ZETES TSP QUALIFIED CA

CERTIFICATION PRACTICE STATEMENT

Certification Practice Statement

for the

ZETES TSP Qualified CA

Publication date :	**16/09/2019**		
Effective date :	**19/09/2019**		
Document OID :	**1.3.6.1.4.1.47718.2.1.1.2**		
Version :	**1.5**	**13/09/2019**	**PMA approved**

Table of Content

Figures

Tables

ABOUT THIS DOCUMENT

Scope

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

This Certification Practice Statement applies to the issuance of Normalized Certificates and of Qualified Certificates meeting the requirements of Regulation (EU) No 910/2014.

Intellectual Property Rights

Document Version History

Version	Publication Date	Effective Date	Information about this Version
1.5	16/09/2019	19/09/2019	Annual review by PMA. No changes were made. Version number update to v1.5 for compliance with CCADB requirements --------
1.4	11/09/2018	14/09/2018	Clarifications regarding key and certificate lifecycle.
1.3	17/07/2017	21/07/2017	Additional clarifications and information ----------
1.2	17/05/2017	22/05/2017	Harmonisation CPS - CP ----------
1.1	27/01/2017	31/01/2017	Update of the CPS in adherence with the Regulation (EU) No 910/2014 and the relevant related Implementation Decisions and Standards such as the ETSI standards EN 319 411 -1 /2. ----
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

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 Trust Service Provider (TSP) as defined in the Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market.

1 INTRODUCTION

1.1 Overview

The ZETES TSP Qualified CA issues Qualified Certificates and Normalized Certificates to natural persons.

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

The present CPS document states the practices to issue Qualified Certificates and Normalized Certificates to natural persons in accordance with the requirements laid down in the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

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

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 relevant ZETES TSP Certificate Policies (CP),
- the relevant ZETES TSP Certificate Terms and Conditions (CTC).

Every certificate issued by the ZETES TSP Qualified CA contains a Certificate Policy OID corresponding to the assurance level of that Certificate as stated in the applicable ZETES TSP (Qualified) CA Certificate Policy. It may be complemented by an OID identifying its domain of issuance and authorised Subscriber.

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.

Non-disclosure

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 parties.

Section 3.6 of the RFC 3647 and clause 5.2 of the ETSI EN 319 411-2 allow for the use of references to distinguish disclosures between public information and security sensitive confidential information.

1.2 Document name and identification

This document is called the 'ZETES TSP Qualified CA – 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 Cryptographic Device,
- the personalisation and delivery service for the Secure Cryptographic 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 through publication of Certificate Revocation Lists and/or through OCSP services),
- 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 Certification Practice Statements and Certificate Policies that are maintained by ZETES TSP.

PKI participants are defined as follows:

Subscribers	An organisation 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	Parties who rely on the validity of the certificate issued by the CA, e.g. for authentication or for validation of a transaction or document.
CA - Certification Authority	The entity issuing certificates to Subjects on request of the RA
CSP - Certificate Service Provider	The entity that has final and overall responsibility for the provision of the (Qualified) Certificates.
RA - Registration Authority	The entity representing the overall organisation of registration authority bodies. The RA as supervising

	authority over the C-RA, SUB-RA and L-RA, authenticates registration/certificate requests from the SUB-RA.
C-RA - Central Registration Authorities	The central infrastructure hosted by ZETES TSP. It handles the registration and vetting of certificate requests received from the SUB-RAs. The C-RA coordinates the certificate creation process between the Secure Cryptographic Device/card personalisation services for Secure Cryptographic Devices/Cards and the CA.
SUB-RA - Subordinate Registration Authorities	The authority for the registration and vetting of Subjects and certificate requests for a specific Subscriber or group of Subscribers. The SUB-RA is 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 and for dissemination of certificate status information.
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 - Local 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, TSP terms and conditions, certificate validation data such as root certificates, certificate revocation lists, etc.
Secure Cryptographic Device - Provisioning Services	ZETES TSP is responsible for supplying the Secure Cryptographic Device.

Secure Cryptographic Device - Personalisation and Delivery Services	The Personalisation Services include a.o. the process of printing the card body of the QSCD, encoding the chip and generating the cryptographic keys on the chip, printing the PIN/PUK letter, etc. The Card Delivery Services include the process of distributing the QSCD and PIN/PUK letters to the Subjects either directly or indirectly via distribution points.

