ZETESCONFIDENS

TSA CERTIFICATION PRACTICE STATEMENT AND CERTIFICATE POLICY

Certification Practice Statement and Certificate Policy

for the

ZETES TSP CA for TSA 001

Publication date :	**08/05/2020**		
Effective date :	**12/05/2020**		
CA Practice Statement OID : **Certificate Policy OID :**	**1.3.6.1.4.1.47718.2.1.1.50** **1.3.6.1.4.1.47718.2.1.2.50**		
Version :	**1.3**	**28/04/2020**	**review**

Copyright :

Table of Content

Figures

Tables

ABOUT THIS DOCUMENT

Scope

The present document is the Certificate Policy (CP) and Certification Practice Statement (CPS) for the ZETES TSP CA for TSA 001.

This Certificate Policy and Certification Practice Statement (CP/CPS) applies to the issuance of certificates for the Time-Stamp Units issuing non-qualified and qualified time-stamps meeting the requirements of Regulation (EU) No 910/2014.

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
1.3	08/05/2020	12/05/2020	Update document addition of applicable ETSI certificate policy QCP-l for qualified TSU’s in chapter 1 and chapter 7
1.2	22/07/2019	29/07/2019	Update document following timestamp key Ceremony 12/07/2019. Modify OID in table 2 and 3 of section 7.1.
1.1	21/03/2019	25/03/2019	Additional key sizes supported from the ZetesConfidens TSUs
1.0	24/12/2018	31/12/2018	first publication --

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, 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 SA is active in the areas of identification documents, travel documents, smartcards, biometric solutions and trust services.

Zetes SA 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 as 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.

ZetesConfidens is acting as the Time-Stamping Authority (TSA) and has final and overall responsibility for the provision of the ZETESCONFIDENS (Qualified) time-stamping service offering, namely:

- Time-stamping provision services: provides the generation of the time-stamps through the ZETESCONFIDENS time-stamping units (TSU)
- Time-stamping management services: provides the monitoring and control of the operation of the time-stamping services to ensure that the service is provided as specified by the Time-Stamping Authority (TSA).

ZETESCONFIDENS operates its own trust infrastructure and acts as a Trusted Service Provider (TSP) as defined in the Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market. To this regard, ZETESCONFIDENS is supervised by the FPS Economy, SMEs, Self-employed and Energy - Quality and Safety, the Belgian Supervisory Body and audited to be listed in the Belgian Trusted List of Qualified TSP issuing Qualified electronic Time-stamps.

1 INTRODUCTION

1.1 Overview

The ZETES TSP CA for TSA issues certificates to its Time-Stamping Units (TSU) in order to create and sign time-stamp tokens (TSTs) on behalf of the Time-Stamping Authority (TSA).

Conformity with European legislation and standards for Trust Service Providers issuing time-stamps

The present CP/CPS document states the practices to issue certificates for its TSU issuing qualified and non-qualified time-stamps in accordance with the requirements laid down in the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.

Also, this CP/CPS conforms to the requirements laid down in ETSI EN 319 411-1 “Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements”, ETSI EN 319 411-2 “Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing Qualified Certificates” where applicable and ETSI EN 319 421 “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”.

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

- the present ZETESCONFIDENS Certificate Policy and Certification Practice Statement (CP/CPS),
- the relevant ZETESCONFIDENS TSA Practice Statement and Time-Stamp Policy,

Every certificate issued by the ZETES TSP CA for TSA contains a Certificate Policy OID corresponding to the assurance level of that Certificate as stated in the applicable ZETESCONFIDENS Time-stamp Policy.

Conformity with RFC 3647

This CP/CPS conforms to the Internet Engineering Task Force (IETF) RFC 3647 framework and template for Certificate Policy and Certification Practice Statement construction. It contains information pertaining to the CA practices, including amongst other, the PKI (CA and related components) certificate profiles, applicability and management lifecycles.

Non-disclosure

For reasons of confidentiality, ZETESCONFIDENS cannot disclose all details on controls in this CPS, but instead included references to internal detailed documents. These documents will only be made available to duly authorised parties.

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

1.2 Document name and identification

This document is called the 'ZETES TSP CA for TSA – Certificate Policy and Certification Practice Statement'.

The unique OID for this Certification Practice Statement is:

dotted notation	1.3.6.1.4.1.47718.2.1.1.50
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) tsa (50) }

The unique OID for this Certificate Policy are :

dotted notation	1.3.6.1.4.1.47718.2.1.2.50
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) tsa (50) }

dotted notation	0.4.0.194112.1.1 ETSI QCP-l (for qualified certificates issued > 08/05/2020)
full notation	{itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal(1)}

1.3 PKI participants

In the context of issuing (Qualified) Certificates for Time-stamping, ZETESCONFIDENS is acting as the Time-Stamping Authority (TSA). ZETESCONFIDENS has final and overall responsibility for the provision of the ZETES (Qualified) time-stamping services offering, namely:

- the Time-stamping provision service through the ZETESCONFIDENS Time-Stamping Unit,
- the Time-stamping management service,
- the Revocation Status Information Service (providing certificate validity status information through publication of Certificate Revocation Lists and/or through OCSP services),
- the Dissemination Services.

ZETESCONFIDENS is only one of several PKI participants. The PKI participants are all the legal entities who are involved in any of the processes and activities of ZETESCONFIDENS as a Time-Stamping Authority and/or who are impacted by the use of certificates issued by ZETESCONFIDENS acting as a Time-Stamping Authority. All participants adhere to or are bound by the Certification Practice Statements, Certificate Policies, TSA Practice Statements and Time-Stamping Policies that are maintained by ZETESCONFIDENS.

PKI participants are defined as follows:

Subscribers	Legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.
Relying Parties	Recipient of a time-stamp who relies on that time-stamp.
CA – Certification Authority	The entity issuing certificates to the TSU on request of the TSA

TSU – Time-Stamping Unit	Set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.
TSA – Time-Stamping Authority	The entity that has final and overall responsibility for the provision of the (Qualified) time-stamping services using one or more time-stamping units.
Time-stamping management	The entity that monitors and controls the operation of the time-stamping services to ensure that the service provided meets the regulatory requirements.
Publication and Repository Services	Online publication of documents such as Certificate Practice Statements, Certificate Policies, TSA Practice Statement and Time-Stamp Policies, certificate validation data such as root certificates, certificate revocation lists, etc.
PMA – Policy Management Authority	The PMA has overall responsibility for the ZETESCONFIDENS TSP Services. The PMA includes senior members of management as well as staff responsible for the operational management of the ZETESCONFIDENS PKI environment

1.3.1 Certification Authorities (CA)

CAs are responsible for:

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

ZETESCONFIDENS operates a 2-level CA hierarchy for issuing certificates to its Time-Stamping Units (TSU) in order to create and sign time-stamp tokens (TSTs) on behalf of the Time-Stamping Authority (TSA) and on request of Subscribers.

