critical assets is non-trivial and contains sufficient variation.

Activation data for Secure Subject Devices:

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

6.5 Computer security controls

ZETES TSP ensures that computer security controls are implemented according the technical standard ETSI EN 319411-2. ZETES operates its both sites involved with TSP activities according ISO 27001 requirements. The Implemented Information Security Management System includes several controls related to computer security and a.o. :

- Firewalls to protect the TSP internal network domain from unauthorized access and to prevent all accesses and protocols that are not required for the operation of the TSP
- Control of sensitive data stored on “demobilized” or reusable storage device

- Local network components are kept in a secure environment and their configuration is periodically checked
- Use of multifactor authentication for account capable to issue certificates
- Enforced access control to modify disseminated information regarding qualified certificates dissemination. The site for dissemination benefits from a https protocol for read access (see section 2)
- Enforced access control to modify revocation status information through a mutual SSL authentication between the CA an the OCSP server and between CA and the CRL publication infrastructure.
- Access control, intrusion detection system and CCTV monitoring to detect, record and react upon unauthorized access to its resources

6.6 Life cycle technical controls

6.6.1 System development controls

Implemented in compliance with ETSI TS 102 042 and ETSI TS 101 456.

6.6.2 Security management controls

Implemented in compliance with ETSI TS 102 042 and ETSI TS 101 456.

6.6.3 Life cycle security controls

Implemented in compliance with ETSI TS 102 042 and ETSI TS 101 456.

6.7 Network security controls

Zetes regards to the CA activities ensures the maintenance of a high-level network of systems security including firewalls. Network intrusions are monitored and detected.

The network segment for the Qualified CA servers

- is protected by a dedicated firewalls,
- is protected by the general firewalls and intrusion detection system of the ZETES TSP / Zetes CardS secure facility for PKI and smartcard personalisation,
- is segregated from other internal network segments and uses dedicated network switching equipment.

The CA servers for the Qualified CA only accept encrypted connections (confidentiality and require strong authentication and mutual authentication for access by administrators, operators and for access by other systems that connect to the CA servers. Strong authentication is implemented by means certificates that issued by the internal management CA of the CA infrastructure itself.

It is prohibited to access sensitive CA resources including CA databases from outside of the CA's own network.

Detailed descriptions of the network security controls is available in internal confidential documents of ZETES TSP and/or Zetes CardS.

6.8 Time-stamping

Not applicable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Overview of the ZETES TSP Qualified CA for which this CSP applies:

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

Certificate profiles for the ZETES TSP Qualified CA:

Table 1 ZETES TSP QUALIFIED CA - Certificate Profile for ZETES TSP QUALIFIED CA 001 root-signed certificate

certificate profile **ZETES TSP QUALIFIED CA 001 - root-signed certificate** version 1.0			
ATTRIBUTES			
Version		-	**0x02** *(= X.509 certificate version 3)*
Serial Number		-	**38 20 EE 9C 74 EC D1 47** < 64-bit random number > compliant with CA/B Forum requirements, validated to ensure uniqueness of the certificate serial number, compliant with RFC 5280 and X.690
Signaturealgorithm	**algorithm**	-	**sha256WithRSAEncryption**
Signature Value		-	< the signature created by the CA >
SubjectPublicKeyInfo	**algorithm**	-	**RSA4096**
	subjectPublicKey	-	value of the public key
Validity	**notBefore**	-	20/05/2016 (20 May 2016)
	notAfter	-	20/05/2026 (20 May 2026)
Issuer	**serialNumber**	-	**001** (*the 3-digit serial number of ZETES TSP ROOT CA 001*)
	commonName	-	**ZETES TSP ROOT CA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
Subject	**serialNumber**	-	**001** (*the 3-digit serial number of ZETES TSP QUALIFIED CA 001*)
	commonName	-	**ZETES TSP QUALIFIED CA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**

EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	**keyIdentifier**	-	**38 BC 5C 30 54 DC E2 BB 20 EF EE 6F 41 A0 31 6E 5C FD 8B 75**
authorityInfoAccess	**accessMethod**	-	Id-ad-2 OID 1.3.6.1.5.5.7.48.2 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) calssuers(2)}
	accessLocation	-	**http://crt.tsp.zetes.com/ ZETESTSPROOTCA001.crt**
	accessMethod	-	Id-ad-1 OID 1.3.6.1.5.5.7.48.1 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
	accessLocation	-	**http://ocsp.tsp.zetes.com**
CRLDistributionPoint	**distributionPointName**	-	-
	fullname	-	**http://crl.tsp.zetes.com/ZETESTSPROOTCA001.crl**
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	**keyIdentifier**	-	**E2 B4 DB 5F 6A 0F 02 50 54 D5 1D EF D2 76 72 72 21 95 46 2B**
EXTENSIONS -- Policy Properties			
keyUsage	**KeyCertSign**	c	true
	CRLSign	c	true
certificatePolicies	**policyIdentifier**	-	**OID=2.5.29.32.0 [AnyPolicy]**
	policyQualifierID	-	Id-qt-1 (**CPS**)
	qualifier	-	**https//repository.tsp.zetes.com**
	policyQualifierID	-	Id-qt-2 (**User Notice**)
	DisplayText	-	**ZETES TSP CPS for NCP+ and QCP+ certificates**
basicConstraints	**subjectType**	c	**CA** (CA=true)
	pathLengthConstraint	c	**0**

