ZETESCONFIDENS

TRUST SERVICES PRACTICE STATEMENT

Publication date :	**26/09/2019**	
Effective date :	**30/09/2019**	
Practice Statement OID :	**[1.3.6.1.4.1.47718].[2.0.1].[1]**	
Version :	**1.0**	**25/09/2019**

Table of Content

ABOUT THIS DOCUMENT **5**

ABOUT ZETES **6**

1 INTRODUCTION **7**
1.1 Conformity with EU legislation and standards for TSP 7
1.2 Document name and identification 7
1.3 PKI management 7
1.3.1 ZetesConfidens Policy Management Authority (PMA) 7
1.4 Certificate usage 8
1.5 Policy administration 8
1.5.1 Organisation administering the document 8
1.5.2 Contact person 8
1.5.3 Person determining suitability for the policy 9
1.5.4 Approval procedures 9
1.6 Definitions and acronyms 10
1.6.1 Acronyms 10
1.6.2 Definitions 10

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES **12**
2.1 Repositories 12
2.2 Publication of certification information 13
2.3 Time or frequency of publication 13
2.4 Access controls on repositories 13

3 IDENTIFICATION AND AUTHENTICATION **14**

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS **14**

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS **14**
5.1 Physical controls 14
5.1.1 Site location and construction 14
5.1.2 Physical access 14
5.1.3 Power and air conditioning 14
5.1.4 Water exposures 14
5.1.5 Fire prevention and protection 14
5.1.6 Media storage 15
5.1.7 Waste disposal 15
5.1.8 Off-site backup 15
5.2 Procedural controls 15
5.2.1 Trusted roles 15
5.2.2 Number of persons required per task 16
5.2.3 Identification and authentication for each role 16
5.2.4 Roles requiring separation of duties 16
5.3 Personnel controls 16
5.3.1 Qualifications, experience, and clearance requirements 16
5.3.2 Background check procedures 16
5.3.3 Training requirements 16
5.3.4 Retraining frequency and requirements 17
5.3.5 Job rotation frequency and sequence 17
5.3.6 Sanctions for unauthorized actions 17
5.3.7 Independent contractor requirements 17
5.3.8 Documentation supplied to personnel 17
5.4 Audit logging procedures 17
5.4.1 Types of events recorded 17
5.4.2 Frequency of processing log 18
5.4.3 Retention period for audit log 18
5.4.4 Protection of audit log 18
5.4.5 Audit log backup procedures 18
5.4.6 Audit collection system (internal vs. external) 18

5.4.7 Notification to event-causing Subject 19
5.4.8 Vulnerability assessments 19
5.5 Records archival 19
5.5.1 Types of records archived 19
5.5.2 Retention period for archive 19
5.5.3 Protection of archives 19
5.5.4 Archive backup procedures 19
5.5.5 Requirements for time-stamping of records 19
5.5.6 Archive collection system 20
5.5.7 Procedures to obtain and verify archive information 20
5.6 Key changeover 20
5.7 Compromise and disaster recovery 21
5.7.1 Incident and compromise handling procedures 21
5.7.2 Computing resources, software and/or data are corrupted 21
5.7.3 Entity private key compromise procedures 21
5.7.4 Business continuity capabilities after a disaster 21
5.8 CA or RA termination 22

6 TECHNICAL SECURITY CONTROLS 23
6.1 Key pair generation and installation 23
6.1.1 Key pair generation 23
6.1.2 Private key delivery to Subscriber or Subject 23
6.1.3 Public key delivery to certificate issuer 23
6.1.4 CA public key delivery to Relying Parties 24
6.1.5 Key sizes 24
6.1.6 Public key parameters generation and quality checking 25
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 25
6.2 Private Key Protection and Cryptographic Module Engineering Controls 26
6.2.1 Cryptographic module standards and controls 26
6.2.2 Private key multi-person control 26
6.2.3 Private key escrow 26
6.2.4 Private key backup 27
6.2.5 Private key archival 27
6.2.6 Private key transfer into or from a cryptographic module 27
6.2.7 Private key storage on cryptographic module 28
6.2.8 Method for activating private keys 28
6.2.9 Method of deactivating private key 29
6.2.10 Method of destroying private key 29
6.2.11 Capabilities and Rating of the Cryptographic Module 29
6.3 Other aspects of key pair management 29
6.3.1 Public key archival 29
6.3.2 Certificate operational periods and key pair usage periods 29
6.4 Activation data 29
6.5 Computer security controls 30
6.6 Life cycle technical controls 31
6.6.1 System development controls 31
6.6.2 Security management controls 31
6.6.3 Life cycle security controls 31
6.7 Network security controls 31
6.8 Time-stamping 31

7 CERTIFICATE, CRL, AND OCSP PROFILES 32

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 32
8.1 Frequency or circumstances of assessment 32
8.2 Identity/qualifications of assessor 32
8.3 Assessor's relationship to assessed entity 32
8.4 Topics covered by assessment 32
8.5 Actions taken as a result of deficiency 33
8.6 Communication of results 33

