ZETESCONFIDENS

DISCLOSURE STATEMENTS FOR THE TIME-STAMP CA AND FOR THE TIME-STAMP SERVICES

English

Title:	ZetesCONFIDENS
Subject:	Disclosure Statements for the timestamp CA and for the time-stamp services
Category:	PDS - public information for Subscribers and Relying Parties
Version:	1.1
Status:	Approved
Publish date:	08/05/2020
CA PDS OID: TSA PDS OID:	1.3.6.1.4.1.47718.2.1.5.50 1.3.6.1.4.1.47718.2.2.5.50
Author:	ZETES TSP (Bart Symons / Jos De Wachter)
Classification:	PUBLIC
Copyright:	© 2018 Zetes - All rights reserved.

1 PKI DISCLOSURE STATEMENT FOR THE CA FOR TSA

Document History:

version	date	Changes
1.1	**27/04/2020**	**Changed title page. Added © statement. Removed confidentiality statement.**
1.0	24/12/2018	Initial 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: https://tsp.zetes.com https://confidens.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://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/CP for the Zetes TSP CA FOR TSA 001:** Certification Practice Statement OID 1.3.6.1.4.1.47718.2.1.1.50 Certificate Policy OID 1.3.6.1.4.1.47718.2.1.2.50

Statement types	Statement descriptions	Specific Requirements of certificate policy
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 CA FOR TSA for qualified time-stamps and non-qualified time-stamps. The relevant Certificate Policy and Certification Practice Statement (CP/CPS) applies to the issuance of certificates for the ZETESCONFIDENS TSA Time-Stamp Units issuing non-qualified time-stamps and qualified time-stamps meeting the requirements of Regulation (EU) No 910/2014. 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.	Records for certificate issuance are maintained for minimum 7 years after any certificate based on these records ceases to be valid (and hence can be made 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 beneficiary of the Certificates issued by the ZETES TSP CA FOR TSA are only Time-Stamping Units internal to ZETESCONFIDENS TSA.
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 certificate status information from the Online Certificate Status Protocol (OCSP) service or the Certificate Revocation List download service which are indicated in the certificates themselves. b) take account of any limitations on the usage of the certificate indicated to the relying party in the certificate itself; and 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 d) 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
Limited warranty and disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	See Certificate Policy and Certification Practice Statement (CP/CPS): 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. *Within the limit set by Belgian Law, in no event (except for fraud or willful misconduct) will ZETESCONFIDENS be liable for:* • *Any loss of profits;* • *Any loss of data;* • *Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;* • *Any other damages beyond proven direct damages as described below.* *In case of liability of ZETESCONFIDENS towards the Subscriber or a Relying Party for proven direct damages, the liability of ZETESCONFIDENS towards any claimant is in any way limited to:* *- paying damages amounting up to a maximum of 2.500 € per transaction, for events where the Relying Party relies on that certificate:* *a) as regards the accuracy at the time of issuance of all information contained in the (Qualified) Certificate and as regards the fact that the Certificate contains all the details prescribed for a (Qualified) Certificate; or* *b) for assurance that at the time of the issuance of the Certificate, the signatory identified in the Qualified Certificate held the private key corresponding to the public key given or identified in the Certificate; or* *c) for assurance that the private key and the public key can be used in a complementary manner;* *and* *- paying damages amounting up to a maximum of 10.000 € in total per TSU Certificate that is underlying to the claim.* *In any case, whatever originating facts and prejudices and their aggregate amounts, ZETESCONFIDENS responsibility will be limited to the amount paid by the Subscriber to ZETESCONFIDENS regarding the originating fact, with respect to the governing law. Unless otherwise legally enacted, any suit from the Subscriber regarding these CP will take place no longer than six months after the fact originating the legal action.*

Statement types	Statement descriptions	Specific Requirements of certificate policy
Problem reporting		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: they 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.	Not applicable.
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 for its CA/QC offering. The Trusted List can be found: https://tsl.belgium.be/tsl-be.xml . ZETES TSP will undergo auditing under the eIDAS – ETSI EN 319 403 – ISO 17065 standards by LSTI to become listed in the future for TSA/QTST offering.