This CPS covers the following combination of roles and organisation 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 related CPs 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:

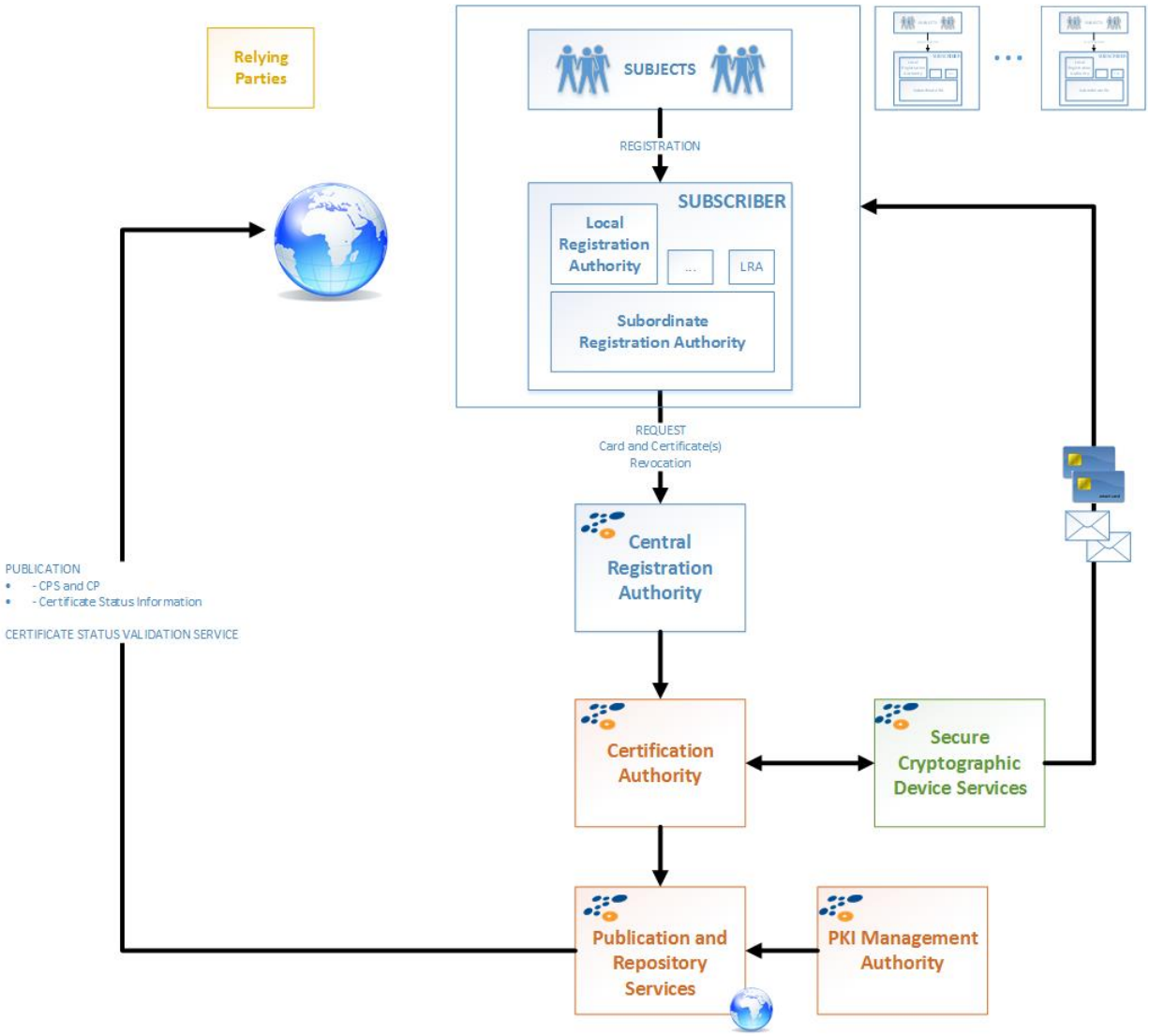

Figure 1 Diagram of the PKI participants

1.3.1 Certification Authorities (CA)

CAs are responsible for:

- Issuing certificates;
- Revoking 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.

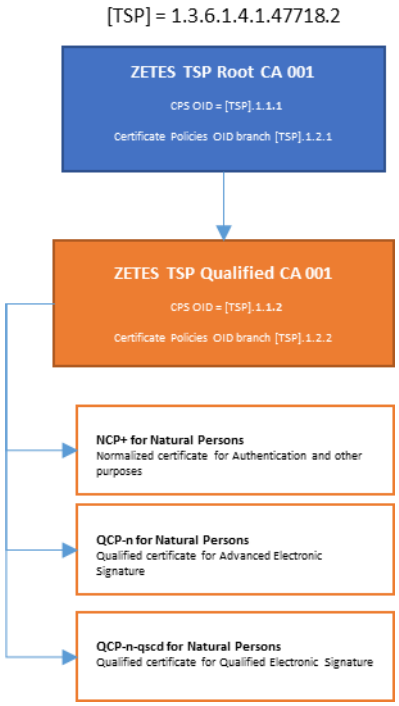

Figure 2 CAs and certificates

1.3.2 Registration Authority (RA)

1.3.2.1 Overview

The Registration Authority is the entity that is responsible for:

- Authenticating and vetting certificate requests and revocation requests;
- Applying the naming conventions defined within this document when creating new entities, so that each entity is uniquely and unambiguously identified;
- Requesting the CAs to produce the certificates for approved certificate application requests;
- Requesting the CAs to revoke the certificates for approved revocation application requests;
- Creating and maintaining an audit log of all significant events related to the RA's fulfilment of the above mentioned responsibilities;
- Providing selective access to the audit log as specified in this document;
- Implementing other operational controls as specified in this document;

- Ensuring that the information that it stores and processes is handled in a manner that is consistent both with the policies and procedures defined in this document and with the ZETES security's regulations.

