ZETESCONFIDENS

PKI DISCLOSURE STATEMENT – CERTIFICATES FOR THE ZETESCONFIDENS SIGNATURE CREATION SERVICE

For certificates issued under
ZetesConfidens Signature Creation Service Issuing CA 001

for the ZetesConfidens - Signature Creation Service

English

Title:	**ZetesConfidens**
Subject:	**PKI Disclosure Statement – certificates for the ZetesConfidens Signature Creation Service**
Category:	**PDS - public information for Subjects and Relying Parties**
Version:	**1.1**
Status:	**Final**
Publish date:	**24/07/2020**
Document OID:	**1.3.6.1.4.1.47718.2.1.5.5 (QCP-n-qscd, NCP+, LCP)**
Author:	**ZETES TSP (Bart Symons / Jos De Wachter)**
Classification:	**PUBLIC**
Copyright:	**© 2020 Zetes - All rights reserved.**

1 PKI DISCLOSURE STATEMENT

Reference Language:

The English version of the PDS shall prevail and be binding even though the PDS is also available in translations to other languages.

Document History:

version	date	changes
1.1	24/07/2020	Updated with unique Zetes policy OIDs for LCP/QCP+/QCP-n-qscd policies.
1.0	15/06/2020	First public version

PKI Disclosure Statement:

Statement types	Statement descriptions	Specific Requirements of certificate policy
TSP contact info:	The name, location and relevant contact information for the CA/PKI (name of responsible person, address, website, info mail, faq, etc.), including clear information on how to contact the TSP to request a revocation.	Contact address: pma@tsp.zetes.com Postal address: ZETES TSP - Straatsburgstraat 3 - 1130 HAREN - BELGIUM Telephone: +32 2 728 37 11 Website: http://tsp.zetes.com

Applicable agreements, CPS, CP:	Identification and references to applicable agreements, CPS, CP and other relevant documents.	The applicable agreements are published on https://repository.tsp.zetes.com and https://pds.tsp.zetes.com and are labelled as follows:
		CPS for the Zetes TSP RootCA 001: Certification Practice Statement OID 1.3.6.1.4.1.47718.2.1.1.1
		CPS for the ZetesConfidens Signature Creation Service issuing CA 001: Certification Practice Statement OID 1.3.6.1.4.1.47718.2.1.1.5
		CP for Certificates under the ZetesConfidens Signature Creation Service issuing CA Certificate Policy for certificates for the ZetesConfidens Signature Creation Service OID 1.3.6.1.4.1.47718.2.1.2.5.1 - OID 1.3.6.1.4.1.47718.2.1.2.5.2 - OID 1.3.6.1.4.1.47718.2.1.2.5.3
Certificate type, validation procedures and usage:	A description of each class/type of certificate issued by the CA, corresponding validation procedures, and any restrictions on certificate usage.	This statement applies to qualified and non-qualified certificates issued by the ZETES TSP Qualified CA.
		The certificates are issued to natural persons after verification of the identity of the person.
		The primary types of certificates issued for the different parties are:
		QCP-n-qscd supporting Qualified Electronic Signature for Natural Persons ETSI policy identifier 0.4.0.194112.1.2 Zetes TSP policy identifier 1.3.6.1.4.1.47718.2.1.2.5.3
		NCP+ supporting signature operations (nonrepudiation) for Natural Persons ETSI policy identifier 0.4.0.2042.1.2 Zetes TSP policy identifier 1.3.6.1.4.1.47718.2.1.2.5.2
		LCP supporting signature operations (nonrepudiation) for Natural Persons ETSI policy identifier 0.4.0.2042.1.3 Zetes TSP policy identifier 1.3.6.1.4.1.47718.2.1.2.5.1
		Qualified Certificates may be used only in accordance with the applicable Certificate Policy and in accordance with Regulation (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
		Non-qualified certificates may be used only in accordance with the applicable Certificate Policy.

Reliance limits:	The reliance limits, if any.	All type of certificates are for use in electronic signatures with non-repudiation. Registration information and TSP event logs are maintained for minimum 7 years after any certificate based on these records ceases to be valid (and hence are available to provide supporting evidence). Reliance on the certificates must take into account the limited warranty by and the limitation of liability for the Certificate Service Provider, see these topics below.