9 OTHER BUSINESS AND LEGAL MATTERS 34

9.1 Fees 34
9.2 Financial responsibility 34
9.2.1 Insurance coverage 34
9.3 Confidentiality of business information 34
9.3.1 Scope of confidential information 34
9.3.2 Information not within the scope of confidential information 34
9.3.3 Responsibility to protect confidential information 34
9.4 Privacy of personal information 34
9.5 Intellectual property rights 36
9.6 Representations and warranties 36
9.6.1 RA representations and warranties 36
9.6.2 Subscriber and Subject representations and warranties 36
9.6.3 Relying party representations and warranties 36
9.7 Disclaimers of warranties 36
9.8 Limitations of liability 36
9.9 Indemnities 37
9.10 Term and termination of the present TSPS 37
9.10.1 Term 37
9.10.2 Termination 37
9.10.3 Effect of termination and survival 37
9.11 Individual notices and communications with participants 38
9.12 Amendments to the present TSPS 38
9.12.1 Procedure for amendment 38
9.12.2 Notification mechanism and period 38
9.12.3 Circumstances under which OID must be changed 38
9.13 Dispute resolution provisions 38
9.14 Governing law 38
9.15 Compliance with applicable law 38
9.16 Miscellaneous provisions 39
9.17 Other provisions 39

ABOUT THIS DOCUMENT

Scope

This document is the Trust Services Practice Statement (TSPS) for the ZetesConfidens trust services operations as a whole. This Practice Statement applies to the common practices in delivering Trust Services such as

- certificate issuance services
- certificate status services
- signature creation services and seal creation services
- timestamp services

Intellectual Property Rights

Document Version History

Version	Publication Date	Effective Date	Information about this Version
1.0	26/09/2019	30/09/2019	first publication ----------

ABOUT ZETES

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

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

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

Zetes NV/SA is registered in Belgium as follows:

In Dutch:	In French:
Zetes NV Straatsburgstraat 3 1130 Brussel België KBO 0408.425.626 BTW BE 0408 425 626	**Zetes SA** 3, Rue de Strasbourg 1130 Bruxelles Belgique BCE 0408.425.626 TVA BE 0408 425 626

1 INTRODUCTION

1.1 Conformity with EU legislation and standards for TSP

Where applicable ZetesConfidens follows 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; and the implementing and delegated acts.

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

ETSI EN 319 411-1	Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements
ETSI EN 319 411-2	Policy and Security Requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing Qualified Certificates
ETSI EN 319 421	Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI TS 119 431-1	Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD /SCDev
ETSI TS 119 431-2	Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation.
ETSI TS 119 432	Protocols for remote digital signature creation
CEN EN 419 241-1	General System Security Requirement

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

1.2 Document name and identification

This document is called the 'ZetesConfidens – Trust Services Practice Statement'.

The unique OID for this Practice Statement is: [1.3.6.1.4.1.47718].[2.0.1].[1].

1.3 PKI management

1.3.1 ZetesConfidens Policy Management Authority (PMA)

The PMA has overall responsibility for the TSP Services. The PMA includes senior members of management as well as staff responsible for the operational management and operational security of the trust services environment.

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

(a) Approving the Trust Services infrastructure and practices.
(b) Approving the Practice Statements and the Policies.
(c) Defining the review process for, including responsibilities for maintaining, the Practice Statements and the Policies
(d) Defining the review process that ensures that applicable Policies are supported by the Practice Statement(s).

(e) Defining the review process that ensures that the Trust Services authorities, such as the Certification Authority and the Time Stamping Authority, as well as all component services, properly implement the applicable practices, policies and procedures.
(f) Authorising part or all component services of the Trust Services to be provided and/or operated by third parties and setting the applicable terms and conditions.
(g) Publication to the Subscribers and Relying Parties of the relevant declaration of practices and of policies.
(h) Continually and effectively managing Trust Services related risks. This includes a responsibility to periodically re-evaluate risks to ensure that the controls that have been defined remain appropriate, and a responsibility to periodically review the controls as implemented, to ensure that they continue to be effective.
(i) Approving cross-certification or mutual recognition procedures and handling related requests.
(j) Defining internal and external auditing processes with the aim to ensure the proper implementation of the applicable practices, policies and procedures.
(k) Initiating and supervising internal and external audits.
(l) Executing the audit recommendations.
(m) Actions to ensure the proper execution of the above responsibilities.
(n) Defining the scope of the Trust Services offering.
(o) Ensuring that practices for each of the above-mentioned entities are defined and implemented in a manner that is consistent with this document;
(p) Mediating in disputes involving Subscribers and/or entities that have been registered by the RA and the entities that have been implemented by or under the responsibility of the TSP.
(q) Initiating when appropriate highly sensitive operations such as CA root key revocation and renewal or termination of the Trust Services.

1.4 Certificate usage

See the applicable Practice Statement and Policy documentation for the specific Trust Service.

1.5 Policy administration

1.5.1 Organisation administering the document

Practice Statements and Policies are administered by the Policy Management Authority (PMA).

1.5.2 Contact person

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

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

1.5.3 Person determining suitability for the policy

The PMA collectively determines the suitability of the Practice Statement documents and Policy documents.

1.5.4 Approval procedures

The PMA collectively determines the suitability of the Practice Statement documents and Policy documents.

A Change Control mechanism will be used to trace all identified changes to the content of the documents.

Practice Statement documents and Policy documents shall be reviewed at least once per year and when major changes are required.

Minor changes, errors or minor updates to Practice Statement documents and Policy documents shall be communicated to the Policy Management Authority.

