

ZETESCONFIDENS PRIVATE TRUST PKI

CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY

*Certification Practice Statement and Certificate Policy
for the
ZetesConfidens Private Trust PKI Root CA*

Publication date :	03/05/2019		
Effective date :	05/05/2019		
CPS OID :	1.3.6.1.4.1.47718.2.1.1.3		
CP OID :	1.3.6.1.4.1.47718.2.1.2.3		
Version :	1.0	30/04/2019	for approval
Copyright :	<p>No part of this document or any of its contents may be reproduced, copied, modified or adapted, without the prior written consent of the author, unless otherwise indicated for stand-alone materials.</p> <p>Commercial use and distribution of the contents of this document is not allowed without express and prior written consent of the author.</p> <p>The following sentence must appear on any copy of this document: "© 2019 – Zetes – All Rights Reserved"</p>		



Table of Content

ABOUT THIS DOCUMENT	6
ABOUT ZETES	6
1 INTRODUCTION	7
1.1 Overview.....	7
1.2 Document name and identification	7
1.3 PKI participants.....	7
1.3.1 Certification Authorities (CA).....	9
1.3.2 Registration and Revocation Authorities ((S)RA)	9
1.3.3 Subscribers and Subjects	9
1.3.4 Relying parties	9
1.4 Certificate usage	9
1.4.1 Appropriate certificate uses	9
1.4.2 Prohibited certificate uses	9
1.5 Policy administration	10
1.5.1 Organization administering the document.....	10
1.5.2 Contact person	10
1.5.3 Person determining suitability for the policy.....	10
1.5.4 Document approval procedures	10
1.6 Definitions and acronyms	10
1.6.1 Acronyms	10
1.6.2 Definitions	10
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	12
2.1 Repositories.....	12
2.2 Publication and frequency of publication.....	12
2.3 Access controls on repositories	12
3 IDENTIFICATION AND AUTHENTICATION	13
3.1 Naming	13
3.1.1 Types of names.....	13
3.1.2 Need for names to be meaningful	13
3.1.3 Anonymity or pseudonymity of Subscribers.....	13
3.1.4 Rules for interpreting various name forms.....	13
3.1.5 Uniqueness of names	13
3.1.6 Recognition, authentication, and role of trademarks.....	13
3.2 Initial identity validation	14
3.2.1 Method to prove possession of private key	14
3.2.2 Authentication of organization identity.....	14
3.2.3 Authentication of individual identity	14
3.2.4 Non-verified Subscriber information	14
3.2.5 Validation of authority.....	14
3.2.6 Criteria for interoperation	14
3.3 Identification and authentication for renewal.....	14
3.4 Identification and authentication for re-key requests.....	14
3.5 Identification and authentication for revocation request	14
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	15
4.1 Certificate Application	15
4.1.1 Who can submit a certificate application	15
4.1.2 Enrolment process and responsibilities.....	15
4.2 Certificate application processing.....	15
4.2.1 Performing identification and authentication functions	15
4.2.2 Approval or rejection of certificate applications	16
4.2.3 Time to process certificate applications	16
4.3 Certificate issuance.....	16
4.3.1 CA actions during certificate issuance	16
4.3.2 Notification of issuance of certificate	16
4.4 Certificate acceptance	16
4.4.1 Conduct constituting certificate acceptance	16
4.4.2 Publication of the certificate by the CA	17

4.4.3	Notification of certificate issuance by the CA to other entities	17
4.5	Key pair and certificate usage	17
4.5.1	Subscriber and Subject private key and certificate usage	17
4.5.2	Relying Party public key and certificate usage	17
4.6	Certificate renewal	17
4.7	Certificate re-key	17
4.8	Certificate modification	17
4.9	Certificate revocation and suspension	17
4.9.1	Circumstances for revocation	17
4.9.2	Parties that can request revocation	18
4.9.3	Procedure for revocation request	18
4.9.4	Revocation request grace period	18
4.9.5	Time within which CA must process the revocation request	18
4.9.6	Revocation checking obligations for Relying Parties	18
4.9.7	CRL issuance frequency (if applicable)	18
4.9.8	Maximum latency for CRLs (if applicable)	18
4.9.9	On-line revocation/status checking availability	18
4.9.10	Requirements on Relying Parties to perform on-line revocation checking	19
4.9.11	Other forms of revocation advertisements available	19
4.9.12	Special requirements re key compromise	19
4.9.13	Circumstances for suspension	19
4.9.14	Who can request suspension	19
4.9.15	Procedure for suspension request	19
4.9.16	Limits on suspension period	19
4.10	Certificate status services	19
4.10.1	Operational characteristics	19
4.10.2	Service availability	20
4.10.3	Optional features	20
4.11	End of subscription	20
4.12	Key escrow and recovery	20
4.12.1	Key escrow and recovery policy and practice	20
4.12.2	Session key encapsulation and recovery policy and practices	20
5	FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	21
5.1	Physical controls	21
5.1.1	Site location and construction	21
5.1.2	Physical access	21
5.1.3	Power and air conditioning	21
5.1.4	Water exposures	21
5.1.5	Fire prevention and protection	21
5.1.6	Media storage	21
5.1.7	Waste disposal	21
5.1.8	Off-site backup	21
5.2	Procedural controls	22
5.2.1	Trusted roles	22
5.2.2	Number of persons required per task	22
5.2.3	Identification and authentication for each role	22
5.2.4	Roles requiring separation of duties	22
5.3	Personnel controls	23
5.3.1	Qualifications, experience, and clearance requirements	23
5.3.2	Background check procedures	23
5.3.3	Training requirements	23
5.3.4	Retraining frequency and requirements	23
5.3.5	Job rotation frequency and sequence	23
5.3.6	Sanctions for unauthorised actions	23
5.3.7	Independent contractor requirements	23
5.3.8	Documentation supplied to personnel	23
5.4	Audit logging procedures	23
5.4.1	Types of events recorded	23
5.4.2	Frequency of processing log	24
5.4.3	Retention period for audit log	24
5.4.4	Protection of audit log	25
5.4.5	Audit log backup procedures	25

