ZETES TSP

PKI DISCLOSURE STATEMENT FOR OVB-OBFG-OAC CERTIFICATES

English

Nederlands

Français

Deutsch

Title:	Zetes TSP
Subject:	PKI Disclosure Statement for OVB-OBFG-OAC certificates
Category:	PDS - public information for Subjects and Relying Parties
Version:	1.3
Status:	Final
Publish date:	11/06/2018
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.

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
1.3	**11/06/2018**	**OAC (lawyers at the Cour de Cassation) joined subscriber**
1.2	19/05/2017	Multi-language version
1.1	21/04/2017	Cosmetic changes and update of CPS and CP.
1.0	27/03/2017	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

Statement types	Statement descriptions	Specific Requirements of certificate policy
		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 1.3 **CP for certificates issued for natural persons on behalf of OVB-OBFG-OAC** Common Certificate Policy for certificates for natural persons, issued on behalf of OVB-OBFG-OAC 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 1.3
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 on behalf of the following three 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 OAC – "Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie", being the Bar Association as defined in Article 481 of the Belgian Judicial Code These organisations are collectively referred to as OVB-OBFG-OAC 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, OBFG and/or OAC when seen in their respective role as organisation fulfilling tasks such as Subordinate Registration Authority (SUB-RA). OVB-OBFG-OAC is the Subscriber, i.e. the certificates are issued on behalf of OVB-OBFG-OAC to natural persons associated with and registered by OVB, OBFG or OAC. OVB, OBFG and OAC are also the Subordinate Registration Authority. The certificates are issued to natural persons after verification of the identity of the person and after confirmation by OVB-OBFG-OAC that this person is entitled to a certificate on behalf of OVB-OBFG-OAC and attestation by OVB-OBFG-OAC 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.

Statement types	Statement descriptions	Specific Requirements of certificate policy
		The primary types of certificates issued for the different parties are: **QCP-n-qscd supporting Qualified Electronic Signature for Natural Persons** ETSI policy identifier 0.4.0.2042.1.2 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 **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 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.	Only QCP-n-qscd type certificates are for use in electronic signatures with non-repudiation. NCP+ type certificates are intended for authentication purposes and should not be used nor relied on for electronic signatures. 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:	The description of, or reference to, the critical subscriber obligations.	The subscriber's 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;

Statement types	Statement descriptions	Specific Requirements of certificate policy
		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.
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.* 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. 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;

Statement types	Statement descriptions	Specific Requirements of certificate policy
		• 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.
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 (i.e. the office of the local Bar Association) or with the Certification Service Provider via the certificate revocation services. OVB-OBFG-OAC as Subscriber and as Subordinate Registration Authority must file a report via the certificate revocation services.

Statement types	Statement descriptions	Specific Requirements of certificate policy
		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 section 9.4 of the CP.
Refund policy:	A description of and reference to the applicable refund policy.	See section 9.1 Fees of the 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 .

2 NL - PKI OPENBAARMAKINGSVERKLARING

Referentietaal:

De Engelstalige versie van de PKI Openbaarmakingsverklaring (PKI Disclosure Statement afgekort als PDS) heeft voorrang en zal bindend zijn, zelfs al is de PDS beschikbaar in vertalingen naar andere talen.

Documentgeschiedenis:

versie	datum	wijzigingen
1.3	**11/06/2018**	**Toevoeging van OAC (Orde van advocaten bij het Hof van Cassatie) aan de subscriber**
1.2	19/05/2017	Meertalige versie
1.1	21/04/2017	Wijzigingen aan het uiterlijk en update van het CPS en de CP
1.0	27/03/2017	Eerste openbare versie

PKI Openbaarmakingsverklaring:

Soorten verklaringen	Omschrijving verklaring	Specifieke Certificate Policy-eisen
Contactgegevens TSP:	De naam, plaats en relevante contactgegevens voor de CA / PKI (naam van de verantwoordelijke, adres, website, mailgegevens, veelgestelde vragen enz.), inclusief duidelijke informatie over hoe de TSP gecontacteerd kan worden om te vragen om een intrekking.	Contactadres: pma@tsp.zetes.com Postadres: ZETES TSP - Straatsburgstraat 3 - 1130 HAREN - BELGIË Telefoon: +32 2 728 37 11 Website: http://tsp.zetes.com
Toepasselijke overeenkomsten, CPS, CP:	Identificatie van en verwijzingen naar toepasselijke overeenkomsten, CPS, CP en andere relevante documenten.	De toepasselijke overeenkomsten staan op https://repository.tsp.zetes.com en https://pds.tsp.zetes.com en zijn als volgt benoemd: **CPS voor de Zetes TSP RootCA 001:** Certification Practice Statement

