ZETES TSP ROOT CA 001

CERTIFICATE POLICY & CERTIFICATION PRACTICE STATEMENT

Identifier:	**Zetes TSP Root CA 001**
Subject:	**Certificate Policy & Certification Practice Statement**
Category:	**CP-CPS**
Version:	**1.7**
Status:	**approved**
Publication Date:	**10/12/2024**
CPS OID:	**1.3.6.1.4.1.47718.2.1.1.1**
Policy OID:	**1.3.6.1.4.1.47718.2.1.2.1**
Effective Date:	**15/12/2024**
Classification:	**PUBLIC**
Copyright:	**© 2020 Zetes NV - All rights reserved.**

Table of Content

DOCUMENT HISTORY

Version	Publication Date Effective Date	Changes
1.7	10/12/2024 15/12/2024	Annual review, no changes made Effective date
1.6	09/10/2023 11/10/2023	Annual review, no changes Effective date
1.5	12/10/2022 14/10/2022	Annual review Effective date
1.4	06/10/2021 07/10/2021	Annual review. Effective date
1.3	02/10/2020 05/10/2020	Alignment of the CPS part of this document with the Trust Service Practice Statement of ZetesConfidens. Update of the document layout, logos and use of confidens.zetes.com in applicable URLs. Explicit mention that issuing CAs are owned by Zetes NV and are operated by the same organizational unit that operates the root CA itself. Removed the "About this document" page and moved its content into the title page and the Document History table. Modified chapter 4.6 Certificate Renewal.
1.2	24/02/2020 24/02/2020	Annual review. Updated "About Zetes" , now mentions Panasonic. The reference to end-entities receiving certificates from subordinated issuing CA's now also include legal persons a.o. to allow for eIDAS electronic seals. Updated references to legislation and norms. Updated the CA-hierarchy schematic in chapter 7.1 and removed the redundant and obsolete schematic in chapter 1.3.1. Clarified FIPS 186-3/4 compliance.
1.1	08/02/2019 11/02/2019	Reviewed. Correction of typos and redundant white space. Updated corporate information (Panasonic, ZetesConfidens). Integration of Certificate Policy OID.
1.0	27/06/2016 29/06/2016	first publication ----------

ABOUT ZETES

Founded in 1984, Zetes NV/SA is a company incorporated in Belgium (European Union) and is part of the Zetes Group, which is fully owned by the Panasonic Group. Zetes NV/SA is active in the areas of identification documents, travel documents, smartcards, biometrics and trust services including the issuance of certificates.

In 2016, Zetes established an operational business unit within Zetes NV/SA to provide certificate services and other trust services for governments, the financial sector and private organizations. Since September 2018 these activities are marketed under the **ZetesConfidens** tradename (before referred to as "Zetes TSP").

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

Zetes NV/SA is registered in Belgium 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.

1 INTRODUCTION

1.1 Overview

ZETESCONFIDENS CA hierarchy.

This document applies to the ZETES TSP ROOT CA 001. The ZETES TSP ROOT CA 001 only issues certificates to subordinate CAs that are owned and operated by ZETES.

The provision and use of subordinate CA certificates issued by ZETES TSP ROOT CA 001 are governed by the present Certification Practice Statement (CPS) and Certificate Policy (CP).

The provision and use of the certificates for end-entities, issued by subordinate CAs, are governed by the related Certification Practice Statement (CPS) and the Certificate Policy (CP) of each subordinate CA and are out of scope of the present document. By default, information related to subordinate CAs and/or end-entities certificates is thus provided in the related documentation. The present document may specify information related to subordinate CAs certificates when needed for the sake of clarity or of conformity to the RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

Conformity with RFC 3647

This document 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.

Non-disclosure

Section 3.6 of the RFC 3647 and clause 5.2 of the ETSI EN 319 411-1 provide for the use of references to divide disclosures between public information and security sensitive confidential information. For reasons of confidentiality, ZETES cannot disclose all details on controls in this document but may instead include references to internal detailed documents. These documents will only be made available to duly authorised auditors.

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)

Conformity with EU legislation and standards for TSP

Where applicable ZetesConfidens follows the requirements laid down in the Regulation (EU) No 910/2014 **[ref. 1]**.

Where applicable ZetesConfidens follows normative standards amongst others set out by ETSI and CEN in the following European Standards (EN), Technical Reports (TR) and Technical Specifications (TS):

ETSI EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
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

ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI TS 119 431-1	Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD /SCDev
ETSI TS 119 431-2	Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation.
ETSI TS 119 432	Protocols for remote digital signature creation
CEN EN 419 241-1	General System Security Requirement

CEN and ETSI are officially recognized as European Standards Organizations by the European Union (EU Regulation 1025/2012).

1.2 Document name and identification

This document is called the 'ZETES TSP Root CA 001 – Certificate Policy & Certification Practice Statement'.

The OID for the Certification Practice Statement is:

dotted notation	1.3.6.1.4.1.47718.2.1.1.1
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) rootca(1) }

The OID for the Certificate Policy is:

dotted notation	1.3.6.1.4.1.47718.2.1.2.1
full notation	{ iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) zetes(47718) zetes-tsp(2) cs(1) cert policy (2) rootca(1) }

1.3 PKI participants

In the context of issuing CA Certificates, ZETESCONFIDENS is the Certification Service Provider (CSP). ZETESCONFIDENS operates a multi-level CA hierarchy. The root CA and the subordinate CAs are owned and operated by ZETES. Subordinate CAs issue end-entity certificates to natural or legal persons.