5.4.6	Audit collection system (internal vs. external)	25
5.4.7	Notification to event-causing Subject	25
5.4.8	Vulnerability assessments	25
5.5	Records archival	25
5.5.1	Types of records archived	25
5.5.2	Retention period for archive	25
5.5.3	Protection of archives	25
5.5.4	Archive backup procedures	25
5.5.5	Requirements for time-stamping of records	25
5.5.6	Archive collection system (internal or external)	26
5.5.7	Procedures to obtain and verify archive information	26
5.6	Key changeover	26
5.7	Compromise and disaster recovery	26
5.7.1	Incident and compromise handling procedures	26
5.7.2	Computing resources, software, and/or data are corrupted	26
5.7.3	Entity private key compromise procedures	26
5.7.4	Business continuity capabilities after a disaster	26
5.8	CA or RA termination	27
6	TECHNICAL SECURITY CONTROLS	28
6.1	Key pair generation and installation	28
6.1.1	Key pair generation	28
6.1.2	CA public key delivery to Relying Parties	28
6.1.3	Public key parameters generation and quality checking	28
6.1.4	Key usage purposes (as per X.509 v3 key usage field)	28
6.2	Private Key Protection and Cryptographic Module Engineering Controls	28
6.2.1	Cryptographic module standards and controls	28
6.2.2	Private key multi-person control	28
6.2.3	Private key escrow	29
6.2.4	Private key backup	29
6.2.5	Private key archival	29
6.2.6	Private key transfer into or from a cryptographic module	29
6.2.7	Private key storage on cryptographic module	29
6.2.8	Method of activating private key	29
6.2.9	Method of deactivating private key	29
6.2.10	Method of destroying private key	29
6.2.11	Capabilities and Rating of the Cryptographic Module	29
6.3	Other aspects of key pair management	30
6.3.1	Public key archival	30
6.3.2	Certificate operational periods and key pair usage periods	30
6.4	Activation data	30
6.5	Computer security controls	30
6.6	Life cycle technical controls	30
6.6.1	System development controls	30
6.6.2	Security management controls	30
6.6.3	Life cycle security controls	30
6.7	Network security controls	30
6.8	Time-stamping	30
7	CERTIFICATE, CRL, AND OCSP PROFILES	31
7.1	Certificate profile	31
7.2	CRL profile	32
7.3	OCSP profile	33
8	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	34
8.1	Frequency or circumstances of assessment	34
8.2	Identity/qualifications of assessor	34
8.3	Assessor's relationship to assessed entity	34
8.4	Topics covered by assessment	34
8.5	Actions taken in response to a deficiency	34
8.6	Communication of results	34
9	OTHER BUSINESS AND LEGAL MATTERS	35
9.1	Fees	35

9.2	Financial responsibility	35
9.2.1	Insurance coverage.....	35
9.2.2	Other assets.....	35
9.2.3	Insurance or warranty coverage for end-entities	35
9.3	Confidentiality of business information.....	35
9.3.1	Scope of confidential information	35
9.3.2	Information not within the scope of confidential information.....	35
9.3.3	Responsibility to protect confidential information.....	35
9.4	Privacy of personal information	36
9.4.1	Information treated as private	36
9.4.2	Information not deemed private	36
9.4.3	Responsibility to protect private information	36
9.4.4	Notice and consent to use private information.....	36
9.4.5	Disclosure pursuant to judicial or administrative process	36
9.4.6	Other information disclosure circumstances.....	36
9.5	Intellectual property rights	36
9.6	Representations and warranties.....	36
9.6.1	CA representations and warranties	36
9.6.2	RA representations and warranties	37
9.6.3	Subscriber and Subject representations and warranties	37
9.6.4	Relying party representations and warranties	37
9.6.5	Representations and warranties of other participants.....	37
9.7	Disclaimers of warranties	37
9.8	Limitations of liability	37
9.9	Indemnities.....	37
9.10	Term and termination.....	37
9.10.1	Term	37
9.10.2	Termination	37
9.10.3	Effect of termination and survival	38
9.11	Individual notices and communications with participants	38
9.12	Amendments	38
9.12.1	Procedure for amendment	38
9.12.2	Notification mechanism and period	38
9.12.3	Circumstances under which OID must be changed	38
9.13	Dispute resolution provisions	38
9.14	Governing law.....	38
9.15	Compliance with applicable law	38
9.16	Miscellaneous provisions.....	39
9.16.1	Entire agreement.....	39
9.16.2	Assignment	39
9.16.3	Severability	39
9.16.4	Enforcement (attorneys' fees and waiver of rights)	39
9.16.5	Force Majeure	39
9.17	Other provisions	39

Tables

Table 1 ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA - Certificate Profile for ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001 self-signed certificate	31
Table 2 ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001 - CRL profile	32
Table 3 ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA - Certificate Profile for OCSP responder	33

ABOUT THIS DOCUMENT

The present document is the Certificate Policy (CP) and Certification Practice Statement (CPS) for the ZetesConfidens Private Trust PKI - Root CA.

Intellectual Property Rights

Without limiting the “all rights reserved” copyright on the present document, and except as duly licensed under written form, no part of this document or any of its contents may be reproduced, copied, modified or adapted, without the prior written consent of the author, unless otherwise indicated for stand-alone materials.

Commercial use and distribution of the contents of this document is not allowed without express and prior written consent of Zetes SA.

The following sentence must appear on any copy of this document: "© 2019 – Zetes – All Rights Reserved"

Document Version History

Version	Publication Date	Effective Date	Information about this Version
1.0	03/05/2019	05/05/2019	first version -----

ABOUT ZETES

About Zetes SA

Founded in 1984, Zetes 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 SA is active in the areas of identification documents, travel documents, smartcards, biometrics and trust services including the issuance of certificates.

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

Zetes is registered as follows:

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

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

About ZETESCONFIDENS business unit

In 2016, Zetes established an operational business unit within Zetes 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 (previously referred to as “Zetes TSP”).