The RA is organised as a multi-tier organisation. The operational tasks of the RA are performed by the Central Registration Authority, one or more Subordinate Registration Authorities and their Local Registration Authorities. The RA also includes a supervisory body to supervise and audit the various other constituent parts of the RA.

This is illustrated below:

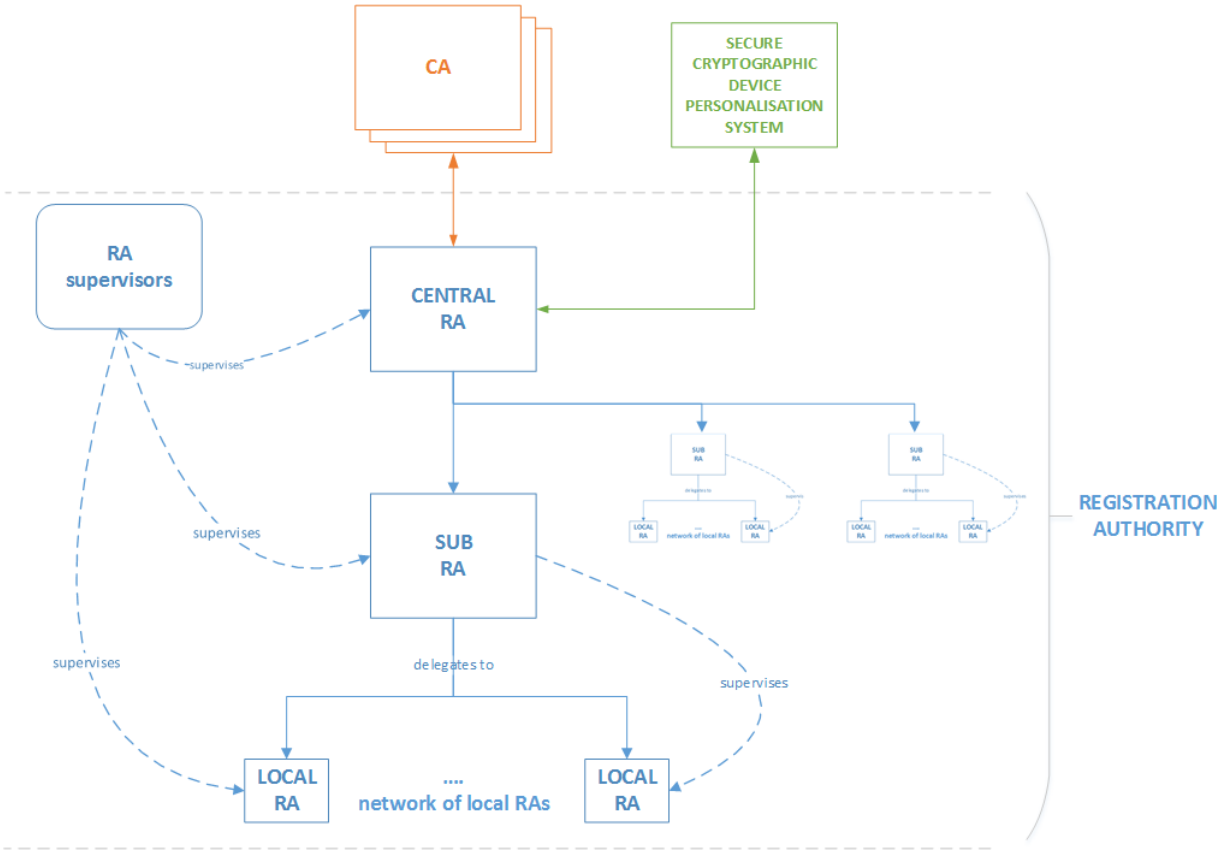

Figure 3 Registration Authority entities

1.3.2.2 Central Registration Authority (C-RA)

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

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

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

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

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

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

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

1.3.2.3 Subordinate Registration Authorities (SUB-RA)

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.

The tasks, responsibilities and identity of the SUB-RA are defined in the Certificate Policy.