ZETESCONFIDENS has final and overall responsibility for the provision of the CA services, namely:

- the provision of service equipment, infrastructure and personnel for the subordinate CA,
- supervision and operation of equipment, infrastructure and personnel for the subordinate CA,
- the certificate generation services, through the ZETESCONFIDENS Root Certification Authority,
- the Registration Management Services, through the ZETESCONFIDENS trusted persons in charge of the management of the PKI and under the responsibility of the ZETESCONFIDENS Policy Management (PMA),
- the Suspension and Revocation Management Services, through the ZETESCONFIDENS trusted persons in charge of the management of the PKI and under the responsibility of the ZETESCONFIDENS Policy Management (PMA),
- the Revocation Status Information Service (providing Certificate validity status information),
- 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 Certification Service Provider (CSP) and/or who use or are

otherwise impacted by certificates issued by ZETESCONFIDENS. All participants adhere to or are bound by the Certification Practice Statements and Certificate Policies that are maintained by ZETESCONFIDENS.

The PKI participants, concerned by the whole CA hierarchy, are defined as follows:

Subscribers	**For certificates for CA and validation services**, the Subscriber is ZETESCONFIDENS, owner and operator of all CA in the CA hierarchy and the related validation services.
Subjects	**For the top level of the CA hierarchy concerned by the present CPS**, subjects are ZETESCONFIDENS Certification Authorities (i.e. a subordinate CA).
Relying Parties	Third parties who rely on the validity of the certificate issued by the CA hierarchy.
CA - Certification Authority	Certification Authority of ZETESCONFIDENS which issues certificates to Subjects (on request of the RA for the second level of the hierarchy, and on request of the PMA for subjects that are CAs).
VA – Validation Authority	Certificate validation services of ZETESCONFIDENS such as OCSP and CRL.
Publication and Repository Services	ZETESCONFIDENS web site for publication of Certification Practice Statements, Certificate Policies, Certificates Terms and Conditions, certificate validation data such as root certificates, certificate revocation lists, etc.

The PKI participants specifically concerned by the second level of the CA hierarchy (which is out of scope of the present document) are defined as follows:

RA - Registration Authority	ZETESCONFIDENS as 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 key generation process on the Subject's signature creation device (either a smartcard or a managed HSM) and the CA. It is the only part of the RA that is in direct contact with the CA or with the Subject key generation infrastructure.
SUB-RA - Subordinate Registration Authorities	The authority for the registration and vetting of Subjects and certificate requests for a specific Subscriber or group of Subscribers. The SUB-RA can be

	internal to the TSP, related to the Subscriber or external.
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.
Subject Device Provisioning Services more commonly referred to as Card Provisioning Services	The Subject Device is also referred to as "card" or as "SSCD" for Secure Signature/Seal Creation Device or "QSCD" for Qualified Signature/Seal Creation Device. ZETESCONFIDENS supplies the device to the Subscribers and Subjects. The device is usually a PKI smartcard but can also be another form factor such as a USB PKI device.
Subject Device Personalisation and Delivery Services more commonly referred to as Card Personalisation and Delivery Services	Card personalisation services by Zetes CardS, i.e. the process of printing the card body, encoding the chip and generating the cryptographic keys on the chip, printing the PIN/PUK letter, etc. Card Delivery Services i.e. the process of distributing the cards and PIN/PUK letters to the Subjects and/or card issuing points.

Within the context of this CP-CPS, ZETESCONFIDENS fulfils all the following roles:

- Certificate Authority, as owner and operator of the root CA
- Subscriber, as owner and operator of the subordinate CA
- Subject, i.e. the subordinate CA
- Publication and Repository Services

ZETESCONFIDENS being both CA and Subscriber, there are no separate bodies for Registration Authority nor for Suspension and Revocation Authority as such. Rather, there are a series of procedure put in place for the issuance of PKI component certificates such as the Root CA self-signed certificate, subordinate CA certificates and certificates for certificate status validation services such as OCSP responder certificates. These procedures are undertaken by ZETESCONFIDENS persons in trusted roles, under multiple control and under the responsibility of the PMA such as further described in the present CPS and its related confidential and internal documentation.

1.3.1 Certification Authorities (CA)

CAs are responsible for:

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

ZETESCONFIDENS operates a CA hierarchy with subordinate CAs with dedicated certificate issuing policies compliant with ETSI 319 411 Lightweight Certificate Policy / Normalized Certificate Policy / Qualified Certificate Policy for natural persons or legal persons and compliant with ETSI 319 421 policy for timestamps.

ZETESCONFIDENS reserves the right to add additional subordinate CA hierarchies under the ZETES TSP Root CA in the future. These subordinate CA hierarchies operate under the authority of ZETESCONFIDENS and must adhere to the terms

and conditions of the CPS for the Zetes TSP Root CA. Each CA in a subordinate CA hierarchy under the ZETES TSP Root CA has a dedicated CPS, adapted to the specific purpose of the certificate issued by that CA hierarchy.