2 TSA DISCLOSURE STATEMENT

Document History:

version	date	changes
1.1	**27/04/2020**	**Changed title page. Added © statement. Removed confidentiality statement.**
1.0	03/10/2018	Initial version

TSA 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: https://tsp.zetes.com https://confidens.zetes.com
Applicable agreements, TSA Practice Statement, Time-stamp Policy:	Identification and references to applicable agreements.	This disclosure statement is merely an iteration of information to be found in the Practice Statements and policy and not the entire agreement. The TSA Practice Statement and Time-stamp Policy, in conjunction with the Certification Practice Statement and Certificate Policy (CPS/CP) of the ZETES TSP CA for TSA, constitutes the main set of terms and conditions for the provision and use of the time-stamp services. A Relying Party can rely on all information available in the present policy and the CPS/CP. All information is available on http://tsp.zetes.com/. The Relying Party shall be deemed to have tacitly accepted other TSP terms and conditions incorporated in the relevant public documents such as the TSA's CA CPS and CP upon relying on the time-stamp.

<table>
<tr><th>Statement types</th><th>Statement descriptions</th><th>Specific Requirements of certificate policy</th></tr>
<tr><td></td><td></td><td>The TSA Practice Statement and Time-stamp Policy is labelled as follows:

TSA Practice Statement and Time-stamp Policy:
TSA Practice Statement
OID 1.3.6.1.4.1.47718.2.2.1
Time-stamp Policy
OID 1.3.6.1.4.1.47718.2.2.2</td></tr>
<tr><td>Electronic time-stamp:

types and usage</td><td>A description of each class/type of electronic time-stamps issued by the TSA (in accordance with each time-stamp policy) and any restrictions on time-stamp usage.</td><td>Time-stamp tokens are signed using a key which is exclusively used for time-stamping. Each TSU has a unique key. Each key is associated with a single and unique certificate.

Time-stamp tokens will contain the following OID for identification of the applicable policy:
<table>
<tr><th>OID</th><th>Description</th></tr>
<tr><td>1.3.6.1.4.1.47718.2.2.2.50</td><td>Zetes OID for this time-stamp policy for qualified time-stamps</td></tr>
<tr><td>1.3.6.1.4.1.47718.2.2.2.51</td><td>Zetes OID for this time-stamp policy for non-qualified time-stamps</td></tr>
</table>
By including these object identifiers in the generated time-stamps, ZETES TSA claims conformance to this time-stamp policy and to the ETSI BTSP best practices policy for time-stamps (OID 0.4.0.2023.1.1).

Information on the algorithms and expected life time per TSU can be found in the below table:
<table>
<tr><th>TSU</th><th>Common Name in the TSU certificate</th><th>Algorithm and Key length</th></tr>
<tr><td>TSU1</td><td>ZETES TSP RSA Qualified TSU1</td><td>RSA3072 or better</td></tr>
<tr><td>TSU2</td><td>ZETES TSP RSA Qualified TSU2</td><td>RSA3072 or better</td></tr>
<tr><td>TSU3</td><td>ZETES TSP EC Qualified TSU3</td><td>ECC256 or better</td></tr>
<tr><td>TSU4</td><td>ZETES TSP EC Qualified TSU4</td><td>ECC256 or better</td></tr>
<tr><td>TSU5</td><td>ZETES TSP RSA TSU5</td><td>RSA3072 or better</td></tr>
<tr><td>TSU6</td><td>ZETES TSP RSA TSU6</td><td>RSA3072 or better</td></tr>
<tr><td>TSU7</td><td>ZETES TSP EC TSU7</td><td>ECC256 or better</td></tr>
<tr><td>TSU8</td><td>ZETES TSP EC TSU8</td><td>ECC256 or better</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Statement types</th><th>Statement descriptions</th><th>Specific Requirements of certificate policy</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>TSU9</td><td>ZetesConfidens RSA Qualified TSU9</td><td>RSA2048 or better</td></tr>
<tr><td>TSU10</td><td>ZetesConfidens RSA Qualified TSU10</td><td>RSA2048 or better</td></tr>
<tr><td>TSU11</td><td>ZetesConfidens EC Qualified TSU11</td><td>ECC256 or better</td></tr>
<tr><td>TSU12</td><td>ZetesConfidens EC Qualified TSU12</td><td>ECC256 or better</td></tr>
<tr><td>TSU13</td><td>ZetesConfidens RSA TSU13</td><td>RSA2048 or better</td></tr>
<tr><td>TSU14</td><td>ZetesConfidens RSA TSU14</td><td>RSA2048 or better</td></tr>
<tr><td>TSU15</td><td>ZetesConfidens EC TSU15</td><td>ECC256 or better</td></tr>
<tr><td>TSU16</td><td>ZetesConfidens EC TSU16</td><td>ECC256 or better</td></tr>
</table>
Information on any limitations on the use of the timestamp and information on how to verify the time-stamp can be found in the Time-stamp policy under section 6.2.
</td></tr>
<tr><td>Reliance limits:</td><td>The reliance limits, if any.</td><td>Indication of the accuracy of the time in the time-stamp, and the period of time for which TSA event logs are
maintained (and hence are available to provide supporting evidence) can be found in the Time-stamp policy under section 6.2 and 6.3.</td></tr>
<tr><td>Obligations of subscribers:</td><td>The description of, or reference to, the critical subscriber obligations.</td><td>Subscribers must verify for each fresh time-stamp token that it has been correctly formatted and correctly signed and check that the TSU certificate is valid and that the certificate expiration date fits the Subscriber’s needs.
Subscribers must use secure cryptographic suites for time-stamping requests.
Subscribers should inform their end-users and other Relying Parties about the Time-Stamp Policy.
Subscribers should include or archive the TSU certificate status information with the object to be time stamped.
Subscribers should rely on DNS services that respect the TTL value of the A record when accessing the time-stamp services and certificate status services.</td></tr>
<tr><td>TSU public key certificate status checking obligations of relying parties:</td><td>The extent to which relying parties are obligated to check the TSU public key certificate status, and references to further explanation.</td><td>Before placing any reliance on a time-stamp, a Relying Party must verify that the time-stamp has been correctly signed and that the certificate used to sign the time-stamp was valid at the time indicated in the timestamp.
The Relying Party must take into account any limitations on usage of the time-stamp indicated by this Time-Stamp Policy.</td></tr>
</table>