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

- ZETES TSP
- the Subscriber
- an authorized third party

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

1.3.2.4 Local Registration Authorities (L-RA)

The Local RA is the organisation that is responsible for the actual registration of the Subject for 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 L-RA are defined in the Certificate Policy.

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

- ZETES TSP
- the Subscriber
- the Subordinate RA
- an authorized third party

1.3.3 Subscribers and Subjects

1.3.3.1 Subscribers (organisations)

Subscribers are organisations 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.

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

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

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.

The Subject's roles and responsibility are detailed in the applicable CP.

1.3.4 Relying parties

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

1.3.5 Other participants

1.3.5.1 Secure Cryptographic Device Provisioning Services

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

The creation of the key pairs is performed by and under control of ZETES as part of the Secure Cryptographic Device personalisation process.

The private key is generated in the Secure Cryptographic Device and cannot be exported in clear text form. Some Secure Cryptographic Devices provide additional controls to prevent use of the private key before the Secure Cryptographic Device or a specific key pair on the Secure Cryptographic Device have been explicitly accepted by the Subject. See also chapter 3.2.1 and chapter 6.2.8 to 6.2.9 for related topics.

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

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

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

1.3.5.2 Dissemination and Repository Services

ZETES is operating the Dissemination Services (publication of Certification Practice Statement, Certificate Policy, TSP terms and conditions, CA certificates, certificate revocation lists and other related, public documents).

This service also provides access to previous versions of these documents (Certification Practice Statement, Certificate Policy, TSP terms and conditions).

Access to CRLs, CA Certificates and OCSP certificate status validation services is made available to all Relying Parties without restrictions.

The Dissemination and Repository Services are provided as described in section 2 of the present Certification Practice Statement.

1.3.5.3 Revocation Management Services and Revocation Status Information Services

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

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 Certificate Policy and (where applicable) the Certificate Terms and Conditions for the certificate.

1.4.2 Prohibited certificate uses

Any usage of a certificate other than the usage explicitly allowed in the relevant CP and (where applicable) the Certificate Terms and Conditions, is prohibited.

1.5 Policy administration

1.5.1 Organisation administering the document

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

1.5.2 Contact person

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

Contact address:	pma@tsp.zetes.com	
Postal address:	Straatsburgstraat 3	3, rue de Strasbourg

	1130 HAREN BELGIË	1130 HAEREN BELGIQUE
Telephone:	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
CTC	Certificate Terms and Conditions
HSM	Hardware Security Module
LRA	Local Registration Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority

1.6.2 Definitions

Activation Data	Data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorised use of the private key.
Certificate	A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.
Certificate Revocation List	A signed list of identifiers of Certificates that have been revoked. Abbreviated as CRL. It is (periodically) made available by the CA to Subscribers and Relying Parties.
Hardware Security Module (HSM)	Hardware Security Module. An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.
Normalized Certificate	A Certificate, issued under the policy and security requirements for TSPs issuing certificates as defined in ETSI EN 319 411 – Part 1, whereby the certification authority *may* support the same level of quality as for issuing Qualified Certificates, but "normalized" for wider applicability and for ease of alignment. The standard is applicable to the general requirements of certification in support of cryptographic mechanisms, including the general use of cryptography for authentication and encryption.
Qualified Certificate	A Certificate which meets the requirements laid down in Regulation (EU) No 910/2014 and Annex I thereof, and is provided by a Qualified Trust Service Provider who fulfils the requirements laid down in the Regulation. The Regulation distinguishes between Qualified Certificates for different purposes: electronic signature, electronic seals, or website authentication. In the context of this *Certification Practice Statement*, the term Qualified Certificate will only reference to “qualified certificates for electronic signature” under the Regulation.
Relying party	In the context of this *Certification Practice Statement*, Relying Parties are as defined in section 1.3.4.
Secure Cryptographic Device	The Secure Cryptographic Devices may come in different form such as e.g. an ID-1 size smartcard, a SIM- size smartcard or a USB device (similar in shape to a USB memory stick), etc. The Secure Cryptographic Device provides some or all of the following functions: • generating electronic signatures over previously externally calculated hash values, • generating keys inside the device • importing keys into the device • the device is able to protect the secrecy of the stored private key, • the device restricts the usage of the key to the authorised owner only by means of a PIN code or an equivalent authentication mechanism such as biometric Match on Card For the purpose of a Qualified Electronic Signature (QES) with a certificate that adheres to the policy [QCP-n-qscd], the Secure Cryptographic Device complies with the following requirements for a Qualified Signature Creation Device (QSCD) as specified in Regulation (EU) No 910/2014 -- Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (eIDAS): • The Secure Cryptographic Device complies with the conditions defined in Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014. • Specifically, the Secure Cryptographic Device has passed security certification in compliance with ETSI EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation and ETSI EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application.