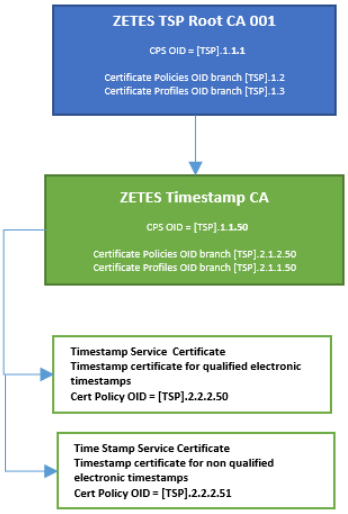
ZETES TSP Root CA 001
CPS OID = [TSP].1.1.1
Certificate Policies OID branch [TSP].1.2
Certificate Profiles OID branch [TSP].1.3
ZETES Timestamp CA
CPS OID = [TSP].1.1.50
Certificate Policies OID branch [TSP].2.1.2.50
Certificate Profiles OID branch [TSP].2.1.1.50
Timestamp Service Certificate
Timestamp certificate for qualified electronic timestamps
Cert Policy OID = [TSP].2.2.2.50
Time Stamp Service Certificate
Timestamp certificate for non qualified electronic timestamps
Cert Policy OID = [TSP].2.2.2.51

Figure 1 CA hierarchy and certificate policies

See chapter 7 for additional information on the CA certificates.

1.3.2 Registration Authority (RA)

End-user certificate applicants for this CA are the internal TSU of the Trust Service Provider. The TSA oversees responsibility of the CA and the TSU, meaning identification and authentication of the TSU are governed by internal procedures to ZETESCONFIDENS acting as TSP.

1.3.3 Subscribers

Subscribers are those parties that request a Time-Stamp Token from from a TSU operated by ZETESCONFIDENS TSA. The Subscriber's roles and responsibility are detailed in the applicable Timestamp Policy and TSA Practice Statement.

1.3.4 Relying parties

The Relying Parties are those parties who are relying on a Time-stamp Token provided by ZETESCONFIDENS (Qualified) TSU for validating the existence of certain data before a particular time.

1.3.5 Other participants

1.3.5.1 Dissemination and Repository Services

ZETESCONFIDENS is operating the Dissemination Services (publication of Certification Practice Statement, Certificate Policy, TSA Practice Statement and Time-Stamp Policy, CA certificates, TSU certificates, certificate revocation lists and other related, public documents).

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

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

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

1.3.6 ZETESCONFIDENS Policy Management Authority (PMA)

The PMA has overall responsibility for the trust Services. The PMA includes senior members of management as well as staff responsible for the operational management of the ZETESCONFIDENS PKI environment.

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

(a) Specifying and approving the PKI infrastructure and practices.

(b) Approving the Practice Statement and the related certificate policies, as well as other declarations of practices and policies for other TSP services when applicable (e.g. time stamping Practice Statement and policies).

(c) Defining the review process for, including responsibilities for maintaining, the Certification Practice Statement and the related certificate policies, as well as other declarations of practices and policies for other PKI services when applicable (e.g. time stamping Practice Statement and policies).

(d) Defining the review process that ensures that applicable certificate policies, and other relevant policies when applicable, are supported by the Practice Statement(s).

(e) Defining the review process that ensures that the PKI authorities, including certification authorities (CAs) and other authorities when applicable (e.g. time stamping authorities – TSAs), as well as all component service of the PKI, properly implements the applicable practices, policies and procedures.

(f) When applicable, authorising part or all component service of the PKI to be provided and/or operated by third parties and the applicable terms and conditions.

(g) Publication to the Subscribers and Relying Parties of the relevant declaration of practices and of policies.

(h) Continually and effectively managing PKI related risks. This includes a responsibility to periodically re-evaluate risks to ensure that the controls that have been defined remain appropriate, and a responsibility to periodically review the controls as implemented, to ensure that they continue to be effective.

(i) Specifying cross-certification or mutual recognition procedures and handling related requests.

(j) Defining internal and external auditing processes with the aim to ensure the proper implementation of the applicable practices, policies and procedures.

(k) Initiating and supervising internal and external audits.

(l) Executing the audit recommendations.

(m) Undertaking any action it considers necessary to ensure the proper execution of the above areas of responsibility.

(n) Defining the scope of the PKI related service offering, among others by:

   1) Defining the certificate classes to be supported by the PKI;

   2) Defining the PKI related entities that will be registered by or under the responsibility of the RA.

   3) Defining the needs for policies that are to be followed for each of the certificate classes;

(o) Ensuring that practices for each of the above mentioned entities are defined and implemented in a manner that is consistent with this document;

(p) Mediating in disputes involving Subscribers and/or entities that have been registered by the RA and the entities that have been implemented by or under the responsibility of the CSP.

(q) Initiating when appropriate highly sensitive PKI operations such as CA root key revocation and renewal or termination of the PKI service.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates created by this CA are solely intended for the purpose of time-stamping. The appropriate certificate usage is further described the ZETESCONFIDENS Time-Stamp Policy.

1.4.2 Prohibited certificate uses

Any usage of a certificate other than the usage explicitly allowed in this Certificate Policy and (where applicable) the Time-Stamp Policy, is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

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

1.5.2 Contact person

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

E-mail address:	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://tsp.zetes.com	

1.5.3 Person determining CPS and CP suitability for the policy

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

1.5.4 CPS and CP approval procedures

The PMA is responsible for the approval of the CP/CPS.

A Change Control mechanism will be used to trace all identified changes to the content of this Certification Practice Statement and Certificate Policy.

This Practice Statement and Policy 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
BTSP	Best practice Time-Stamp Policy
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
TSA	Time-Stamping Authority
TST	Time-stamp token
TSU	Time-Stamping Unit
UTC (k)	Time-scale maintained by the Bureau International des Poids et Mesures (BIPM), which forms the basis of a coordinated dissemination of standard frequencies and time signals

1.6.2 Definitions

Certificate
A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.

Certificate Revocation List
A signed list of identifiers of Certificates that have been revoked. Abbreviated as CRL. It is (periodically) made available by the CA to Subscribers and Relying Parties.

Hardware Security Module (HSM)
Hardware Security Module. An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.

Relying party
In the context of this *Certification Practice Statement*, Relying Parties are as defined in section 1.3.4.

Time-Stamp
Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

Qualified time-stamp	Electronic time-stamp which meets the following requirements: • Binds the date and time to data so as to reasonably prevent the possibility of any undetected change of the data • It is based on an accurate time source that can be traced to UTC(k) It is signed using an advanced electronic signature of the qualified trust service provider, or some equivalent method.
Subscriber	In the context of this *Certificate Policy and Certification Practice Statement*, the Subscribers are as defined in section **Error! Reference source not found.**.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ZETESCONFIDENS operates services 24/7 for the publication of information for Subscribers and Relying Parties.