Soorten verklaringen	Omschrijving verklaring	Specifieke Certificate Policy-eisen
		OID 1.3.6.1.4.1.47718.2.1.1.1 Versie 1.0 **CPS voor de Zetes TSP Qualified CA 001:** Certification Practice Statement OID 1.3.6.1.4.1.47718.2.1.1.2 Versie 1.3 **CP voor certificaten afgegeven voor natuurlijke personen namens de OVB-OBFG-OAC** Common Certificate Policy voor certificaten voor natuurlijke personen, afgegeven namens de OVB-OBFG-OAC OID 1.3.6.1.4.1.47718.2.1.2.2.3.10 en OID 1.3.6.1.4.1.47718.2.1.2.2.1.10 Versie 1.3
Certificaattype, valideringsprocedures en gebruik:	Een omschrijving van elk type certificaat afgegeven door de CA, de bijbehorende valideringsprocedures en alle beperkingen betreffende het certificaatgebruik.	Deze verklaring is van toepassing op gekwalificeerde en niet-gekwalificeerde certificaten afgegeven door ZETES TSP Qualified CA namens de volgende twee organisaties: OVB - Orde van Vlaamse Balies, bestaande uit de Belgische (Nederlandstalige) plaatselijke Ordes van Advocaten zoals bepaald in Artikel 488 van het Belgisch Gerechtelijk Wetboek OBFG - de Ordre des Barreaux francophones et germanophone de Belgique, bestaande uit de Belgische (Franstalige en Duitstalige) plaatselijke Ordes van Advocaten zoals bepaald in Artikel 488 van het Belgisch Gerechtelijk Wetboek OAC – “Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie”, de Orde zoals bepaald in Article 481 van het Belgisch Gerechtelijk Wetboek Deze organisaties worden gezamenlijk de OVB-OBFG-OAC genoemd en worden als één entiteit gezien wanneer ze de abonnee zijn van de certificaten zoals in dit beleid. Ze kunnen afzonderlijk de OVB, OBFG of OAC genoemd worden in hun respectieve rol van organisatie die taken vervult bijvoorbeeld als Subordinate Registration Authority (SUB-RA). De OVB-OBFG-OAC is de abonnee, wat betekent dat de certificaten afgegeven worden namens de OVB-OBFG-OAC aan natuurlijke personen die gelieerd zijn aan en geregistreerd zijn door de OVB, OBFG of OAC. De OVB, OBFG en OAC zijn ook de Subordinate Registration Authority. De certificaten worden afgegeven aan natuurlijke personen na verificatie van de identiteit van de persoon en na bevestiging door de OVB-OBFG-OAC dat deze persoon recht heeft op een certificaat namens de OVB-OBFG-OAC en attestering door de OVB-OBFG-OAC met betrekking tot de beroepstitel en -bekwaamheid van de persoon. De identiteitsverificatie gebeurt aan de hand van de nationale identiteitskaart, de Europese verblijfskaart of het paspoort van de persoon. De belangrijkste types certificaten die afgegeven worden voor de verschillende partijen zijn: **QCP-n-qscd met ondersteuning van de gekwalificeerde elektronische handtekening voor natuurlijke personen** ETSI policy identifier 0.4.0.2042.1.2

Soorten verklaringen	Omschrijving verklaring	Specifieke Certificate Policy-eisen
		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 **NCP+ met ondersteuning van authentificatie voor natuurlijke personen** 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 Gekwalificeerde certificaten mogen enkel gebruikt worden overeenkomstig de toepasselijke Certificate Policy en overeenkomstig Verordening (EU) Nr. 910/2014 VAN HET EUROPEES PARLEMENT EN DE RAAD van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Niet-gekwalificeerde certificaten mogen enkel gebruikt worden overeenkomstig de toepasselijke Certificate Policy.
Betrouwbaarheidsbeperkingen:	De betrouwbaarheidsbeperkingen, indien van toepassing.	Enkel certificaten van het type QCP-n-qscd zijn bedoeld voor gebruik in elektronische handtekeningen met onweerlegbaarheid. Certificaten van het type NCP+ zijn bedoeld voor authentificatiedoeleinden en mogen niet gebruikt worden noch vertrouwd worden voor elektronische handtekeningen. De registratiegegevens en TSP-gebeurtenissenlogboeken worden minimaal gedurende 7 jaar vanaf het niet langer geldig zijn van een bij deze records horend certificaat bewaard (en zijn dus beschikbaar als bewijsmateriaal). Bij het vertrouwen op de certificaten moet rekening worden gehouden met de beperkte garantie door en de beperking van aansprakelijkheid van de Certificate Service Provider; zie onderstaande onderwerpen.
Plichten van de abonnees:	De omschrijving van, of verwijzing naar, de cruciale plichten van de abonnee.	Voor de abonnee gelden onder meer de volgende plichten: a) er moet correcte en volledige informatie aangeleverd worden aan de TSP, met name met betrekking tot de registratie; b) het sleutelpaar mag enkel gebruikt worden in overeenstemming met de aan de abonnee gemelde beperkingen; c) ongeoorloofd gebruik van de private sleutel van de houder moet vermeden worden; d) de private sleutel(s) van de houder mogen enkel gebruikt worden voor cryptografische functies binnen de veilige cryptografieapparatuur; e) de TSP dient zonder redelijk uitstel op de hoogte gebracht te worden indien de volgende gebeurtenissen zich voordoen tot aan het einde van de in het certificaat aangegeven geldigheidsduur: i) de private sleutel van de houder is kwijtgeraakt, gestolen, mogelijkerwijs gecompromitteerd; ii) de controle over de private sleutel van de houder is kwijt vanwege compromittatie van activeringsgegevens (bv. pincode) of andere redenen; of iii) onjuistheid of wijzigingen van de inhoud van het certificaat, zoals gemeld aan de abonnee of aan de houder.

