



**ZETESCONFIDENS**

**TSA PRACTICE STATEMENT AND TIME-STAMP POLICY**

**TSA Practise Statement and Time-Stamp Policy**

Publication date :	22/07/2019		
Effective date :	29/07/2019		
TSA Practice Statement OID:	1.3.6.1.4.1.47718.2.2.1.50		
Time-Stamp Policy OID :	1.3.6.1.4.1.47718.2.2.2.50 1.3.6.1.4.1.47718.2.2.2.51		
Version :	1.2	15/07/2019	draft
<b>Copyright :</b>  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.  The following sentence must appear on any copy of this document: "© 2019 – Zetes – All Rights Reserved"			

## Table of Content

<b>ABOUT ZETES .....</b>	<b>4</b>
<b>1 SCOPE.....</b>	<b>5</b>
<b>2 REFERENCES .....</b>	<b>7</b>
<b>3 DEFINITIONS AND ABBREVIATIONS .....</b>	<b>8</b>
3.1 Definitions .....	8
3.2 Abbreviations.....	8
<b>4 GENERAL CONCEPTS.....</b>	<b>10</b>
4.1 Time-Stamping Services (TSS).....	10
4.2 Time-Stamping Authority (TSA).....	10
4.3 Subscriber .....	10
4.4 Practice Statement and Time-Stamp Policy.....	10
<b>5 TIME-STAMP POLICIES.....</b>	<b>11</b>
5.1 General .....	11
5.2 Identification .....	11
5.3 User Community and Applicability .....	11
5.4 Policy administration .....	11
5.4.1 Organization administering the document .....	11
5.4.2 Contact person.....	12
5.4.3 Policy Approval procedures .....	12
<b>6 POLICIES AND PRACTICES .....</b>	<b>13</b>
6.1 Risk assessment .....	13
6.2 Trust Service Policy Management Authority .....	13
6.2.1 Time-stamp format .....	14
6.2.2 Accuracy of the time .....	14
6.2.3 Limitations on usage of the service.....	15
6.2.4 Obligations of the subscriber .....	15
6.2.5 Obligations of relying parties .....	15
6.2.6 Verification of the timestamp .....	15
6.2.7 Applicable law .....	15
6.2.8 Service Availability .....	16
6.3 Terms and conditions .....	16
6.3.1 Trust service policy being applied .....	16
6.3.2 Retention of trust service event logs .....	16
6.4 Information for relying parties .....	16
<b>7 TSA MANAGEMENT AND OPERATION .....</b>	<b>17</b>
7.1 Internal organization .....	17
7.2 Personnel security .....	17
7.3 Asset management .....	17
7.4 Access control .....	17
7.5 Cryptographic controls .....	18
7.5.1 General .....	18
7.5.2 TSU key generation .....	18
7.5.3 TSU private key protection .....	18
7.5.4 TSU public key certificate.....	18
7.5.5 Rekeying TSU's key .....	18
7.5.6 Life cycle management of signing cryptographic hardware - BSY.....	19
7.5.7 End of TSU key life cycle - BSY.....	19
7.6 Timestamping and Clock synchronization with UCT.....	19
7.7 Physical and environmental security .....	19
7.8 Operation security .....	20
7.9 Network security .....	20
7.10 Incident management.....	20
7.11 Collection of evidence .....	20

7.12	Business continuity management.....	20
7.13	TSA termination and termination plans.....	21
7.14	Conformance .....	21
<b>8</b>	<b>TIME-STAMP TOKENS AND CERTIFICATES.....</b>	<b>22</b>
8.1	TSU time-stamp token profiles .....	22
8.2	TSU public key certificates .....	22
8.2.1	ZETES TSP RSA Qualified TSU1 .....	23
8.2.2	ZETES TSP RSA Qualified TSU2 .....	25
8.2.3	ZETES TSP EC Qualified TSU3 .....	27
8.2.4	ZETES TSP EC Qualified TSU4 .....	29
8.2.5	ZETES TSP RSA TSU5.....	31
8.2.6	ZETES TSP RSA TSU6.....	33
8.2.7	ZETES TSP EC TSU7.....	35
8.2.8	ZETES TSP EC TSU8.....	37
8.2.9	ZetesConfidens RSA Qualified TSU9.....	39
8.2.10	ZetesConfidens RSA Qualified TSU10.....	41
8.2.11	ZetesConfidens EC Qualified TSU11 .....	43
8.2.12	ZetesConfidens EC Qualified TSU12 .....	45
8.2.13	ZetesConfidens RSA TSU13 .....	47
8.2.14	ZetesConfidens RSA TSU14 .....	49
8.2.15	ZetesConfidens EC TSU15 .....	51
8.2.16	ZetesConfidens EC TSU16 .....	53
<b>9</b>	<b>TSA ISSUING NON-QUALIFIED AND QUALIFIED ELECTRONIC TIME-STAMPS AS PER REGULATION (EU) NO 910/2014 .....</b>	<b>55</b>

## ABOUT ZETES

### About Zetes SA

Founded in 1984, Zetes SA is a company incorporated in Belgium (European Union) and is part of the Zetes Group, which is fully owned by the Panasonic Group.

Zetes SA is active in the areas of identification documents, travel documents, biometrics and trust services including the issuance of certificates.

All further references to “Zetes” in this document refer to the legal entity Zetes SA unless explicitly stated otherwise.

Zetes SA is active in the areas of identification documents, travel documents, smartcards, biometric solutions and trust services.

Zetes SA is registered as follows:

Dutch language	French language	English language
<b>Zetes NV<sup>(*)</sup></b>	<b>Zetes SA<sup>(*)</sup></b>	<b>Zetes SA<sup>(*)</sup></b>
Straatsburgstraat 3 1130 Brussel België  BTW BE 0408 425 626	Rue de Strasbourg 3 1130 Bruxelles Belgique  TVA BE 0408 425 626	Rue de Strasbourg 3 1130 Brussels Belgium  VAT BE 0408 425 626

*(\*) Under Belgian law, NV (Dutch Naamloze Vennootschap) and SA (French Société Anonyme) are equivalent terms.*

### About ZetesConfidens business unit

In 2016, Zetes Trust Services Provider (ZETES TSP) was established as an operational business unit within Zetes SA to provide certificate services and other trust services for governments, the financial sector and private Organizations. Since September 2018 these activities are marketed under the ZetesConfidens name. Previous reference to ZETES TSP can be replaced by ZETESCONFIDENS.