1 INTRODUCTION

1.1 Overview

ZETESCONFIDENS operates *publicly* trusted infrastructure and is a (Qualified) Trusted Service Provider (TSP) as defined in Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. ZETESCONFIDENS is supervised by the Belgian Supervisory Body for its QTSP services.

ZETESCONFIDENS *Private Trust PKI* is a separate PKI hierarchy, which is not publicly trusted. This PKI is not subject to the audit and compliance requirements of eIDAS for Qualified status. However, the PKI is operated by the principles and practices laid down in ETSI EN 319 401 and ETSI EN 319 411.

ZETESCONFIDENS Private Trust PKI is a 2-tier CA hierarchy. This document applies to the ZETESCONFIDENS Private Trust PKI - Root CA for issuance of certificates to subordinate CAs also called issuing CAs. The ZETESCONFIDENS Private Trust PKI - Root CA only issues CA certificates for subordinate CAs that are part of the ZETESCONFIDENS Private Trust PKI environment.

ZETESCONFIDENS Private Trust PKI - Issuing CAs are CA services that are managed and operated by ZETESCONFIDENS managed by third party Organizations but operated by ZETESCONFIDENS (outsourced services).

The provisioning and use of a subordinate CA certificate issued by ZETESCONFIDENS Private Trust PKI - Root CA is governed by the present Certification Practice Statement (CPS) and Certificate Policy (CP).

The provision and use of the certificates for end-entities, issued by a subordinate CA, are governed by the related Certification Practice Statement (CPS) and the Certificate Policy of said subordinate CA and are out of scope for the present document.

Information related to a ZETESCONFIDENS subordinate CA is provided in the respective documentation set of said subordinate CA. The present document may specify information related to subordinate CAs certificates when needed for the sake of clarity or for conformity.

This document conforms to the Internet Engineering Task Force (IETF) RFC 3647 framework and template for Certificate Policy and Certification Practice Statement. 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 distinguish disclosure of public information and security sensitive confidential information.

1.2 Document name and identification

This document is called the 'ZetesConfidens Private Trust PKI - Root CA – Certification Practice Statement and Certificate Policy'.

The OID for this Certification Practice Statement is:

dotted notation	1.3.6.1.4.1.47718.2.1.1.3
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) privatetrustrootca(3) }

The OID for this Certificate Policy is:

dotted notation	1.3.6.1.4.1.47718.2.1.2.3
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) privatetrustrootca(3) }

1.3 PKI participants

ZETESCONFIDENS has final and overall responsibility for the provision of the ZETESCONFIDENS Private Trust PKI Root CA certificates offering, namely:

- 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 Authority (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 services,

- the dissemination services.

Whereas for its Publicly Trusted TSP services ZETESCONFIDENS holds final and overall responsibility for the provision of the ZETESCONFIDENS certificates including for RA services, for the Private Trust PKI ZETESCONFIDENS may be released of any and all responsibility for part of its subordinated certification services such as Registration Management Services for its subordinated CA certificate issuing based on contractual agreement with Subscribers in a closed user community.

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 are impacted using 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, concerned by the whole CA hierarchy, include:

Subscribers	<p>For the top level of the CA hierarchy concerned by the present document, the Subscriber is ZETESCONFIDENS, operator of a subordinate CA.</p> <p>For the second level of the CA hierarchy, the Subscriber is an organization that enters into a contractual agreement with ZETESCONFIDENS on behalf of Subjects.</p>
Subjects	<p>For the top level of the CA hierarchy concerned by the present CPS, subjects are ZETESCONFIDENS operated entities such as Certification Authorities (i.e. a subordinate CA).</p> <p>For the second level of the CA hierarchy, subjects are parties whose identity or identifier is encoded in the end user certificate issued by a CA.</p>
Relying Parties	Third parties who rely on the validity of the certificate issued by the CA hierarchy.
CA - Certification Authorities	Certification Authority 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).
RA - Registration Authorities	The entities representing the organisation of registration management services.
Publication and Repository Services	Publication of documents such as Certification Practice Statements, Certificate Policies, Certificates Terms and Conditions, certificate validation data such as root certificates, certificate revocation lists, etc.

Within the context of this CPS for the Root CA, ZETESCONFIDENS fulfils the following roles:

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

ZETESCONFIDENS being both CSP and Subscriber, there are no separate bodies for Registration Authority nor for Suspension and Revocation Authority as such. Rather, there are procedures for the issuance of PKI component certificates such as the Private Trust PKI Root CA self-signed certificate, subordinate CA certificates, certificates for certificate status validation services such as OSCP responder certificates and certificates for internal use for CA and RA management. These procedures are executed by ZETESCONFIDENS staff in trusted roles, under multiple control and under the responsibility of the PMA as further described in the present CPS and its related confidential and internal documentation.

1.3.1 Certification Authorities (CA)

The subordinate CAs are operated by ZETESCONFIDENS and adhere to the terms and conditions of the present CPS for the ZETESCONFIDENS Private Trust PKI - Root CA. A subordinate CA may have a CP which is specific to the subordinate.

ZETESCONFIDENS provides the Dissemination Services for the CA such as publication the full archival of Certification Practice Statement, Certificate Policy, Certificates Terms and Conditions, CA certificates, certificate revocation lists.

The Dissemination and Repository Services are described in section 2 of the present document.

For closed user groups access to certain subordinate CA Certificates and related documents or certificate status validation services may be restricted to authorised parties subject to contractual agreement with the Subscriber .

ZETESCONFIDENS is responsible for operating the Revocation Management Services and the Revocation Status Information Services.

1.3.2 Registration and Revocation Authorities ((S)RA)

Within the context of the ZETESCONFIDENS Private Trust PKI - Root CA, all entities involved in the registration of a subject/subscriber are part of ZETESCONFIDENS. The RA is the organisational structure and the infrastructure within ZETESCONFIDENS that is tasked with the following duties:

- authenticate and validate the subordinate CA
- validate and process the certificate request from a subordinate CA
- issue the certificate for the subordinate CA

The RA acts under direct authority and supervision of the ZETESCONFIDENS Policy Management Authority (see section 0).