The CA certificates and certificate status information is made available in formats and through protocols that support automated certificate validation by standard-compliant software applications.

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

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

http://tsp.zetes.com **https://tsp.zetes.com**	This URL refers to the welcome page of the web site for ZETESCONFIDENS. This web site provides: • general information about Zetes SA and the ZETESCONFIDENS business unit • announcements and notifications • a section with technical support and documentation and software downloads for users of the cards and/or certificates that are issued by ZETESCONFIDENS • a section with user friendly web pages for downloading documents such as the terms and conditions, certificate policies, etc. • a section with user friendly web pages for downloading CA certificates and certificate revocation lists (the URLs for these download pages are listed further down in this table) • a contact page
https://repository.tsp.zetes.com **https://pds.tsp.zetes.com**	These URL refer to the pages for downloading documents such as the • CPS - Certificate Practice Statements, • CP -Certificate Policies, • TSA Practice Statement and Time-Stamp Policy, • PDS - PKI Disclosure Statements • etc.
http://crt.tsp.zetes.com	This URL refers to 1. a web page for manual interactive download of CA certificates 2. a server for automated direct download of CA certificates (the direct download link is encoded in the certificates)
http://crl.tsp.zetes.com	This URL refers to 1. a web page for manual interactive download of ARL and CRL 2. a server for automated direct download of ARL and CRL (the direct download link is encoded in the certificates)
http://ocsp.tsp.zetes.com	This URL refers to the OCSP service for immediate online certificate status checks. The OCSP service is synchronised with the latest CRL to provide answers and checks the expiration before the revocation.

2.2 Publication of certification information

Availability

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

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

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

Publication of CA and Time-Stamping Units (TSU) certificates in a repository

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

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

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

info@tsp.zetes.com

Certificate Status Information

ZETESCONFIDENS shall provide CRL and OCSP services for checking the status of the Time-Stamping Units certificates issued by this CA as well as the status of the CA certificate itself:

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

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

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

The OCSP services provide certificate status information for TSU certificates on behalf of the ZETES TSP CA for TSA 001. The OCSP services provide certificate status information for the ZETES TSP CA for TSA 001 root-signed certificate on behalf of the ZETES TSP Root CA 001.

The OCSP infrastructure consists of multiple OCSP responders which are accessible via a common URL. The OCSP responses are signed by an OCSP responder signing key. The OCSP responder signing certificate is issued by the corresponding CA. For the OCSP certificate profiles, see section 7.

Certificate status information in CRLs and the OCSP service shall be updated at least until all certificates that were issued by the respective CA have expired. For qualified Time-Stamping Units certificates, the certificate status information shall remain available beyond the validity period of the certificate, until the issuing CA certificate has expired.

2.3 Time or frequency of publication

Publication of CA certificates in a repository

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

Certificate Status Information

The CRLs are renewed before the CRL is about to expire and may be renewed any time, e.g. when certificates have been revoked. CRLs and delta-CRLs will be available for download within 20 minutes after creation.

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

See chapter 7.2 for the CRL renewal frequency.

Publication of terms and conditions, CSP, etc.

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

2.4 Access controls on repositories

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

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

ZETESCONFIDENS will take reasonable measures to protect and prevent against abuse of the repositories and the OCSP service and will strive to give all parties equal and unhindered access.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The DN for the ZETES TSP CA for TSA certificate is:

CN= ZETES TSP CA FOR TSA 001

SN= 001

O= ZETES SA (VATBE-0408425626)

C= BE

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

TSU certificates bear Distinguished Name (DN) as defined in ETSI EN 319 421. See the Timestamp Policy for the TSU certificates.

3.1.2 Need for names to be meaningful

Names are meaningful. Refer to clause 3.1.1. Names for the TSU certificates are unique for each TSU.

3.1.3 Anonymity or pseudonymity of Subscribers

The ZETES TSP CA for TSA does not issue certificates to subscribers of the Time-Stamp Service.

3.1.4 Rules for interpreting various name forms

The rules for interpreting the names are provided in clauses 3.1 of the present document.

3.1.5 Uniqueness of names

ZETESCONFIDENS TSU DN and ZETESCONFIDENS components DNs are guaranteed to be unique across the ZETESCONFIDENS PKI Domain.

3.1.6 Recognition, authentication, and role of trademarks

No stipulations.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Proof of Possession of Private Key for PKI Components

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

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

3.2.2 Authentication of Organization identity

Organizational entities that are internal to Zetes

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

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

3.2.3 Authentication of individual identity

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

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

3.2.4 Non-verified Subscriber information

Not applicable.

3.2.5 Validation of authority

Not applicable.

3.2.6 Criteria for interoperation

Not applicable.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

See applicable Timestamp Policy.

3.3.2 Identification and authentication for re-key after revocation

See applicable Timestamp Policy.

3.4 Identification and authentication for revocation request

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

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

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

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

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

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

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate Application for internal PKI Participants

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

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

Certificate Application for external PKI Participants

Not applicable.

4.1.2 Enrolment process and responsibilities

The processes and procedures used to enrol the PKI component services (e.g. TSUs, CRLs signers, 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

Identification and Authentication for CA certificate or PKI components certificate

ZETESCONFIDENS, acting as Time-Stamping Authority, is the owner and custodian of the keys and certificates of the CA hierarchy for the ZETES TSP CA for TSA.

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

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

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

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

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

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

4.2.2 Approval or rejection of certificate applications

Approval or Rejection for a CA certificate or PKI components certificate

ZETESCONFIDENS, acting as Time-Stamping Authority, is the owner and custodian of the keys and certificates of the CA hierarchy for the ZETES TSP CA for TSA.

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

ZETESCONFIDENS as TSA is responsible for the validation and vetting of certificate requests for CAs, TSUs and internal PKI components.

4.2.3 Time to process certificate applications

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

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

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Issuance of a certificate for a TSU or a PKI Component

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

4.3.2 Notification of issuance of certificate

Notification of issuance of a certificate for a PKI/TSU Component

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

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

4.4.2 Publication of the certificate by the CA

See section 2 for information on the publication of the certificate.

4.4.3 Notification of certificate issuance by the CA to other entities

See applicable TSA Practice Statement and Time-Stamp policy.

4.5 Key pair and certificate usage

4.5.1 Relying party public key and certificate usage

See the applicable Time-Stamp Policy.

4.6 Certificate renewal

See the applicable Time-Stamp Policy.

4.7 Certificate re-key

See the applicable Time-Stamp Policy.

4.8 Certificate modification

See the applicable Time-Stamp Policy.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

Circumstances for Revocation of a TSU certificate

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

- The PMA has reason to believe or suspect that the TSU's private key has been compromised.

Circumstances for Revocation of a CA certificate

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

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

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

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

Circumstances for Revocation of a PKI components certificate

As specified in the internal procedures of the ZETESCONFIDENS PKI environment.