1.6 Definitions and acronyms

1.6.1 Acronyms

ARL	Authority Revocation List
CA	Certificate Authority
CP	Certificate Policy
CSP	Certificate Service Provider
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CTC	Certificate Terms and Conditions
DN	Distinguished Name
HSM	Hardware Security Module
IDP	Identity Provider
LRA	Local Registration Authority
LSRA	Local Suspension and Revocation Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PMA	Policy Management Authority
QSCD	Qualified Signature Creation Device
RA	Registration Authority
SRA	Suspension and Revocation Authority
SUB-RA	subordinate Registration Authority
SUB-SRA	subordinate Suspension and Revocation Authority
TSA	Time Stamp Authority
TSP	Trust Service Provider
TSPS	Trust Services Practice Statement
TSU	Time Stamp Unit

1.6.2 Definitions

Activation Data	Data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorised use of the private key.
Certificate	A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.
Certificate Revocation List	A signed list of identifiers of Certificates that have been revoked. Abbreviated as CRL. It is (periodically) made available by the CA to Subscribers and Relying Parties.
Hardware Security Module (HSM)	Hardware Security Module. An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.
Normalized Certificate	A Certificate, issued under the policy and security requirements for TSPs issuing certificates as defined in ETSI EN 319 411 – Part 1, whereby the certification authority *may* support the same level of quality as for issuing Qualified Certificates, but "normalized" for wider applicability and for ease of alignment. The standard is

	applicable to the general requirements of certification in support of cryptographic mechanisms, including the general use of cryptography for authentication and encryption.
Qualified Certificate	A Certificate which meets the requirements laid down in Regulation (EU) No 910/2014 and Annex I thereof and is provided by a Qualified Trust Service Provider who fulfils the requirements laid down in the Regulation. The Regulation distinguishes between Qualified Certificates for different purposes: electronic signature, electronic seals, or website authentication. In the context of this *Certification Practice Statement*, the term Qualified Certificate will only reference to "qualified certificates for electronic signature" under the Regulation.
Relying party	In the context of this *Certification Practice Statement*, Relying Parties are as defined in section **Error! Reference source not found.**.
Secure Cryptographic Device	The Secure Cryptographic Devices may come in different form such as e.g. an ID-1 size smartcard, a SIM- size smartcard or a USB device (similar in shape to a USB memory stick), etc. The Secure Cryptographic Device provides some or all of the following functions: • generating electronic signatures over previously externally calculated hash values, • generating keys inside the device • importing keys into the device • the device is able to protect the secrecy of the stored private key, • the device restricts the usage of the key to the authorised owner only by means of a PIN code or an equivalent authentication mechanism such as biometric Match on Card For the purpose of a Qualified Electronic Signature (QES) with a certificate that adheres to the policy [QCP-n-qscd], the Secure Cryptographic Device complies with the following requirements for a Qualified Signature Creation Device (QSCD) as specified in Regulation (EU) No 910/2014 -- Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (eIDAS): • The Secure Cryptographic Device complies with the conditions defined in Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014. • Specifically, the Secure Cryptographic Device has passed security certification in compliance with ETSI EN 419211-2:2013 — Protection profiles for secure signature creation device — Part 2: Device with key generation and ETSI EN 419211-4:2013 — Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted channel to certificate generation application. Note: the term "SSCD" or "Secure Signature Creation Device" is deprecated as of 1st July 2016.
Subscriber	In the context of this *Trust Services 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, Subjects and Relying Parties.

The CA certificates and certificate status information are 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(s)://tsp.zetes.com **http(s)://confidens.zetes.com**	The main web site provides: • welcome page of the web site for ZetesConfidens • 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 for downloading documents such as the terms and conditions, certificate policies, etc. • a section for downloading CA certificates and certificate revocation lists (the URLs for these download pages are listed further down in this table) • a contact page
https://repository.tsp.zetes.com **https://repository.confidens.zetes.com** **https://pds.tsp.zetes.com** **https://pds.confidens.zetes.com**	Web services for downloading documents such as the Certificate Practice Statements, Certificate Policies, Public Disclosure Statements and Terms and Conditions.
http://crt.tsp.zetes.com **http://crt.confidens.zetes.com**	Web services for: 1. manual interactive download of CA certificates 2. automated direct download of CA certificates
http://crl.tsp.zetes.com **http://crl.confidens.zetes.com**	This URL refers to 1. a web page for manual download of ARL and CRL 2. a server for automated direct download of ARL and CRL
http://ocsp.tsp.zetes.com **http://ocsp.confidens.zetes.com**	This URL refers to the OCSP service for immediate online certificate status checks. The OCSP service is synchronised with the latest CRL to provide answers and checks the expiration before the revocation.

2.2 Publication of certification information

Availability

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

Planned maintenance periods will be announced on the web site 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 Subject certificates in a repository

Subject certificates may be published in a repository, depending on the applicable policy. Access to the repository may be restricted, depending on the applicable policy.

Publication of CA certificates in a repository

ZetesConfidens publishes its CA certificates in the public certificate repository. These certificates can be downloaded manually by means of a web browser or automatically by software applications. The fingerprint information for these certificates is stated in the Certification Practice Statement document for each CA.

Relying parties who wish to validate these values before installing the CA certificates, can obtain out-of-band confirmation via info@tsp.zetes.com.

Certificate Status Information

For more information, see section **Error! Reference source not found.** and the Certification Practice Statement a nd applicable Certificate Policy documents.

2.3 Time or frequency of publication

Publication of CA certificates in a repository

CA certificates will be published in the repository before end-entity certificates emanating from these CAs are made available to the Subjects. CA certificates remain available in the repository at least all certificates that were issued by the respective CA key have expired or have been revoked. In case of CA certificate renewal the latest certificate will replace the preceding certificate as the reference certificate in the repository.