	Note: the term “SSCD” or “Secure Signature Creation Device” is deprecated as of 1st July 2016.
Subscriber	In the context of this *Certification Practice Statement*, the Subscribers are as 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 **https://pds.tsp.zetes.com**	These URL refer to the pages for downloading documents such as the • CPS - Certificate Practice Statements, • CP -Certificate Policies, • PDS - PKI Disclosure Statements • 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 TSP shall make best endeavours to reinstate availability of the service within 5 working days.

Publication of Subject/Subscriber certificates in a repository

See applicable CP.

Publication of CA certificates in a repository

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

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

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

info@tsp.zetes.com

Certificate Status Information

For more information, see section 4.10 and the applicable Certificate Policy.

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 CRLs or delta-CRLS are renewed before the CRL or delta-CRL is about to expire and may be renewed when certificates have been revoked. CRLs and delta-CRLs will be available for download within 20 minutes after creation.

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

CRLs are updated until all certificates that were issued by the respective CA key have expired.

Publication of terms and conditions, CSP, etc.

Updates to the Certificate Policy, Certification Practice Statement or other public documents are published whenever a change occurs, ensuring a period of minimum two (2) days between the publication date and the effective date (see section 9.12).

2.4 Access controls on repositories

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

Subscribers, Subjects and Relying Parties have read-only access via the internet to all the repositories mentioned in section 2.1.

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.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

End-entities certificates bear Distinguished Name (DN) as defined in the applicable Certificate Policies.

The DN for the ZETES TSP Qualified CA certificate 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 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.

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 Cryptographic Devices

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

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

The Secure Cryptographic Device is selected by Zetes.

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

For Qualified Certificates, the Secure Cryptographic Device complies with the conditions defined in Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014.

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

Specifically, the Secure Cryptographic Device has passed security certification in compliance with ETSI EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation and ETSI EN 419 211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application.

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

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

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

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

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

The secure environment includes:

- the card personalisation facility of Zetes,
- the card & key management system operated by Zetes ,
- the infrastructure for post-issuance personalisation
- the security mechanisms of the Secure Cryptographic Device

- the virtual environment of keys and codes used for authentication, authorization and protecting card personalisation operations and the physical infrastructure that is used to protect these keys and codes

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

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 organisation identity

Organisation acting as a Subscriber

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

Organisations acting as Subscriber are authenticated by ZETES TSP in accordance with the rules and regulations for the naming and identification of organisations as applicable in the Kingdom of Belgium or as applicable in the country where the organisation is registered.

ZETES TSP also verifies the organisation's mandate (as Subscriber) to represent a well-defined group of natural persons (as Subjects) based on ETSI EN 319 411-1 requirements. In particular, ZETES TSP requires a verifiable proof and description of the Subscriber's mandate and relationship with the Subjects.

See applicable CP for details on particular cases.

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 authentication procedure to verify the identity of a Subject, the link between a Subscriber as an organisation and a Subject, is as specified in the relevant documents ETSI EN 319 411-1, ETSI EN 319-411-2 and Regulation (EU) No 910/2014 for the following certificate profiles: [NCP+], [QCP-n] and [QCP-n-qscd].

It is part of the registration with a Local RA of the designated Subordinate RA.

See applicable CP.

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., as specified in the applicable CP.

The Subscriber may attest to a Subject's membership of the organisation it represents such as member, employee, associate, role, department, etc., as specified in the applicable CP.

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

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

See applicable CP.

3.2.5 Validation of authority

See applicable CP.

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

See applicable CP.

3.3.2 Identification and authentication for re-key after revocation

See applicable CP.

3.4 Identification and authentication for revocation request

Revocation Requests for Subject certificates

See applicable CP.

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.

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

See applicable CP.

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 section 1.3.2.

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

Each RA entity archives the received or added information for each enrolment. The archive must be kept in a secure location or on a secure system according to the requirements defined in the present CPS, the applicable CP and applicable national laws.

4.1.2.2 Enrolment of Subjects

See applicable CP.

4.1.2.3 Enrolment of Subscribers

ZETES TSP enters into a Subscriber Agreement with Subscribers but does not “enrol” Subscribers.

See applicable CP for more details.

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

ZETES TSP RA may delegate tasks to organisations that are not part of Zetes SA. Typically, the Subordinate RA and its local RA have their own legal entity. These external organisations 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

See applicable CP.

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 component 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 component 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

See applicable CP.

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

See applicable CP.

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 Cryptographic Device for a Subject

The certificate is issued as part of the personalisation process of the Secure Cryptographic Device. The CA will only receive certificate requests from the Central RA in conjunction with the personalisation system for the Secure Cryptographic Devices. The CA, the Central RA and the personalisation system are integrated systems and communicate over closed network connections. The CA will only process requests that originate from a trusted system which is internal to ZETES TSP.