Soorten verklaringen	Omschrijving verklaring	Specifieke Certificate Policy-eisen
		f) na compromittatie dient het gebruik van de private sleutel van de houder onmiddellijk en permanent gestaakt te worden, behalve voor het decoderen van de sleutel; g) ingeval geïnformeerd wordt dat het certificaat van de houder ingetrokken is of dat de afgevende CA gecompromitteerd is, dient ervoor gezorgd te worden dat de private sleutel niet gebruikt wordt door de houder.
Verplichting van vertrouwende partijen voor het controleren van de certificaatstatus:	De mate waarin vertrouwende partijen verplicht zijn om de certificaatstatus te controleren en verwijzingen naar verdere uitleg.	Vertrouwende partijen zijn verplicht om: a) de geldigheid, opschorting of intrekking van het certificaat te controleren aan de hand van de huidige intrekkingsstatusgegevens zoals aangegeven aan de vertrouwende partij via de Online Certificate Status Protocol (OCSP)-dienst: http://ocsp.tsp.zetes.com; b) rekening te houden met de beperkingen betreffende het gebruik van het certificaat zoals aangegeven aan de vertrouwende partij in de Certificate Policy (en zoals hieronder vermeld); en c) alle andere voorzorgsmaatregelen te nemen zoals voorgeschreven in het CPS en de toepasselijke CP en ook de probleemmeldingsinstructies na te leven (zie onder).
Beperkte garantie en uitsluiting / Beperking van aansprakelijkheid:	Overzicht van de garantie, uitsluitingen, aansprakelijkheidsbeperking en alle toepasselijke garantie- of verzekeringsprogramma's.	*Zie CPS en/of toepasselijke CP: Paragraaf 9.2 over verzekeringsdekking, Paragraaf 9.6 'Garanties', Paragraaf 9.7 'Uitsluitingen van garanties' en Paragraaf 9.8 'Beperking van aansprakelijkheid'.* ZETES TSP Qualified CA wijst uitdrukkelijk elke aansprakelijkheid af jegens houders en vertrouwende partijen in alle gevallen waarin niet-gekwalificeerde certificaten (zoals certificaten met Certificate Profile: [NCP+]) gebruikt worden in het kader van toepassingen die het gebruik van dergelijke certificaten voor het genereren van gekwalificeerde elektronische handtekeningen mogelijk maken. Binnen de grenzen van de Belgische wet, kan ZETES TSP in geen geval (met uitzondering van fraude of bedrog) aansprakelijk gesteld worden voor: • Winstderving; • Gegevensverlies; • Indirecte, bestraffende of gevolgschade als gevolg van of in verband met het gebruik, de levering, de licentie en het functioneren of niet functioneren van certificaten of digitale handtekeningen; • Elke andere schade naast bewezen directe schade zoals onder beschreven. In geval van aansprakelijkheid van ZETES TSP jegens de abonnee, de houder of een vertrouwende partij voor bewezen directe schade, is de aansprakelijkheid van ZETES TSP jegens een eiser in elk geval beperkt tot: • Het betalen van schadevergoedingen van maximaal € 2500,- per transactie, voor gebeurtenissen waarbij de vertrouwende partij op het betreffende certificaat vertrouwt voor wat betreft: a) de juistheid, op het tijdstip van afgifte, van alle gegevens in het gekwalificeerde certificaat en de opneming in het certificaat van alle voor een gekwalificeerd certificaat voorgeschreven gegevens; of b) de garantie dat de in het gekwalificeerde certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, houder was van de private sleutel die overeenkwam met de in het

Soorten verklaringen	Omschrijving verklaring	Specifieke Certificate Policy-eisen
		certificaat gegeven of geïdentificeerde publieke sleutel; of c) de garantie dat de private sleutel en de publieke sleutel complementair kunnen worden gebruikt; en • Het betalen van schadevergoedingen van in het totaal maximaal € 10.000,- per certificaat dat ten grondslag ligt aan de claim.
Probleemmelding		Abonnees, vertrouwende partijen, applicatiesoftwareleveranciers en andere derden zijn gebonden aan deze instructies voor het melden van Private Key-compromittatie, certificaatmisbruik of andere soorten fraude, compromittatie, misbruik en ongepast gedrag of elk ander probleem met betrekking tot certificaten: Natuurlijke personen die certificaathouder zijn moeten een melding indienen bij de registratiebeambte in het lokale RA-kantoor (het kantoor van de plaatselijke Orde van Advocaten) of bij de Certification Service Provider via de certificaatintrekkingsdiensten. De OVB-OBFG-OAC moet als abonnee en als Subordinate Registration Authority een melding indienen via de certificaatintrekkingsdiensten. Vertrouwende partijen, applicatiesoftwareleveranciers en andere derden kunnen probleemmeldingen indienen per e-mail aan report@tsp.zetes.com of per brief of telefonisch via de contactgegevens op http://tsp.zetes.com.
Privacybeleid:	Een omschrijving van of verwijzing naar het toepasselijke privacybeleid.	Zie paragraaf 9.4 van de CP.
Restitutiebeleid:	Een omschrijving van of verwijzing naar het toepasselijke restitutiebeleid.	Zie paragraaf 9.1 'Vergoedingen' van de CP: ZETES TSP voert een 'geen restitutie'-beleid.
Toepasselijk recht, klachten en geschillenbeslechting:	Bepaling van de gekozen wetgeving, klachtenprocedure en geschillenbeslechtingsmechanismen (in de regel vaak voorzien van een verwijzing naar de arbitragediensten van de Internationale Kamers van Koophandel).	Op de afdwingbaarheid, uitvoering, interpretatie en geldigheid van de contractuele verbintenissen met betrekking tot het CPS en de toepasselijke CP zijn de Belgisch wetten van toepassing (zonder uitvoering van enige bepaling inzake wetsconflicten die de toepassing van andere wetgevingen tot gevolg kan hebben).
TSP en databankvergunningen, keurmerken en audits:	Overzicht van alle overheidsvergunningen, keurmerkprogramma's en een beschrijving van de auditprocedure en, indien van toepassing, het accountantskantoor.	ZETES TSP staat op de Belgische vertrouwenslijst: https://tsl.belgium.be/tsl-be.xml .

3 FR – DECLARATION DE DIVULGATION DE L'INFRASTRUCTURE A CLES PUBLIQUES (ICP)

Langue de référence :

La version anglaise de la Déclaration de Divulgation de l'ICP prévaudra et sera contraignante même si la Déclaration de Divulgation de l'ICP est également disponible dans des traductions vers d'autres langues. .