ZetesConfidens is acting as the Time-stamping Authority (TSA) and has final and overall responsibility for the provision of the ZETESCONFIDENS (Qualified) time-stamping service offering, namely:

- Time-stamping provision services: provides the generation of the time-stamps through the ZETESCONFIDENS time-stamping units (TSU)
- Time-stamping management services: provides the monitoring and control of the operation of the time-stamping services to ensure that the service is provided as specified by the Time-Stamp Authority (TSA).

ZETESCONFIDENS operates its own trust infrastructure and acts as a Trusted Service Provider (TSP) as defined in the Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market [9]. To this regard, ZETESCONFIDENS is supervised by the FPS Economy, SMEs, Self-employed and Energy - Quality and Safety, the Belgian Supervisory Body and audited to be listed in the Belgian Trusted List of Qualified Trust Service Providers.

## 1 SCOPE

---

A time-stamp service provides proof that a data object existed at a particular moment in time and that it has not changed since it was time-stamped. This service can be used to provide additional support to non-repudiation service, to support long term archiving and to prove that an electronic signature was actually generated during the period the public key certificate was valid. ZETESCONFIDENS Time-stamping services are provided according to IETF RFC 3161.

The present document is the “TSA Practise Statement and Time-Stamp Policy” to which the ZETESCONFIDENS Time Stamping Authority (TSA) conforms to.

The policy applies to the issuance of electronic time stamps meeting the requirements of Regulation (EU) No 910/2014 [9].

The provision and use of (Qualified) Time-Stamp issued by ZETES TSA are governed by the following documents:

- this TSA Practise Statement and Time-Stamp Policy,
- the ZETESCONFIDENS Certification Practice Statement and Certificate Policy for the ZETESCONFIDENS CA for TSA,

### Conformity with European legislation and standards for Trust Service Providers issuing time-stamps

This policy is in accordance with the requirements laid down in the Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. It respects requirements for Qualified Trust Services Providers issuing Time-Stamps where applicable.

This Time-Stamp Policy conforms to the requirements laid down in ETSI EN 319 421 [4] “Policy and Security Requirements for Trust Service Providers issuing Time-Stamps” and ETSI EN 319 422 [5] “Time-stamping protocol and time-stamp token profiles”.

### Intellectual Property Rights

Without limiting the “all rights reserved” copyright on the present document, and except as duly licensed under written form, 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 Zetes SA.

The following sentence must appear on any copy of this document:

"© 2018 – Zetes – All Rights Reserved"

**Document Version History**

Version	Publication Date	Effective Date	Information about this Version
1.2	22/07/2019	29/07/2019	Correction of typos.  Update of the TSU certificate information in chapter 8.2 due to renewal of the certificates.  Clarification of the TSU key lifecycle log retention period in chapter 6.3.2
1.1	21/03/2019	25/03/2019	Additional ZetesConfidens TSUs
1.0	24/12/2018	31/12/2018	first publication -----

## 2 REFERENCES

---

The following documents contain provisions which are relevant to the ZETESCONFIDENS Timestamp Policy:

- [1] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
- [2] ETSI EN 319 401, v2.2.1 (2018-04): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
- [3] ETSI EN 319 403, v2.2.2 (2015-08): Electronic Signatures and Infrastructures (ESI). Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- [4] ETSI EN 319 421, v1.1.1 (2016-03) Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.
- [5] ETSI EN 319 422 v1.1.1 (2016-03), Electronic Signatures and Infrastructures (ESI); Timestamping Protocol and Time-stamp Token Profiles.
- [6] ETSI TS 119 312 v1.2.1 (2017-05): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- [7] IETF RFC 3161 (2001), "Internet X.509 Public Key Infrastructure Time-stamp Protocol (TSP)".
- [8] IETF RFC 5816 "ESSCertIDV2 update to RFC 3161"
- [9] Regulation (EU) No 910/2014 of 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. (eIDAS regulation)
- [10] BIPM Circular T. (Available from the BIPP website <http://www.bipm.org/>)
- [11] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules"

## 3 DEFINITIONS AND ABBREVIATIONS

### 3.1 Definitions

<b>Certificate</b>	A unit of information contained in a file that is digitally signed by the Certification Authority. It contains, at a minimum, the issuer, a public key, and a set of information that identifies the entity that holds the private key corresponding to the public key.
<b>Certificate Revocation List (CRL)</b>	A signed list of identifiers of Certificates that have been revoked. Abbreviated as CRL. It is (periodically) made available by the CA to Subscribers and Relying Parties.
<b>Coordinated Universal Time (UTC)</b>	Time-scale maintained by the Bureau International des Poids et Mesures (BIPM), which forms the basis of a coordinated dissemination of standard frequencies and time signals as defined in Recommendation ITU-RTF.460-6[1]
<b>Hardware Security Module (HSM)</b>	An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.
<b>Qualified time-stamp</b>	Electronic time-stamp which meets the following requirements: <ul style="list-style-type: none"> <li>• Binds the date and time to data so as to reasonably prevent the possibility of any undetected change of the data</li> <li>• It is based on an accurate time source that can be traced to UTC(k)</li> </ul> It is signed using an advanced electronic signature of the qualified trust service provider, or some equivalent method.
<b>Relying party</b>	Recipient of a time-stamp who relies on that time-stamp.
<b>Subscriber</b>	Legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.
<b>Time-stamp</b>	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.
<b>Time-stamp Authority (TSA)</b>	TSP providing time-stamping services using one or more time-stamping units.
<b>Time-stamp Service (TSS)</b>	Trust service for issuing time-stamps
<b>Time-Stamp Token (TST)</b>	Data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.
<b>Time-Stamping Unit (TSU)</b>	A set of hardware and software which is managed as a unit and has a single private signing key active at a time
<b>Trust Service Provider (TSP)</b>	Entity which provides one or more trust services
<b>TSA system</b>	Composition of IT products and components organized to support the provision of time-stamping services
<b>UTC(k)</b>	Time-scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach $\pm 100\text{ns}$ .