4.9.2 Parties that can request revocation

Parties that can request Revocation of a TSU certificate

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

Parties that can request Revocation of a CA certificate

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

Parties that can request Revocation of a PKI component certificate.

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

4.9.3 Procedure for revocation request

Procedure for revocation of TSU certificates

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

Procedure for revocation of CA certificates

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

4.9.4 Revocation request grace period for the Subscriber

Not applicable.

4.9.5 Time within which CA must process the revocation request

Process time for revocation of TSU certificates

Under normal operational conditions a TSU key and certificate is replaced before it is revoked, to guarantee continuity of the Time-stamping service towards Subscribers and Relying Parties.

In case of a key compromise, ZETESCONFIDENS undertakes best effort to revoke the certificate without delay within 24 hours. The process time for revocation of a TSU certificate for any other reason will be determined on a case by case basis.

Process time for revocation of CA certificates or PKI component certificates

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

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

4.9.6 Revocation checking obligations for Relying Parties

See the applicable Time-stamp Policy.

4.9.7 CRL issuance frequency

The ZETES TSP CA for TSA issues CRLs at pre-defined intervals or ad hoc when appropriate.

The CRLs are signed and time-marked by the CA.

See chapter 7.2 for the CRL renewal frequency.

4.9.8 Maximum latency for CRLs

Latency for CRLs after revocation of TSU certificates and CA certificates

ZETESCONFIDENS updates the CRL with certificate status information for TSU and CA certificates not later than 1 hour after the actual revocation.

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

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

4.9.9 On-line revocation/status checking availability

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

http://ocsp.tsp.zetes.com

See section 4.10 for more information.

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

See the applicable Time-Stamp Policy.

4.9.11Other forms of revocation advertisements available

Revocation of CA and TSU 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

4.9.12Special requirements re key compromise

No stipulations.

4.9.13Circumstances for suspension

Suspension is currently not supported.

4.9.14Who can request suspension

Not applicable.

4.9.15Procedure for suspension request

Not applicable.

4.9.16Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

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

The ZETES TSP CA for TSA provides CRL and OCSP services for checking the status of the TSU certificates issued by the ZETES TSP CA for TSA as well as the status of the ZETES TSP CA's for TSA own CA certificates.

Download service for ARLs and CRLs

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

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

OCSP service

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

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

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

Retention period for Certificate Status Information after expiration of the certificates

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

4.10.2 Service availability

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

ZETESCONFIDENS maintains a monitoring service for the CRL repository to validate that the CRLs are published in time and in sequence and are readily accessible via the internet for relying parties.

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

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

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

4.10.3 Optional features

No stipulations.

4.11 End of subscription

See the applicable TSA Practice Statement and Time-stamp Policy.

4.12 Key escrow and recovery

No key escrow and no key recovery. The usage of the certificates issued by the ZETES TSP CA for TSA is electronic signature of Time-Stamp Tokens, therefore key escrow is not recommended. Key escrow is not compliant with the applicable regulations and legislation for electronic signatures.

4.12.1 Key escrow and recovery policy and practice

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

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 unauthorized 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 authorized personnel.

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

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

Premises are protected from any water damages.

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

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 and time-stamping related technologies.

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

Trusted roles within 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
- PKI Solutions and Implementation Manager
- Security & Quality Manager
- PKI Administrator
- PKI Operator
- PKI System Administrator
- Registration Officer
- Revocation Officer
- IT System Administrator
- HR Manager
- System Auditor
- Spokesperson
- Key Custodians

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 controls are 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 controls are detailed in the PKI system and documented in the CA key ceremonies reports and related records.

5.2.3 Identification and authentication for each role

Each member of 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 CA can be attributed to the components of the CA and the member of the CA staff that has performed the action.

Zetes ensures separation among the following discreet work groups documented in internal documents “ZETESCONFIDENS – Organization”

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

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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

5.3.2 Background check procedures

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

The background checks include:

- criminal convictions for serious crimes,
- misrepresentations by the candidate,
- appropriateness of references,
- any clearances as deemed appropriate,
- privacy protection,
- confidentiality conditions.

5.3.3 Training requirements

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

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

5.3.6 Sanctions for unauthorized actions

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

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

5.3.7 Independent contractor requirements

There are no independent contractors who perform a trusted role in ZETES Time-Stamping Authority

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

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

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

The following records concerning the operation of time-stamping services are maintained and made available upon Subscriber request or if required by court order:

- Time-stamp requests and created time-stamps
- Events related to TSA administration
- Events related to the life-cycle of TSU keys and Certificates

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

- Issuance of a time-stamp: request, approval or rejection (with reason) of request, Identification of the issuing TSU, created timestamp.
- Publishing of a CRL

The audit logs records contain:

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

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

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

The PKI audit collection system is internal.

5.4.7 Notification to event-causing Subject

Not applicable.

5.4.8 Vulnerability assessments

The entire infrastructure is subject of a vulnerability assessment 4 times per year and penetration testing once a year. Whenever a critical part of the infrastructure is affected. The assessment covers the ICT infrastructure, the special cryptographic equipment, the physical environment, data storage, software, personnel, processes and procedures and communication.

Vulnerability assessment of the audit log is part of the 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 critical records is 7 years after the expiration of the certificate.

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.

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, TSA and VA service are signed and time stamped, the signature key is protected by an HSM and the time source is the same as for the CA, TSA and VA 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 authorized personnel of ZETESCONFIDENS and with exception of obligations by law or by court order.

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

Disclosure of information from the archive upon request by an implicated party other than the Subscriber 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

Key changeover of the CA key requires procedures to provide the new CA related information to Subscribers and Relying Parties, following a re-key by the CA.

The new CA certificate will be made available to Subscribers and Relying Parties through the ZETESCONFIDENS repository.

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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 s and TSAs 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 to be fully tested at least once a year and the report is reviewed by the PMA.

5.7.3 Entity private key compromise procedures

In case of a CA compromise, ZETESCONFIDENS will

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

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

In case of TSU certificates compromise, revocation shall be performed and a new certificate shall be issued provided that the cause of compromise has been discarded. PKI participants' obligations are detailed in the applicable sections of the CPS and the CP.

For additional information see the relevant Timestamp Practice Statement and Timestamp Policy.

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 and TSUs 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), TSA and other PKI component services is an event as important as their initiation. Both require planning of the physical, logical, operational, procedural and human aspects. Security of information and reputation is at risk. Furthermore, legal requirements apply.

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

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

<u>In the context of a scheduled termination:</u>

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

<u>In the context of an unscheduled termination:</u>

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 TSUs Qualified Certificates

6 TECHNICAL SECURITY CONTROLS

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

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

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

The present document provides information on the related technical security controls when applicable.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation for CAs

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

Key pair generation for the OCSP service

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

Key pair generation for the other PKI components

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

Key pair generation for the TSU

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

6.1.2 Private key delivery to Subscriber

Not applicable.

