



ZETES TSP

PUBLIC DISCLOSURE STATEMENT FOR OVB-OBFG CERTIFICATES

Title:	Zetes TSP
Subject:	Public Disclosure Statement for OVB-OBFG certificates
Category:	PDS - public information for Subjects and Relying Parties
Version:	1.0
Status:	Final
Publish date:	27/03/2017
Document OID:	1.3.6.1.4.1.47718.2.1.5.2.1.10 (NCP+) 1.3.6.1.4.1.47718.2.1.5.2.3.10 (QCP-n-qscd)
Author:	ZETES TSP (Bart Symons / Jos De Wachter)
Classification:	PUBLIC
Copyright:	© 2017 Zetes - All rights reserved.

The content of this document is confidential and needs to be treated as such.

No part of this document or any of its contents may be reproduced, copied, modified or adapted, without the prior written consent of the author, unless otherwise indicated for stand-alone materials.

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

Document History:

version	date	changes
1.0	27/03/2017	first version / english

1 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 Version 1.0 CPS for the Zetes TSP Qualified CA 001: Certification Practice Statement OID 1.3.6.1.4.1.47718.2.1.1.2 Version 1.1 CP for certificates issued for natural persons on behalf of OVB-OBFG Common Certificate Policy for certificates for natural persons, issued on behalf of OVB-OBFG OID 1.3.6.1.4.1.47718.2.1.2.2.3.10 and OID 1.3.6.1.4.1.47718.2.1.2.2.1.10 version v1.0 (23/03/2017)
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 on behalf of the following two organisations: OVB - Orde van Vlaamse Balies, composed of the Belgian (Dutch speaking) local Bar Associations as defined in Article 488 of the Belgian Judicial Code OBFG - l'Ordre des Barreaux Francophones et Germanophone de Belgique, composed of the Belgian (French and German speaking) local Bar Associations as defined in Article 488 of the Belgian Judicial Code

Statement types	Statement descriptions	Specific Requirements of certificate policy
		<p>These organisations are collectively referred to as OVB-OBFG and are considered as a single entity when seen as the Subscriber for the certificates under this policy. They may be referred to separately as OVB and/or OBFG when seen in their respective role as organisation fulfilling tasks such as Subordinate Registration Authority (SUB-RA).</p> <p>OVB-OBFG is the Subscriber, i.e. the certificates are issued on behalf of OVB-OBFG to natural persons associated with and registered by OVB or OBFG. OVB and OBFG are also the Subordinate Registration Authority and the operators of the Local Registration Authority offices.</p> <p>The certificates are issued to natural persons after verification of the identity of the person and after confirmation by OVB-OBFG that this person is entitled to a certificate on behalf of OVB-OBFG and attestation by OVB-PBFG as to the person’s professional title or capacity. Identity verification is based on the person’s national identity card, European residence permit card or passport.</p> <p>The primary types of certificates issued for the different parties are:</p> <p>QCP-n-qscd supporting Qualified Electronic Signature for Natural Persons ETSI policy identifier 0.4.0.2042.1.2 Zetes TSP policy identifier 1.3.6.1.4.1.47718.2.1.2.2.3.10 Zetes TSP certificate profile identifier 1.3.6.1.4.1.47718.2.1.3.2.3.10</p> <p>NCP+ supporting Authentication for Natural Persons ETSI policy identifier 0.4.0.194112.1.2 Zetes TSP policy identifier 1.3.6.1.4.1.47718.2.1.2.2.1.10 Zetes TSP certificate profile identifier 1.3.6.1.4.1.47718.2.1.3.2.1.10</p> <p>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.</p> <p>Non-qualified certificates may be used only in accordance with the applicable Certificate Policy.</p>
Reliance limits:	The reliance limits, if any.	<p>Only QCP-n-qscd type certificates are for use in electronic signatures. NCP+ type certificates should not be used nor relied on for electronic signatures.</p> <p>Registration information and TSP event logs are maintained for minimum 7 years counting from the date of the issued certificate (and hence are available to provide supporting evidence).</p> <p>Reliance on the certificates must take into account the limited warranty by and the limitation of liability for the</p>

Statement types	Statement descriptions	Specific Requirements of certificate policy
		Certificate Service Provider, see these topics below.
Obligations of subscribers:	The description of, or reference to, the critical subscriber obligations.	<p>The subscriber's obligations shall include amongst others:</p> <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.
Certificate status checking obligations of relying parties:	The extent to which relying parties are obligated to check certificate status, and references to further explanation.	<p>Relying parties are obligated to:</p> <ul style="list-style-type: none"> 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).

Statement types	Statement descriptions	Specific Requirements of certificate policy
<p>Limited warranty and disclaimer/Limitation of liability:</p>	<p>Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.</p>	<p><i>See CPS and 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.</i></p> <p>ZETES TSP Qualified CA 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.</p> <p>Within the limit set by Belgian Law, in no event (except for fraud or wilful misconduct) will ZETES TSP be liable for:</p> <ul style="list-style-type: none"> • 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. <p>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:</p> <ul style="list-style-type: none"> • Paying damages amounting up to a maximum of 2500 € per transaction, for events where the Relying Party relies on that certificate: <ul style="list-style-type: none"> 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; <p>and</p> <ul style="list-style-type: none"> • Paying damages amounting up to a maximum of 10.000 € in total per Certificate that is underlying to the claim.

Statement types	Statement descriptions	Specific Requirements of certificate policy
Problem reporting		<p>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:</p> <p>Natural Persons who are certificate holders must file a report with the registration officer in the Local RA office (i.e. the office of the local Bar Association) or with the Certification Service Provider via the certificate revocation services.</p> <p>OVB-OBFG as Subscriber and as Subordinate Registration Authority must file a report via the certificate revocation services.</p> <p>Relying Parties, Application Software Providers or other third parties can file problem reports . report@tsp.zetes.com or by letter or by phone via the contact information published on http://tsp.zetes.com.</p>
Privacy policy:	A description of and reference to the applicable privacy policy.	See section 9.4 of the CPS and CP.
Refund policy:	A description of and reference to the applicable refund policy.	See section 9.1 Fees of the CPS and CP: ZETES TSP operates a no refund policy.
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 -----