### 3.2 Abbreviations

<b>BIPM</b>	Bureau International des Poids et Mesures
<b>BTSP</b>	Best practices Time-Stamp Policy
<b>CA</b>	Certificate Authority
<b>CP</b>	Certificate Policy
<b>CPS</b>	Certification Practice Statement
<b>CRL</b>	Certificate Revocation List
<b>CSP</b>	Certification Service Provider



<b>DN</b>	Distinguished Name
<b>HSM</b>	Hardware Security Module
<b>OCSP</b>	Online Certificate Status Protocol
<b>OID</b>	Object Identifier
<b>PKI</b>	Public Key Infrastructure
<b>PMA</b>	Policy Management Authority
<b>RA</b>	Registration Authority
<b>TSA</b>	Time-Stamp Authority
<b>TSS</b>	Time-stamp System
<b>TST</b>	Time-stamp token
<b>TSU</b>	Time-Stamp Unit
<b>UTC(k)</b>	Coordinated Universal Time

## 4 GENERAL CONCEPTS

---

The present document references ETSI EN 319 401 [2] for generic policy requirements common to all classes of trust service providers services and ETSI EN 319 421 [4] for policy requirements that are specific to the time-stamping trust service.

### 4.1 Time-Stamping Services (TSS)

---

Time-Stamp Services (TSS) include the following component services:

- **Time-stamping provisioning:** The service component that generates time-stamps.
- **Time-stamping management:** The service component that monitors and controls the operation of the time-stamping services, including synchronization with UTC time source(s). Time-stamping management is also responsible for the installation and de-installation of the time-stamping provisioning service.

### 4.2 Time-Stamping Authority (TSA)

---

Under this policy Zetes SA Time-Stamp Authority (TSA) is providing the time-stamping services (TSS) as identified in paragraph 4.1.

The TSA operates multiple environments with TSUs which generate time-stamp tokens on behalf of the TSA. The TSUs responsible for issuing a time-stamp are identifiable by signing the time-stamp tokens using a key generated exclusively for this purpose.

The TSA has overall responsibility for meeting the requirements defined in the present document.

### 4.3 Subscriber

---

The Subscriber enters into a contractual agreement with Zetes SA. The Subscriber is a legal or natural person for whom time-stamp is issued and who is bound to the subscriber obligations.

If the subscriber is an organization, it comprises several end-users or an individual end-user and some of the obligations that apply to that organization will also apply to the end-users. As the subscriber, the organization will be responsible in case the obligations from the end-users are not correctly fulfilled. The subscriber has the obligation to inform the end-users about their obligations and about the conditions of use of the time-stamp service.

If the subscriber is the end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

### 4.4 Practice Statement and Time-Stamp Policy

---

The present document constitutes and combines the practice statement and the time-stamp policy. The practice statement and time-stamp policy provide information as to how the provided time-stamping services meet the requirements through proper infrastructure, management, organization, etc.

## 5 TIME-STAMP POLICIES

---

### 5.1 General

---

This policy defines a set of processes for the trustworthy creation of time-stamp tokens.

The time-stamp tokens adhere to the requirements laid down in RFC 3161 (updated by RFC 5816), ETSI EN 319 421 [4] and ETSI EN 319 422 [5].

The certificates for the TSUs are issued by a CA dedicated to timestamp purposes. These certificates adhere to the requirements laid down in ETSI EN 319 411 part 1 and where required ETSI EN 319 411 part 2.

### 5.2 Identification

---

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:

OID	Description
1.3.6.1.4.1.47718.2.2.2.50	Zetes OID for this time-stamp policy for qualified time-stamps
1.3.6.1.4.1.47718.2.2.2.51	Zetes OID for this time-stamp policy for non-qualified time-stamps

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 which is identified by the OID 0.4.0.2023.1.1 (itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)).

The TSA may provide time-stamp tokens for test purposes but signed with the genuine TSU certificates. These time-stamp tokens will contain OID with a prefix 2.999 for identification of the applicable:

OID	Description
2.999.1.3.6.1.4.1.47718.2.2.2.50	Zetes OID for test purposes in relation to this time-stamp policy

### 5.3 User Community and Applicability

---

This policy is aimed at meeting the requirements of time-stamp for long term validity (e.g. as defined in ETSI EN 319 122) but is generally applicable to any use which has a requirement for equivalent quality.

The time-stamping service is used by the Subscribers for the purpose and user community the Subscriber sees fit. The Subscriber assumes full responsibility for the time-stamp tokens' application and purpose. It is the responsibility of the Subscriber to manage and inform its user community.

### 5.4 Policy administration

---

#### 5.4.1 Organization administering the document

The present document is administered by the ZETESCONFIDENS Policy Management Authority (PMA).

The PMA determines the present document's suitability for the ZETESCONFIDENS trust services.

### 5.4.2 Contact person

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

<b>E-mail address:</b>	pma@tsp.zetes.com	
<b>Postal address:</b>	Straatsburgstraat 3	3, rue de Strasbourg
	1130 HAREN	1130 HAEREN
	BELGIË	BELGIQUE
<b>Telephone:</b>	0032 2 728 37 11	
<b>Web site:</b>	<a href="http://tsp.zetes.com">http://tsp.zetes.com</a>	

### 5.4.3 Policy Approval procedures

The PMA is responsible for the approval of the policies and practice statements.

A Change Control mechanism will be used to trace all identified changes to the content of this Certification Practice Statement and Certificate Policy.

This Practice Statement and Policy shall be reviewed in its entirety every year or when major changes are implemented.

Errors, updates, or suggested changes to this Certification Practice Statement shall be communicated to the Policy Management Authority.

## 6 POLICIES AND PRACTICES

---

### 6.1 Risk assessment

---

ZETESCONFIDENS performs risk assessments on a regular basis to ensure the quality and reliability of the time-stamping services. ZETESCONFIDENS risk assessment and risk management program are documented internally.

### 6.2 Trust Service Policy Management Authority

---

The PMA has overall responsibility for all Trust Services. The PMA includes senior members of management as well as staff responsible for the operational management.