1.3.2 Registration Authority and Revocation Authority

Within the context of the Zetes TSP Root CA 001 all entities involved in the registration of a subject/subscriber are part of ZETESCONFIDENS. The organisational structure and the infrastructure within ZETESCONFIDENS constitutes the RA and that is tasked with the following duties:

- process subordinate CAs' certificate requests
- authenticate and validate the Subordinate CA and the certificate request itself
- act upon the result of this validation and, if approved, on the Zetes TSP Root CA infrastructure
    - select the appropriate Certificate Profile
    - submit a certificate request to the appropriate Root CA
    - retrieve the certificate from the CA

For these duties, the RA acts under direct authority and supervision of the Zetes TSP Policy Management Authority (see section 1.3.6).

1.3.3 Subscribers and Subjects

ZetesConfidens as operator of a Subordinate CA is the Subscriber.

The Subject is the PKI Component entity that is certified by the Zetes TSP Root CA; the Subjects are either a subordinate CA of ZetesConfidens or a certificate status validation service of ZetesConfidens, such as an OCSP responder.

1.3.4 Relying parties

The Relying Parties are those parties who are relying on a certificate that is issued by a CA belonging to a CA hierarchy of the ZetesConfidens PKI.

1.3.5 Other participants

1.3.5.1 Dissemination and Repository Services

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

This service also provides access to previous versions of these documents (Certification Practice Statement, Certificate Policy, Certificates Terms and Conditions).

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

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

1.3.5.2 Revocation Management Services and Revocation Status Information Services

ZETES is responsible for operating the Revocation Management Services and the Revocation Status Information Services (which provide Certificate validity status information).

1.3.6 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 and operational security of the trust services environment.

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

(a) Approving the Trust Services infrastructure and practices.
(b) Approving the Practice Statements and the Policies.
(c) Defining the review process for, including responsibilities for maintaining, the Practice Statements and the Policies

(d) Defining the review process that ensures that applicable Policies are supported by the Practice Statement(s).
(e) Defining the review process that ensures that the Trust Services authorities, such as the Certification Authority and the Time Stamping Authority, as well as all component services, properly implement the applicable practices, policies and procedures.
(f) Authorising part or all component services of the Trust Services to be provided and/or operated by third parties and setting 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 Trust Services 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) Approving 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) Actions to ensure the proper execution of the above responsibilities.
(n) Defining the scope of the Trust Services offering.
(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 TSP.
(q) Initiating when appropriate highly sensitive operations such as CA root key revocation and renewal or termination of the Trust Services.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

The appropriate certificate usage is described in the present CPS for all PKI components certificates.

The CA uses private signing keys and the related certificates only for signing subscriber's certificates, C(A)RLs and PKI services certificates (e.g. sub-CA's, OCSP server) in accordance with the intended use of each of these keys. Other usages are restricted.

It is the responsibility of the Subject to use the certificates accordingly. It is the Subject's or the Subscriber's responsibility to use software applications that correctly interprets, displays and uses the information and restrictions encoded in the certificates, such as but not limited to key usage, limited liability per transaction, etc.

It is the responsibility of the Subscriber, the Subject and the Relying Party to decide for which purpose the certificates are considered trustworthy. A Relying Party must always take into account the level of assurance and other information in the present CPS, the QCA CPS and related CP, before deciding on the applicability of the certificate.

1.4.2 Prohibited certificate uses

Any usage of a certificate, other than the usage explicitly allowed in the CPS and the CP, is prohibited.

Root CA

The use of the Root-CA certificate to sign end-entities certificates is prohibited, to the exception of internal certificates used to secure the PKI.

Subordinate CAs

Subordinate CAs cannot issue CA's certificates.

1.5 Policy administration

1.5.1 Organization administering the document

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

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

1.5.2 Contact person

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

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

1.5.3 Person determining suitability for the policy

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

1.5.4 Document approval procedures

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

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

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

1.6 Definitions and acronyms

1.6.1 Acronyms

ARL	Authority Revocation List
CA	Certificate Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DN	Distinguished Name
HSM	Hardware Security Module
LRA	Local Registration Authority

OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority

1.6.2 Definitions

Activation Data	Data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorised use of the private key.
Certificate	A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.
Certificate Revocation List	A signed list of identifiers of Certificates that have been revoked. Abbreviated as CRL. It is made available by the CA to Subscribers and Relying Parties. The CRL is updated after each Certificate revocation process. The CRL does not necessarily contain identifiers of revoked Certificates that are past their validity date (that is, expired).
Hardware Security Module	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, under the Lightweight certificate policy [LCP] 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.
Relying party	Person or organisation acting upon a Certificate, typically to verify signatures by the Subscriber or to perform encryption towards the Subscriber. The Relying Party relies upon the accuracy of the binding between the Subscriber public key distributed via that Certificate and the identity and/or other attributes of the Subscriber contained in that Certificate. In the context of this *Certification Practice Statement*, Relying Parties are as further defined in section 1.3.4.

Subscriber	Person or organisation contracting with the Certification Authority, for being issued one or more Certificates. In the context of this *Certification Practice Statement*, the Subscribers are as further defined in section 1.3.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ZETESCONFIDENS 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 repository web sites. Supporting information such as the various (versions of) Certification Practice Statement documents, Certificate Policy documents, etc. are also available for download from the same web site.

The complete overview of online repositories and services is as follows:

https://confidens.zetes.com	Commercial presentation of ZETESCONFIDENS
https://tsp.zetes.com **https://confidens.zetes.com**	This URL refers to the welcome page of the web site for ZETESCONFIDENS. This web site provides: • general information about Zetes SA and the ZETESCONFIDENS 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 ZETESCONFIDENS • 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://repository.confidens.zetes.com**	This URL refers directly to the page for downloading documents such as the • Certificate Terms and Conditions, • Certification Practice Statements, • Certificate Policies, • etc.
http://crt.tsp.zetes.com **http://crt.confidens.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 **http://crl.confidens.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 **http://ocsp.confidens.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 ZETESCONFIDENS or any other reason, Zetes SA shall make best endeavors to reinstate availability of the service within 5 working days.