Historique de révision :

version	date	modifications
1.3	**11/06/2018**	**OAC rejoigne l'abonné**
1.2	19/05/2017	Version multi-langues
1.1	21/04/2017	Changements mineurs et mise à jour de la DPC et de la PC
1.0	27/03/2017	Première version publique

Déclaration de Divulgation de l'Infrastructure à Clés Publiques (ICP):

Type de déclaration	Description de la déclaration	Exigences spécifiques prévues par la politique de certification (PC)
Coordonnées du TSP :	Nom, situation et informations de contact pertinentes pour l'autorité de certification/infrastructure à clés publiques (nom de la personne responsable, adresse, site web, e-mail, FAQ, etc.), y compris des informations claires sur la procédure de contact du prestataire de services de confiance (TSP) pour formuler une demande de révocation.	E-mail de contact : pma@tsp.zetes.com Adresse : ZETES TSP - Straatsburgstraat 3 - 1130 HAREN - BELGIQUE Téléphone : +32 2 728 37 11 Site web : http://tsp.zetes.com

Type de déclaration	Description de la déclaration	Exigences spécifiques prévues par la politique de certification (PC)
Accords applicables, DPC, PC :	Identification des accords applicables, de la déclaration des pratiques de certification (DPC), de la politique de certification (PC) et d'autres documents pertinents, ou toute référence à ceux-ci.	Les accords applicables sont publiés sur les pages https://repository.tsp.zetes.com et https://pds.tsp.zetes.com et sont identifiés comme suit : **DPC concernant l'autorité de certification racine (Root CA 001) Zetes TSP :** Déclaration des pratiques de certification OID 1.3.6.1.4.1.47718.2.1.1.1 Version 1.0 **DPC concernant l'autorité de certification qualifiée (Qualified CA 001) Zetes TSP :** Déclaration des pratiques de certification OID 1.3.6.1.4.1.47718.2.1.1.2 Version 1.3 **PC concernant les certificats délivrés à des personnes physiques pour le compte de l'OVB-OBFG-OAC** Politique de certification commune concernant les certificats relatifs à des personnes physiques, émis pour le compte de l'OVB-OBFG-OAC OID 1.3.6.1.4.1.47718.2.1.2.2.3.10 et OID 1.3.6.1.4.1.47718.2.1.2.2.1.10 Version 1.3
Type de certificat, procédures de validation et utilisation :	Description de chaque classe/type de certificat émis par l'autorité de certification, ainsi que les procédures de validation correspondantes et toute restriction d'utilisation des certificats.	Cette déclaration s'applique aux certificats qualifiés et non qualifiés délivrés par l'autorité de certification qualifiée ZETES TSP pour le compte des deux organisations suivantes : L'OVB (Orde van Vlaamse Balies), qui regroupe les barreaux locaux belges (néerlandophones) en vertu de l'article 488 du code judiciaire belge L'OBFG (Ordre des barreaux francophones et germanophone de Belgique), qui comprend les barreaux locaux belges (francophones et germanophone) en vertu de l'article 488 du code judiciaire belge OAC – “Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie”, l’ordre en vertu de l'article 481 du code judiciaire belge Ces organisations sont désignées collectivement comme l'OVB-OBFG-OAC et sont considérées comme une seule entité lorsqu'elles sont envisagées en tant qu'abonné pour lequel les certificats sont délivrés en vertu de la présente politique. Elles peuvent être désignées séparément en tant qu'OVB, OBFG et/ou OAC dès lors qu'elles sont perçues dans leur rôle respectif d'organisation exécutrice de tâches, notamment en tant qu'autorité d'enregistrement subordonnée (SUB-RA).

Type de déclaration	Description de la déclaration	Exigences spécifiques prévues par la politique de certification (PC)
		L'OVB-OBFG-OAC est l'abonné, c'est-à-dire que les certificats sont émis au nom de l'OVB-OBFG-OAC pour des personnes physiques associées à l'OVB, à l'OBGF ou à l'OAC et enregistrées par l'une de ces organisations. L'OVB, l'OBFG et l'OAC constituent également l'autorité d'enregistrement subordonnée. Les certificats sont délivrés à des personnes physiques après vérification de leur identité, ainsi qu'après confirmation par l'OVB-OBFG-OAC que la personne peut obtenir un certificat pour le compte de l'OVB-OBFG-OAC et attestation de la part de l'OVB-OBFG-OAC du titre ou de la capacité professionnelle de cette personne. La vérification de l'identité est basée sur la carte d'identité nationale, la carte de résident européen ou le passeport. Voici les principaux types de certificat émis pour les différentes parties : **QCP-n-qscd — prise en charge de la signature électronique qualifié des personnes physiques** Identifiant de politique ETSI 0.4.0.2042.1.2 Identifiant de politique Zetes TSP 1.3.6.1.4.1.47718.2.1.2.2.3.10 Identifiant de profil de certificat Zetes TSP 1.3.6.1.4.1.47718.2.1.3.2.3.10 **NCP+ — prise en charge de l'authentification des personnes physiques** Identifiant de politique ETSI 0.4.0.194112.1.2 Identifiant de politique Zetes TSP 1.3.6.1.4.1.47718.2.1.2.2.1.10 Identifiant de profil de certificat Zetes TSP 1.3.6.1.4.1.47718.2.1.3.2.1.10 Les certificats qualifiés peuvent uniquement être utilisés conformément à la politique de certification applicable et au règlement (UE) 910/2014 du PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Les certificats non qualifiés peuvent uniquement être utilisés conformément à la politique de certification applicable.
Limites de confiance :	Limitation de la confiance, le cas échéant.	Seuls les certificats de type QCP-n-qscd peuvent être utilisés pour la signature électronique avec fonction de non-répudiation. Les certificats de type NCP+ sont destinés à des fins d'authentification et ne doivent pas être utilisés ni considérés comme fiables pour la signature électronique. Les informations d'enregistrement et les journaux d'événements du prestataire de services de confiance sont conservés pendant minimum 7 ans après la fin de validité du certificat reposant sur ces enregistrements (et sont par conséquent disponibles pour fournir des éléments de preuve).