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

- (a) Specifying and approving the infrastructure and practices.
- (b) Approving the practice statements and the related policies
- (c) Defining the review process for, including responsibilities for maintaining, the Certification Practice Statement and the related certificate policies, as well as other practice statements and policies for other PKI services.
- (d) Defining the review process that ensures that applicable policies are supported by the practice statement(s).
- (e) Defining the review process that ensures that the applicable practices, policies and procedures are implemented and carried out.
- (f) When applicable, authorising part or all component service of the infrastructure to be provided and/or operated by third parties and the applicable terms and conditions.
- (g) Publication to the Subscribers and Relying Parties of the relevant practice statements and policies.
- (h) Continually and effectively managing related risks. This includes a responsibility to periodically re-evaluate risks to ensure that the controls that have been defined remain appropriate, and a responsibility to periodically review the controls as implemented, to ensure that they continue to be effective.
- (i) Specifying cross-certification or mutual recognition procedures and handling related requests.
- (j) Defining internal and external auditing processes with the aim to ensure the proper implementation of the applicable practices, policies and procedures.
- (k) Initiating and supervising internal and external audits.
- (l) Executing the audit recommendations.
- (m) Undertaking any action it considers necessary to ensure the proper execution of the above areas of responsibility.
- (n) Defining the scope of the PKI related service offering, among others by:
  - 1) Defining the certificate classes to be supported by the PKI;
  - 2) Defining the PKI related entities that will be registered by or under the responsibility of the Registration Authority.
  - 3) Defining the needs for policies that are to be followed for each of the certificate classes;
- (o) Ensuring that practices for each of the above-mentioned entities are defined and implemented in a manner that is consistent with this document;
- (p) Mediating in disputes involving Subscribers and/or entities that have been registered by the Registration Authority and the entities that have been implemented by or under the responsibility of the Trust Service Provider.

- (q) Initiating when appropriate highly sensitive PKI operations such as CA root key revocation and renewal or termination of a service.

### 6.2.1 Time-stamp format

The time-stamp token format is compliant with RFC 3161 [7], RFC 5816 [8] and ETSI EN 319 422 [5].

The cryptographic suites used follow the recommendation stated in ETSI TS 119 312 [6].

The accepted hash algorithms are SHA224, SHA256, SHA384 and SHA512.

### 6.2.2 Accuracy of the time

#### Accuracy and UTC

Unless stated otherwise in the time-stamp token, the guaranteed time accuracy is 1 second for qualified time stamps and 1 minute for non-qualified time stamps.

The time-stamping service maintains accurate date and time through synchronisation with UTC. UTC is derived from atomic clocks located in the National Physics Laboratories of various countries and is based on the international definition of the second.

ZetesConfidens operates a set of Stratum-1 multi-GNSS referenced NTP servers that synchronize the system clock of each TSU with at least 3 of these external time references from:

- UTC(ROB) from the public NTP services of the Royal Observatory of Belgium
- GPST from the GPS satellite network
- GST from the Galileo satellite network
- GLONASST from the GLONASS satellite network

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

In any event, each TSU system will also independently check for deviation of the time and automatically stop issuing time-stamp tokens if the accuracy of the time source cannot be assured.

The TSA implements security mechanisms and security controls to ensure only authorized configuration and calibration operations on a TSA System and the time infrastructure are possible.

#### Leap Seconds

In order to compensate for the divergence of UTC from solar time, leap seconds are occasionally introduced.

The UTC standard allows leap seconds to be applied at the end of any UTC month, with first preference to June and December and second preference to March and September. As of January 2017, all of them have been inserted at the end of either June 30 or December 31.

Insertion of each UTC leap second is usually decided about six months in advance by the International Earth Rotation and Reference Systems Service (IERS).

ZetesConfidens NTP servers adjust for leap-seconds to maintain proper synchronisation with UTC for use by the TSS.

### 6.2.3 Limitations on usage of the service

The time-stamping service does not provide any information or assurance about nor accepts any liability for the data which is timestamped other than the assurance that the signed hash representing said data existed at the date and time of the timestamping operation.

### 6.2.4 Obligations of the subscriber

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.

### 6.2.5 Obligations of relying parties

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.

For qualified time-stamps, ETSI EN 319 421 [4] 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 [4].

### 6.2.6 Verification of the timestamp

See the guidelines for verification of the timestamp in chapter 6.2.5.

### 6.2.7 Applicable law

#### **Applicable Belgian law:**

21 JULI 2016. - Wet tot uitvoering en aanvulling van de verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende de elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, houdende invoeging van titel 2 in boek XII "Recht van de elektronische economie" van het Wetboek van economisch recht, en houdende invoeging van de definities eigen aan titel 2 van boek XII en van de rechtshandhabingsbepalingen eigen aan titel 2 van boek XII, in de boeken I, XV en XVII van het Wetboek van economisch recht

21 JUILLET 2016. - Loi mettant en œuvre et complétant le règlement (UE) n° 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, portant insertion du titre 2 dans le livre XII " Droit de l'économie électronique " du Code de droit économique et portant insertion des définitions propres au titre 2 du livre XII et des dispositions d'application de la loi propres au titre 2 du livre XII, dans les livres I, XV et XVII du Code de droit économique

**Applicable EU law:**

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 [9].

### 6.2.8 Service Availability

ZETESCONFIDENS has implemented the following measures to ensure availability of the service:

- Redundant setup of IT systems, including HSM infrastructure and Stratum-1 NTP servers, in order to avoid single point of failures
- Redundant internet connections in order to avoid loss of service
- Use of uninterruptable power supplies

The time-stamping service is only available to customers of ZETESCONFIDENS and the service levels are specified in an SLA contract with each customer.

## 6.3 Terms and conditions

---

The present 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://repository.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.

### 6.3.1 Trust service policy being applied

The present document represents the applied trust service policy.

### 6.3.2 Retention of trust service event logs

Service event logs are retained for at least three months. Logs relating to the life cycle of the TSU keys are retained until 7 years after the certificate for the TSU key ceases to be valid due to expiration or revocation.

## 6.4 Information for relying parties

---

The relying party must:

- verify that the time-stamp token has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification. ZETESCONFIDENS TSA provides several ways to do so, see clause 6.2.
- take into account any limitations on the usage of the timestamp indicated by this timestamp policy
- take into account any other precautions prescribed in agreements or elsewhere



## 7 TSA MANAGEMENT AND OPERATION

---

### 7.1 Internal organization

---

ZETESCONFIDENS maintains non-disclosed documentation that specifies operational controls concerning personnel security, access controls, risk assessment...etc.

This internal documentation is audited by independent conformity assessment body to confirm compliance of the service against ETSI TS 319 401 [2].

### 7.2 Personnel security

---

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

All members of the staff operating the key management operations, administrators, security officers, system auditors or any other operations that materially affect such operations are considered as serving in a trusted position.

Trusted roles within ZETESCONFIDENS are activities conducted to operate, maintain, monitor, review and communicate about trust service activities. Trusted roles are allocated to duly identified persons by the PMA.

Zetes conducts an initial investigation of all members of staff who are candidates to serve in trusted roles to make due diligence attempt to determine their trustworthiness and competence.