Publication of CA certificates in a repository

ZETESCONFIDENS, as a matter of policy, publishes its CA certificates in a public certificate repository:

http://crt.tsp.zetes.com

http://crt.confidens.zetes.com

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

The fingerprint information for the Zetes TSP Root CA 001 is printed in section 7.1 of this document.

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@confidens.zetes.com

Certificate Status Information

Certificate status information for CA certificates issued by the Root CA is made available in two formats:

- as downloadable CRLs
- as OCSP service

CRLs are published at regular intervals on the CRL distribution point

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

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

The CRLs are renewed when certificates have been revoked or when the CRL is about to expire. Expired certificates that were revoked before their expiration dates are removed from the certificate revocation lists. CRLs are updated until all certificates that that were issued by the respective CA key have expired.

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

The OCSP service is synchronised with the latest CRL. More information is available in section 4.10.

2.3 Time or frequency of publication

Publication of CA certificates in a repository

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

Certificate Status Information

The CRL is created either every 12 months or when a CA certificate is revoked.

CRLs are published in the repository immediately following creation, and will be available for download within 3 hours after creation.

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

Publication of terms and conditions, CP, CPS, etc.

Updates to the Certificate Policy, Certification Practice Statement, Certificates Terms and Conditions, and other public documents are published whenever a change occurs, ensuring a period of minimum two (2) days between the publication date and the effective date (see section 9.12.2 of the Trust Services Practice Statement document).

2.4 Access controls on repositories

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

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

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

ZETESCONFIDENS 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.

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

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

All CA certificates only contain names that represent legal entities. Names associated with natural persons are not allowed. The DN for the ZETES TSP ROOT CA is:

CN= ZETES TSP ROOT CA 001

SN= 001

O= ZETES SA (VATBE-0408425626)

C= BE

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

3.1.2 Need for names to be meaningful

The names used in the certificates are chosen such that:

- it is clear that the certificate is a CA certificate,
- it is clear what the purpose of the CA is,
- it includes an unambiguous identification of the legal entity of the Subscriber.

The CA certificates issued for ZetesConfidens will include the following name information:

O= ZETES SA (VATBE-0408425626)

C= BE

Many software applications use the commonName field to show a choice of certificates to the end user. To help the end user choose the appropriate certificate, the commonName field may also contain plain wording describing the intended usage of the certificate (i.e. “Qualified CA”).

serialNumber	a unique identifier
commonName	**meaningful name of the subordinate CA**
organizationName	**official registered name of the Subscribing CA as a corporation or organization, including an official registered unique number or unique identifier of the Subscriber as a corporation or organization** As formatted in ETSI EN 319 412-1 (e.g. VATBE-0123456789) together with a semantic identifier. It is representing the registration number of the organization as stated in the official records.

3.1.3 Anonymity or pseudonymity of Subscribers

Not applicable.

3.1.4 Rules for interpreting various name forms

No stipulations.

3.1.5 Uniqueness of names

The DN are guaranteed to be unique across the ZETESCONFIDENS 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

The certificate request is an industry standard format that contains the public key for the new certificate and is signed with the corresponding private key. The key generation process for the request and the creation of the request itself is performed by employees of ZetesConfidens in trusted role. The request is transferred to the Root CA on a secure medium to prevent unauthorized access and protect the request from manipulation or replacement. As a general rule, the creation of the certificate request and the issuance on the certificate is performed on the same day, by the same ZetesConfidens employees and in the same location.

The PMA provides a written authorisation to re-instated the Root CA for this sole purpose.

The methods to prove the possession of private key for CAs, are detailed in internal confidential documentation.

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

3.2.2 Authentication of organization identity

The ZETESCONFIDENS Root CA only issues certificates for subordinate CAs or for itself (as self-signed certificate or for its own certificate status validation services (CRL signing and OCSP responders)). For both cases, the organization identity is ZetesConfidens or other organisation entities that are part of the same legal entity Zetes SA. Identification and authentication procedures for the registration of the PKI component services (e.g. CAs, OCSP responders, etc.) are detailed in internal confidential documentation.

3.2.3 Authentication of individual identity

The ZETESCONFIDENS Root CA only issues certificates for PKI components. The ZETESCONFIDENS Qualified CA does not issue certificates to individuals. Authentication of an individual as the Subject of the certificate is therefore not applicable.

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

Not applicable.

3.2.5 Validation of authority

Not applicable.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

Not applicable. Certificate re-keying is not allowed.

3.4 Identification and authentication for revocation request

The following participants may request revocation of a Subject certificate:

- ZETESCONFIDENS as operator of the Zetes TSP Root CA
- the Subscriber, i.e. ZETESCONFIDENS as operator of the Subordinate CA

Each revocation request must be approved by the Policy Management Authority (section 1.3.6). The procedures and conditions may be more explicitly defined per Subordinate CA in internal confidential documents. See section 4.9 for more information about the procedures for revocation of a PKI component certificate.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The procedures relating to PKI component services (e.g. CAs, OCSP responders, etc.) and the related persons/roles operating them are described in this CPS and in internal confidential documentation. The following sections only present the elements of these documents that can be publicly disclosed.