Type de déclaration	Description de la déclaration	Exigences spécifiques prévues par la politique de certification (PC)
		La confiance accordée aux certificats doit tenir compte de la garantie limitée accordée par le prestataire de services de certification et des limitations de responsabilité de ce dernier (voir les points correspondants ci-dessous).
Obligations de l'abonné :	Description des obligations essentielles de l'abonné ou toute référence à celles-ci.	Les obligations de l'abonné incluent notamment : a) le dépôt d'informations précises et complètes auprès du prestataire de services de confiance, notamment en ce qui concerne l'enregistrement ; b) l'utilisation de la paire de clés conformément aux limitations qui lui ont été notifiées ; c) la prévention de toute utilisation non autorisée de la clé privée du détenteur ; d) la seule utilisation de la ou des clés privées du détenteur à des fins cryptographiques dans l'appareil cryptographique sécurisé ; e) la notification du prestataire de services de confiance dans un délai raisonnable, sans retard, dans chacun des cas suivants et ce, jusqu'à la fin de la période de validité indiquée dans le certificat : i) perte, vol ou éventuelle compromission de la clé privée du détenteur ; ii) perte de contrôle sur la clé privée du détenteur suite à la compromission des données d'activation (par ex. le code PIN) ou pour d'autres raisons ; ou iii) correction ou modification apportée au contenu du certificat, telle que notifiée à l'abonné ou au détenteur. f) à la suite d'une compromission, la cessation immédiate et permanente de l'utilisation de la clé privée du détenteur sauf à des fins de déchiffrement de clé ; g) s'il est informé de la révocation du certificat du détenteur ou de la compromission de l'autorité de certification émettrice, la prévention de toute utilisation de la clé privée par le détenteur.
Obligations des parties utilisatrices en matière de vérification de l'état du certificat :	Mesure dans laquelle les parties utilisatrices sont tenues de vérifier l'état du certificat, et références à des explications supplémentaires.	Les parties utilisatrices sont tenues de : a) vérifier la validité, la suspension ou la révocation du certificat sur la base des informations d'état de révocation actuelles, telles qu'indiquées à la partie utilisatrice à la partie utilisatrice via le service OCSP (Online Certificate Status Protocol) : http://ocsp.tsp.zetes.com ;

Type de déclaration	Description de la déclaration	Exigences spécifiques prévues par la politique de certification (PC)
		b) tenir compte de toute restriction d'utilisation du certificat indiquée à la partie utilisatrice dans la politique de certification (et énoncée ci-dessous) ; et c) prendre toute autre précaution prévue dans la DPC et dans la PC applicable, ainsi que suivre les instructions relatives à la déclaration de problèmes (voir ci-dessous).
Limitation et exclusion de garantie / Limitation de responsabilité :	Synthèse des garanties, décharges, limitations de responsabilité et tout programme de garantie ou d'assurance applicable.	*Voir la DPC et/ou la PC applicable : Sections 9.2 sur la couverture d'assurance, 9.6 Déclarations et garanties, 9.7 Exclusions de garanties et 9.8 Limitations de responsabilité.* L'autorité de certification qualifiée ZETES TSP décline explicitement toute responsabilité envers les détenteurs et les parties utilisatrices dans tous les cas où des certificats non qualifiés (notamment des certificats dont le profil de certificat est [NCP+]) sont utilisés dans le contexte d'applications autorisant l'utilisation de tels certificats pour la génération de signatures électroniques qualifiées. Dans les limites fixées par le droit belge, ZETES TSP ne sera en aucun cas (sauf fraude ou faute intentionnelle) tenu responsable en cas de : • perte de profits ; • perte de données ; • dommages indirects, consécutifs ou exemplaires découlant de ou en rapport avec l'utilisation, la délivrance, l'octroi sous licence et l'exécution ou la non-exécution de certificats ou de signatures numériques ; • tout autre dommage en dehors des dommages directs prouvés tels que décrits ci-dessous. En cas de responsabilité de ZETES TSP envers l'abonné, le détenteur ou une partie utilisatrice pour des dommages directs prouvés, la responsabilité de ZETES TSP envers le requérant est quoi qu'il en soit limitée à ce qui suit : • Le paiement de dommages-intérêts s'élevant à 2 500 € maximum par transaction, dans le cas d'événements où la partie utilisatrice se fie à ce certificat pour ce qui est de : a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré, et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié ; ou b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le

Type de déclaration	Description de la déclaration	Exigences spécifiques prévues par la politique de certification (PC)
		certificat qualifié détenait la clé privée correspondant à la clé publique donnée ou identifiée dans le certificat ; ou c) l'assurance que la clé privée et la clé publique puissent être utilisées de façon complémentaire ; et • Le paiement de dommages-intérêts s'élevant à 10 000 € maximum au total par certificat sous-jacent à la requête.
Déclaration de problèmes		Les abonnés, parties utilisatrices, fournisseurs d'applications logicielles et autres tierces parties doivent suivre ces instructions pour signaler des cas présumés de compromission de clé privée, d'utilisation abusive de certificat ou d'autres types de fraude, compromission, abus, conduite inappropriée, ainsi que tout autre problème relatif aux certificats : Les personnes physiques détentrices d'un certificat doivent remplir un rapport auprès de l'agent d'enregistrement dans le bureau de l'autorité locale d'enregistrement (c.-à-d. le bureau du barreau local) ou auprès du prestataire de services de certification via les services de révocation de certificat. L'OVB-OBFG-OAC en tant qu'abonné et autorité d'enregistrement subordonnée doit remplir un rapport via les services de révocation de certificat. Les parties utilisatrices, fournisseurs d'applications logicielles et autres tierces parties peuvent signaler tout problème par e-mail à l'adresse report@tsp.zetes.com ou par courrier ou téléphone à l'aide des informations de contact disponibles sur le site http://tsp.zetes.com.
Politique de confidentialité :	Description de la politique de confidentialité applicable ou toute référence à celle-ci.	Voir la section 9.4 de la PC.
Politique de remboursement :	Description de la politique de remboursement applicable ou toute référence à celle-ci.	Voir la section 9.1 de la PC : ZETES TSP pratique une politique de non-remboursement.
Droit applicable, réclamations et règlement des litiges :	Enoncé du choix de la législation applicable, de la procédure de réclamation et des mécanismes de résolution de litiges (prévoit souvent une	L'applicabilité, l'élaboration, l'interprétation et la validité des relations contractuelles dans le cadre de la DPC et de la PC applicable sont régies par le droit belge (sans égard à aucun principe de conflit de droit qui entraînerait l'application d'autres législations).