### 7.3 Asset management

---

All IT systems used within the service are clearly identified, categorized and filed in an asset management database.

Media are stored securely. Backup media are also stored in a separate location that is physically secure and protected from fire and water damages.

### 7.4 Access control

---

ZETESCONFIDENS operates its sites involved with trust services activities according ISO 27001 requirements. The implemented Information Security Management System includes several controls related to computer security and a.o. :

- Firewalls to protect the internal network domain from unauthorized access and to prevent all accesses and protocols that are not required for the operation of the TSP
- Control of sensitive data stored on “demobilized” or reusable storage device
- Local network components are kept in a secure environment and their configuration is periodically checked
- Use of multifactor authentication for accounts capable to issue certificates
- Enforced access control to modify disseminated information regarding Qualified Certificates. The site for dissemination provides https protocol for read access.
- Enforced access control to modify revocation status information through a mutual SSL authentication between the CA and the OCSP server and between CA and the CRL publication infrastructure.
- Access control, intrusion detection system and CCTV monitoring to detect, record and react upon unauthorized physical access to its resources

## 7.5 Cryptographic controls

---

### 7.5.1 General

The TSA uses service-specific private keys for the Certification Authority, OCSP responders and the Time-Stamp Units. Private keys are generated and stored in a secure Hardware Security Module which has a relevant security certification as specified in ETSI TS 319 421 [4].

### 7.5.2 TSU key generation

The generation of the TSU's signing key(s) is undertaken in a physically secured environment by personnel in trusted roles under dual control. The personnel authorized to carry out this function is limited to those in trusted roles authorized to do so under the TSA's practices.

The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS 140-2, level 3 [11].

The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key is recognized by any national supervisory body, or in accordance with existing current state of the art, as being fit for the purposes of time-stamps as issued by the TSA.

### 7.5.3 TSU private key protection

For operational use the TSU's signing key(s) are secured out within a cryptographic module which is conformant to FIPS 140-2, level 3 [11].

For backup the TSU private keys are copied, stored and recovered only by authorized personnel in trusted roles using dual control in a physically secured environment. The personnel authorized to carry out this function shall be limited to those requiring doing so under TSA's practices.

### 7.5.4 TSU public key certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

- TSU signature verification (public) keys are available to relying parties in the form of a public key certificate. The certificates are published at: <https://crt.tsp.zetes.com/>
- The TSU does not issue a time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device. When obtaining a signature verification (public key) certificate, the TSA verifies that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

### 7.5.5 Rekeying TSU's key

Rekeying for a TSU means that a new key and certificate will be created for an existing TSU identifier.

TSU private signing keys are replaced before the end of their validity period, (i.e., when the algorithm or key size is determined to be vulnerable).

The life-time of TSU's certificate is no longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see clause 9.3 in TS 119 312 [6]).

Once a year or when significant changes occur, the TSA verifies all cryptographic algorithm used in the TSA infrastructure against the algorithm recognized as suitable.

If an algorithm becomes compromised or is not suitable anymore, the PMA will instruct the TSA to rekey any affected private keys.

### 7.5.6 Life cycle management of signing cryptographic hardware

The used cryptographic hardware is inspected by trustworthy personnel in dual control during shipment and storing.

Specifically, the hardware is checked for

- a) any damages of security seals
- b) any damages of the case of the hardware (e.g. scratches, bumps...)
- c) any damages of the packing of the hardware

Additionally, the following applies:

- d) The Installation and activation of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles using, at least, dual control in a physically secured environment.
- e) TSU private signing keys stored on TSU cryptographic module are erased upon device retirement in a way that it is practically impossible to recover them.

### 7.5.7 End of TSU key life cycle

TSU private keys will not be used beyond the validity of the corresponding certificate. After expiration of the private keys, the private keys within the cryptographic hardware are destroyed in a manner such that the private keys cannot be retrieved or used anymore.

## 7.6 Timestamping and Clock synchronization with UCT

---

The ZETESCONFIDENS time-stamping service issues Time-stamps conform to the time-stamp profile as defined in ETSI EN 319 422 [5].

The TSA time servers are synchronized with UTC [1]. In the case the TSA clock's accuracy cannot be maintained, no timestamp will be issued until re-synchronization of the clock.

Audit and calibration records are maintained. Clock synchronization is maintained when a leap second occurs as notified by the appropriate body.

See chapter 6.2.2 for additional information.

## 7.7 Physical and environmental security

---

ZETESCONFIDENS has established physical security measures and environmental controls commensurate with the value and critical nature of the assets they apply to. Physical and environmental security is aimed to prevent, deter, detect and delay unauthorized access, loss, theft, damage, compromise, interferences and interruption to business activities.

ZETESCONFIDENS facilities are organized, partitioned and segregated into distinct areas with specific physical security measures according the type and sensitivity of assets and the operations conducted.

The sites hosting the services implement proper security controls, including access control, intrusion detection and CCTV. Access to the sites is limited to authorized personnel.

The secure premises within these sites are located in an area appropriate for high-security operations. These premises feature numbered zones and locked rooms, cages, safes, and cabinets.

Physical access is restricted by implementing mechanisms to control access from one area of the facility to another or access into high-security zones such as locating operations in a secure computer room physically monitored and supported by security alarms and requiring movement from zone to zone to be accomplished using a token and access control lists.

Power and air conditioning operate with a high degree of redundancy.

Premises are protected from any water damages.

Prevention and protection as well as measures against fire exposures are implemented.

To prevent unwanted disclosure of sensitive data, waste is disposed of in a secure manner.

## 7.8 Operation security

---

ZETESCONFIDENS ensures that all components of the TSA infrastructure are secure and correctly operated. Operational risks and security risks are mitigated as best as possible.

The operational procedures and security practices meet the requirements laid down in ETSI EN 319 421 [4].

Capacity management is done on a regular basis to evaluate the infrastructure's capacity and performance based on the monitoring figures and new business perspectives.

## 7.9 Network security

---

ZETESCONFIDENS ensures the maintenance of a high-level network of systems security including firewalls. Network intrusions are monitored and detected.

The network segment for the TSU servers

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

Not needed connections and services are explicitly forbidden, blocked or deactivated.

A description of the network security controls is available in internal confidential documents of ZETESCONFIDENS and/or Zetes.