6.1.3 Public key delivery to certificate issuer

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

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

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

6.1.4 CA public key delivery to Relying Parties

ZETESCONFIDENS CA certificates are published on a secure web site:

https://repository.tsp.zetes.com

Relying Parties can authenticate the web site by means of the SSL/TLS server authentication certificate which is issued by a public CA that is external to the ZETESCONFIDENS CA hierarchy.

The authentic "thumbprint" of the ZETESCONFIDENS CA certificates is published in this 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 CA certificates by means of an out-of-band channel such as a telephone call, e-mail or letter.

6.1.5 Key sizes

The current PKI infrastructure for the ZETES TSP CA for TSA may use the following algorithms and key sizes:

CA	RSA4096	generated and used on HSM
OCSP service	RSA2048	generated and used on HSM
	ECDSA-P256	generated and used on HSM
CA Internally signed audit logs	RSA2048	generated and used on HSM
TSA service TSUs	RSA2048	generated and used on HSM
	RSA3072	generated and used on HSM
	ECDSA-P256	generated and used on HSM
TSA Internally signed audit logs	RSA2048	generated and used on HSM
	ECDSA-P256	generated and used on HSM

ZETESCONFIDENS reserves the right to introduce other algorithms, protocols or longer key lengths in the future.

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.

6.1.6 Public key parameters generation and quality checking

Public key parameters are generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Public key parameters are generated and tested in accordance with the FIPS 186-2 standard which ensures the quality of the key material.

The following parameters are used depending on the algorithm family:

RSA:

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

ECDSA, ECDH:

- the HSM is used in FIPS mode
- key generation relies on the deterministic random number generator that is compliant with FIPS 186-2 Appendix 3.1,
- only elliptic curves P-192, P-224, P-256, P-384, P-521, K-163, K-233, K-283, K-409, K-571, B-163, B-233, B-283, B-409 or B-571 as specified in FIPS 186-2 Appendix 6 are used

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

ZETESCONFIDENS ensures that the key usage properties encoded in the certificates correspond with the intended use of the certificates as described in this Certificate Practice Statement and in the applicable Time-stamp Policies.

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

Key usage for CA certificates:	keyCert signing CRL signing
Key usage for OCSP certificates:	digitalSignature - OCSP signing
Key usage for Timestamping certificates:	digitalSignature - Time Stamping
Key usage for Qualified Timestamping certificates:	digitalSignature, -Time Stamping

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Private keys for CA, TSA and OCSP

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

6.2.2 Private key multi-person control

Private keys for CA, TSA and OCSP

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

Private keys for Secure Cryptographic Devices

Not applicable.

6.2.3 Private key escrow

Private keys for CA, TSA and OCSP

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

6.2.4 Private key backup

Private keys for CA,TSA and OCSP

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

The backups are exclusively used for:

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

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

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

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

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

6.2.5 Private key archival

Private keys for CA, TSA and OCSP

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

6.2.6 Private key transfer into or from a cryptographic module

Private keys for CA, TSA and OCSP

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

6.2.7 Private key storage on cryptographic module

Private keys for CA, TSA and OCSP

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

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

6.2.8 Method for activating private keys

Private keys for CA

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

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

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

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

Private keys for OCSP services

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

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

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

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

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

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

6.2.9 Method of deactivating private key

See section 6.2.8.

6.2.10Method of destroying private key

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

See section 6.2.7.

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

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

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

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

6.2.11Capabilities and Rating of the Cryptographic Module

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

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

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

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and key pair usage periods

The ZETES TSP CA for TSA will not issue certificates that exceed the certificate expiration date of the CA certificate.

The key usage period of a CA key is aligned with the expiration date / lifetime of the certificates issued with that key.

6.4 Activation data

Activation data for the CA, TSA and for OCSP

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

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

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

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

6.5 Computer security controls

ZETESCONFIDENS ensures that computer security controls are implemented according the technical standard ETSI EN 319 411-2. ZETES operates its both sites involved with TSP activities according ISO 27001 requirements. The Implemented Information Security Management System includes several controls related to computer security and a.o. :

- Firewalls to protect the ZETESCONFIDENS internal network domain from unauthorized access and to prevent all accesses and protocols that are not required for the operation of the TSP
- Control of sensitive data stored on "demobilized" or reusable storage device
- Local network components are kept in a secure environment and their configuration is periodically checked
- Use of multifactor authentication for account capable to issue certificates
- Enforced access control to modify disseminated information regarding Qualified Certificates. The site for dissemination provides https protocol for read access (see section 2)
- Enforced access control to modify revocation status information through a mutual SSL authentication between the CA and the OCSP server and between CA and the CRL publication infrastructure.
- Access control, intrusion detection system and CCTV monitoring to detect, record and react upon unauthorized physical access to its resources

6.6 Life cycle technical controls

6.6.1 System development controls

Implemented in compliance with ETSI EN 319 411

6.6.2 Security management controls

Implemented in compliance with ETSI EN 319 411

6.6.3 Life cycle security controls

Implemented in compliance with ETSI EN 319 411

6.7 Network security controls

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

The network segment for the ZETES TSP CA for TSA servers

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

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

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

Detailed description of the network security controls is available in internal confidential documents of ZETESCONFIDENS and/or Zetes.

6.8 Time-stamping

ZETESCONFIDENS operates as a Time-Stamping Authority. See the applicable Time-stamp Policy.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

Overview of the ZETES TSP CA for TSA hierarchy

ZETES TSP Root CA 001

| Subject serialNumber = 001
| certificate serial number = 02 54 1A A9 50 D7 CE 1F
| SHA1 thumbprint = 37 53 D2 95 FC 6D 8B C3 9B 37 56 50 BF FC 82 1A ED 50 4E 1A
|
---- **ZETES TSP CA FOR TSA 001**
Subject serialNumber = 001
certificate serial number = 2E 31 E4 74 F6 05 91 BA
SHA1 thumbprint = 37 02 B9 F1 77 AF AA 8D 07 7C 06 C3 E4 94 82 C5 A1 75 D3 2C

Note: the TSU Certificate profiles are provided in the applicable Time-stamp Policy.