7.2 CRL profile

Generic CRL profile for consolidated CRL:

Table 2 ZETES TSP QUALIFIED CA - CRL profile

CRL profile **ZETES TSP QUALIFIED CA - CRL** version 1.0				
ATTRIBUTES				
Version		-	MS	**2**
Signaturealgorithm	**algorithm**	-	MS	**sha256WithRSAEncryption**
		-	MD	< the signature created by ZETES TSP QUALIFIED CA 001 >
Issuer	**serialNumber**	-	MS	**001** (*the 3-digit serial number of the CA*)
	commonName	-	MS	**ZETES TSP QUALIFIED CA 001**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
thisUpdate		-	MS	<time of issue >
nextUpdate		-	MS	<time of issue + 1 day>
Revoked Certificates	**userCertificate**	-	MD	<certificate serial number>
	revocationDate	-	MD	<revocation time>
	crlEntryExtension **reasonCode**	-	MD	<reason for revocation> - included for every certificate -
CRL EXTENSIONS				
Freshest CRL	**distributionPointName** **fullName**	-	MS	**http://crl.tsp.zetes.com/ZETESTSPQUALIFIEDCA001-delta.crl**
Authority Key Identifier		-	MS	SHA1 of the public key of the CA
CRL Number		-	MD	assigned by the CA

Generic CRL profile for delta CRL:

Table 3 ZETES TSP QUALIFIED CA - delta CRL profile

CRL profile **ZETES TSP QUALIFIED CA - delta CRL** version 1.0				
ATTRIBUTES				
Version		-	MS	**2**
Signaturealgorithm	**algorithm**	-	MS	**sha256WithRSAEncryption**
		-	MD	< the signature created by ZETES TSP QUALIFIED CA 001 >
Issuer	**serialNumber**	-	MS	**001** (*the 3-digit serial number of the CA*)
	commonName	-	MS	**ZETES TSP QUALIFIED CA 001**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
thisUpdate		-	MS	<time of issue >
nextUpdate		-	MS	<time of issue + 1 hour>
Revoked Certificates	**userCertificate**	-	MD	<certificate serial number>
	revocationDate	-	MD	<revocation time>
	crlEntryExtension **reasonCode**	-	MD	<reason for revocation> - included for every certificate -
CRL EXTENSIONS				

Authority Key Identifier		-	MS	< SHA1 of the public key of the CA >
delta CRL Number		-	MD	< incremental number assigned by the CA >
delta CRL Indicator		c	MD	< assigned by the CA , it is the BaseCRLNumber (the number of the base CRL to which the delta CRL belongs) >

7.3 OCSP profile

Generic certificate profile for a ZETES TSP Qualified CA OCSP responder certificate:

Table 4 ZETES TSP QUALIFIED CA - Certificate Profile for OCSP responder

certificate profile **ZETES TSP QUALIFIED CA - OCSP responder certificate**				
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 ZETES TSP QUALIFIED CA 001 >
SubjectPublicKeyInfo	**algorithm**	-	MS	**RSA2048**
	subjectPublicKey	-	MD	< value of the public key >
Validity	**notBefore**	-	MS	< certificate validity start date >
	notAfter	-	MS	< certificate validity start date + 1 year >
Issuer	**serialNumber**	-	MS	**001** (*the 3-digit serial number of the ZETES TSP QUALIFIED CA 001*)
	commonName	-	MS	**ZETES TSP QUALIFIED CA 001**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
Subject	**commonName**	-	MS	**ZetesTSPQualifiedCA001OCSP**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
EXTENSIONS -- Authority Properties				
authorityKeyIdentifier	**keyIdentifier**	-	MS	SHA-1 hash of the public key of the CA (as specified in RFC 5280)
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
enhancedKeyUsage	**OCSP Signing**	c	MS	true
OCSPNoCheck		-	MS	null

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 this CPS.

8.1 Frequency or circumstances of assessment

ZETES TSP' Qualified Certificates issuance process and related services including Registration and Revocation processes will be audited at least once a year for compliance with

- the present CPS and appropriate CP's.
- the technical standards ETSI 319401 and ETSI 319411-2

The PMA reserves the right to organize further audits e.g. in the context of changes in the infrastructure, changes in the organization, security incident…

8.2 Identity/qualifications of assessor

Compliance audits will be performed by a Conformity Assessment Body as defined in point 13 of article 2 of Regulation EC N°765/2008 and compliant with the CA/B Forum requirement for qualified auditors as per CA/Browser Forum version 1.3.4 (March 15,2016) section 8.2.