Within the context of the Zetes TSP Root CA, only employees of ZETESCONFIDENS who are assigned to the CA entities are authorized to perform certificate lifecycle operations. ZETESCONFIDENS is responsible for these employees and assures that each person, for the assigned duties:

- is screened for appropriate security clearance,
- receives the required training and information,
- is properly informed about the obligations and responsibilities
- is given proper authorization from the PKI Policy Management Authority.

All certificate lifecycle operations described in this chapter are performed under control and witnessing of several trusted employees. Transfer to and from the offline Root CA system is done using a dedicated secure storage medium which protects the data against manipulation.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

The ZETESCONFIDENS Root CA does not issue certificates to natural persons, to organisations or to individuals representing an organisation. Certification requests can only originate from ZETESCONFIDENS as operator of a Subordinate CA and must be for a PKI component such as for a subordinate CA of ZetesConfidens or for the certificate validations services of ZETESCONFIDENS.

Each certification request must be approved by the PKI Policy Management Authority (section 1.3.6).

The procedures and conditions may be more explicitly defined per Subordinate CA in internal confidential documents.

4.1.2 Enrolment process and responsibilities

The enrolment process for a CA's certificate request

Since the Subscriber is ZETESCONFIDENS and the Subject is a PKI component of ZETESCONFIDENS, the enrolment process is a purely internal procedure. The identification and authentication of the Subscriber is implicit.

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 1.3.2.
- consists of internal processes such as the definition of the purpose and content of the certificate, the key ceremony for the creation of the key pair, configuration of internal applications and systems. These processes must be approved by the PKI Policy Management Authority (section 1.3.6).

The enrolment process for a Root CA's component certificate request

The processes and procedures used to enrol the PKI component services (e.g. CAs, OCSP responders, etc.) and to enroll 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

ZETESCONFIDENS is the owner, operator and custodian of the keys and certificates of the CA hierarchy under the ZETESCONFIDENS Root CA.

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 root CA PKI components or for a subordinate CA.

Only a selected group of authorized trusted employees, entitled by the PMA, are in charge of processing a certificate request for a root CA PKI components or for a subordinate CA.

Such requests are validated by the appropriate CA trusted roles that are involved in the process.

4.2.2 Approval or rejection of certificate applications

Root CA

The authorisation to issue a self-signed certificate comes from the PMA only.

The technical validation of the request is performed by the PKI administrator during Root CA key self-certification ceremony in presence of the quorum.

Subordinate CAs

Such as described in internal document, ZETESCONFIDENS as RA is responsible to approve or reject an issuing CA certificate application.

The technical validation of the request is performed by the PKI administrator during a Key Ceremony in presence of the Root CA quorum.

ZETESCONFIDENS as RA is responsible for the validation and vetting of certificate requests for CAs and internal Root CA PKI components.

The information to validate the certificate before it will be installed on the PKI component for which the certificate is intended, is recorded.

4.2.3 Time to process certificate applications

Not applicable.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

All certificate requests for CAs and for PKI components are vetted and validated by personnel of ZETESCONFIDENS on systems that are internal to the ZETESCONFIDENS PKI infrastructure. Import of certificate requests and export of certificates and certificate status information is done within a closed loop circuit and by ZetesConfidens trusted employees.

4.3.2 Notification of issuance of certificate

Notification of issuance of a certificate by the Zetes TSP Root CA for an internal PKI component is implicit and is specified in the internal documentation pertaining to the specific procedure or ceremony.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Before the certificate is installed on the PKI component for which it is intended, the CA operators validate the certificate and compare the certificate's content and validation information with the reference information that is recorded when the certificates were issued on the Root CA.

The certificate is considered accepted upon completion of the installation and/or activation procedure on the PKI component for which the certificate is intended.

The certificate will be rejected when one or more of the following objections apply:

- the information in the certificate is incorrect,
- the information in the certificate became invalid since the date of registration,
- the information in the certificate became invalid since the date of issuance,
- the procedure was not respected.

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

Notification of issuance of a certificate by the Zetes TSP Root CA for an internal PKI component is implicit and is specified in the internal documentation pertaining to the specific procedure or ceremony.

4.5 Key pair and certificate usage

4.5.1 Subscriber and Subject private key and certificate usage

ZetesConfidens is the issuer and is the user of the certificates issued by the Zetes TSP Root CA.

The ZETESCONFIDENS is responsible for

- providing a secure Cryptographic Module to host and protect the private key,
- initializing the secure Cryptographic Module and its initial associated Activation Data
- using the keys only for the intended use as defined in the Certification Practice Statements and Certificate Policies for the subordinate CA hierarchy and as encoded in the certificates
- using tools that can correctly interpret the key usage as encoded in the certificate and that respect the key usage conditions
- correct usage of the Cryptographic Module

The use of a Root or a subordinate CA's private key and its associated certificate is strictly limited to the usage defined in chapters 1.4.1 and 1.4.2.

4.5.2 Relying Party public key and certificate usage

Responsibilities of relying parties, which are related to the use of public keys and certificates issued by the Zetes PKI hierarchy are specified in the related CPs.

4.6 Certificate renewal

The subordinate CA are owned and operated by ZETESCONFIDENS. Renewal requests therefor always originate from within ZetesConfidens and are conducted as a CA key ceremony. Renewal for subordinate CA certificates is possible only with approval from the PMA.