Statement types	Statement descriptions	Specific Requirements of certificate policy
		For qualified time-stamps, ETSI EN 319 421 states: "The relying party is expected to use a Trusted List to establish whether the timestamp unit and the timestamp are qualified. If the public key of the TSU is listed in the Trusted List and the service it represents is a qualified time-stamping service, then the time-stamps issued by this TSU can be considered as qualified." During the TSU certificate validity period, the status of the certificate can be checked using the relevant CRL. ZETESCONFIDENS CA certificates, TSU certificates and the related CRLs are published at https://crt.tsp.zetes.com and https://crl.tsp.zetes.com. Relying parties should rely on DNS services that respect the TTL value of the A record when accessing the time-stamp services and certificate status services. If this verification takes place after the end of the validity period of the certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421.
Limited warranty and disclaimer/Limitation of liability:	Summary of the warranty, disclaimers, limitations of liability and any applicable warranty or insurance programs.	See Certificate Policy and Certification Practice Statement (CP/CPS) for CA for TSA: 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 *Within the limit set by Belgian Law, in no event (except for fraud or willful misconduct) will ZETESCONFIDENS be liable for:* • *Any loss of profits;* • *Any loss of data;* • *Any indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of certificates or digital signatures;* • *Any other damages beyond proven direct damages as described below.* *In case of liability of ZETESCONFIDENS towards the Subscriber or a Relying Party for proven direct damages, the liability of ZETESCONFIDENS towards any claimant is in any way limited to:* *- paying damages amounting up to a maximum of 50 € per transaction, for events where the Relying Party relies on the certificate and time-stamp token (TST):* *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*

Statement types	Statement descriptions	Specific Requirements of certificate policy
		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; or* *d) as regards the accuracy of the time mentioned in the TST;* *and* *- paying damages amounting up to a maximum of 200 € in total per TSU Certificate that is underlying to the claim.* *In any case, whatever originating facts and prejudices and their aggregate amounts, ZETESCONFIDENS responsibility will be limited to the amount paid by the Subscriber to ZETESCONFIDENS regarding the originating fact, with respect to the governing law. Unless otherwise legally enacted, any suit from the Subscriber regarding these CP will take place no longer than six months after the fact originating the legal action.* Additional limitations of liability between ZETESCONFIDENS and the Subscriber can be part of the Subscriber agreement concluded between the parties.
Privacy policy:	A description of and reference to the applicable privacy policy.	See section 9.4 of the Certificate Policy and Certification Practice Statement (CP/CPS) for CA for TSA.
Refund policy:	A description of and reference to the applicable refund policy.	No refund is being made.
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 TSA Practice Statement and applicable Time-stamp Policy (without giving effect to any conflict of law provision that would cause the application of other laws).

Statement types	Statement descriptions	Specific Requirements of certificate policy
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.	ZETESCONFIDENS (ZETES TSP) is listed on the Belgian Trusted List for its CA/QC offering. The Trusted List can be found: https://tsl.belgium.be/tsl-be.xml . ZETESCONFIDENS will undergo auditing under the eIDAS – ETSI EN 319 403 – ISO 17065 standards by LSTI to become listed in the future for TSA/QTST offering.

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