Certificate Status Information

The CRLs or delta-CRLS are refreshed periodically before the respective CRL or delta-CRL is about to expire. CRLs or delta-CRLs and may be refreshed when certificates have been revoked. CRLs and delta-CRLs for issuing CAs will be available within 20 minutes after creation. CRLs and delta-CRLs are refreshed until all certificates that were issued by the respective CA key have expired or have been revoked, after which a final CRL is created.

Publication of terms and conditions, policies, etc.

Updates of public document such as Policy documents, Practice Statement documents or other public documents are published allowing 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 add resources in these repositories.

Subscribers, Subjects and Relying Parties have read-only access to public information. Access to Subject certificate repositories may be restricted or not available to the public, depending on the applicable policy.

ZetesConfidens will take reasonable measures to protect and prevent against abuse of the repositories and the OCSP service and will strive to give equal and unhindered access to all parties that show good faith and reasonable use.

3 IDENTIFICATION AND AUTHENTICATION

See the applicable Practice Statement and Policy documentation for the specific Trust Service.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

See the applicable Practice Statement and Policy documentation for the specific Trust Service.

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 Trust Services are hosted in sites that implement proper security controls, including access control, intrusion detection and CCTV. Access to the sites is limited to authorized personnel. The Trust Service zones within these sites are located in areas appropriate for high-security operations. These areas 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 trust service 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 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 data are also stored in a separate location that is physically secured 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 site / disaster recovery site located in separate site with similar protection measures. In case of adverse situation as a natural disaster, fire or act of terrorism, ZetesConfidens has implemented the necessary measures to recover its services according its legal and contractual requirements.

5.2 Procedural controls

5.2.1 Trusted roles

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

All members of the staff operating the key management operations, administrators, security officers, 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:

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

ZetesConfidens conducts and completes an initial investigation of all members of staff who are candidates to serve in trusted roles before they are admitted in their function. ZetesConfidens ensures that they to possess the necessary expertise, reliability, experience, and qualifications. They will have received training to bring awareness regarding security and personal data protection rules as appropriate for the offered services and the job function.

5.2.2 Number of persons required per task

Critical assets are protected by means of dual control or multiple controls. At least two trusted roles need to combine their respective assets and/or (split) knowledge to be able to perform critical operations.

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 either using MFA or under dual control supervision.

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 – Organisation"

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

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

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 regard to the Trust Services 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

ZetesConfidens with regard to the Trust Services activities makes available relevant technical training for their personnel to perform their functions. Training and credentials, or actual experience, or a combination of the two, will include security practices.

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. This shall include (at least every 12 months) updates on new threats and current security practices.

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 regard to the Trust Services 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 violation is evaluated by the PMA. The PMA ensures that the sanction taken is both appropriate and proportional to the violation.

5.3.7 Independent contractor requirements

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

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

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

5.3.8 Documentation supplied to personnel

ZetesConfidens with regard to the Trust Services activities makes available documentation to personnel, during initial training, retraining, or otherwise.

5.4 Audit logging procedures

5.4.1 Types of events recorded

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

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

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

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

- Issuance of a certificate: request, approval or rejection (with reason) of request, registration information, Identification of the RA approving or processing the request, certificate generation/activation.

- Revocation of a certificate: revocation request, approval or rejection (with reason) of request, Identification of the RA approving or processing the request, Identification of the requestor.
- Publishing of a CRL
- personalisation of the Secure Subject Device

The audit logs records contain:

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

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

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

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

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

5.4.5 Audit log backup procedures

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

5.4.6 Audit collection system (internal vs. external)

The PKI audit collection system is internal.

5.4.7 Notification to event-causing Subject

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

5.4.8 Vulnerability assessments

The entire infrastructure is subject of a vulnerability assessment at least every three months (with penetration testing at least once a year) and whenever a critical part of the infrastructure is affected. The assessment covers the ICT infrastructure, the special cryptographic equipment, the physical environment, data storage, software, personnel, processes and procedures and communication.

Vulnerability assessment of the audit log is part of the ZetesConfidens risk assessment and risk management program documented internally.

5.5 Records archival

5.5.1 Types of records archived

See section 5.4.1 and 5.5.2.

5.5.2 Retention period for archive

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

- issued certificates for a period of 7 years after the certificate ceases to be valid,
- audit trails on the issuance of certificates for a period of minimum 7 years after the certificate ceases to be valid,
- copies of identification documents are retained 7 years after any certificate based on these records ceases to be valid,
- audit trail of the revocation of a certificate for a period of minimum 7 years after revocation of the certificate,
- CRLs for at least 7 years after creation of the CRL,
- documentation supporting the issuance and use of the certificate is kept for a period of at least 10 years after the expiration of the last certificate supported by the documentation.

5.5.3 Protection of archives

The archives are protected against manipulation or wilful destruction. As far as possible archive will be retained and protected in electronic form.

Paper-based records are archived and under control of the respective roles that process them. Paper-based archive may be stored on multiple locations according the requirements laid down in the applicable Policy document. Registration information will be securely stored to provide reasonable assurance regarding secrecy, integrity and availability.

5.5.4 Archive backup procedures

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

5.5.5 Requirements for time-stamping of records

The date and time source for audit logs created by the core Trust Service components are synchronised with UTC using dedicated NTP equipment.