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

- The CA will check that the request originates from a trusted source

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

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

The same checks are performed as for the issuance of a certificate for a Secure Cryptographic Device for a Subject, detailed above. The procedure of issuance is however different as described under section 6.1.1.

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 Cryptographic Device for a Subject

See applicable CP.

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

As specified in the internal documentation.

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

See applicable CP.

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

See applicable CP.

4.5 Key pair and certificate usage

4.5.1 Subject private key and certificate usage

See the applicable CP.

4.5.2 Relying party public key and certificate usage

See the applicable CP.

4.6 Certificate renewal

Certificate renewal for CAs

The CA may not issue certificates that have an expiration date that surpasses that of the CA's proper certificate. When the CA certificate nears its expiration date the PMA may decide to replace the CA certificate.

This requires a new key and a new CA certificate with unique identifiers, subject serial number and certificate serial number.

The new CA certificate can be created before the old CA certificate expires. The transition period until the expiration date of the old CA certificate must provide sufficient time for the dissemination of the new CA certificate and related policy information to Subscribers, Subjects and relying parties.

The set of policy documents will be updated to include references to the new key and certificate.

Existing Subscribers for which this changeover may have an operational impact will be informed by Zetes through the proper channels for each Subscriber. This is handled on a case by case basis.

Subscribers that are a legal person representing a community of Subjects and with whom Zetes has entered into a contractual agreement for issuing certificates to Subjects, will be informed in full and in time. This may include one or more of the following: a copy of the new CA certificate for distribution by the Subscriber, CP/CPS/PDS documents, agreement on the date and modalities of the switchover to the new CA for the Subscriber's certificates, the impact on the update or replacement of Signature Creation Devices, etc.

Zetes will make the new CA certificate and all other public policy documents available via its web site.

Zetes will make a best effort to make the new CA certificate available via other available channels to all entities that rely on the CA certificate. This may involve participation of third parties that are not controlled by Zetes, e.g. platform providers such as Microsoft, Apple, Adobe, etc. and for which actions' Zetes cannot be held accountable.

Certificate renewal for Subjects

See the applicable CP.

4.7 Certificate re-key

Certificate re-key for CAs

See chapter 4.6.

Certificate re-key for Subjects

See the applicable CP.

4.8 Certificate modification

Certificate modification for CAs

Not applicable.

Certificate modification for Subjects

See the applicable CP.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Circumstances for Revocation of a Subject certificate

See the applicable CP.

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

See the applicable CP.

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.

Within the context of a specific Certificate Policy, at least one of the following procedures is available to the Subject:

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 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.

Zetes supports the following possibilities:

CHANNEL	SUBSCRIBER AUTHENTICATION MECHANISMS
E-MAIL	**identification** • a combination of e-mail address, name, organisation and role **authentication mechanisms** • signed e-mail or an e-mail with a signed attachment using a trusted certificate
EXTRANET OR RA-SPECIFIC APPLICATION	**identification** • a combination of account name, unique identifier, e-mail address, name, organisation and role **authentication mechanisms** • logon to extranet or RA specific application using a trusted certificate

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

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

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

A Subordinate RA/SRA or a Local RA/SRA may request revocation of a Subject Certificate either upon its own initiative or upon explicit request of the Subject.

The conditions, 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.

For more information, see the applicable CP.

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

See the applicable CP.

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

See the applicable CP.

4.9.7 CRL issuance frequency

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

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

Periodicity:

	Expiration Period	Publication cycle (max. renewal period)
CRL	24 hours	< 1 hour
delta-CRL	30 minutes	< 30 minutes

4.9.8 Maximum latency for CRLs

Latency for CRLs after revocation of Subject certificates and CA certificates

Zetes TSP updates the CRL with certificate status information for Subject certificates and CA certificates not later than 60 minutes after the actual revocation.

Latency for CRLs after revocation of OCSP certificates or CRL signer certificates

Zetes TSP updates the CRL with certificate status information for OCSP certificates or CRL signer not later than 3 hours after the actual revocation.

4.9.9 On-line revocation/status checking availability

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

http://ocsp.tsp.zetes.com

See section 4.10 for more information.

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

See the applicable CP.

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.

4.10Certificate status services

4.10.1 Operational characteristics

The Zetes TSP Qualified CA maintains an internal database of the status information for all Subject certificates.

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 -
- Online Certificate Status Protocol service

Download service for ARLs, CRLs and delta-CRLs

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

CRLs and delta-CRLs shall be published at regular intervals on the general CRL distribution point at http://crl.tsp.zetes.com and/or a CRL distribution indicated in the certificate (see the Certificate Policy and certificate profile for the certificate). CRLs or delta-CRLs may be renewed when certificates have been revoked. CRLs or delta-CRLs shall be renewed before the CRL or delta-CRL is about to expire.