Type de déclaration	Description de la déclaration	Exigences spécifiques prévues par la politique de certification (PC)
	référence aux services d'arbitrage des Chambres de commerce internationales).	
Prestataire de services de confiance (TSP), licences de référentiel, marques de confiance et audit :	Synthèse des licences gouvernementales et programmes d'agrément ; description du processus d'audit et, le cas échéant, de la société d'audit.	ZETES TSP apparaît dans la liste de confiance des prestataires de services établis en Belgique : https://tsl.belgium.be/tsl-be.xml.

4 DE - PKI OFFENLEGUNGSERKLÄRUNG

Referenzsprache:

Die englische Version der PKI Offenlegungserklärung ist maßgeblich und verbindlich, obschon die PKI Offenlegungserklärung auch in Übersetzungen in anderen Sprachen verfügbar ist. .

Revisionsverlauf des Dokuments:

Version	Datum	Änderungen
1.3	11/06/2018	OAC tritt den Abonnent bei
1.2	19/05/2017	Mehrsprachige Version
1.1	21/04/2017	Kosmetische Änderungen und Aktualisierung der Erklärung zum Zertifizierungsbetrieb (CPS) und der Zertifizierungsrichtlinie (CP)
1.0	27/03/2017	Erste veröffentlichte Version

PKI Offenlegungserklärung:

Arten von Erklärungen	Beschreibungen der Erklärungen	Besondere Anforderungen an die Zertifikatsrichtlinie
Kontaktinfo des Vertrauensdiensteanbieters (TSP):	Name, Ort und betreffende Kontaktdaten für die Zertifizierungsstelle (CA) / PKI (Name der zuständigen Person, Adresse, Website, Mailadresse für Auskünfte, FAQ usw.), einschließlich eindeutiger Angaben dazu, wie der TSP für die Anforderung eines Widerrufs kontaktiert werden kann.	Kontaktadresse: pma@tsp.zetes.com Postanschrift: ZETES TSP - Straatsburgstraat 3 - 1130 HAREN - BELGIEN Telefon: +32 2 728 37 11 Website: http://tsp.zetes.com
Geltende Verträge, CPS, CP:	Nennung und Referenzen zu geltenden Verträgen, CPS, CP und anderen relevanten Unterlagen.	Die geltenden Verträge sind unter https://repository.tsp.zetes.com und https://pds.tsp.zetes.com veröffentlicht und wie folgt ausgewiesen: **CPS für das Zetes TSP RootCA 001:** Certification Practice Statement OID 1.3.6.1.4.1.47718.2.1.1.1 Version 1.0 **CPS für das Zetes TSP Qualified CA 001:** Certification Practice Statement OID 1.3.6.1.4.1.47718.2.1.1.2 Version 1.3 **CP für im Auftrag von OVB-OBFG-OAC an natürliche Personen ausgegebene Zertifikate** Common Certificate Policy (Allgemeine Zertifizierungsrichtlinie) für im Auftrag von OVB-OBFG-OAC an natürliche Personen ausgegebene Zertifikate OID 1.3.6.1.4.1.47718.2.1.2.2.3.10 und OID 1.3.6.1.4.1.47718.2.1.2.2.1.10 Version 1.3
Zertifikatstyp, Validierungsverfahren und Nutzung:	Beschreibung der einzelnen Klassen/Arten von Zertifikaten, die von der CA ausgegeben werden, sowie der entsprechenden Validierungsverfahren und etwaiger Beschränkungen bezüglich der Zertifikatsnutzung.	Diese Erklärung gilt für qualifizierte und nicht qualifizierte Zertifikate, die von der ZETES TSP Qualified CA im Auftrag für die beiden folgenden Organisationen ausgegeben werden: OVB – Orde van Vlaamse Balies, bestehend aus den (flämischsprachigen) belgischen lokalen Anwaltsvereinigungen gemäß der Definition in Artikel 488 der belgischen Zivilprozessordnung

Arten von Erklärungen	Beschreibungen der Erklärungen	Besondere Anforderungen an die Zertifikatsrichtlinie
		OBFG – l'Ordre des Barreaux Francophones et Germanophone de Belgique, bestehend aus den (französisch- und deutschsprachigen) lokalen Anwaltsvereinigungen gemäß der Definition in Artikel 488 der belgischen Zivilprozessordnung OAC – "Ordre des avocats à la Cour de cassation - Orde van advocaten bij het Hof van Cassatie", Anwaltsvereinigung gemäß der Definition in Artikel 481 der belgischen Zivilprozessordnung Auf diese Organisationen wird zusammen als „OVB-OBFG-OAC" Bezug genommen und sie werden in ihrer Eigenschaft als Abonnent für die Zertifikate gemäß dieser Richtlinie als ein Rechtsträger betrachtet. Bei Bezug auf ihre jeweilige Rolle als einzelne Aufgaben erfüllende Organisation, z. B. als Untergeordnete Registrierungsstelle (Subordinate Registration Authority, SUB-RA) können sie einzeln als OVB, OBFG oder OAC bezeichnet werden. OVB-OBFG-OAC ist der Abonnent, d. h. die Zertifikate werden im Auftrag für OVB-OBFG-OAC an natürliche Personen ausgegeben, die mit der OVB oder der OBFG verbunden und bei dieser registriert sind. OVB, OBFG und OAC sind außerdem die Untergeordnete Registrierungsstelle (Subordinate Registration Authority, SRA). Bevor die Zertifikate an natürliche Personen ausgegeben werden, wird ihre Identität überprüft, und OVB-OBFG-OAC muss bestätigen, dass die betreffende Person zu einem Zertifikat im Auftrag für OVB-OBFG-OAC berechtigt ist, sowie die Berufszulassung bzw. -ausübungsberechtigung der betreffenden Person bescheinigen. Die Identitätsprüfung wird anhand des Personalausweises, der Blauen Karte EU oder des Reisepasses durchgeführt. Für die verschiedenen Parteien werden die folgenden Haupttypen von Zertifikaten ausgegeben: **QCP-n-qscd zur Unterstützung der qualifizierten elektronischen Signatur für natürliche Personen** ETSI Richtlinienidentifikator 0.4.0.2042.1.2 Zetes TSP Richtlinienidentifikator 1.3.6.1.4.1.47718.2.1.2.2.3.10 Zetes TSP Zertifikatsprofilidentifikator 1.3.6.1.4.1.47718.2.1.3.2.3.10 **NCP+ zur Unterstützung der Authentifizierung für natürliche Personen** ETSI Richtlinienidentifikator 0.4.0.194112.1.2 Zetes TSP Richtlinienidentifikator 1.3.6.1.4.1.47718.2.1.2.2.1.10 Zetes TSP Zertifikatsprofilidentifikator 1.3.6.1.4.1.47718.2.1.3.2.1.10 Qualifizierte Zertifikate dürfen nur gemäß der geltenden Zertifikatsrichtlinie (CP) und gemäß der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG verwendet werden.