Renewed CA certificates are made available to end users and to relying parties via the same channels as the original certificate. The Authority Information Access URL does not change and the renewed certificate will replace the preceding

certificate for this URL. The renewed certificate and the preceding certificate(s) will be available for download from the repository.

4.7 Certificate re-key

Not applicable.

4.8 Certificate modification

Not applicable.

4.9 Certificate revocation and suspension

Certificates issued by the Zetes TSP Root CA are never suspended but can be revoked. Certificate revocation is irreversible.

4.9.1 Circumstances for revocation

ZETESCONFIDENS as a certification service provider (CSP), under prior or explicit approval of the PMA, must revoke a certificate issued by the Zetes TSP Root CA for security reasons or in an 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 private key's activation data has been compromised,
- if the certified data is invalid or no longer valid.

ZETESCONFIDENS as a certification service provider (CSP), under prior or explicit approval of the PMA, may revoke a certificate issued by the Zetes TSP Root CA 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 the CA or the certificate status service is decommissioned,
- if the key is renewed,
- if the CA or the certificate status service is decommissioned.

4.9.2 Parties that can request revocation

A Revocation Request for a CA certificate can only originate from the PMA. A Revocation Request for a PKI component certificate can originate from the PMA or can be requested by the ZetesConfidens CA operational team, under the authority of the PMA and through the operational procedures for the PKI component in question. Under special circumstances, (see section 4.9.1) the PMA will convene without delay to decide on the matter.

4.9.3 On-line revocation/status checking availability

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

http://ocsp.tsp.zetes.com

http://ocsp.confidens.zetes.com

4.9.4 Procedure for revocation request

See section 4.9.2.

4.9.5 Revocation request grace period

ZetesConfidens operators are instructed to notify the PMA immediately upon discovering a reason for revocation of a certificate.

4.9.6 Time within which CA must process the revocation request

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.

4.9.7 Revocation checking obligations for Relying Parties

Relying parties must use at least one of the services for checking certificate status information that are made available by ZETESCONFIDENS. If the preferred service is unavailable, then the Relying Party is responsible for exhausting all other services. The Relying Party is responsible for making the final decision whether or not to trust the certificate, regardless of the availability of the certificate status information services.

See section 2.2 and section 4.5.2.

4.9.8 CRL issuance frequency (if applicable)

The ZETESCONFIDENS Root CA issues CRLs at pre-defined intervals or ad hoc when needed. The renewal period is set to 12 months (1 year). The CRL is signed and time-marked by the Root CA. CRLs are archived for future reference.

4.9.9 Maximum latency for CRLs (if applicable)

ZETESCONFIDENS will make best effort to update the certificate status information to Relying Parties within 3 hours from the actual revocation.

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

ZETESCONFIDENS maintains an Online Certificate Status Protocol (OCSP) service free of charge for use by Subjects and free of charge for normal use by Relying Parties The free OCSP service is accessible without client authentication and accepts unsigned requests

See section 2.4 for information on Access Control and Restrictions regarding the use of the OCSP service.

4.9.11 Other forms of revocation advertisements available

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

https://repository.confidens.zetes.com

4.9.12 Special requirements re key compromise

No stipulations.

4.9.13 Circumstances for suspension

Not applicable.

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

ZETESCONFIDENS provides two services for checking the status of the certificates issued by the ZETESCONFIDENS Root CA:

- Certificate Revocation Lists
- Online Certificate Status Protocol service, open for unsigned requests

4.10.2 Service availability

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

Planned maintenance periods will be announced on http://tsp.zetes.com at least 24 hours in advance.

In case of unavailability due to an act of God, failure of infrastructure outside the control of ZETESCONFIDENS or any other reason, Zetes SA shall make best endeavours to reinstate availability of the service within 5 working days.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

Within the context of the Zetes TSP Root CA, the Subscriber is ZETESCONFIDENS itself and the Subject is a subordinate CA or a PKI component of ZETESCONFIDENS. The end of a subscription, or the termination of a Subject, is the result of the internal decision to decommission the subordinate CA or PKI component.

Upon termination of the subscription, the certificates issued on behalf of the Subscriber will be revoked.

With regards to ZETESCONFIDENS's obligations towards the Subscriber, Subjects and Relying Parties of a decommissioned subordinate CA, ZETESCONFIDENS will continue to provide certificate status information for as long as contractually and legally required.

4.12 Key escrow and recovery

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

- Physical controls
- Procedural controls
- Personnel controls
- Audit logging procedures
- Records archival
- Key changeover
- Compromise and disaster recovery
- CA or RA termination

6 TECHNICAL SECURITY CONTROLS

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

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

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation for CAs

The key pairs for the Zetes TSP Root 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 operators

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

The SSCD for PKI operators are stored in a secure location, separate from the HSM equipment. The operators are handed the SSCD as and when needed to perform an authorized task.

6.1.2 Private key delivery to Subscriber or Subject

Not applicable.

6.1.3 Public key delivery to certificate issuer

The ZETESCONFIDENS 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 ZETESCONFIDENS Qualified CA) and for public keys for OCSP services that act on behalf of the ZETESCONFIDENS 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 that the requester is in possession of the private key for which the certificate is requested.

6.1.4 CA public key delivery to Relying Parties

ZETESCONFIDENS CA certificates are published in the public repository.

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 ZETESCONFIDENS CA hierarchy.