OCSP service

The OCSP service is available for unsigned requests via http://ocsp.tsp.zetes.com and is synchronised with the latest certificate status information.

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

The OCSP infrastructure consists of multiple OCSP responders which are accessible via a common URL. The OCSP responses are signed by an OCSP responder signing key. The OCSP responder signing certificate is issued by the corresponding CA. For the OCSP certificate profiles, see section 7.3.

Retention period for Certificate Status Information after expiration of the certificates

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

4.10.2 Service availability

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

Zetes TSP maintains a monitoring service for the (delta-)CRL repository to validate that the (delta-)CRLs are published in time and in sequence and are readily accessible via the internet for relying parties.

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

Zetes TSP maintains a monitoring service for the OCSP service to validate that the service is operational and readily accessible via the internet for relying parties.

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

4.10.3 Optional features

No stipulations.

4.11 End of subscription

See the applicable CP.

4.12 Key escrow and recovery

See the applicable CP.

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, 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 ZETES TSP competences management system and include:

- Plant Manager
- PKI Manager
- IT Manager
- PKI Solutions and Implementation Manager
- Security & Quality Manager
- PKI Administrator
- PKI Operator
- PKI System Administrator
- Registration Officer
- Revocation Officer
- IT System Administrator
- HR Manager
- System Auditor
- Spokesperson
- Key Custodians
- [Local Registration Authority Officer (LRAO)]
- [Local Suspension and Revocation Authority Officer (LSRAO)]

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.

Where ZETES TSP involves subcontractors, such as L-RA and L-SRA, the LRAO and LSRAO will be vetted and supervised for them to possess the necessary expertise, reliability, experience, and qualifications. They will have received training to bring awareness regarding security and personal data protection rules as appropriate for the offered services and the job function. An evaluation of the training is performed.

5.2.2 Number of persons required per task

Where dual or multiple controls are required, at least two trusted roles need to bring their respective and split knowledge to be able to proceed with the ongoing operation.

Circumstances requiring dual or multiple controls 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 provide reasonable assurance regarding trustworthiness and competence of the members 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.

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.

5.3.3 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 ensures that the sanction taken is both appropriate and proportional to the violation.

5.3.7 Independent contractor requirements

There are no independent contractors who perform a trusted role other than the LRAO/LSRAO as defined in section 5.2.1.

For independent contractors performing general work in relation to the ZETES PKI, Zetes implements similar practices as for its own personnel that provide reasonable assurance regarding trustworthiness and competence. They can be subjected to similar background checks and they will be contractually required to protect privacy and confidentiality.

For Local Registration Authority Officers (LRAO) and Local Suspension and Revocation Authority Officers (LSRAO) specific training, evaluation and supervision is put in place targeted for their specific job function. (See section 5.2.1.)

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 may 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
- personalisation of the Secure Subject Device

The audit logs records contain:

- The identification of the operation.
- The date and time of the operation.
- The identification of the certificate, if applicable.
- The identity of the transaction.

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.

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 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 kept on secure storage systems or media and located or stored in a secure 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 and 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 every three months (with penetration testing 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 7 years after the certificate ceases to be valid,
- audit trails on the issuance of certificates for a period of minimum 7 years after the certificate ceases to be valid,
- copies of identification documents are retained 7 years after any certificate based on these records ceases to be valid,
- audit trail of the revocation of a certificate for a period of minimum 7 years after revocation of the certificate,
- CRLs for at least 10 years after creation of the CRL,
- documentation supporting the issuance and use of the certificate is kept for a period of at least 10 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 locations 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 of the CA key requires procedures to provide the new CA related information to Subjects and Relying Parties, following a re-key by the CA.

The new CA certificate will be made available to Subjects and Relying Parties through the Zetes TSP repository and other appropriate means such as inclusion on Secure Cryptographic Devices for Subjects or appropriate distribution channels that are specific to a Subscriber.

Unless forced by exceptional circumstances, Zetes TSP will make the new CA public key and certificate available 3 months in advance and will foresee a transition period of no less than 3 months during which both the old and the new CA certificate are in use.

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 to 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 of the 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 organisation or transfer from an old CA to a new CA are not in scope.

The Zetes TSP Termination Plan covers the procedures to be completed in a situation where all services provided by ZETES TSP associated with Qualified Certificates are terminated. The following is a summary of the minimum procedures that are applicable in such a case.

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 require 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.

The processes and procedures applicable to the Subjects key pairs are provided in section 6 of the CP. The present CPS provides the related technical security controls when applicable.

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 a Secure Cryptographic Device, under the authority 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 a Secure Cryptographic Device as an integrated part of the Secure Cryptographic Device personalisation service.

6.1.2 Private key delivery to Subscriber or Subject

See the applicable CP.

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. Certificate requests (which include the public key of the requester) are transferred by means of a secure network connection between the environment for the personalisation of Secure Cryptographic Devices and the environment for the CA.