ZetesConfidens operates Stratum-1 multi-GNSS referenced NTP infrastructure to synchronize the system clocks of critical infrastructure with at least 3 of these external time references from UTC(ROB) from the public NTP services of the Royal Observatory of Belgium.

The Observatory maintains 4 of the atomic clocks of the worldwide UTC network and disseminates the time via the Network Time Protocol (ntp1.oma.be and ntp2.oma.be). As of May 2018 the Belgian legal time is by law aligned with Universal Time Coordinated (UTC). The legal time in Belgium is UTC+1h in winter and UTC+2h in summer.

The ZTS NTP infrastructures uses at least one of the following satellite navigation services as additional time source:

- GPST from the GPS satellite network
- GST from the Galileo satellite network (after 2021)
- GLONASST from the GLONASS satellite network

In the unlikely case that none of the external time sources are available, the NTP infrastructure can maintain accurate time independently by means of high-precision oscillators until at least one of the external time references is available again.

5.5.6 Archive collection system

The archive collection system for the Trust Service components operated by ZetesConfidens is internal infrastructure of ZetesConfidens. The archive collection system for Subordinate RA and the Local RA is done by the respective parties. ZetesConfidens as RA supervisor will assist these entities to create and maintain an archive for their activities.

5.5.7 Procedures to obtain and verify archive information

The contents of the archive are not accessible except for authorized personnel of 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.).

The Certificate Subject may access information related to his personal information and registration form by written request addressed to the ZetesConfidens Central RA Officer.

Disclosure of information from the archive upon request by an implicated party other than the Certificate Subject is at the discretion of 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 a CA key requires procedures to provide the new CA related information to Subjects and Relying Parties, following a re-key by the CA.

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

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

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

ZetesConfidens defined an incident management procedure including incident reporting and handling procedure.

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

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

5.7.2 Computing resources, software and/or data are corrupted

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

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

The distance between both locations is sufficient in case of a local natural disaster. The communication infrastructure and services between the two sites is sufficiently fast and secure to ensure data integrity and effective recovery point.

Disaster recovery infrastructure and procedures are to be fully tested at least once a year.

5.7.3 Entity private key compromise procedures

In case of a key compromise pertaining to a critical Trust Service component, ZetesConfidens will

- decommission the compromised key
- notify impacted parties
- 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 key and certificates to resume service.

In case of a key compromise pertaining to an end-entity, revocation shall be performed, and a new certificate shall be issued provided that the cause of compromise has been discarded. The end-entity (or the subscriber) has to notify ZetesConfidens of any compromise or suspicion of compromise of their private key. PKI participants' obligations are detailed in the applicable sections of the applicable CPS and CP.

5.7.4 Business continuity capabilities after a disaster

A Business Continuity Plan is in effect to ensure business continuity following a natural or other disaster.

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

Recovery of off-line Root CAs is ensured by the activation of the Root CA's backup at the secondary site. Resources and secrets are distributed across several sites to ensure that all the needed resources and secrets to continue the service will still be available in case one site is completely and definitely destroyed.

The PMA will assess the measures to be taken regarding taking into account the cause of the disaster and their effects, the protection of sensitive resources and information on the disabled site

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

5.8 CA or RA termination

Terminating a certification service and as a result terminating, when applicable, the CA(s) and other PKI component services is an event as important as their initiation. Both require planning of the physical, logical, operational, procedural and human aspects. Security of information and reputation is at risk. Furthermore, legal requirements apply.

For clarification, the cessation of the issuance of new Qualified Certificates by the ZetesConfidens Qualified CA while all other component services are kept under full normal operations, including the provision of certificate validity status information services (e.g. CRLs, OCSP services), is not in scope. Also, the controlled transfer of services and components from ZetesConfidens to another organisation 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 Qualified Certificates are terminated. The following is a summary of the minimum procedures that are applicable in such a case.

In the context of a scheduled termination:

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

In the context of an unscheduled termination:

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

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

6 TECHNICAL SECURITY CONTROLS

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation for CAs

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

Key pair generation for the OCSP service

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

Key pair generation for 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 PKI operators

The key pairs for RA operators and SRA operators are generated on-board a Secure Cryptographic Device, under the authority of the PMA, under supervision of a Security Officer and under dual control.

Key pair generation for Subjects

See the applicable CPS/CP. When no other information is given, the key pairs for Subjects are generated on-board a Secure Cryptographic Device such as a smartcard or HSM.

6.1.2 Private key delivery to Subscriber or Subject

See the applicable Practice Statement and Policy documentation for the specific Trust Service.

6.1.3 Public key delivery to certificate issuer

Public Key delivery to the offline Root CA

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

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

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

Public Key delivery to the issuing (Qualified) CA

The ZetesConfidens issuing CA has a network connection to internal systems of ZetesConfidens for certificate revocation and for generating certificates. Certificate requests (which include the public key of the requester) are transferred by means of a secure network connection between the environment for the personalisation of Secure Cryptographic Devices and the environment for the CA.

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

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

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

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

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

6.1.4 CA public key delivery to Relying Parties

ZetesConfidens CA certificates are published on a secure web site:

https://repository.confidens.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 a document in PDF/A format.

Relying parties may contact ZetesConfidens via e-mail at info@tsp.zetes.com to receive confirmation of the authentic “thumbprint” of the 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 ZETESCONFIDENS Root CA infrastructure uses the following algorithms and key sizes:

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

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

CA	RSA4096	generated and used on HSM
	ECC384	
	ECC512	

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

The hash algorithm is SHA256 or better.