8.3 Assessor's relationship to assessed entity

To carry out the audits there will be an independent auditor appointed who will not be affiliated directly or indirectly in any way with the CSP.

8.4 Topics covered by assessment

The planned annual audit covers –but is not limited to – all aspects of the CA's operations and related services as specified in the present CPS and related CP's according to section 8.1 of the present CPS.

8.5 Actions taken as a result of deficiency

Detected deficiencies and non-conformities will be reported to the PMA in written. Additional oral comments and clarifications can be provided by the auditor.

The PMA will assess the severity and the extent of the detected deficiencies. In accordance with the auditor, the PMA will determine the time frame and the actions to be conducted to rectify the deficiencies.

A follow-up audit to verify the effectiveness of the actions conducted can be decided by the PMA to ensure compliance.

8.6 Communication of results

Audit report and findings are communicated by the auditor to the audited entities and to the PMA.

In some circumstances, e.g. suspicion of internal fraud, the auditor will not disclose his findings to the audited entity.

Audit report and findings will list all detected deficiencies with their level of severity but without disclosing any information that could be used to attack the system.

By default, audit reports are classified at level "CONFIDENTIAL" and distributed on a need to know basis.

9 OTHER BUSINESS AND LEGAL MATTERS

The ZETES TSP Certificates 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 Certificates 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 Certificates 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 Certificates 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 Certificates 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 Certificates 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 Subscribers and its Subjects. The most common business model that will be used is the application of a fee per certificate issued or renewed, which will include standard CRL publishing, OCSP and revocation services. For high-volume certificate validation requests, special commercial agreement will be made with the Subscriber.

Next to these fees, a yearly maintenance & support contract will need to be agreed upon before Subscriber Agreement can be signed.

Commercial agreement will need be discussed and agreed case by case with every Subscriber before Subscriber Agreement can be signed.

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

9.2 Financial responsibility

9.2.1 Insurance coverage

Each PKI Participant not being a Subscriber or a Relying Party of the ZETES TSP Qualified CA shall contract an insurance policy covering the risks identified in the insurance policy with respect to their services and maintain a

sufficient amount of insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

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

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

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

9.2.1.1 Qualified certificates

As far as the issuance by ZETES TSP Qualified CA of Qualified Certificates is concerned, Article 14 of the Electronic Signatures Law governs the liability of the CSP.

Following this provision, the CSP is liable for damage caused to any entity or legal or natural person who reasonably 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;

(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;

(c) for assurance that the private key and the public key can be used in a complementary manner;

The CSP is liable for damage caused to any entity or legal or natural person who reasonably relies on the certificate for failure to register revocation of the certificate unless the CSP proves that he has not acted negligently.

9.2.1.2 Certificates that cannot be considered as Qualified Certificates

Subject to any limitation of liability referred to in the CPS, 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 S.A. 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. Information that is published in the (Qualified) Certificate is NOT confidential.

- the Subscriber's or Relying Parties' confidential information supplied to ZETES in support requests (other than any information that is published in a ZETES TSP Qualified CA issued Certificate)
- 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
- this Certification Practice Statement

9.3.3 Responsibility to protect confidential information

ZETES TSP and Subscriber Obligations of Confidentiality are described in the Certificates 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 CPS, 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 "Certificates Terms and Conditions".

9.6 Representations and warranties

9.6.1 CA representations and warranties

Zetes S.A. 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 TS 102 042 [4] or ETSI TS 101 456 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 applicable 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 S.A. 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 applicable CP, the verification procedures, and the CPS as applicable at the time of issuance. In addition other warranties may be implied in the applicable 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 "Certificates 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 applicable 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 a 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

9.7 Disclaimers of warranties

Except as expressly provided elsewhere in the CPS, the applicable 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

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.

9.9 Indemnities

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

9.10 Term and termination

9.10.1Term

This CPS 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.

9.10.2Termination

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 CPS will be communicated via the ZETES TSP web site upon termination. That communication will outline the provisions that may survive termination of this CPS 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 CPS shall be in writing and shall be sent, except provided explicitly in the CPS, 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 advanced electronic signature based on a Certificate and a (secure) signature creation device ((S)SCD) and be addressed to:

ZETES TSP PMA, Zetes S.A., Rue de Strasbourg 3, 1130 Bruxelles, Belgium, Fax +32 2 728 37 51.

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 present CPS.

The only changes that the PMA may make to these CPS specifications without notification are minor changes that do not affect the assurance level of this CPS, 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 the present CPS, 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 present 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 present 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 present CPS and provision of CA certification services are compliant to relevant and applicable laws of Belgium.

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----------