This applies to public keys for Secure Cryptographic Devices and to public keys for the OCSP services.

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.

For keys generated on Secure Cryptographic Devices personalised by Zetes, two methods are supported:

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

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

6.1.4 CA public key delivery to Relying Parties

ZETES TSP CA certificates are 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
Secure Cryptographic Devices	RSA2048	generated and used on the SCD

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 are generated and tested in accordance with the FIPS 186-2 standard which ensures the quality of the key material.

The following parameters are used depending on the algorithm family:

RSA:

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

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 digitalSignature
Key usage for user certificates for electronic signatures:	nonRepudiation

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).

Private keys for Secure Cryptographic Devices

The Secure Cryptographic Device contains an embedded security controller which provides a secure environment for the generation and storage of cryptographic keys and to perform secure execution of cryptographic operations with these keys.

For the purpose of a Qualified Electronic Signature (QES) with a certificate that adheres to the policy [QCP-n-qscd], the Secure Cryptographic Device's embedded security controller complies with the following requirements for a Qualified Signature Creation Device (QSCD) as specified in Regulation (EU) No 910/2014 -- Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (eIDAS):

- The Secure Cryptographic Device complies with the conditions defined in Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014.
- Specifically, the Secure Cryptographic Device have passed security certification in compliance with ETSI EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation and ETSI EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application.

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 approval by the authorized Security Officer to be allowed access to the activation assets or activation data under their care.

Private keys for Secure Cryptographic Devices

Not applicable.

6.2.3 Private key escrow

Private keys for CA and OCSP

Private keys cannot and are never extracted in non-encrypted format from the HSM on which they are generated. Private keys are never put in escrow. Private keys in encrypted form are only used for backup & restore purposes.

Private keys for Secure Cryptographic Devices

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

6.2.4 Private key backup

Private keys 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
- initializing 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 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 Cryptographic Devices

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

6.2.5 Private key archival

Private keys for CA and OCSP

Private keys 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 Cryptographic Devices

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

6.2.6 Private key transfer into or from a cryptographic module

Private keys 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 Cryptographic Devices

Private keys on a Secure Cryptographic 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 Cryptographic Devices

Private keys on a Secure Cryptographic Device are stored in secure memory. The embedded microchip protects private keys and other security related information against hacks.

6.2.8 Method for activating private keys

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 Cryptographic Devices

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

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

6.2.9 Method of deactivating private key

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 Cryptographic Devices

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

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 of 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 Cryptographic Devices

Activation data for Secure Cryptographic 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 319 411-2. 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 Zetes 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. The site for dissemination provides https protocol for read access (see section 2)
- Enforced access control to modify revocation status information through a mutual SSL authentication between the CA and 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 physical access to its resources

6.6 Life cycle technical controls

6.6.1 System development controls

Implemented in compliance with ETSI EN 319 411

6.6.2 Security management controls

Implemented in compliance with ETSI EN 319 411

6.6.3 Life cycle security controls

Implemented in compliance with ETSI EN 319 411

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 firewall,
- is protected by the general firewalls and intrusion detection system of the ZETES 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 of certificates that are 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 description of the network security controls is available in internal confidential documents of ZETES TSP and/or Zetes.

6.8 Time-stamping

Not applicable.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Overview of the ZETES TSP Qualified CA hierarchy

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

Note: the Subject Certificate profiles are provided in the applicable CP.

Certificate profile 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) caIssuers(2)}
	accessLocation	-	**7.1.1.1.1.1 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 certificate 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 Supervisory Body (FOD Economie, Algemene Directie Kwaliteit en Veiligheid), 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 319 401 and ETSI 319 411-2

The PMA reserves the right to organize further audits e.g. in the context of changes in the infrastructure, changes in the organisation or security incidents.

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

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

9.1 Fees

Commercial agreement are discussed and agreed case by case with every Subscriber before Subscriber Agreement can be signed. See applicable CP for more details.

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.

The liability of ZETES TSP Qualified CA towards the Subscriber or a Relying Party may be limited according to the applicable CP.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

See the applicable CP.

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

See the applicable CP.

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.

See applicable CP, Subscriber Agreement or Subject Agreement for more details.

9.5 Intellectual property rights

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

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

9.6 Representations and warranties

See applicable CP.

9.7 Disclaimers of warranties

See applicable CP.

9.8 Limitations of liability

See applicable CP.

9.9 Indemnities

See applicable CP.

9.10 Term and termination of the present CPS

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

See applicable CP.

9.12 Amendments to the present CPS

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

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

9.13 Dispute resolution provisions

See applicable CP.

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 (including the directly applicable Regulation (EU) No 910/2014).

9.16 Miscellaneous provisions

See applicable CP.

9.17Other provisions

Not applicable.

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