ZETESCONFIDENS is not in any way held to continue using the current algorithms, protocols or key lengths should ZETESCONFIDENS decide that the current algorithms, protocols or key lengths provide insufficient assurance and security for the intended purpose and the intended use period.

6.1.6 Public key parameters generation and quality checking

Public key parameters 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 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 is compliant with FIPS 186
- public exponent '010001'

ECDSA, ECDH:

- the HSM is used in FIPS mode
- key generation is compliant with FIPS 186,
- Elliptic curves as specified in FIPS 186 Appendix D 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 Certificate Policies.

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

Key usage for CA certificates:	KeyCert signing
	CRL signing
Key usage for OCSP certificates:	digitalSignature - OCSP signing
Key usage for user certificates for authentication purposes:	digitalSignature - keyEncipherment
	digitalSignature
Key usage for user certificates for electronic signatures:	nonRepudiation
Key usage for user certificates for electronic signatures:	nonrepudiation + digitalSignature

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

HSM

To protect the private keys used by the Trust Services, the ZetesConfidens (Qualified) CA uses state of the art cryptographic modules (HSM). The HSM of the infrastructure comply with the following security certifications:

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

Secure Cryptographic Devices

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

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

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

6.2.2 Private key multi-person control

Private keys for HSM for PKI infrastructure keys

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

Private keys for Secure Cryptographic Devices for Subject keys

Not applicable.

6.2.3 Private key escrow

Private keys for HSM for PKI infrastructure keys

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

Private keys for Secure Cryptographic Devices for Subject keys

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

6.2.4 Private key backup

Private keys for HSM for PKI infrastructure keys

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

The backups are exclusively used for:

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

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

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

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

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

Private keys for Secure Cryptographic Devices for Subject keys

Private keys on a SCD smartcard are generated on-board the device and cannot be extracted from the device. Private keys on an SCD HSM are generated on-board the device and can be extracted in secure form for backup purposes or for high-availability key storage.

6.2.5 Private key archival

Private keys for HSM for PKI infrastructure keys for CA

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

Private keys for Secure Cryptographic Devices for Subject keys

Private keys on a SCD smartcard are generated on-board the device and cannot be extracted from the device. Private keys on an SCD HSM are generated on-board the device and can be extracted in secure form for operational purposes but are not extracted for archival purposes.

6.2.6 Private key transfer into or from a cryptographic module

Private keys for HSM for PKI infrastructure keys

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

Private keys for Secure Cryptographic Devices for Subject keys

Private keys on a SCD smartcard are generated on-board the device and cannot be extracted from the device. Private keys on an SCD HSM are generated on-board the device and can be transferred in secure form for backup purposes or for high-availability key storage.

6.2.7 Private key storage on cryptographic module

Private keys for HSM for PKI infrastructure keys

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

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

Private keys for Secure Cryptographic Devices for Subject keys

The SCD for Subject keys is a smartcard or equivalent device or a HSM. Private keys on a Secure Cryptographic Device are stored in secure memory. The embedded security controller circuit protects private keys and other security related information against hacks.

6.2.8 Method for activating private keys

Private keys for HSM for PKI infrastructure keys (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 ZetesConfidens (Qualified) CA requires at least two authorized administrators and operators.

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

Private keys for HSM for PKI infrastructure keys (OCSP service)

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

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

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

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

Deactivation of the private key for the ZetesConfidens Qualified CA requires at least two authorized administrators and operators.

Activation of the private key for the ZetesConfidens Qualified CA requires at least two authorized administrators and operators.

Private keys for Secure Cryptographic Devices for Subject keys

For an SCD smartcard or equivalent, the device is under the sole control of the Subject. The private key is activated by means of a PIN code or an equivalent mechanism such as biometric Match-on-Card. The Secure Cryptographic Device may also provide a security feature to prevent use of the private key prior to explicit commissioning of the key by the Subject, typically as part of the initial handover procedure of the Secure Cryptographic Device or as part of a post-issuance update procedure e.g. for certificate re-keying or for adding new keys and certificates to a Secure Cryptographic Device already in use.

For an SCD HSM the key object on the device is under the sole control of the Subject. The private key is activated by means of a an assertion which is derived from a user consent procedure involving single-factor or two-factor authentication of the Subject, depending on the signature creation policy.

6.2.9 Method of deactivating private key

See section 6.2.8.

6.2.10 Method of destroying private key

HSM - controlled destruction of all Private Keys in the HSM

The HSM's internal mechanism for reset to factory or for zeroize is used to 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.

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

HSM - selective destruction of a Private Key in the HSM

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

Private keys for Secure Cryptographic Devices for Subject keys

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

6.2.11 Capabilities and Rating of the Cryptographic Module

The HSM-infrastructure for the CA 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 for the Root CA infrastructure is certified FIPS 140-2 level 3 and CC EAL4+ (AVA_VAN.5) in compliance with the eIDAS Transitional Measures (Article 51).

The HSM used for issuing CA and OCSP infrastructure (subordinate CAs) is certified FIPS 140-2 level 3 in compliance with the eIDAS Transitional Measures (Article 51).

6.3 Other aspects of key pair management

6.3.1 Public key archival

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

6.3.2 Certificate operational periods and key pair usage periods

The ZETESCONFIDENS Root CA will not issue certificates that exceed the certificate expiration date of the CA certificate. The ZetesConfidens issuing CA will not issue certificates that exceed the certificate expiration date of the CA certificate. The key usage period of a CA key is aligned with the expiration date / lifetime of the certificates issued with that key.