The authentic "thumbprint" of the ZETESCONFIDENS CA certificates is published in a document in PDF/A format.

Relying parties may contact ZETESCONFIDENS via e-mail at info@confidens.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 Zetes TSP Root CA 001 uses the following algorithms and key sizes:

Root CA	RSA4096	generated and used on HSM
OCSP	RSA2048	generated and used on HSM (of the OCSP infrastructure)
Internally signed audit logs	RSA2048	generated and used on HSM
Secure Cryptographic Devices	RSA2048	generated and used on SCD

The CA infrastructure for the issuing CAs may use the following algorithms and key sizes:

CA	RSA4096	generated and used on HSM
	ECC384	
	ECC512	
	ECC521	
OCSP service	RSA2048	generated and used on HSM
	ECC256	
	ECC384	
Internally signed audit logs	RSA2048	generated and used on HSM
	ECC256	
	ECC384	
Secure Cryptographic Devices	RSA2048	generated and used on SCD
	ECC256	
	ECC384	

The hash algorithm is SHA256 or better.

ZETESCONFIDENS is not in any way held to continue using the current algorithms, protocols or key lengths should ZETESCONFIDENS 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 for the Zetes TSP Root CA are generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Public key parameters shall be generated and tested in accordance with the FIPS 186-3 standard which ensure the quality of the key material.

The following parameters are used:

- the HSM operates in FIPS140-2 level 3 mode

- key generation relies on the HSM's deterministic (pseudo) random number generator
- key generation is compliant with FIPS 186-4

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

ZetesConfidens ensures that the key usage properties encoded in the certificates correspond with the intended use of the certificates as described in the applicable Certificate Policies.

	Key Usage	**Extended Key Usage**
CA	keyCertSign + cRLSign	-
Delegated OCSP	digitalSignature	OCSPSigning

An additional restriction on key usage applies to all the keys that are used for internal purposes by PKI 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 ZetesConfidens PKI environment.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

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

The HSM of the Zetes TSP Root CA has the following security certifications:

- NIST FIPS 140-2 level 3
- Common Criteria certification evaluation assurance level EAL4+

6.2.2 Private key multi-person control

The activation and/or use of the private keys in the HSM infrastructure that hold the private keys for the Zetes TSP Root CA is protected by access control and activation mechanisms that require multiple 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.

6.2.3 Private key escrow

Private keys are never put in escrow.

6.2.4 Private key backup

Private keys on an HSM for the CA or OCSP infrastructure are generated on-board the HSM and are backed up, encrypted by means of a backup encryption key.

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

The backup encryption key is itself is generated inside the HSM during the installation and initialization of HSM and is split into key shares which are stored on a set of HSM backup cards.

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

Private keys and other security critical data is always encrypted (backup operation) or decrypted (restore operation) inside the HSM itself. The encryption key is split over a set of m HSM 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.

6.2.5 Private key archival

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

6.2.6 Private key transfer into or from a cryptographic module

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.

6.2.7 Private key storage on cryptographic module

All private keys inside the HSM are loaded into and decrypted inside the HSM, and can only be used for operational purposes when loaded in the HSM. Multi-personnel control by means of *n-of-m* HSM cards is required to load and activate the keys into the HSM. The sensory controller of the HSM can, in a case of an alarm, delete or render useless the key material in the HSM.

6.2.8 Method of activating private key

Private keys for the Root CA

Activation of the private keys in the ZETESCONFIDENS Root CA requires multiple authorized administrators and operators for activating the HSM by means of *n-of-m* HSM cards and for accessing the control interface of the CA application.

Private keys on the dedicated HSM for the Root 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.

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. Deactivation of the private key requires at least two authorized administrators and operators.

6.2.9 Method of deactivating private key

Private keys on the dedicated HSM for the Root 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.

6.2.10 Method of destroying private key

Destruction of a private key requires authorization of the PMA. When a key is decommissioned, the private key is deleted from all HSM equipment by means of the HSM secure key destruction mechanism and appropriate measures are taken to prevent that a backup of the can be restored.

6.2.11 Capabilities 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 CC EAL4+ (AVA_VAN.5) in compliance with the eIDAS Transitional Measures (Article 51).

6.3 Other aspects of key pair management

6.3.1 Public key archival

ZETESCONFIDENS maintains an internal archive of all CA public keys and all public keys certified by the ZETESCONFIDENS Root CA in the form of the certificates that contain the public key.

6.3.2 Certificate operational periods and key pair usage periods

The ZETESCONFIDENS Root 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

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 in 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.

6.5 Computer security controls

ZETESCONFIDENS ensures that computer security controls are implemented according the technical standard ETSI EN 319411-2. ZETES operates its 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.:

- Exclusively offline usage, the Zetes TSP Root CA is not connected to any network
- Exclusively switched on, on a need to use basis, the Zetes TSP Root CA is switched off and stored in a safe, the equipment is only taken out of the safe and switched on when necessary.
- Control of sensitive data stored on “demobilized” or reusable storage device
- Use of multifactor authentication for accounts capable to issue certificates
- Access control, intrusion detection system and CCTV monitoring to detect, record and react upon unauthorized access to its resources

6.6 Life cycle technical controls

6.6.1 System development controls

Implemented in compliance with ETSI 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

Not applicable. The Zetes TSP Root CA is not connected to any network.

6.8 Time-stamping

See section 5 of the Trust Services Practice Statement [ref. 4].