Obligations of subscribers and subjects:	The description of, or reference to, the critical subscriber and subjects obligations.	**The subscriber's and the subjects obligations shall include amongst others:**
		
		a) accurate and complete information is submitted to the TSP, particularly with regards to registration;
		
		b) the key pair is only used in accordance with any limitations notified to the subscriber;
		
		c) unauthorized use of the subject's private key is avoided;
		
		d) only use the subject's private key(s) for cryptographic functions within the secure cryptographic device;
		
		e) notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
		
		    i) the subject's private key has been lost, stolen, potentially compromised;
		
		    ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; or
		
		    iii) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.
		
		f) following compromise, the use of the subject's private key is immediately and permanently discontinued, except for key decipherment;
		
		g) in the case of being informed that the subject's certificate has been revoked, or the issuing CA has been compromised, ensure that the private key is not used by the subject.
		
		Additional obligations for server signing apply:
		
		• the private key shall not be used for signing except within a QSCD.
		
		• the subject's private key shall be used under the subject's sole control.
		
		• the subject's key pair should be used only for electronic signatures.

Certificate status checking obligations of relying parties:	The extent to which relying parties are obligated to check certificate status, and references to further explanation.	Relying parties are obligated to: a) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party through the Online Certificate Status Protocol (OCSP) service: http://ocsp.tsp.zetes.com; b) take account of any limitations on the usage of the certificate indicated to the relying party in the certificate policy (and stated here below); and c) take any other precautions prescribed in the CPS and applicable CP, as well as follow the problem reporting instructions (see below).
Limited warranty and disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	*See CPS and/or applicable CP: Section 9.2 on insurance coverage, Section 9.6 Representation and warranties, Section 9.7 Disclaimers of warranties and section 9.8 Limitations of liabilities.* ZetesConfidens explicitly declines all liability towards relying parties and Subjects in all cases where • a certificate was used improperly, • a certificate was used for any purpose other than the certificate's intended use, • the validity of the certificate was not properly checked at the relevant time, • an authentication certificate was used in a private setting between private parties, which is beyond authentication that is required under national law or by administrative practice to access a service provided by a public sector body online , • the concepts or principles on which the security and trust were based become moot due to a disruptive scientific or technological development. Within the limit set by Belgian Law, in no event (except for fraud or wilful misconduct) will ZETES TSP 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 ZETES TSP towards the Subscriber, the Subject or a Relying Party for proven direct damages, the liability of ZETES TSP 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. Liability in specific cases can be excluded: see ZetesConfidens Trust Services Practice Statement, clause 9.8.
Problem reporting		Subscribers, Relying Parties, Application Software Suppliers, and other third parties should follow these instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates: Natural Persons who are certificate holders must file a report with the registration officer in the Local RA office or with the Certification Service Provider via the certificate revocation services. Subscribers must file a report via the certificate revocation services. Relying Parties, Application Software Providers or other third parties can file problem reports by email report@tsp.zetes.com or by letter or by phone via the contact information published on http://tsp.zetes.com.
Privacy policy:	A description of and reference to the applicable privacy policy.	See ZetesConfidens Privacy Statement, published on the repository website.
Refund policy:	A description of and reference to the applicable refund policy.	Commercial agreements are discussed and agreed case by case with every Subscriber before Subscriber Agreement can be signed.

Version   1.1

Status   Final

PUBLIC

p. 6

Applicable law, complaints and dispute resolution:	Statement of the choice of law, complaints procedure and dispute resolution mechanisms (anticipated to often include a reference to the International Chambers of Commerce's arbitration services).	The Belgian laws shall govern the enforceability, construction, interpretation, and validity of the contractual relationships with regard to the CPS and applicable CP (without giving effect to any conflict of law provision that would cause the application of other laws).
TSP and repository licenses, trust marks, and audit:	Summary of any governmental licenses, seal programs; and a description of the audit process and if applicable the audit firm.	ZETES TSP is listed on the Belgian Trusted List: https://tsl.belgium.be/tsl-be.xml .

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