Certificate profile for the ZETES TSP CA FOR TSA 001

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

certificate profile **ZETES TSP CA FOR TSA 001- root-signed CA certificate** version 1.0			
ATTRIBUTES			
Version		-	**0x02** *(= X.509 certificate version 3)*
Serial Number		-	**2E 31 E4 74 F6 05 91 BA**< 64-bit random number > compliant with CA/B Forum requirements, validated to ensure uniqueness of the certificate serial number, compliant with RFC 5280 and X.690
Signaturealgorithm	**algorithm**	-	**sha256WithRSAEncryption**
Signature Value		-	< the signature created by the CA >
SubjectPublicKeyInfo	**algorithm**	-	**RSA4096**
	subjectPublicKey	-	value of the public key
Validity	**notBefore**	-	19/10/2017 (19 October 2017)
	notAfter	-	19/10/2035 (19 October 2035)
Issuer	**serialNumber**	-	**001** (*the 3-digit serial number of ZETES TSP ROOT CA 001*)
	commonName	-	**ZETES TSP ROOT CA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
Subject	**serialNumber**	-	**001** (*the 3-digit serial number of ZETES TSP CA for TSA 001*)
	commonName	-	**ZETES TSP CA FOR TSA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**

EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	keyIdentifier	-	**38 BC 5C 30 54 DC E2 BB 20 EF EE 6F 41 A0 31 6E 5C FD 8B 75**
authorityInfoAccess	accessMethod	-	Id-ad-2 OID 1.3.6.1.5.5.7.48.2 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) caIssuers(2)}
	accessLocation	-	**http://crt.tsp.zetes.com/ZETESTSPROOTCA001.crt**
	accessMethod	-	Id-ad-1 OID 1.3.6.1.5.5.7.48.1 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
	accessLocation	-	**http://ocsp.tsp.zetes.com**
CRLDistributionPoint	distributionPointName	-	-
	fullname	-	**http://crl.tsp.zetes.com/ZETESTSPROOTCA001.crl**
EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	keyIdentifier	-	**2D 51 4B 49 DB 84 2D B0 4D 2B E8 05 38 53 A9 E5 BE 1F B7 45**
EXTENSIONS -- Policy Properties			
keyUsage	KeyCertSign	c	True
	CRLSign	c	True
certificatePolicies	policyIdentifier	-	**OID=2.5.29.32.0 [AnyPolicy]**
	policyQualifierID	-	Id-qt-1 (**CPS**)
	qualifier	-	**https://repository.tsp.zetes.com**
	policyQualifierID	-	Id-qt-2 (**User Notice**)
	DisplayText	-	**ZETES TSP CPS for Time-stamping**
basicConstraints	subjectType	c	**CA** (CA=true)
	pathLengthConstraint	c	**0**

Certificate profile for TSU for qualified time-stamps

Table 2 ZETES TSP CA FOR TSA 001 - Certificate Profile for TSU for qualified time-stamps

certificate profile **ZETES TSP CA FOR TSA 001 - TSU certificate for qualified time-stamps** version 1.0			
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**	-	< signature algorithm used by the CA >
Signature Value		-	< the signature created by the CA >
SubjectPublicKeyInfo	**algorithm**	-	**RSA or elliptic curve compliant with ETSI TS119 312 recommendations**
	subjectPublicKey	-	value of the public key
Validity	**notBefore**	-	Start date of the certificate
	notAfter	-	Expiration date of the certificate
Issuer	**serialNumber**	-	**001** (*the 3-digit serial number of the CA*)
	commonName	-	**ZETES TSP CA for TSA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
Subject	**commonName**	-	unique name of the TSU, the name may include indicators as to the type of certificate, e.g. contain the text "RSA" or "Qualified"
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	**keyIdentifier**	-	unique key identifier of the CA key
authorityInfoAccess	**accessMethod**	-	Id-ad-2 OID 1.3.6.1.5.5.7.48.2 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) caIssuers(2)}
	accessLocation	-	**http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt**
	accessMethod	-	Id-ad-1 OID 1.3.6.1.5.5.7.48.1 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
	accessLocation	-	**http://ocsp.tsp.zetes.com**
CRLDistributionPoint	**distributionPointName**	-	-
	fullname	-	**http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl**

EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	**keyIdentifier**	-	Unique identifier of the subject key
EXTENSIONS -- Policy Properties			
keyUsage	**digitalSignature**	c	True
certificatePolicies	**policyIdentifier**	-	**OID = 0.4.0.194112.1.1 (for certificates issued > 08/05/2020)** **OID=1.3.6.1.4.1.47718.2.1.2.50**
	policyQualifierID	-	Id-qt-1 (**CPS**)
	Qualifier	-	**https://repository.tsp.zetes.com**
	policyQualifierID	-	Id-qt-2 (**User Notice**)
	DisplayText	-	**ZETES TSP Qualified certificate for time-stamping compliant with ETSI TS 319 421.**
basicConstraints	**subjectType**	c	end entity
extendedKeyUsage	**timeStamping**	c	True
QCStatements	**esi4-qcStatement-1**	-	True (EU qualified certificate)
	esi4-qcStatement-5	-	URL pointing to the PKI Disclosure Statement repository – language “en”

Certificate profile for TSU for non-qualified time-stamps

Table 3 ZETES TSP CA FOR TSA 001 - Certificate Profile for TSU for non-qualified time-stamps

certificate profile **ZETES TSP CA FOR TSA 001- TSU certificate for non-qualified time-stamps** version 1.0			
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**	-	< signature algorithm used by the CA >
Signature Value		-	< the signature created by the CA >
SubjectPublicKeyInfo	**algorithm**	-	**RSA or elliptic curve compliant with ETSI TS119 312 recommendations**
	subjectPublicKey	-	value of the public key
Validity	**notBefore**	-	Start date of the certificate
	notAfter	-	Expiration date of the certificate
Issuer	**serialNumber**	-	**001** (*the 3-digit serial number of the CA*)
	commonName	-	**ZETES TSP CA for TSA 001**
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
Subject	**commonName**	-	unique name of the TSU, the name may include indicators as to the type of certificate, e.g. contain the text "RSA" or "Qualified"
	organizationName	-	**ZETES SA (VATBE-0408425626)**
	countryName	-	**BE**
EXTENSIONS -- Authority Properties			
authorityKeyIdentifier	**keyIdentifier**	-	unique key identifier of the CA key
authorityInfoAccess	**accessMethod**	-	Id-ad-2 OID 1.3.6.1.5.5.7.48.2 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) caIssuers(2)}
	accessLocation	-	**http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt**
	accessMethod	-	Id-ad-1 OID 1.3.6.1.5.5.7.48.1 {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) ad(48) ocsp(1)}
	accessLocation	-	**http://ocsp.tsp.zetes.com**
CRLDistributionPoint	**distributionPointName**	-	-
	fullname	-	**http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl**

EXTENSIONS -- Subject Properties			
subjectKeyIdentifier	**keyIdentifier**	-	Unique identifier of the subject key
EXTENSIONS -- Policy Properties			
keyUsage	**digitalSignature**	c	True
certificatePolicies	**policyIdentifier**	-	**OID=1.3.6.1.4.1.47718.2.1.2.50**
	policyQualifierID	-	Id-qt-1 (**CPS**)
	Qualifier	-	**https://repository.tsp.zetes.com**
	policyQualifierID	-	Id-qt-2 (**User Notice**)
	DisplayText	-	**ZETES TSP Qualified certificate for time-stamping compliant with ETSI TS 319 421.**
basicConstraints	**subjectType**	c	end entity
extendedKeyUsage	**timeStamping**	c	True

7.2 CRL profile

Generic CRL profile for consolidated CRL:

The CRL publication frequency is 7 days.