6.4 Activation data

Activation data for the CA and for OCSP

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

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

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

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

Activation data for distributed Secure Cryptographic Devices

Activation data for Secure Cryptographic Device for Subjects or for RA/SRA personnel consist of PIN codes, PUK codes or are derived from the biometric characteristics of the Subject (e.g. fingerprint for biometric Match on Card). PIN codes and PUK codes are provided to the Subject in a protective tamper-evident container such as a PIN-letter and/or a sealed envelope.

Activation data for non-distributed Secure Cryptographic Devices (HSM) for Subjects

A Subject must first be registered by a Registration Authority (RA). To access the application and the subsequent signing and seal creation service, the user also needs to login using the credentials defined in the registration process. Some or all authentication factors are verified by an external identity provider (IdP) that will issue a SAML Assertion. If all the credentials are verified by the IdP these must correspond to an authentication means equivalent to Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 for assurance level substantial or higher . If only some of the credentials are verified by the IdP and these are not enough to correspond to an authentication means equivalent to Commission Implementing Regulation (EU) 2015/1502 for assurance level substantial or higher, an additional factor is required to trigger the seal or signing operation. This factor may be one of the following supported token-types: OATH-TOTP, OATH-HOTP, OATH-OCRA, SMS, Belgian Mobile itsme®, FIDO token or other additional factor. The SAML assertion is send to the SAM, which verifies the assertion.

6.5 Computer security controls

The computer security controls are implemented according the technical standard ETSI EN 319 411-1 (and where applicable part 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 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 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

ZetesConfidens with regard to the Trust Services 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 CA servers

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

The CA servers for the issuing CAs 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 Stratum-1 multi-GNSS referenced NTP infrastructure to synchronize the system clocks of critical infrastructure with the NTP services of the Royal Observatory of Belgium (UTC(ROB)). The Observatory maintains 4 of the atomic clocks of the worldwide UTC network and disseminates the time via the Network Time Protocol (ntp1.oma.be and ntp2.oma.be). As of May 2018 the Belgian legal time is by law aligned with Universal Time Coordinated (UTC). The legal time in Belgium is UTC+1h in winter and UTC+2h in summer.

The NTP infrastructures uses at least one of the following satellite navigation systems as additional time source:

- GPST from the GPS satellite network
- GST from the Galileo satellite network
- GLONASST from the GLONASS satellite network

In the unlikely event that none of the UTC time sources are available, the internal NTP infrastructure can maintain accurate time independently by means of high-precision oscillators until at least one of the external time references is available again.

7 CERTIFICATE, CRL, AND OCSP PROFILES

See the applicable Practice Statement and Policy documentation for the specific Trust Service.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Besides the supervision by the Belgian Supervisory Body (FOD Economie, Algemene Directie Kwaliteit en Veiligheid), ZetesConfidens PMA organizes its own compliance audit to ensure that it meets requirements, standards, procedures and service levels in accordance with the combined set of Practice Statements and Policies.

8.1 Frequency or circumstances of assessment

ZetesConfidens' Trust Services are regularly audited. Qualified Trust Services shall be audit at the least every 24 months. Annual audits can take place depending on other requirements, e.g. the Microsoft Trusted Root Certificate Program, the Common CA Database, etc.

CA services for Qualified Certificates shall be audited at least once a year for compliance with

- the applicable Practice Statements and Policies
- the technical standards ETSI 319 401, ETSI 319 411-1 and ETSI 319 411-2

TSA services for Qualified Time-stamp shall be audited at least once every 2 years for compliance with

- the applicable Practice Statements and Policies
- the technical standards ETSI 319 401 and ETSI 319 421

The PMA reserves the right to organize additional audits e.g. in the context of changes in the infrastructure, changes in the organisation or security incidents, on request of a Subscriber, on request of the Supervisory Body, etc..

8.2 Identity/qualifications of assessor

Compliance audits will be performed by a Conformity Assessment Body as defined in point 13 of article 2 of Regulation EC N°765/2008 and compliant with the CA/B Forum requirement for qualified auditors as per CA/Browser Forum version 1.3.4 (March 15, 2016) section 8.2.

8.3 Assessor's relationship to assessed entity

An independent auditor who will not be affiliated directly or indirectly in any way with ZETESCONFIDENS is appointed to carry out the audits.

8.4 Topics covered by assessment

The planned annual audits cover –but are not limited to – all aspects of the TSP's operations and related services as specified in the applicable Practice Statements and related policies according to section 8.1 of the present TSPS.

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 terms and conditions for the provision and use of ZetesConfidens Trust Services offering are first and foremost mentioned in the applicable Practice Statement documents and the relevant Policy documents.

Where applicable a Subscriber Agreement shall be concluded that contains obligations for Subscriber and TSP.

End-entity Subjects shall ratify a Subject Agreement for the provisioning of Certificates according to ETSI EN 319 411-1. A Subject Agreement may include Certificate Terms and Conditions (CTC) reiterating the main obligations for Subjects and make use of reference to the applicable CPS-CP.

Relying parties may turn to the PKI Disclosure Statements on the repository for reference to the applicable documents.

9.1 Fees

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

9.2 Financial responsibility

9.2.1 Insurance coverage

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

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

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

See the applicable Policy document or Subscriber Agreement.

