ZETESCONFIDENS

ZETES TSP QUALIFIED CA 001 - CPS

Certification Practice Statement

for the

ZETES TSP Qualified CA 001

Publication date :	**03/09/2020**	
Effective date :	**04/09/2020**	
Document OID :	**1.3.6.1.4.1.47718.2.1.1.2**	
Version :	**1.7**	**01/09/2020l**

Table of Content

Figures

Tables

ABOUT THIS DOCUMENT

Scope

The present document is the Certification Practice Statement (CPS) for the 'ZETES TSP Qualified CA 001'.

This Certification Practice Statement applies to the issuance of Lightweight and Normalized Certificates meeting the requirements of ETSI EN 319 411-1 **[ref. 2]** and of Qualified Certificates meeting the requirements of Regulation (EU) No 910/2014 **[ref. 1]** and ETSI EN 319 411-2 **[ref. 3]**.

Intellectual Property Rights

Document Version History

Version	Publication Date	Effective Date	Information about this Version
1.7	03/09/2020	04/09/2020	Update in descriptions of the RA and SRA roles to make the distinction between these roles clearer and to clarify that RA and SRA can be different entities.
1.6	09/03/2020	13/03/2020	Annual review by PMA. Introduction of the general Trust Service Practice Statement and Lightweight Certificates. Introduction of possibility that Subject Device includes "soft keys" management. Possibility of SCD Management.
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 ----------

References

[ref. 1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

[ref. 2] ETSI EN 319 411-1: "Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements"

[ref. 3] ETSI EN 319 411-2: "Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"

[ref. 4] ZETESCONFIDENS Trust Services Practice Statement (TSPS) (OID 1.3.6.1.4.1.47718.2.0.1.1)

ABOUT ZETES

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

1 INTRODUCTION

1.1 Overview

The 'ZETES TSP Qualified CA 001' issues Qualified Certificates as well as Lightweight 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 Lightweight and Normalized Certificates to natural persons in accordance with the requirements (where applicable) laid down in the Regulation (EU) No 910/2014 **[ref. 1]**.

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 001' are governed by the present ZetesConfidens Qualified CA Certification Practice Statement (CPS), any relevant certificate policy (CP), and the applicable certificate terms and conditions as indicated in the relevant CP.

Every certificate issued by the ZETES TSP Qualified CA 001 contains a Certificate Policy OID corresponding to the assurance level of that Certificate as stated in the applicable ZetesConfidens (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 319 411-1 allow for the use of references to distinguish disclosures between public information and security sensitive confidential information.

1.2 Document name and identification

This document is called the 'ZETESCONFIDENS Qualified CA – Certification Practice Statement'. In prior versions the naming was '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, ZetesConfidens is acting as the Certification Service Provider (CSP). ZetesConfidens has final and overall responsibility for the provision of the ZetesConfidens (Qualified) Certificates offering, namely:

- the provisioning service for the Secure Cryptographic Device (SCD),
- the personalisation and delivery service for the Subject Device,
- the Certificate Generation Services through the ZetesConfidens Certification Authority,
- the Registration Management Services through the ZetesConfidens Registration Authority network of subordinate and local RAs,
- the Suspension and Revocation Management Services through the ZetesConfidens Suspension and Revocation Authority network,
- the Revocation Status Information Service (providing certificate validity status information through publication of Certificate Revocation Lists and/or through OCSP services),
- the Dissemination Services.

ZetesConfidens 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 ZetesConfidens as a CSP and/or who are impacted by the use of certificates issued by ZetesConfidens acting as a CSP. All participants adhere to or are bound by the Certification Practice Statements and Certificate Policies that are maintained by ZetesConfidens.

PKI participants are defined as follows:

Subscribers	An organisation that enters into a contractual agreement with ZetesConfidens on behalf of Subjects
Subjects	Natural persons whose identity or identifier is encoded in the end user certificate issued by a CA. A Subject adheres to a Subscriber.
Relying Parties	Parties who rely on the validity of the certificate issued by the CA, e.g. for authentication or for validation of a transaction or document.
CA - Certification Authority	The entity issuing certificates to Subjects on request of the RA
CSP - Certificate Service Provider	The entity that has final and overall responsibility for the provision of the (Qualified) Certificates. It is a Trust Service Provider as defined in the European Regulation **[ref. 1]**
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 ZetesConfidens. It handles the registration and vetting of certificate requests received from the SUB-RAs. The C-RA coordinates the certificate creation process between the Subject Device Provisioning Services / SCD Management 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	ZetesConfidens is the SRA. The SRA is the entity responsible for the supervision and control of all certificate revocation and suspension activities
Publication and Repository Services	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.
Subject Device - Provisioning Services	ZetesConfidens is responsible for provisioning the Subject Device to the Subject: ZetesConfidens prepares, and provides or makes available secure cryptographic devices (SCD), or other secure devices, to subjects. Where Subject Device Provisioning entails the provisioning of a SCD, it may come e.g. in the form of a smartcard handed over to the Subject. Subject Device Provisioning also covers the "soft keys" management.
Subject Device - Personalisation and Delivery Services	The Personalisation Services include when applicable the process of printing the card body of the SCD that are handed over to the Subject, 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 SCD (e.g. secure cards) and PIN/PUK letters to the Subjects either directly or indirectly via distribution points.
(Qualified) Secure Cryptographic Device (SCD) – Management Services	ZetesConfidens is responsible for the management of the SCD, either until the SCD is handed over to the Subject or for the lifetime of the SCD. For the ZetesConfidens Signature Creation Service by remote server signing, the Secure Cryptographic Device refers to the SCD managed by ZetesConfidens itself (an HSM). No actual delivery of the SCD to the Subject takes place.

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:

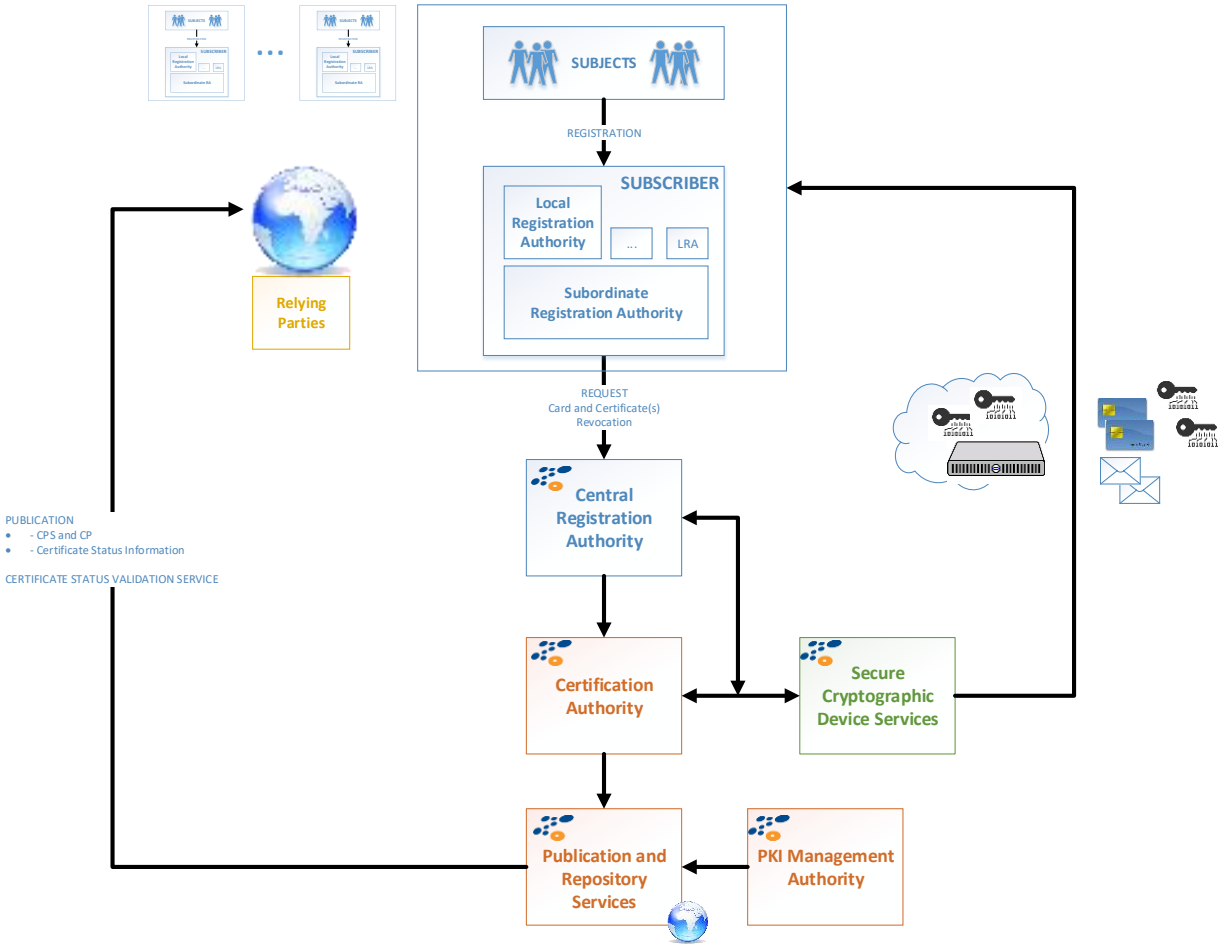

Figure 1 Diagram of the PKI participants

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

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

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 ZetesConfidens 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:

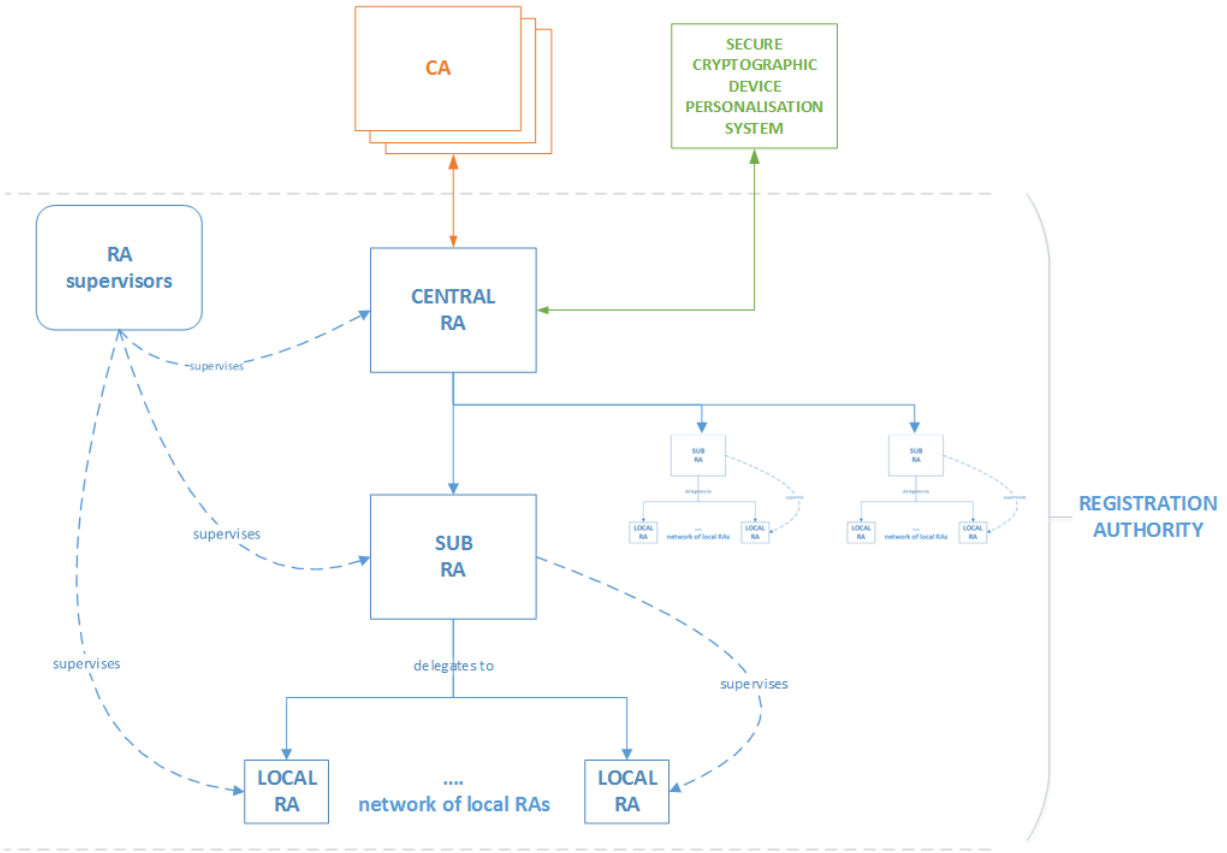

Figure 2 Registration Authority entities

1.3.2.2 Central Registration Authority (C-RA)

The Central RA is the organisational structure and the infrastructure within ZetesConfidens 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 subject device personalisation process and/or SCD Management for key generation
    - submit a certificate request to the appropriate CA

- retrieve the certificate from the CA
- interact with the subject device personalisation process and/or SCD Management for encoding the certificate.