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CA hierarchy

Overview of this root CA and the CA hierarchy:

ZETES TSP ROOT CA 001
- certificate serial number = 02 54 1A A9 50 D7 CE 1F
- certificate thumbprint = 37 53 D2 95 FC 6D 8B C3 9B 37 56 50 BF FC 82 1A ED 50 4E 1A
- CPS OID = 1.3.6.1.4.1.47718.2.1.1.1
- CP OID = 1.3.6.1.4.1.47718.2.1.2.1

---- Zetes TSP Qualified CA 001
- certificate serial number = 38 20 EE 9C 74 EC D1 47
- certificate thumbprint = 16 98 DC 47 F4 F5 FF 95 6C 56 03 24 E1 96 5A A7 ED 38 E2 9D

---- ZETES TSP CA FOR TSA 001
- certificate serial number = 2E 31 E4 74 F6 05 91 BA
- certificate thumbprint = 37 02 B9 F1 77 AF AA 8D 07 7C 06 C3 E4 94 82 C5 A1 75 D3 2C

---- ZetesConfidens - Signature Creation Service - issuing CA 001
- certificate serial number = 2F F6 42 AD 1A EA 7E 0B
- certificate thumbprint = 36 9B 53 56 13 C8 90 27 27 50 7B 92 6D 3F 57 F5 42 31 28 E0

Note: the Certificate profiles for the subordinate CAs are provided in the CP document of the respective CAs.

7.2 Certificate profile

Certificate profile for the ZETES TSP Root CA:

Table 1 ZETES TSP ROOT CA - Certificate Profile for ZETES TSP ROOT CA 001 self-signed certificate

certificate profile **ZETES TSP ROOT CA - self-signed root certificate**			
ATTRIBUTES			
Version		-	**0x02** (= X.509 certificate version 3)
Serial Number		-	**02 54 1A A9 50 D7 CE 1F** *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 *(dd/mm/yyyy)*
	notAfter	-	20/05/2036 *(dd/mm/yyyy)*
Issuer	**serialNumber**	-	**001** (*the 3-digit serial number of the CA*)
	commonName	-	**ZETES TSP ROOT CA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
Subject	**serialNumber**	-	**001**
	commonName	-	**ZETES TSP ROOT 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**
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	**keyIdentifier**	-	**38 BC 5C 30 54 DC E2 BB 20 EF EE 6F 41 A0 31 6E 5C FD 8B 75**
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**
basicConstraints	**subjectType**	c	CA path length constraint = none

7.3 CRL profile

Generic CRL profile for consolidated CRL:

Table 2 ZETES TSP ROOT CA 001 - CRL profile

CRL profile **ZETES TSP ROOT CA 001 - CRL**			
ATTRIBUTES			
Version		-	**2**
Signaturealgorithm	**algorithm**	-	**sha256WithRSAEncryption**
		-	<the signature created by ZETES TSP ROOT CA 001 >
Issuer	**serialNumber**	-	**001**
	commonName	-	**ZETES TSP ROOT CA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
ThisUpdate		-	<time of issue >
NextUpdate		-	<time of issue + 1 year>
Revoked Certificates	**userCertificate**	-	<certificate serial number>
	revocationDate	-	<revocation time>
	crlEntryExtension CRLReason	-	<reason for revocation> - included for every certificate -
EXTENSIONS			
Authority Key Identifier		-	**38 BC 5C 30 54 DC E2 BB 20 EF EE 6F 41 A0 31 6E 5C FD 8B 75**
CRL Number		-	dynamically assigned by the CA

7.4 OCSP profile

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

Table 3 ZETES TSP ROOT CA - Certificate Profile for OCSP responder

certificate profile **ZETES TSP ROOT CA 001 - OCSP responder certificate**			
ATTRIBUTES			
Version		-	**0x02** (= X.509 certificate version 3)
Serial Number		-	< 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 ZETES TSP ROOT CA 001 >
SubjectPublicKeyInfo	**algorithm**	-	**RSA2048**
	subjectPublicKey	-	< value of the public key >
Validity	**notBefore**	-	< certificate validity start date >
	notAfter	-	< certificate validity start date + 1 year >
Issuer	**serialNumber**	-	**001** (*the 3-digit serial number of the CA*)
	commonName	-	**ZETES TSP ROOT CA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
Subject	**commonName**	-	**ZETES TSP ROOT CA 001 OCSP responder**
	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**
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	**keyIdentifier**	-	< 4-bit value 0l00 + 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	< set >
enhancedKeyUsage	**OCSP Signing**	c	< set >
OCSPNoCheck		-	< set >

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

See section 8 of the Trust Services Practice Statement [ref. 4].

- Frequency or circumstances of assessment
- Identity/qualifications of assessor
- Assessor's relationship to assessed entity
- Topics covered by assessment
- Actions taken as a result of deficiency
- Communication of results

9 OTHER BUSINESS AND LEGAL MATTERS

See section 9 of the Trust Services Practice Statement [ref. 4].

- Fees
- Financial responsibility
- Confidentiality of business information
- Privacy of personal information
- Intellectual property rights
- Representations and warranties
- Disclaimers of warranties
- Limitations of liability
- Indemnities
- Term and termination
- Individual notices and communications with participants
- Amendments
- Dispute resolution provisions
- Governing law
- Compliance with applicable law
- Miscellaneous provisions
- Other provisions

---------- Last page of this document ----------