Table 4 ZETES TSP CA FOR TSA 001 - CRL profile

CRL profile **ZETES TSP CA FOR TSA 001 - CRL** version 1.0				
ATTRIBUTES				
Version		-	MS	**2**
Signaturealgorithm	**algorithm**	-	MS	**sha256WithRSAEncryption**
		-	MD	< the signature created by ZETES TSP CA FOR TSA 001 >
Issuer	**serialNumber**	-	MS	**001** (*the 3-digit serial number of the CA*)
	commonName	-	MS	**ZETES TSP CA FOR TSA 001**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
thisUpdate		-	MS	<time of issue >
nextUpdate		-	MS	<time of issue + CRL publication frequency>
Revoked Certificates	**userCertificate**	-	MD	<certificate serial number>
	revocationDate	-	MD	<revocation time>
	crlEntryExtension reasonCode	-	MD	<reason for revocation>
CRL EXTENSIONS				
Authority Key Identifier		-	MS	SHA1 of the public key of the CA
CRL Number		-	MD	assigned by the CA

7.3 OCSP certificate profile

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

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

certificate profile **ZETES TSP CA for TSA - OCSP responder certificate**				
ATTRIBUTES				
Version		-	MS	**0x02** (= X.509 certificate version 3)
Serial Number		-	MD	< 64-bit random number > (compliant with CA/B Forum requirements), validated to ensure uniqueness of the certificate serial number, compliant with RFC 5280 and X.690
Signaturealgorithm	**algorithm**	-	MS	**sha256WithRSAEncryption**
Signature Value		-	MD	< the signature created by ZETES TSP CA FOR TSA 001 >
SubjectPublicKeyInfo	**algorithm**	-	MS	**RSA2048**
	subjectPublicKey	-	MD	< value of the public key >
Validity	**notBefore**	-	MS	< certificate validity start date >
	notAfter	-	MS	< certificate validity end date >
Issuer	**serialNumber**	-	MS	**001** (*the 3-digit serial number of the ZETES TSP QUALIFIED CA 001*)
	commonName	-	MS	**ZETES TSP CA FOR TSA 001**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
Subject	**commonName**	-	MS	**ZETES TSP CA for TSA 001 OCSP responder**
	organizationName	-	MS	**ZETES SA (VATBE-0408425626)**
	countryName	-	MS	**BE**
EXTENSIONS -- Authority Properties				
authorityKeyIdentifier	**keyIdentifier**	-	MS	SHA-1 hash of the public key of the CA (as specified in RFC 5280)
EXTENSIONS -- Subject Properties				
subjectKeyIdentifier	**keyIdentifier**	-	MD	4-bit value 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	MS	true
enhancedKeyUsage	**OCSP Signing**	c	MS	true
OCSPNoCheck		-	MS	null

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Besides the supervision by the Belgian Supervisory Body (FOD Economie, Algemene Directie Kwaliteit en Veiligheid), ZETESCONFIDENS through its PMA organizes with regards to its CA activities a compliance audit to ensure that it meets requirements, standards, procedures and service levels according to this CPS.

8.1 Frequency or circumstances of assessment

ZETESCONFIDENS' Certificates issuance process for (Qualified) Time-stamping and related services will be audited annually for compliance with

- the present CPS and appropriate CP's.
- the technical standards ETSI 319 401, ETSI 319 411-1 and 2, ETSI 319 421 and ETS 319 422

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

8.2 Identity/qualifications of assessor

Compliance audits will be performed by a Conformity Assessment Body as defined in point 13 of article 2 of Regulation EC N°765/2008 and compliant with the CA/B Forum requirement for qualified auditors as per CA/Browser Forum version 1.4.9 (July 11, 2017) section 8.2.

8.3 Assessor's relationship to assessed entity

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

8.4 Topics covered by assessment

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

8.5 Actions taken as a result of deficiency

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

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

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

8.6 Communication of results

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

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

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

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

9 OTHER BUSINESS AND LEGAL MATTERS

The CP/CPS, the relevant TSA Practice Statement and Time-stamp Policy and the Subscriber Agreement constitute the main set of terms and conditions for the provision and use of ZETESCONFIDENS TSA offering. For example, they provide general information about the conditions of use of ZETESCONFIDENS Certificates, the rights and obligations of ZETESCONFIDENS, the Subscribers and Relying Parties, including the duration and termination conditions, their liability, the claim process, or the applicable law and jurisdiction.

The sections below provide useful information about certain terms and conditions governing the provision or use of ZETESCONFIDENS TSA offering.

9.1 Fees

Commercial agreement are discussed and agreed case by case with every Subscriber before Subscriber Agreement can be signed. See applicable TSA Practice Statement and Time-Stamp Policy for more details.

9.2 Financial responsibility

9.2.1 Insurance coverage

Each PKI Participant not being a Subscriber or a Relying Party of the ZETES TSP CA for TSA shall contract an insurance policy covering the risks identified in the insurance policy with respect to their services and maintain a sufficient amount of insurance coverage for its liabilities to other Participants, including Subscribers and Relying Parties.

The liability of ZETES TSP CA for TSA towards the Subscriber or a Relying Party may be limited according to the applicable CP and TSA Practice Statement and Time-stamp Policy.

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 ZETES TSP CA for TSA offering under this Certification Practice Statement and elsewhere in its Agreements.

9.2.3 Insurance or warranty coverage for end-entities

Not applicable.

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 ZETESCONFIDENS at the time of its subscription.

- the Subscriber's or Relying Parties' confidential information supplied to ZETESCONFIDENS in support requests
- the private key(s) of Certificates

9.3.2 Information not within the scope of confidential information

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

- the information published in a ZETES TSP CA for TSA issued Certificate
- the revocation records of a Certificate
- this Certification Practice Statement and Certificate Policy

9.3.3 Responsibility to protect confidential information

ZETESCONFIDENS and Subscriber Obligations of Confidentiality are described in the present CP and relevant TSA Practice Statement and Time-stamp Policy.

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

The ZETES TSP CA for TSA operates within the boundaries of the Belgian Law of 30 July 2018 on Privacy Protection in relation to the Processing of Personal Data, and the General Data Protection regulation (EU) N ° 679/2016. And conform the Law of 13 June 2005 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

The ZETES TSP CA for TSA does not store any personal data on certificates.

For the purpose of providing the Services under the Agreement between ZETESCONFIDENS and the Subscriber, the Subscriber is the data controller and ZETESCONFIDENS is the data processor. The Subscriber acknowledges that ZETESCONFIDENS processes any personal data in the frame of the Services under the Subscriber's responsibility, and that the legal obligations to inform data subjects (i.e. Subjects) and to notify national data protection authorities are the Subscriber's.

See applicable Subscriber Agreement and Time-stamp Policy for further details.