The infrastructure for the Central RA is closely integrated with the Subject Device Personalisation and Delivery Services and/or the SCD Management.

When a Subject Device (most often in the form of a smart card) is actually delivered to the Subject:

- 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:

- ZetesConfidens
- 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:

- ZetesConfidens
- 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 ZetesConfidens (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 Subject Device Provisioning and Secure Cryptographic Device Management Services

Unless Lightweight or Normalized Certificate Policies allow the use of a Subject Device other than a Secure Cryptographic Device (e.g. in case of "soft keys" management), the Secure Cryptographic Devices required to contain the private key corresponding with the certified public key are provided by ZetesConfidens.

The creation of the key pairs is performed by and under control of ZetesConfidens as part of the Subject Device Provisioning process and/or the Secure Cryptographic Device Management.

When the private key is generated in the Secure Cryptographic Device, it 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 has been explicitly accepted by the Subject. See also chapter 3.2.1.

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. ZetesConfidens 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.

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

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

ZetesConfidens is operating the Revocation Management Services and the Revocation Status Information Services (which provide Certificate validity status information) with regards to the ZetesConfidens (Qualified) Certificates under the applicable 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 ZetesConfidens in its role as Certification Service Provider as ruled by the present Certification Practice Statement.

1.3.6 ZetesConfidens 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 ZetesConfidens 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) Organising specific TSP lifecycle events such as key ceremonies.
(q) 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.
(r) 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 with further reference to (the case being) the applicable 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 ZetesConfidens 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 or pma@confidens.zetes.com	
Postal address:	Straatsburgstraat 3 1130 HAREN BELGIË	3, rue de Strasbourg 1130 HAEREN BELGIQUE
Telephone:	0032 2 728 37 11	
Web site:	http://tsp.zetes.com or http://confidens.zetes.com	

1.5.3 Person determining CPS suitability for the policy

The PMA determines the present document's suitability for the ZetesConfidens 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.
Lightweight Certificate	A Certificate, issued under the policy and security requirements for TSPs issuing certificates as defined in ETSI EN 319 411 – Part 1, whereby a Lightweight Certificate Policy (LCP) is applicable, offering a quality of service less onerous than the NCP (requiring less demanding policy requirements) for use where a risk assessment does not justify the additional burden of meeting all requirements of the NCP (e.g. physical presence), for certificates used in support of any type of transaction (such as digital signatures, web authentication).
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

The information can be found in the TSPS **[ref. 4]** under the same section heading.

2.2 Publication of certification information

The information can be found in the TSPS **[ref. 4]** under the same section heading.

2.3 Time or frequency of publication

The information can be found in the TSPS **[ref. 4]** under the same section heading.

2.4 Access controls on repositories

The information can be found in the TSPS **[ref. 4]** under the same section heading.

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 001 does not issue certificates that use pseudonyms or any form of anonymous identifiers.

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.

3.1.4 Uniqueness of names

Subject DNs (including where ZetesConfidens is its own Subscriber) are guaranteed to be unique across the ZetesConfidens PKI Domain.

3.1.5 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 or tamper proof environment 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 Device is most often a secure smartcard as a Subject Device or in case of remote server signing an HSM operated by ZetesConfidens itself.

The Subject Device with an embedded PKI chip has 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.

In case of remote server signing with the use of an HSM, similar features exist however the use of the private key can only be triggered based on multi-factor authentication (MFA) with sufficient assurance level.

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 Subject Device and the Secure Cryptographic Device Management. Initialization, pre-issuance personalisation and post-issuance personalisation of a Subject Device is performed on behalf of ZetesConfidens and under supervision of ZetesConfidens in a secure environment and under controlled conditions. These processes involve participation of one more other actors such as the Subject 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 001 does not issue certificates to organisations, but to natural persons only.

Organisations acting as Subscriber are authenticated by ZetesConfidens 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.

ZetesConfidens 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, ZetesConfidens 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, 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: [LCP], [NCP], [NCP+], [QCP-n] and [QCP-n-qscd].

The authentication procedure to verify 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 ZetesConfidens. 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

ZetesConfidens 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

ZetesConfidens 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 ZetesConfidens
- 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 ZetesConfidens 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

ZetesConfidens, 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 001.

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

ZetesConfidens, 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 001.

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

ZetesConfidens 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 Subject

The certificate is issued as part of the personalisation process of the Subject Device and/or the Secure Cryptographic Device Management. The CA, the Central RA, the Subject Device Provisioning and SCD Management systems 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 ZetesConfidens.