1.3.3 Subscribers and Subjects

The Subscriber is the operator of the subordinate CA, i.e. ZETESCONFIDENS

The Subject is the PKI Component entity that is certified by ZETESCONFIDENS Private Trust PKI - Root CA; the Subjects are either a subordinate CA of ZETESCONFIDENS or a certificate status validation service of ZETESCONFIDENS, such as an OCSP responder or a designated RA.

1.3.4 Relying parties

The Relying Parties are those parties who rely on a certificate that is issued from the CA hierarchy of the ZETESCONFIDENS Private Trust PKI.

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 subordinate CA 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, the exception of internal certificates used to secure the PKI.

Subordinate CAs

Subordinate CA's of ZETESCONFIDENS Private Trust PKI cannot issue CA 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 Policy Management Authority (PMA):

E-mail:	pma@tsp.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://confidens.zetes.com http://tsp.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/CP. The existing ZETES Change Control mechanism will be used to trace all identified changes to the content of this document. This CPS/CP 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
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,
-----------------	------------------------------------------------------------------------------------------------------------------------------------------------------

Certificate	<p>passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorised use of the private key.</p> <p>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.</p>
Certificate Revocation List	<p>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).</p>
Hardware Security Module	<p>Hardware Security Module. An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.</p>
Relying party	<p>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.</p> <p>In the context of this <i>Certification Practice Statement</i>, Relying Parties are as further defined in section 1.3.4.</p>
Subscriber	<p>Person or organisation contracting with the Certification Authority, for being issued one or more Certificates.</p> <p>In the context of this <i>Certification Practice Statement</i>, the Subscribers are as further defined in section 1.3.3</p>

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ZETESCONFIDENS operates the following online repositories and services available:

https://confidens.zetes.com	Commercial web site of ZETESCONFIDENS
httpS://tsp.zetes.com	Technical web site of ZETESCONFIDENS
https://repository.confidens.zetes.com	CPS/CP/PDS/TC document repository
http://crt-ptpki.confidens.zetes.com/ZCPTPKIROOTCA001.crt	Root CA certificate direct download
http://crt.tsp.zetes.com	Certificate repository landing page
http://crl-ptpki.confidens.zetes.com/ZCPTPKIROOTCA001.crl	ARL and CRL repository
http://ocsp-ptpki.confidens.zetes.com	OCSP service

2.2 Publication and frequency of publication

Publication of CA certificates

The certificate for the ZETESCONFIDENS Private Trust PKI - Root CA and subordinate CA certificates are published in a public certificate repository. A subscriber may request not to publish its subordinate CA certificates in the public repository. In said case, is the Subscriber's duty to distribute the publish or distribute the CA certificate via other channels.

The thumbprint value for the ZETESCONFIDENS Private Trust PKI - Root CA is printed in section 7.1 of this document. Alternatively, authorised Relying Parties who wish to validate the thumbprint value before installing the CA certificates can request out-of-band confirmation via info@tsp.zetes.com.

Publication of Certificate Status Information

Certificate status information for certificates issued by the Root CA is made available as CRLs or via an OCSP service (optional).

The CRL of the Root CA is updated either every 12 months or when a subordinate CA certificate is revoked. The CRL is published in the repository within 3 hours after creation. The OCSP service is synchronised with the latest CRL when that CRL is published.

The CRLs of the subordinate CAs are published at regular intervals as indicated in each CRL itself. CRLs may be renewed early when certificates have been revoked. The CRLs are updated until all certificates that that were issued by the respective CA have expired or have been revoked. Expired certificates that were revoked before their expiration dates are removed from the certificate revocation lists.

The OCSP service is at least as accurate as the latest CRL. More information is available in section 4.10.

2.3 Access controls on repositories

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

Relying Parties have read-only access to all the repositories mentioned in section 2.1.

ZETESCONFIDENS will take reasonable measures to protect and prevent against abuse of the repositories and services 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.

ZETESCONFIDENS internal documents not published in the repository are made available only to Participants in the Private Trust PKI when deemed necessary by the PMA.

3 IDENTIFICATION AND AUTHENTICATION

All certificates shall have a distinguished name that complies with the X.501 standard for distinguished names.

All CA and OCSP certificates shall have names that comply with this certificate policy.

End entity certificates issued by a subordinate CA should adhere to the naming policy defined in the certificate policy for that subordinate CA. Each subordinate can have different naming conventions.

3.1 Naming

3.1.1 Types of names

Certificates for CAs and OCSP responders only contain names that represent organisations (i.e. not individuals).

The distinguished name (DN) may contain the following fields:

- Common Name CN
- Organisation O
- Organisational Unit OU
- Country C
- State S
- domain name components DC

3.1.2 Need for names to be meaningful

Names shall be meaningful and unambiguous.

For subordinate CAs ZETESCONFIDENS validates the names for the creation of the DN such that:

- it is clear that the certificate is for a subordinate CA,
- it is clear what the purpose of the certificate is,
- it is clear to which user community the CA belongs,
- it includes an unambiguous and meaningful association with the legal name or registered name of the user community it represents.

For OCSP responders ZETESCONFIDENS defines the names such that

- it is clear what the purpose of the certificate is,

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 for CA are guaranteed to be unique.

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 uses an industry standard format that contains the public key for the new certificate and is signed with the corresponding private key. The creation of the request and the validation of the requests is performed by employees of ZETESCONFIDENS in a trusted role.

3.2.2 Authentication of organization identity

The ZETESCONFIDENS Private Trust PKI - Root CA only issues certificates for subordinate CAs or for itself (as self-signed certificate or for its own CRL signer and OSCP responders). For both cases, the organization identity is ZETESCONFIDENS or other organisation entities that are part of the same legal entity Zetes SA.

3.2.3 Authentication of individual identity

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

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 renewal

Not applicable.

3.4 Identification and authentication for re-key requests

Not applicable.

3.5 Identification and authentication for revocation request

The following participants may request revocation of a Subject certificate:

- ZETESCONFIDENS as operator of the ZETESCONFIDENS Private Trust PKI - Root CA
- ZETESCONFIDENS as operator of the Subordinate CA

A revocation request of a CA certificate must be approved by the Policy Management Authority (section 0) or by the security policy. 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 and the related persons/roles operating them are described in this CPS and in internal confidential documentation. The following sections present the elements of these documents that can be publicly disclosed.