Network security is verified by means of regular vulnerability scans and penetration tests. A record is maintained as evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

## 7.10 Incident management

---

ZETESCONFIDENS defined an incident management procedure for incident reporting and incident handling.

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

## 7.11 Collection of evidence

---

ZETESCONFIDENS records all relevant information regarding the operations as a TSA for a defined period. This information can be made available to external parties for the purpose of legal proceedings under condition of approval by the PMA.

## 7.12 Business continuity management

---

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

Continuity of the TSA services is ensured by maintaining independent TSUs in at least two separate sites and by also providing continuity of operations for the CA and VA (see the CPS and CP of the CA for more information)

Depending on the cause of the disaster and their effects, the PMA will assess the measures to be taken regarding

- the protection of sensitive resources and information on the disabled site
- the need to revoke certificates impacted by the disaster (as the protection of disabled site cannot be ensured)
- the setup of a new site

A Business Continuity Plan has been implemented to ensure business continuity following a natural or other disaster and is available as a separate internal document.

### 7.13 TSA termination and termination plans

---

ZETESCONFIDENS maintains a Termination Plan that covers the procedures in case of termination of TSA services. ZETESCONDIENS will make a best effort to minimize the impact for Subscribers and Relying Parties.

The following is a summary of the minimum procedures that are applicable in such a case.

In the context of a scheduled termination:

- Cessation of the issuance of any new time-stamp
- Termination notification to the Belgian Supervisory Body and to the Subscribers within 3 months and no later than 2 months before the effective termination
- Preservation and transfer of auditing and archival records to the arranged custodian
- Revocation of unexpired and unrevoked TSU Certificates
- Creation of a last CRL
- Decommissioning of the TSU keys
- Possible cessation of the OCSP service for the TSU certificates

In the context of an unscheduled termination:

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

- Shorter or even no delay for the notification of the interested parties
- Shorter or no delay for the revocation of certificates

### 7.14 Conformance

---

For qualified time-stamps conformance to the present policy is audited and testified by a duly recognized Conformity Assessment Body as defined in EU Regulation No 910/2014 [9] and ETSI EN 319 403 [3]. ZETESCONFIDENS is supervised by the Belgian Ministry for Economy, SMEs, the Self-employed, Energy - Quality and Safety, the Belgian Supervisory Body and listed in the Belgian Trusted List of Qualified TSP issuing Qualified electronic Time-stamps.

Relying parties can use the 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."

## 8 TIME-STAMP TOKENS AND CERTIFICATES

### 8.1 TSU time-stamp token profiles

Profile for qualified time-stamp tokens:

- standard RFC 3161 and RFC 5816 format
- qcStatements in RFC 3739 format: esi4-qtstStatement-1

Profile for non-qualified time-stamp tokens:

- standard RFC 3161 and RFC 5816 format

### 8.2 TSU public key certificates

TSU	Active	Common Name	Validity	Key	Serial Number
TSU1	A	ZETES TSP RSA Qualified TSU1	12/07/2019 – 12/07/2025	RSA3072	14:81:32:A1:6A:CD:84:B8
TSU2	A	ZETES TSP RSA Qualified TSU2	12/07/2019 – 12/07/2025	RSA3072	1E:56:CD:74:24:2F:6E:70
TSU3	-	ZETES TSP EC Qualified TSU3	16/05/18–13/05/30 revoked 12/07/2019	ECC256	3B:2D:48:07:68:95:D3:9D
TSU4	-	ZETES TSP EC Qualified TSU4	16/05/18–13/05/30 revoked 12/07/2019	ECC256	7D:BF:1C:7F:E9:83:90:B5
TSU5	-	ZETES TSP RSA TSU5	16/05/18–14/05/24 revoked 12/07/2019	RSA3072	25:45:01:D5:CE:7A:F4:63
TSU6	-	ZETES TSP RSA TSU6	16/05/18–14/05/24 revoked 12/07/2019	RSA3072	6E:AF:D7:1E:5D:EF:99:50
TSU7	-	ZETES TSP EC TSU7	16/05/18–13/05/30 revoked 12/07/2019	ECC256	34:A2:7C:04:14:FB:23:C1
TSU8	-	ZETES TSP EC TSU8	16/05/18–13/05/30 revoked 12/07/2019	ECC256	0D:13:C8:6E:1E:2A:C5:56
TSU9	A	ZetesConfidens RSA Qualified TSU9	12/07/2019 – 12/07/2022	RSA2048	1D:C8:F3:C3:43:D4:47:F9
TSU10	A	ZetesConfidens RSA Qualified TSU10	12/07/2019 – 12/07/2022	RSA2048	59:C5:4C:A5:FC:6E:F5:89
TSU11	A	ZetesConfidens EC Qualified TSU11	12/07/2019 – 12/07/2025	ECC256	02:CF:13:87:C6:2C:85:BC
TSU12	A	ZetesConfidens EC Qualified TSU12	12/07/2019 – 12/07/2025	ECC256	5A:C7:28:39:EC:DE:AE:05
TSU13	A	ZetesConfidens RSA TSU13	12/07/2019 – 12/07/2022	RSA2048	46:97:BE:E8:42:72:7F:B0
TSU14	A	ZetesConfidens RSA TSU14	12/07/2019 – 12/07/2022	RSA2048	69:D8:11:E7:E1:A2:B5:1B
TSU15	-	ZetesConfidens EC TSU15	22/01/2019-20/01/2025 revoked 12/07/2019	ECC256	2F:F7:15:65:BE:21:B5:A0
TSU16	-	ZetesConfidens EC TSU16	22/01/2019-20/01/2025 revoked 12/07/2019	ECC256	56:8B:16:BC:77:ED:91:3A