Arten von Erklärungen	Beschreibungen der Erklärungen	Besondere Anforderungen an die Zertifikatsrichtlinie
		Nicht qualifizierte Zertifikate dürfen nur gemäß der geltenden Zertifikatsrichtlinie (CP) verwendet werden.
Vertrauensgrenzen:	Die Grenzen des Vertrauens auf die Zertifikate, sofern zutreffend.	Nur Zertifikate vom Typ QCP-n-qscd sind zur Verwendung in elektronischen Signaturen mit Non-Repudiation bestimmt. Zertifikate vom Typ NCP+ sind für Authentifizierungszwecke bestimmt und dürfen für elektronische Signaturen weder verwendet noch darf diesen für elektronische Signaturen vertraut werden. Registrierungsinformationen und Ereignisprotokolle des TSP werden mindestens sieben (7) Jahre gespeichert, nachdem ein Zertifikat auf Basis dieser Unterlagen die Gültigkeit verliert (und sind somit als Nachweise während dieser Frist verfügbar). Beim Vertrauen auf die Zertifikate ist die beschränkte Garantie vom Zertifizierungsdienstanbieter (Certificate Service Provider, CSP) und die Haftungsbeschränkung für diesen zu berücksichtigen (siehe unten unter den entsprechenden Themen).
Pflichten des Abonnenten:	Beschreibung der kritischen Abonnentenpflichten bzw. Verweis darauf.	Der Abonnent hat unter anderem die folgenden Pflichten: a) Übermittlung richtiger und vollständiger Informationen an den TSP, insbesondere bezüglich der Registrierung; b) Verwendung des Schlüsselpaares nur gemäß etwaigen dem Abonnenten mitgeteilten Beschränkungen; c) Vermeidung der unbefugten Nutzung des privaten Schlüssels der Person; d) Verwendung des oder der privaten Schlüssel der Person nur für kryptografische Funktionen innerhalb des sicheren kryptografischen Geräts; e) unverzügliche Benachrichtigung des TSP, wenn vor dem Ende des im Zertifikat genannten Gültigkeitszeitraums einer der folgenden Umstände eintritt: i) Verlust, Diebstahl oder potenzielle Kompromittierung des privaten Schlüssels der Person; ii) Verlust der Kontrolle über den privaten Schlüssel der Person aufgrund einer Kompromittierung von Aktivierungsdaten (z. B. PIN-Nummer) oder aus anderen Gründen; oder iii) Unrichtigkeit oder Änderungen am Zertifikatsinhalt gemäß Benachrichtigung an den Abonnenten oder an die Person; f) unverzüglicher und dauerhafter Verzicht auf die weitere Nutzung des privaten Schlüssels der Person im Anschluss auf eine Kompromittierung (außer zur Entschlüsselung des Schlüssels);

Arten von Erklärungen	Beschreibungen der Erklärungen	Besondere Anforderungen an die Zertifikatsrichtlinie
		g) im Falle einer Benachrichtigung darüber, dass das Zertifikat der Person widerrufen oder dass die ausgebende CA kompromittiert wurde, dafür Sorge zu tragen, dass der private Schlüssel von der Person nicht mehr verwendet wird.
Pflichten der vertrauenden Parteien zur Überprüfung des Zertifikatsstatus:	Der Umfang, in dem die vertrauenden Parteien verpflichtet sind, den Zertifikatsstatus zu prüfen, und Verweise auf weitere Erläuterungen.	Die vertrauenden Parteien haben folgende Pflichten: a) die Gültigkeit, Aussetzung oder den Widerruf des Zertifikats mithilfe aktueller Informationen zum Widerrufstatus zu überprüfen, die der vertrauenden Partei über den Online Certification Status Protocol (OCSP)-Dienst angegeben werden: http://ocsp.tsp.zetes.com; b) Nutzungsbeschränkungen für das Zertifikat zu beachten, auf die die vertrauende Partei in der Zertifikatsrichtlinie (CP) hingewiesen wird (und die unten in diesem Dokument angegeben sind); sowie c) weitere Vorsichtsmaßnahmen zu treffen, die in der CPS und in der geltenden CP vorgeschrieben sind, sowie die Anweisungen zur Meldung von Problemen (siehe unten) zu befolgen.
Beschränkte Garantie und Haftungsausschluss bzw. Haftungsbeschränkung:	Zusammenfassung der Garantie, Haftungsausschlüsse, Haftungsbeschränkungen und etwaiger geltenden Garantien oder Versicherungsprogramme.	*Siehe CPS und/oder geltende CP: Abschnitt 9.2 zur Versicherungsdeckung, Abschnitt 9.6 Garantien und Gewährleistungen, Abschnitt 9.7 Gewährleistungsausschlüsse und Abschnitt 9.8 Haftungsbeschränkungen.* ZETES TSP Qualified CA lehnt ausdrücklich jegliche Haftung gegenüber Personen und vertrauenden Parteien in sämtlichen Fällen ab, in denen nicht qualifizierte Zertifikate (z. B. Zertifikate mit dem Zertifikatsprofil: [NCP+]) im Zusammenhang mit Anwendungen verwendet werden, die die Nutzung besagter Zertifikate für die Generierung qualifizierter elektronischer Signaturen zulassen. Innerhalb der gemäß belgischem Recht geltenden Grenzen haftet ZETES TSP in keinem Fall (ausgenommen bei Betrug oder vorsätzlichem Fehlverhalten) für: • entgangene Gewinne, • Datenverluste, • mittelbare Schäden, Folgeschäden oder Strafe einschließende Schäden, die sich aus oder in Verbindung mit der Nutzung, Bereitstellung, Lizenz und Ausführung oder Nichtausführung von Zertifikaten oder digitalen Signaturen ergeben, • sonstige Schäden, die über nachweisliche unmittelbare Schäden gemäß nachfolgender Beschreibung hinausgehen.