Only employees of ZETESCONFIDENS who are assigned to the CA entities are authorised 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.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Since the Subscriber is ZETESCONFIDENS and the Subject is a PKI component of ZETESCONFIDENS, the application process is a purely internal procedure. An application for a subordinate CA certificate must be approved by the Policy Management Authority (section 0).

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 0).

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

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

ZETESCONFIDENS is the owner, operator and custodian of the keys and certificates of the CA hierarchy under the ZETESCONFIDENS Private Trust PKI - 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.

Only a selected group of authorised trusted employees, entitled by the PMA, are in charge of generating keys and certificates for a root CA or for a subordinate CA.

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, the Root CA 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 CSP 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 ZETESCONFIDENS Private Trust PKI - 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 ZETESCONFIDENS Private Trust PKI - 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 ZETESCONFIDENS Private Trust PKI - 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 Private Trust PKI hierarchy are specified in the related end-entities CPs.

4.6 Certificate renewal

Not applicable.

4.7 Certificate re-key

Not applicable.

4.8 Certificate modification

Not applicable.

4.9 Certificate revocation and suspension

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 ZETESCONFIDENS Private Trust PKI - 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 ZETESCONFIDENS Private Trust PKI - 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.

4.9.3 Procedure for revocation request

Revocation requests for CA certificates and OCSP certificates is done through manual intervention of authorized staff.

4.9.4 Revocation request grace period

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

4.9.5 Time within which CA must process the revocation request

In case of a key compromise ZETESCONFIDENS undertakes best effort to revoke the certificate within 24 hours. The time to process a revocation request of a CA certificate or a PKI component certificate for any other reason is determined on a case by case basis.

4.9.6 Revocation checking obligations for Relying Parties

Relying parties must use at least one of the services for checking certificate status information that are made available by 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 0 and section 4.5.2.

4.9.7 CRL issuance frequency (if applicable)

The ZETESCONFIDENS Private Trust PKI - 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.

4.9.8 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.

4.9.9 On-line revocation/status checking availability

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

<http://ocsp.tsp.zetes.com>

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

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 2.3 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>

<http://crt.tsp.zetes.com>

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

4.9.12 Special requirements re key compromise

No stipulations.

4.9.13 Circumstances for suspension

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 Private Trust PKI - Root CA:

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

4.10.2 Service availability

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 ZETESCONFIDENS Private Trust PKI - 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

5.1 Physical controls

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

5.1.1 Site location and construction

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

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

5.1.2 Physical access

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

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

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

Premises are protected from any water damages.

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

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

5.2 Procedural controls

5.2.1 Trusted roles

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

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

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

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

- Plant Manager
- PKI manager
- IT Manager
- Security Officer
- PKI administrator
- PKI operator
- System administrator
- System auditor
- System operator
- Registration officer (not applicable for the Root CA activities)
- Revocation officer (not applicable for the Root CA activities)
- Key custodians

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

5.2.2 Number of persons required per task

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

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

5.2.3 Identification and authentication for each role

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

5.2.4 Roles requiring separation of duties

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

Zetes ensures separation among the following discrete work groups documented in internal documents:

- PKI administration personnel
- System and network administration personnel
- Security personnel,
- Audit personnel.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

5.3.2 Background check procedures

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

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorised actions

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

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

5.3.7 Independent contractor requirements

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

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

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

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

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

- Issuance of a certificate: request, approval or rejection (with reason) of request, registration information, identification of the members of the PMA approving, identification of the trusted roles processing the request, certificate generation/activation, ...
- Revocation of a certificate: revocation request, approval or rejection (with reason) of request, identification of the members of the PMA approving, identification of the trusted roles processing the request, identification of the requestor, ...
- Publication of a CRL
- Request to and answers from the OCSP services (responders)

The audit logs records contain:

- The identification of the operation.
- The date and time of the operation.
- The identification of the certificate involved in the operation.
- The identity of the transaction requestor (e.g. one or more members of the PMA).

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

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

Auditing events are not given log notice.

All events occurring prior and during a Root CA ceremony are logged in a log sheet. This cover:

- Ceremony authorisation by the PMA
- Root CA key (initial) key generation and self-certification
- Issuance of CRL
- Issuance of a subordinate CA certificate
- Revocation of a subordinate CA certificate
- Root CA key recovery

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

System logs are retained for 12 months. For audit logs for the CA and PKI components, see section 5.5.2.

5.4.4 Protection of audit log

The audit logs of the critical PKI components application software are digitally signed and time stamped. The signature key is protected by an HSM.

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

The PKI audit collection system is internal.

5.4.7 Notification to event-causing Subject

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

5.4.8 Vulnerability assessments

The entire infrastructure is subject of a vulnerability assessment. The assessment covers the ICT infrastructure, the special cryptographic equipment, the physical environment, data storage, software, personnel, processes and procedures and communication. Vulnerability assessment of the audit log is part of the ZETESCONFIDENS risk assessment and risk management program documented internally.

5.5 Records archival

5.5.1 Types of records archived

See section 5.4.1 and 5.5.2.

5.5.2 Retention period for archive

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

- 10 years after the certificate ceases to be valid,
- Audit trails on the issuance or revocation of certificates for a period of 10 years from the event,
- In the case of a legal dispute regarding the authenticity or validity of any data included in the certificate, until the legal dispute is closed with a final decision,
- CRLs for at least 10 years after creation,
- Documentation supporting the issuance and use of the certificate is kept for a period of at least 10 years after the expiration of the last certificate supported by the documentation.

5.5.3 Protection of archives

The archives are protected against manipulation or wilful destruction. As far as possible archive will be retained and protected in electronic form. Paper-based records are archived and under control of the respective roles that process them. Paper-based archive may be stored on multiple locations. The information will be securely stored to provide reasonable assurance regarding secrecy, integrity and availability.

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

The audit logs created by the CA service are signed and time stamped.