9.4.1 Privacy plan

9.4.1.1 ZETESCONFIDENS shall:

a) If any, only process personal data on behalf of the Subscriber and according to the purposes communicated by and the instructions of the Subscriber;

b) treat all personal data as confidential in accordance with Section 9.3, unless the Subscriber's determines otherwise;

c) take adequate technical and Organizational measures ensuring the security of the processing of personal data in line with the Belgian Act on the protection of privacy with respect to the processing of personal data and the General Data Protection Regulation (hereinafter Personal Data Protection Acts);

d) provide the Subscriber the opportunity to appropriately assess the adequacy of the implemented technical and Organizational measures mentioned under (c);

e) notify the Subscriber as soon as possible of any request made by a data subject relating to the processing of his personal data;

f) duly assist the Subscriber in handling any reasonable request or complaint of a data subject relating to the processing of his personal data where whole or part of the processing is done by ZETESCONFIDENS;

g) refrain from transferring any personal data to sub-contractors or other third parties without the express permission of the Subscriber;

h) refrain from transferring any personal data outside the European Economic Area without the express permission of the Subscriber;

i) subject to the limitations set out elsewhere in this CP/CPS or in the Subscriber agreement, indemnify the Subscriber for any liability caused by processing personal data in breach of the provisions of this Section or its legal obligations as a data processor.

9.4.1.2 ZETESCONFIDENS warrants that:

a) the technical and Organizational measures offer an appropriate level of protection in proportion to the risks involved against the accidental or unauthorised destruction, loss, alteration or access to personal data or any other form of unauthorised processing of personal data;

b) its personnel shall only have access to personal data insofar the access is necessary for performing their duties in providing the Services;

c) its personnel charged with the processing of personal data have been duly informed of the applicable obligations under the Personal Data Protection Act and their obligations under this Clause.

9.4.1.3 The Subscriber shall:

a) inform ZETES TSP in a clear and comprehensive manner of the intended purposes of the processing and provide clear and comprehensive directions regarding the extent to which ZETES TSP can access and use personal data;

b) indemnify ZETES TSP for any liability which is the direct result of processing personal data in line with the directions of the Subscriber.

9.4.2 Information treated as private

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.3 Information not deemed private

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.4 Responsibility to protect private information

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.5 Notice and consent to use private information

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.6 Disclosure pursuant to judicial or administrative process

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.4.7 Other information disclosure circumstances

Refer to the intro text of Section 9.4 and Section 9.4.1.

9.5 Intellectual property rights

Any and all intellectual property rights ("IPR") (including title, ownership rights, database rights, and any other intellectual property rights) in ZETESCONFIDENS TSA 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 in respect of ZETESCONFIDENS TSA offering other than those expressly granted under this Certification Practice Statement, the TSA Paractice Statement and Time-stamp Policy or elsewhere in the Subscriber Agreement.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Zetes SA acting as CSP through its ZETES TSP CA for TSA issues X509 v3-compatible Certificates (ISO 9594-8).

ZETES TSP CA for TSA issues Certificates compliant with ETSI EN 319 411 requirements. To this end, the CA publishes the elements supporting this statement of compliance.

ZETESCONFIDENS guarantees that all the requirements set out in the present CPS/CP (and indicated in the Certificate in accordance with Section 7) are complied with.

The sole guarantee provided by ZETESCONFIDENS acting as CSP through ZETES TSP CA for TSA is that its procedures are implemented in accordance with the CPS and the verification procedures then in effect, and that all Certificates issued with a CP Object Identifier (OID) have been issued in accordance with the relevant provisions of the present CP, the verification procedures, and the CPS as applicable at the time of issuance.

9.6.2 RA representations and warranties

9.6.3 Subscriber representations and warranties

The Subscriber agrees to the CPS/CP and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the CPS and the present CP, the TSA Practice Statement and Time-stamp Policy.

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 Time-stamp.
- the validation of a ZETESCONFIDENS Certificate by using the 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

ZETESCONFIDENS warrants that it operates the Dissemination and Repository Services, and the Revocation Management Services and the Revocation Status Information Services in conformity with the CPS.

9.7 Disclaimers of warranties

Except as expressly provided elsewhere in the CP/CPS, in the TSA Practice Statement and Time-stamp Policy or 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 "non repudiation" of any Certificate or message. 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 beyond proven direct damages as described below.

In case of liability of ZETESCONFIDENS towards the Subscriber or a Relying Party for proven direct damages, the liability of ZETESCONFIDENS towards any claimant is in any way limited to:

- paying damages amounting up to a maximum of 2500 € per transaction, for events where the Relying Party relies on that certificate:

a) as regards the accuracy at the time of issuance of all information contained in the (Qualified) Certificate and as regards the fact that the Certificate contains all the details prescribed for a (Qualified) Certificate; or

b) for assurance that at the time of the issuance of the Certificate, the signatory identified in the Qualified Certificate held the private key corresponding to the public key given or identified in the Certificate; or

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

and

- paying damages amounting up to a maximum of 10.000 € in total per TSU Certificate that is underlying to the claim.

In any case, whatever originating facts and prejudices and their aggregate amounts, ZETESCONFIDENS responsibility will be limited to the amount paid by the Subscriber to ZETESCONFIDENS regarding the originating fact, with respect to the governing law. Unless otherwise legally enacted, any suit from the Subscriber regarding these CP will take place no longer than six months after the fact originating the legal action.

9.9 Indemnities

ZETESCONFIDENS is allowed to ask the Subscriber for indemnities if the Subscriber does not respect the agreement with ZETESCONFIDENS.

9.10 Term and termination of the present CPS

9.10.1Term

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

9.10.2Termination

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

9.10.3Effect 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 CP or the CPS shall be in writing and shall be sent, except provided explicitly in the CP, 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 electronic document or electronic message with an advanced electronic signature or a qualified electronic signature and be addressed to the contact information mentioned in chapter 1.5.2.

9.12 Amendments to the present CPS

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 CP/CPS.

The only changes that the PMA may make to these CP/CPS specifications without notification are minor changes that do not affect the assurance level of this CP/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 CP/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

For a non minor modification, the new CP/CPS will be published for comments, which an indication of the proposed effective date.

When a new version of the CP/CPS is published, all the Subscribers and Relying Parties of the ZETESCONFIDENS TSA Offering are informed of the nature, the time and the date of change, through a publication on ZETESCONFIDENS repository web site.

At the end of the comment period, the PMA can decide to publish the new CP, the restart the amendment process with a new version or to withdraw the proposed version.

Unless otherwise stated, the new version of the CP/CPS will take effect 14 working days after its publication and will remain in effect until a new version takes effect.

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

All disputes associated with the CP/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 CP/CPS (without giving effect to any conflict of law provision that would cause the application of other laws).

9.15 Compliance with applicable law

The present CPS and provision of CA certification services are compliant to relevant and applicable laws of Belgium (including the directly applicable Regulation (EU) No 910/2014).

9.16 Miscellaneous provisions

No stipulations.

9.17Other provisions

Not applicable.

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