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 Operators and Administrators
The same checks are performed as for the issuance of a certificate 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 001 only issues PKI Component certificates for the ZetesConfidens 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 Subject

See applicable CP.

Notification of issuance of a certificate 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 ZetesConfidens 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.

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

ZetesConfidens 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 ZetesConfidens 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 the Subscriber 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
SUBSCRIBER	**identification** • a combination of name, date of birth, member number, card number, etc. **authentication mechanisms** • an official identification document such as a national ID card or a passport • 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 ZetesConfidens 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 ZetesConfidens 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, 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 entity

A Subordinate RA or a Local RA 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 Agreement.

The SRA entity shall decide to revoke a Subject's certificate(s).

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 ZetesConfidens. 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, ZetesConfidens 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 001 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	< 24 hour
delta-CRL	1 hour	< 1 hour

4.9.8 Maximum latency for CRLs

Latency for CRLs after revocation of Subject certificates and CA certificates

Zetes TSP posts the delta-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

ZetesConfidens posts 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

ZetesConfidens maintains an Online Certificate Status Protocol (OCSP) service:

http://ocsp.tsp.zetes.com or http://ocsp.confidens.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 ZetesConfidens repository pages:

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

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

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

4.9.12 Special requirements re key compromise

No stipulations.

4.9.13 Circumstances for suspension

Suspension is currently not supported.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

The Zetes TSP Qualified CA 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 001 as well as the status of the ZETES TSP Qualified CA 001 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 general CRL distribution point: http://crl.tsp.zetes.com or http://crl.confidens.zetes.com.

CRLs and delta-CRLs shall be published at regular intervals on the general CRL distribution point 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 or http://ocsp.confidens.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 ZetesConfidens or any other reason, ZetesConfidens 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

See for inclusion section 5 of the Trust Services Practice Statement **[ref. 4]** for:

- Facility, management and operational controls (i.e. physical controls, procedural controls and personnel controls),
- Provisions on security compromise and disaster recovery, and on termination of all or parts of the trust service activities.

6 TECHNICAL SECURITY CONTROLS

This section covers the technical security controls for the end entity key pair. For the technical security controls (including key management) for the CA, RA and other PKI components, we refer to section 6 of the Trust Services Practice Statement **[ref. 4]**.

The processes and procedures applicable to the Subjects key pairs are provided in section 6 of the relevant 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 Subjects

Unless otherwise specified in the applicable Certificate Policy, the key pairs for Subjects are generated on-board a Secure Cryptographic Device as an integrated part of the Secure Cryptographic Device Management service.

See also sections 1.3.5, 3.2.1, 6.2.8 and 6.2.9.

6.1.2 Private key delivery to Subscriber or Subject

See the applicable CP.

6.1.3 Public key delivery to certificate issuer

See the TSPS **[ref. 4]** under the same section heading.

6.1.4 CA public key delivery to Relying Parties

See the TSPS **[ref. 4]** under the same section heading.

6.1.5 Key sizes

See the TSPS **[ref. 4]** under the same section heading.

6.1.6 Public key parameters generation and quality checking

See the TSPS **[ref. 4]** under the same section heading.

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

See additionally the TSPS **[ref. 4]** under the same section heading.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

See the TSPS **[ref. 4]** under the same section heading.

6.3 Other aspects of key pair management

See the TSPS **[ref. 4]** under the same section heading.

6.4 Activation data

See the TSPS **[ref. 4]** under the same section heading.

6.5 Computer security controls

See the TSPS **[ref. 4]** under the same section heading.

6.6 Life cycle technical controls

See the TSPS **[ref. 4]** under the same section heading.

6.7 Network security controls

See the TSPS **[ref. 4]** under the same section heading.

6.8 Time-stamping

See the TSPS **[ref. 4]** under the same section heading.

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

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

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

See the TSPS **[ref. 4]** under the same section heading.

9 OTHER BUSINESS AND LEGAL MATTERS

Section 9 of the TSPS **[ref. 4]** applies to this CPS.

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 001 offering.

For example, they provide general information about the conditions of use of ZetesConfidens Certificates, the rights and obligations of ZetesConfidens, 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 001 offering. Unless specific terms and conditions are concluded in a written Subject Agreement, the published ZetesConfidens Certificate Terms and Conditions on the repository website https://repository.confidens.zetes.com will be applicable.

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