The audit logs created by the OCSP service are time stamped.

The time source is the same as for the CA or OCSP service.

5.5.6 Archive collection system (internal or external)

The archive collection system for the CA and PKI components operated by ZETESCONFIDENS is internal infrastructure of ZETESCONFIDENS.

5.5.7 Procedures to obtain and verify archive information

The contents of the archive are not accessible except for authorised personnel of ZETESCONFIDENS and with exception of obligations by law or by court order. Access to archive by authorised personnel must be motivated (e.g. in case of incident investigation, to test the "retrieval" procedure, etc.). Disclosure of information from the archive upon request by an implicated party is at the discretion of ZETESCONFIDENS and requires approval by the PMA. ZETESCONFIDENS reserves the right to charge a compensation to cover the expenses of the retrieval of the information from the archives.

5.6 Key changeover

Not applicable, as CA certificates will be issued with a validity time within the validity time of the Root CA certificates.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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

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

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

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

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

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

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

5.7.3 Entity private key compromise procedures

In case of a CA compromise, ZETESCONFIDENS will

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

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

5.7.4 Business continuity capabilities after a disaster

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

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

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

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

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

5.8 CA or RA termination

Terminating a certification service and as a result terminating, when applicable, the CA(s) and other PKI component requires planning physical, logical, operational, procedural and human aspects.

For clarification, the cessation of the issuance of new certificates by the ZETESCONFIDENS Private Trust PKI - Root CA while all other component services are kept under full normal operations, including the provision of certificate validity status information services (e.g. CRLs, OCSP services), is not termination. Also, the controlled transfer of services and components from ZETESCONFIDENS to another organization or transfer from an old CA to a new CA is not termination.

This section describes the minimum procedures to be completed in a situation where all or a part of the certificate issuance or management operations provided by ZETESCONFIDENS Private Trust PKI are terminated:

In the context of a scheduled termination:

- Cessation of the issuance of any new certificate
- Termination notification to the Subscribers who in turn must inform their Subjects via the designated contact person
- Termination notification to the Subjects and Relying Parties via the web site
- Dissemination of relevant information
- Preservation and transfer of auditing and archival records to the arranged custodian
- Revocation of unexpired and unrevoked Subjects' Certificates
- Creation of a last CRL
- If applicable, decommissioning of the CA keys

In the context of an unscheduled termination:

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

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

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Private keys for the ZETESCONFIDENS PKI infrastructure are protected by means of Hardware Security Modules. Physical access to the HSM and administration of the HSM is limited to authorised personnel only. The HSMs are installed in a secure environment. Operational use of the HSM equipment is strictly controlled. Activation assets and activation data are assigned to multiple custodians and are stored in a secure location, separate from the HSM equipment.

Key pairs for CAs are generated on-board an HSM, under the authority of the PMA, under supervision of a Security Officer as part of a formal key ceremony. Key pairs for OCSP responders are generated on-board an HSM either manually by authorized personnel or by an automatically scheduled process.

6.1.2 CA public key delivery to Relying Parties

ZETESCONFIDENS root CA certificates are published on a secure public repository. The authentic “thumbprint” of the root CA certificates are published in a document in PDF/A format.

Relying parties may contact ZETESCONFIDENS via e-mail at info@tsp.zetes.com to receive confirmation of the authentic “thumbprint” of the root CA certificates by means of an out-of-band channel such as a telephone call, e-mail or letter.

Distribution of the subordinate CA certificates to Relying Parties is the responsibility of the owner of the user community to which the subordinate CA pertains.

6.1.3 Public key parameters generation and quality checking

Public key parameters for the ZETESCONFIDENS Private Trust PKI - 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 HSM operates in FIPS140-2 level 3 mode. Key generation relies on the HSM’s deterministic (pseudo) random number generator

6.1.4 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.

Key usage for CA certificates:	KeyCert signing CRL signing
Key usage for OCSP certificates:	digitalSignature - OCSP signing

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 CAs and the OCSP service, the ZETESCONFIDENS Qualified CA uses state of the art cryptographic modules. The HSMs are prepared, initialized and managed in compliance with ETSI EN 319 401 and ETSI EN 319 411 part 1. The HSMs have the security certification NIST FIPS 140-2 level 3.

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 ZETESCONFIDENS Private Trust PKI - 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 authorised 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 OSCP 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 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 *n-of-m* 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 related security critical data is always encrypted (backup operation) or decrypted (restore operation) inside the HSM itself. 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 operational purposes. 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 OSCP 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 are generated inside an HSM. Keys can be backed up and restored into the HSM but 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

Activation of the private keys for the CA requires multiple authorised administrators and operators for activating the HSM

Activation of the private keys for the OSCP service is automated without requiring further intervention.

6.2.9 Method of deactivating private key

Access to the control interface for activating or deactivating a group is uses 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 for HSM in 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.

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 Private Trust PKI - 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 Private Trust PKI - 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

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 enough variation.

6.5 Computer security controls

ZETESCONFIDENS ensures that computer security controls are implemented according the technical standard ETSI EN 319 411-1. 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 amongst others:

- CA are activated only when necessary.
- Control of sensitive data stored on “demobilized” or reusable storage device
- Use of multifactor authentication and/or named accounts for critical user accounts
- Access control, intrusion detection system and CCTV monitoring to detect, record and react to unauthorised access

6.6 Life cycle technical controls

6.6.1 System development controls

Implemented in compliance with ETSI EN 319 401 and ETSI EN 319 411 part 1.

6.6.2 Security management controls

Implemented in compliance with ETSI EN 319 401 and ETSI EN 319 411 part 1.

6.6.3 Life cycle security controls

Implemented in compliance with ETSI EN 319 401 and ETSI EN 319 411 part 1.

6.7 Network security controls

Not applicable. The ZETESCONFIDENS Private Trust PKI - Root CA is not connected to any network.

6.8 Time-stamping

Not applicable.

ZETESCONFIDENS is not in any way held to continue using the current algorithms, protocols or key lengths for any purpose, 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.