Arten von Erklärungen	Beschreibungen der Erklärungen	Besondere Anforderungen an die Zertifikatsrichtlinie
		Im Falle der Haftung von ZETES TSP gegenüber dem Abonnenten, der Person oder einer vertrauenden Partei für nachweisliche unmittelbare Schäden ist die Haftung von ZETES TSP gegenüber jeglichem Geschädigten in jedem Fall beschränkt auf: • die Zahlung von Schäden bis zu einem Höchstbetrag von 2500 € pro Transaktion, für Ereignisse, bei denen die vertrauende Partei auf das betreffende Zertifikat vertraut: a) bezüglich der Richtigkeit zum Zeitpunkt der Ausgabe sämtlicher im qualifizierten Zertifikat enthaltenen Informationen und bezüglich der Tatsache, dass das Zertifikat sämtliche für ein qualifiziertes Zertifikat vorgeschriebenen Details enthält; oder b) für die Versicherung, dass der im qualifizierten Zertifikat genannte Signatar zum Zeitpunkt der Ausgabe des Zertifikats im Besitz des privaten Schlüssels war, der dem im Zertifikat vergebenen oder genannten öffentlichen Schlüssel entspricht; oder c) für die Versicherung, dass der private Schlüssel und der öffentliche Schlüssel zusammen verwendet werden können; sowie • die Zahlung von Schäden in einer Höhe von insgesamt maximal 10.000 € pro Zertifikat, das der Schadenersatzforderung zugrunde liegt.
Meldung von Problemen		Abonnenten, vertrauende Parteien, Anwendungssoftwarelieferanten und andere Drittparteien sollten die folgenden Anweisungen für die Meldung mutmaßlicher Kompromittierungen privater Schlüssel, Zertifikatsmissbräuche oder anderer Arten von Betrug, Kompromittierungen, Missbräuchen, unangemessenem Verhalten oder anderweitigen Angelegenheiten in Bezug auf Zertifikate befolgen: Natürliche Personen, die Inhaber von Zertifikaten sind, müssen eine Meldung beim Registrierungsreferenten der lokalen RA-Geschäftsstelle (d. h. der Geschäftsstelle der lokalen Anwaltsvereinigung) oder beim Zertifizierungsdienstanbieter (Certificate Service Provider, CSP) über die Zertifizierungswiderrufsdienste erstatten. OVB-OBFG-OAC als Abonnent und als Untergeordnete Registrierungsstelle (Subordinate Registration Authority) muss eine Meldung über die Zertifizierungswiderrufsdienste erstatten.

Arten von Erklärungen	Beschreibungen der Erklärungen	Besondere Anforderungen an die Zertifikatsrichtlinie
		Vertrauende Parteien, Anwendungssoftwareanbieter oder andere Drittparteien können Meldungen von Problemen per E-Mail bei report@tsp.zetes.com oder auf dem Postweg oder telefonisch über die auf http://tsp.zetes.com veröffentlichten Kontaktinformationen erstatten.
Datenschutzrichtlinie:	Eine Beschreibung der geltenden Datenschutzrichtlinie und Verweis auf diese.	Siehe Abschnitt 9.4 der CP.
Erstattungsrichtlinie:	Eine Beschreibung der geltenden Erstattungsrichtlinie und Verweis auf diese.	Siehe Abschnitt 9.1 „Gebühren“ der CP. Die Erstattungsrichtlinie von ZETES TSP sieht keine Erstattungen vor.
Anwendbares Recht, Beschwerden und Beilegung von Streitigkeiten:	Erklärung über die Rechtswahl, das Beschwerdeverfahren und die Mechanismen zur Beilegung von Streitigkeiten (so geregelt, dass sie oft einen Verweis auf die Schiedsgerichtsdienste der Internationalen Handelskammer einschließen).	Für die Durchsetzbarkeit, Auslegung, Interpretation und Gültigkeit der vertraglichen Beziehungen bezüglich der CPS und der geltenden CP ist das belgische Recht maßgeblich. (Gesetzeskollisionen, die zur Anwendung eines anderen Rechts führen würden, sind nicht wirksam.)
TSP- und Repository-Lizenzen, Vertrauenskennzeichen und Prüfung:	Zusammenfassung von Regierungslizenzen, Siegelprogrammen sowie eine Beschreibung des Prüfprozesses und gegebenenfalls der Prüfungsfirma.	ZETES TSP ist auf der belgischen Liste vertrauenswürdiger Anbieter gelistet: https://tsl.belgium.be/tsl-be.xml.

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