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 Certificate
- the revocation records of a Certificate
- this Trust Services Practice Statement

9.3.3 Responsibility to protect confidential information

See the applicable Policy document or Subscriber Agreement.

9.4 Privacy of personal information

ZetesConfidens operates within the boundaries of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, the Belgian Law of 30 July 2018 on

Privacy Protection in relation to the Processing of Personal Data. And conform the Law of 13 June 2005 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

PRIVACY PLAN

ZetesConfidens shall:

a) where it processes personal data on its own behalf or on behalf of a controller do so in line with the GDPR and the Act of 30 July 2018 on the protection of privacy with respect to the processing of personal data (hereinafter Personal Data Protection Act).
b) when on behalf of the Subscriber only process personal data according to the purposes communicated by and the instructions of the Subscriber;
c) treat all personal data as confidential, unless the Subscriber's determines otherwise;
d) take adequate technical and organisational measures ensuring the security of the processing of personal data in line with the GDPR and the Personal Data Protection Act);
e) provide the Subscriber the opportunity to appropriately assess the adequacy of the implemented technical and organisational measures mentioned under (d);
f) notify the Subscriber as soon as possible of any request made by a data subject relating to the processing of his personal data;
g) 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;
h) refrain from transferring any personal data to sub-contractors or other third parties without the express permission of the Subscriber;
i) refrain from transferring any personal data outside the European Economic Area without the express permission of the Subscriber;
j) subject to the limitations set out elsewhere in this TSPS 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.

ZetesConfidens warrants that:

a) the technical and organisational 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.

A Subscriber shall:

a) inform ZetesConfidens in a clear and comprehensive manner of the intended purposes of the processing and provide clear and comprehensive directions regarding the extent to which ZetesConfidens can access and use personal data;
b) indemnify ZetesConfidens for any liability which is the direct result of processing personal data in line with the directions of the Subscriber.

See applicable Policy document, Subscriber Agreement or Subject Agreement for more details.

9.5 Intellectual property rights

Any and all intellectual property rights ("IPR") (including title, ownership rights, database rights, and any other intellectual property rights) in ZetesConfidens Trust Services 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 Trust Services offering other than those expressly granted under this Trust Services Practice Statement or elsewhere in the Subscriber Agreement.

9.6 Representations and warranties

9.6.1 RA representations and warranties

The RA needs under contractual obligation to comply with the CPS, and with the RA relevant internal procedures.

Third party LRAs warrant that:

- There are no material misrepresentations of fact in the Certificate known to, or which reasonably ought to be known to, the LRA or its agents;
- There are no errors in the information in the Certificate that were introduced by the LRA or its agents as a result of a failure to exercise reasonable care; and
- Their Certificates meet all material requirements of the CP/CPS.

Additional representations and warranties relevant to LRAs may be included in the Subscribers Agreements for specific Certificate Policies.

9.6.2 Subscriber and Subject representations and warranties

The Subscriber and Subject accept the "Certificate Terms and Conditions".

The Subscriber agrees to the CPS and to his/her relevant responsibilities, liabilities and obligations as provided in the relevant sections of the CPS and the CP.

In particular, the Subject is liable towards Relying Parties for any use that is made of his / her SCD, including the keys or Certificate(s), unless (s)he can prove that (s)he has taken all the necessary measures for a timely revocation of his / her Certificate(s) when required.

9.6.3 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 Certificate
- the validation of a Certificate by using the ZetesConfidens Certificate Revocation Lists (CRLs)
- the immediate termination of any reliance on a Certificate if it has been revoked or when it has expired

See also applicable Policy document.

9.7 Disclaimers of warranties

See applicable Policy document.

9.8 Limitations of liability

Exclusion of Certain Elements of Damages

ZetesConfidens explicitly declines all liability towards Subjects and Relying Parties in all cases where non-Qualified Certificates (such as Certificates with certificate profile: [NCP+]) are used in the context of applications allowing the use of such certificates for the generation of qualified electronic signatures.

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, the Subject 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 Certificate that is underlying to the claim.

See also applicable Policy document.

9.9 Indemnities

See applicable Policy document.

9.10 Term and termination of the present TSPS

9.10.1Term

This TSPS 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 TSPS will be communicated via the ZetesConfidens web site upon termination. That communication will outline the provisions that may survive termination of this TSPS and remain in force. The responsibilities for protecting business confidential and private personal information

shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the validity periods of such Certificates.

9.11 Individual notices and communications with participants

See applicable Policy document.

9.12 Amendments to the present TSPS

9.12.1 Procedure for amendment

ZetesConfidens acting as TSP is responsible via its Policy Management Authority (PMA) for approval and changes of the present TSPS.

The only changes that the PMA may make to these TSPS specifications without notification are minor changes that do not affect the assurance level of this TSPS, 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 TSPS, section 1.5.4. Such communication must include a description of the change, a change justification, and contact information of the person requesting the change.

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

9.12.2 Notification mechanism and period

All changes to the present TSPS shall be disseminated via the repository website. The date of issuance and the effective date are indicated on the title page of the present TSPS. The effective date will be at least 2 days later than the date of publication.

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

See applicable Policy document.

9.14 Governing law

The Belgian laws shall govern the enforceability, construction, interpretation, and validity of the present TSPS (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 TSPS is compliant to relevant and applicable laws of Belgium (including the directly applicable Regulation (EU) No 910/2014).

9.16 Miscellaneous provisions

See applicable Policy document.

9.17 Other provisions

Not applicable.

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