7.2 CRL profile

Generic CRL profile for consolidated CRL:

Table 2 ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001 - CRL profile

CRL profile			
ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001 - CRL			
ATTRIBUTES			
Version		-	2
Signaturealgorithm	algorithm	-	sha256WithRSAEncryption
		-	<the signature created by ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001 >
Issuer	serialNumber	-	001
	commonName	-	ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001
	organizationName	-	ZETES SA
	countryName	-	BE
ThisUpdate		-	<time of issue >
NextUpdate		-	<time of issue + 6 months>
Revoked Certificates	userCertificate	-	<certificate serial number>
	revocationDate	-	<revocation time>
	crEntryExtension CRLReason	-	<reason for revocation> - included for every certificate -
EXTENSIONS			
Authority Key Identifier		-	6D EB 00 8E 0E 06 13 9D C6 C1 23 63 32 FC 0E B4 39 44 78 64
CRL Number		-	dynamically assigned by the CA

7.3 OCSF profile

Generic certificate profile for a ZETESCONFIDENS Private Trust PKI - Root CA OCSF responder certificate:

Table 3 ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA - Certificate Profile for OCSF responder

certificate profile			
ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001 - OCSF 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 ZETESCONFIDENS PRIVATE TRUST PKI - 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 (<i>the 3-digit serial number of the CA</i>)
	commonName	-	ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001
	organizationName	-	ZETES
	countryName	-	BE
Subject	commonName	-	ZETESCONFIDENS PRIVATE TRUST PKI - ROOT CA 001 OCSF
	organizationName	-	ZETES SA
	countryName	-	BE
EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	keyIdentifier	-	6D EB 00 8E 0E 06 13 9D C6 C1 23 63 32 FC 0E B4 39 44 78 64
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	keyIdentifier	-	< 4-bit value 0100 + 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	< true >
enhancedKeyUsage	OCSF Signing	c	< true >
OCSFNoCheck		-	< null >

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The ZETESCONFIDENS Private Trust PKI is not subject to the audit assessments that apply to publicly trusted PKI's.

8.1 Frequency or circumstances of assessment

ZETESCONFIDENS internal audits to ensure that the requirements, standards, procedures and service levels according to this CPS/CP are upheld.

ZETESCONFIDENS is audited by an independent auditor at least once a year as part of Zetes SA's broader scope ISO 27001 audit.

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

8.2 Identity/qualifications of assessor

The annual ISO 27001 audits are performed by a duly accredited auditor.

8.3 Assessor's relationship to assessed entity

Internal audits are carried out by ZETESCONFIDENS staff.

The annual ISO 27001 audits are carried out by an independent auditor who is not affiliated either directly or indirectly in any way with Zetes SA.

8.4 Topics covered by assessment

Internal audits cover the security aspects and operational aspects ZETESCONFIDENS' operations.

The annual ISO 27001 audits cover the information security aspects of ZETESCONFIDENS' operations.

8.5 Actions taken in response to a deficiency

Detected deficiencies and non-conformities shall be assessed for the severity and the extent of the detected deficiencies. In accordance with the auditor, the ZETESCONFIDENS will determine the time frame and the actions to be conducted to rectify the deficiencies. A follow-up audit to verify the effectiveness of the actions conducted can be decided by the PMA to ensure compliance.

8.6 Communication of results

Audit report and findings are communicated by the auditor to the audited entities. In some circumstances, e.g. suspicion of internal fraud, the auditor will not disclose his findings to the audited entity but to the PMA instead. Audit report and findings will list all detected deficiencies with their level of severity but without disclosing any information that could be used to attack the system. By default, audit reports are classified at level "CONFIDENTIAL" and distributed on a need to know basis.

9 OTHER BUSINESS AND LEGAL MATTERS

The provision and use of end-entities Certificates issued by ZETESCONFIDENS Private Trust PKI issuing CA's are governed by the related Certification Practice Statement (CPS) and Terms and Conditions and are out of scope of the present document.

The sections below only provide useful information about certain terms and conditions governing the use of ZETESCONFIDENS Private Trust PKI - Root CA's service.

9.1 Fees

See the applicable end-entity's Terms and Conditions. Issuing CA's and Registration Authorities within the ZETESCONFIDENS Private Trust PKI hierarchy will make available all applicable fees upon request.

9.2 Financial responsibility

9.2.1 Insurance coverage

The liability of ZETESCONFIDENS towards the Subscriber or a Relying Party may be limited according to the applicable CPS/CP.

Subject to any limitation of liability referred to in the applicable CPS/CP, the general rules on liability apply with regard to any damage caused to any entity or legal or natural person who reasonably relies on a certificate issued by ZETESCONFIDENS.

ZETESCONFIDENS explicitly declines all liability towards Relying Parties in all cases where Certificates are used beyond the limitation expressed in this present CPS and the relevant CP and CPS of the Certificate.

9.2.2 Other assets

ZETESCONFIDENS shall monitor on a regular basis that it maintains adequate resources to meet its obligations regarding the provision and use of its ZETESCONFIDENS offering under this Certification Practice Statement and elsewhere in its Agreements.

9.2.3 Insurance or warranty coverage for end-entities

Zetes S.A. benefits from insurance coverage covering ZETESCONFIDENS services for public, product and professional liabilities.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Examples of confidential business information include:

- the Subscriber's confidential information supplied to ZETES at the time of its subscription. Information that is published in the Certificate is NOT confidential.
- the Subscriber's or Relying Parties' confidential information supplied to ZETES in support requests (other than any information that is published in a ZETESCONFIDENS issued Certificate)
- the private key(s) of Certificates

9.3.2 Information not within the scope of confidential information

For the avoidance of any doubt, the following information is not considered as confidential:

- the information published in a ZETESCONFIDENS issued Certificate
- the revocation records of a Certificate
- this Certification Practice Statement

9.3.3 Responsibility to protect confidential information

ZETESCONFIDENS and Subscriber Obligations of Confidentiality are described in the applicable Certificates Terms and Conditions.

ZETESCONFIDENS will keep confidential and not disclose the confidential information to any person save as expressly permitted by law or foreseen in the Agreement.

ZETESCONFIDENS will protect the confidential information against unauthorised disclosure by using the same degree of care as it takes to preserve and safeguard its own confidential information of a similar nature, being at least a reasonable degree of care and skill in accordance with the state-of-the-art.

9.4 Privacy of personal information

ZETESCONFIDENS operates within the boundaries of the Belgian Law of 30 July 2018 on Privacy Protection in relation to the Processing of Personal Data with reference to the General Data Protection Regulation (EU) n° 2016/679. And conform the Law of 13 June 2005 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Without consent of the data subject or explicit authorization by law, personal data processed by the CSP will not be used for other purposes.

For end-entities certificates, see the applicable end-entity's Terms and Conditions for more information on the privacy plan.

9.4.1 Information treated as private

Refer to the intro text of Section 9.4.

9.4.2 Information not deemed private

Refer to the intro text of Section 9.4.

9.4.3 Responsibility to protect private information

Refer to the intro text of Section 9.4.

9.4.4 Notice and consent to use private information

Refer to the intro text of Section 9.4.

9.4.5 Disclosure pursuant to judicial or administrative process

Refer to the intro text of Section 9.4.

9.4.6 Other information disclosure circumstances

Refer to the intro text of Section 9.4.

9.5 Intellectual property rights

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

No rights are granted by ZETESCONFIDENS other than those expressly granted under this Certification Practice Statement or elsewhere in the applicable Subscriber Agreement.

The IPR with regards to Zetes acting as CSP, are ruled by the applicable "Certificates Terms and Conditions".

9.6 Representations and warranties

9.6.1 CA representations and warranties

Zetes S.A. acting as CSP issues X509 v3-compatible Certificates (ISO 9594-8).

ZETESCONFIDENS issues Certificates compliant with ETSI EN 319 401 and EN 319 411-1 requirements.

ZETESCONFIDENS guarantees that all the requirements set out in the applicable CP (and indicated in the Certificate in accordance with Section 7 of the CP) are complied with. It also assumes responsibility for ensuring such compliance and providing these services in accordance with the applicable CPS.

The sole guarantee provided by Zetes S.A. acting as CSP is that its procedures are implemented in accordance with the applicable CPS and the verification procedures then in effect, and that all Certificates issued with a CP Object Identifier (OID) have been issued in accordance with the relevant provisions of the applicable CP, the verification procedures, and the CPS as

applicable at the time of issuance. In addition, other warranties may be implied in the applicable CP definition by operation of law.

9.6.2 RA representations and warranties

See the applicable end-entity's Terms and Conditions.

9.6.3 Subscriber and Subject representations and warranties

The Subscriber accepts the "Certificates Terms and Conditions". The Subscriber agrees to the CPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the applicable CPS and CP.

9.6.4 Relying party representations and warranties

Examples of Relying Parties' obligations and responsibilities include (without limitation):

- the successful performance of public key operations as a pre-condition for relying on a ZETESCONFIDENS Certificate
- the validation of a ZETESCONFIDENS Certificate by using the applicable Certificate Revocation Lists (CRLs)
- the immediate termination of any reliance on a ZETESCONFIDENS Certificate if it has been revoked or when it has expired

9.6.5 Representations and warranties of other participants

No additional stipulation.

9.7 Disclaimers of warranties

Except as expressly provided elsewhere in the CPS, the applicable CP and in the applicable legislation, ZETESCONFIDENS disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaims any and all liability for negligence and lack of reasonable care on the part of Subscribers and Relying Parties.

ZETESCONFIDENS does not warrant any software.

9.8 Limitations of liability

Exclusion of Certain Elements of Damages

Within the limit set by Belgian Law, in no event (except for fraud or wilful misconduct) will ZETESCONFIDENS be liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;
- Any other damages.

9.9 Indemnities

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

9.10 Term and termination

9.10.1 Term

This CPS and any amendments hereto shall become effective after publication in the Repository and in accordance with section 9.12.2 and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This shall remain in force until it is amended or replaced by a new version in accordance with this Section 9.10.

9.10.3 Effect of termination and survival

The conditions and effect resulting from termination of this CPS will be communicated via the ZETESCONFIDENS web site upon termination. That communication will outline the provisions that may survive termination of this CPS and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11 Individual notices and communications with participants

All notices and other communications which may or are required to be given, served or sent pursuant to the CPS shall be in writing and shall be sent, except provided explicitly in the CPS, either by (i) registered mail, return receipt requested, postage prepaid, (ii) an internationally recognised “overnight” or express courier service, (iii) hand delivery (iv) facsimile transmission, deemed received upon actual delivery or completed facsimile, or (v) an advanced electronic signature based on a Certificate and a (secure) signature creation device ((S)SCD) and be addressed to:

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

9.12 Amendments

9.12.1 Procedure for amendment

ZETESCONFIDENS acting as CSP is responsible via its Policy Management Authority (PMA) for approval and changes of the present CPS.

The only changes that the PMA may make to these CPS specifications without notification are minor changes that do not affect the assurance level of this CPS, e.g., editorial or typographical corrections, or changes to the contact details.

Errors, updates, or suggested changes to this document shall be communicated as identified in the present CPS, section 1.5.4. Such communication must include a description of the change, a change justification, and contact information of the person requesting the change.

The PMA shall accept, modify or reject the proposed change after completion of a review phase.

9.12.2 Notification mechanism and period

All changes to the present CPS under consideration by the PMA shall be disseminated to interested parties for a period of minimum 10 days. The date of issuance and the effective date are indicated on the title page of the present CPS. The effective date will be at least 2 days later than the date of publication.

9.12.3 Circumstances under which OID must be changed

Not applicable.

9.13 Dispute resolution provisions

All disputes associated with the present CPS will be resolved according to the Belgian laws.

9.14 Governing law

The Belgian laws shall govern the enforceability, construction, interpretation, and validity of the present CPS (without giving effect to any conflict of law provision that would cause the application of other laws).

9.15 Compliance with applicable law

The present CPS and provision of CA certification services are compliant to relevant and applicable laws of Belgium.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

Not applicable.

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