## 8.2.1 ZETES TSP RSA Qualified TSU1

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
14:81:32:a1:6a:cd:84:b8  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001  
Validity  
Not Before: Jul 12 07:19:43 2019 GMT  
Not After : Jul 12 07:19:43 2025 GMT  
Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZETES TSP RSA Qualified TSU1  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public-Key: (3072 bit)  
Modulus:  
00:b5:29:ea:5d:8e:6f:69:7a:4e:a3:26:7d:e5:01:  
22:70:7a:5f:3f:c2:69:a6:5c:fa:28:7e:e8:4e:6e:  
c3:be:56:b5:0c:b4:ec:20:de:bd:e7:55:41:2d:8b:  
bc:d2:a7:d9:f5:dc:31:88:ff:62:cb:33:d6:82:f4:  
d6:c9:ec:1a:f5:c5:54:94:65:56:da:84:41:a9:5c:  
84:6b:15:59:c5:15:c5:70:2a:47:1f:06:da:e2:f0:  
0c:f7:43:c5:81:bb:b4:7c:0b:a2:6e:d9:c2:c7:d8:  
47:c2:55:c2:11:e2:93:6a:a5:a5:ae:49:89:bf:d8:  
83:5f:5b:94:3b:9f:bb:21:0d:43:d1:a8:e3:65:dd:  
de:69:fd:b0:b3:51:bd:69:36:6d:0d:05:e2:b8:86:  
45:d4:7d:f1:86:54:17:cb:8e:ae:79:68:b8:bc:3e:  
ce:f1:e3:9a:72:64:18:5d:ac:b4:17:8a:03:50:60:  
32:1e:6a:f8:44:60:fe:eb:fb:ad:97:d6:d1:5a:bf:  
5b:a2:d5:b0:26:f5:64:12:50:87:ac:f9:48:c5:f5:  
fd:54:ed:b6:28:65:02:52:95:a6:14:eb:24:be:01:  
2d:1b:50:5c:8f:5c:ee:04:78:30:85:8b:a0:61:95:  
c8:f7:ea:57:f7:a8:c0:b9:e5:dc:d1:29:01:e0:32:  
48:15:4c:c0:e0:d0:ac:7c:ff:f3:8f:cc:2d:bf:e6:  
7b:08:86:62:65:67:c1:e3:3b:cf:d2:19:c4:62:f2:  
f4:74:7b:ec:9d:55:2a:a1:a4:a8:de:11:ca:0b:9e:  
f6:e4:e8:ed:c3:90:12:ee:07:51:69:17:df:d4:cb:  
be:71:7c:2c:38:f7:c9:51:1b:65:91:c1:14:1d:dc:  
e2:f7:1b:c8:5c:4e:bd:31:a4:40:97:8d:db:30:c4:  
df:f5:b8:f1:55:9b:86:08:79:c6:06:ec:f2:21:f6:  
ec:82:e4:4d:7d:dc:b0:d8:3f:e2:3c:b4:dd:ae:5e:  
5d:14:a6:02:1d:6a:8a:69:81:f5  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
Authority Information Access:  
CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt  
OCSP - URI:http://ocsp.tsp.zetes.com  
  
X509v3 Subject Key Identifier:  
6D:C0:73:6E:09:ED:C6:6B:8F:D1:E1:1C:FD:92:F1:33:DD:7D:5A:30  
X509v3 Basic Constraints: critical  
CA:FALSE  
X509v3 Authority Key Identifier:  
keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45  
  
qcStatements:  
070.....F..0+.....F..0!0...https://pds.tsp.zetes.com..en  
X509v3 Certificate Policies:  
Policy: 1.3.6.1.4.1.47718.2.1.2.50  
CPS: https://repository.tsp.zetes.com  
User Notice:  
Explicit Text:  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl  
  
X509v3 Key Usage: critical  
Digital Signature  
X509v3 Extended Key Usage: critical  
Time Stamping  
Signature Algorithm: sha256WithRSAEncryption  
89:e1:a8:7c:7a:12:23:4a:4c:aa:4d:ad:6b:5a:29:86:15:b1:  
49:b3:03:3d:5c:99:30:c6:97:12:73:30:ff:4d:1e:f6:73:ef:  
e2:d8:85:40:29:c3:3e:91:b1:d0:fd:2f:99:f8:00:a3:e5:b0:  
fe:c9:46:5e:83:b3:c4:fb:11:0e:9c:01:52:23:ec:16:0c:73:  
b5:4d:cd:04:0b:56:30:4d:86:e1:97:dc:11:e4:c2:24:54:be:  
2e:fc:77:37:62:a9:28:e3:a7:95:3e:5b:c9:ef:fc:e8:bd:8e:  
7f:6d:46:d1:e9:64:14:47:2c:22:b7:6b:07:81:31:8b:8d:f6:  
db:5e:2c:df:c3:2b:35:61:ce:c7:31:12:a2:e1:34:05:81:11:  
1b:a7:db:66:a5:41:fb:0f:7c:6b:8b:17:b3:78:ee:e4:a2:8c:

42:28:83:c2:dd:09:ba:f2:ef:ae:f4:86:4d:16:79:75:cf:00:  
b1:11:4e:31:4c:20:46:90:38:b1:c6:5d:55:c9:19:68:91:7c:  
d6:69:40:a5:36:c8:a9:6d:39:ab:09:e3:f6:c4:ea:e2:4a:e1:  
ab:f7:f8:2b:68:ce:93:2a:82:61:1e:c7:f8:32:b0:91:84:f7:  
7e:90:02:1f:81:21:0c:cf:a4:fe:13:41:07:77:b5:f4:3a:ce:  
bb:38:a3:2d:b7:bc:c1:32:b6:5b:7b:04:2f:93:ac:cc:c4:a9:  
81:ac:c5:0c:f6:54:43:82:0e:4d:97:ca:bc:4c:a2:8c:b0:28:  
f0:be:6a:fd:73:83:52:cb:a3:44:c4:5a:c4:3d:64:01:7b:37:  
57:16:ce:09:b4:2d:fd:7e:21:c3:76:41:8c:2b:e9:6a:d5:a1:  
de:72:4d:a1:8e:d8:b7:df:bf:74:43:51:94:4d:f0:ab:7e:c0:  
2f:9d:42:f0:a4:b3:d8:9b:39:da:16:c5:e2:c7:09:09:57:af:  
b3:e9:32:0b:9a:d9:1e:da:1b:59:dd:7f:8d:58:fb:f3:07:3a:  
78:5c:f3:5a:ba:50:26:d0:75:7c:d2:3c:ee:28:9e:a0:ad:e4:  
65:25:a1:a9:9d:2c:69:fe:6e:94:f4:61:57:73:3c:63:0e:8d:  
ab:08:bb:84:3f:45:12:fd:a2:c2:11:6f:4f:04:b7:9a:aa:4f:  
fc:bb:e9:75:9a:29:0a:b4:6f:e0:85:16:b5:44:84:6a:5b:ea:  
a9:fe:ff:13:bc:d5:e0:ea:a0:54:13:7b:78:ab:78:b0:6c:31:  
f6:81:ad:ce:ba:f4:30:4d:4f:13:b2:1e:b2:a7:82:56:ca:a9:  
01:a3:d3:b9:df:f2:e9:35:70:18:16:53:3a:c8:4e:6b:f3:f3:  
cf:f2:69:1c:bd:ca:ff:43  
-----BEGIN CERTIFICATE-----  
MIIH0zCCBS0gAwIBAgIIIEyOwRnHlGwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE  
BhMCQkUxJDAiBgNVBAAoMG1pFVEVTFIENBChWQVRCSR0wNDANdI1NjI2KTEMMAAoG  
A1UEBRMDMDAxMSEwHwYDVQDDbHARVRFUyBUU1AgQ0EGRk9SIFRTQSAwMDEwHhcN  
MTk0NzE5MDcxOTQzWzWjUwNzE5MDcxOTQzWjBaMQswCQYDVQGEWJCRTEKMCIG  
A1UECgwbWVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSUwIwYDVQDDbHARVRF  
UyBUU1AgU1NBFFIYXWpZml1ZCBU1UxMIIBojANBgkqhkiG9w0BAQEFAAOCAy8AM  
IIBigCAYEAtSnqXY5vaXpOoyZ95QEicHpfP8Jpplz6KH7oTm7Dv1a1DLTsIN69  
51VBLyU80qfZ9dwxip9iyzPWgvtWYewa9cVULGVW2oRBqVYExVZxRXFcCpHHwba  
4vAM90PFgbu0fAu1bntC9xHw1XCEeKtaqWlrmJv9iDX1uU05+7IQLD0ajjZd3e  
af2ws1G9aTztDQXiuiZFLH3xhlQXy46ueWi4vD7O8eOacmQYXay0F4oDUGAYHmr4  
RGD+6/utl9bRWR9botWwJvVKElChRP1IXfX9VO22KGUCUPWmF0skvgEtG1Bcjlzu  
BHghwYugY2XI9+px96jAueXc0SkB4DJIFUZ44NCsfP/zj8wtv+Z7CIZiZWfB4zvP  
0hneYvL0dHvsnVUqoaSo3hHKC57250jtw5AS7gdRaRf1Mu+cXwsOPfJURtlkcEU  
Hdz19xvIXE69MaRA143bMMTf9bjxVZuGCHnGBuzyIfbsguRNfdy2D/iPLTdlr15d  
FKYCHWqKaYH1AgMBAAAgggJ5MIICdTBwBggrBgEFBQCBAQRkMG1wOYIKWYBBQUH  
MAKGLWh0dHA6Ly9jcNQuHhNwLnpldGVzLmNvbS9aRVRFU1RTUFRtQUNBMDAxLmNy  
dDA1BggrBgEFBQCwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4E  
FgQUbcBzbgnxtmuP0eEc/ZLxM919WjAwDAYDVR0TAQH/BAIwADAFBgNVHSMEGDAW  
gBQQtUUt24Qtse0r6AU4U6nlvh+3RTBFBggrBgEFBQCBAWQ5MDcwCAAYBACORgEB  
MCsGBGQAJkYBTAHMB8WGW0dHBz0i8vcGRzLnRzcC56ZXRLcy5jb20TAmVUMIIB  
AgYDVRO0gBIH3MIH0BgwrBgEEAYL0ZgIBAJIwgeMwLAYIKWYBBQUHAGEWIGH0  
dHBz0i8vcMvWb3NpdG9yeS50c3AuemV0ZXMuY29tMIGYBggrBgEFBQCBAjCBPr6B  
ogBaAEUAVABFAFMAIABUAFMAUAAgAFEAQBHAGwAaQBmAGkAZQBkACAAYWBLAHIA  
dABpAGYAAQBJAGEAdABlACAAZgBvAHIAIAB0AGkAbQBLAC0AcwB0AGEAbQBWAGKA  
bgBnACAAAYWbVAG0AcABsAGkAYQBuaHQAIAB3AGkAdABoACAAARQBUAFMASQAQAFQA  
UwAgADMAMQA5ACAANAAYADEALjA+BGNVHR8ENzAlMD0gMaAvhi1odHRwOi8vY3Js  
LnRzcC56ZXRLcy5jb20vWkVURVNUU1BUU0FDQTAwMS5jcmmwDgYDVRO0PAQH/BAQD  
AgeAMBYGAILUdjQEB/wQMAAGCCSGAQUFBwMIMA0GCSqGSIb3DQEBCwUA4ICAQCJ  
4ah8ehIjSkyqTAlrWimGfbFJswM9XJkwXpcSczD/TR72c+/i2IVAKcm+kbHQ/S+Z  
+ACj5bd+yUZeg7PE+xEOnAFSI+wWDH01Tc0EC1YwTYbh19wR5MIkVL4u/Hc3Yqko  
46eVPlvJ7/zovY5/fUbr6WQURywt2sHgTGLjfbXizfwys1Yc7HMRKi4TQFgREB  
p9tmpUH7D3xrixeze07kooxCKIPC3Qm68u+u9IZNFnl1zwCxEU4xtCBGkdixx11V  
yRloKxWauCLNsiPbTmrCeP2xOrisuGr9/gram6TKoJhHsf4MrcRHpd+kAifgSEM  
z6T+E0EHd7X00s67OKMt7zBMrZbewQvk6zMxKMBRmUM91RDgg5N18q8TKKMsCjw  
vmr9c4NSy6NEXFrEPWQBezdxFs4JtC39fiHddkGMK+1qlaHeck2hjt33790Q1GU  
TFcRfsAvnULwPLPYmznafSxiXwkJV6+z6TILmtke2ht23X+NWpVzBzp4XPNaulAm  
OHV80jzuKJ6greRlJaGpnSxp/m6U9GFxczxjDo2rCLUEP0US/aLCEW9PBLEaqk/8  
u+l1miKktG/ghRa1RIRqW+qp/v8TvNXG6qBUE3t4q3iwbDH2ga3OuvQwTU8Tsh6y  
p4JWYqkBo9053/LpNXAYFLM6yE5r8/PP8mkcvcr/Qw==  
-----END CERTIFICATE-----



## 8.2.2 ZETES TSP RSA Qualified TSU2

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      1e:56:cd:74:24:2f:6e:70
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001
    Validity
      Not Before: Jul 12 07:24:47 2019 GMT
      Not After : Jul 12 07:24:47 2025 GMT
    Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZETES TSP RSA Qualified TSU2
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (3072 bit)
      Modulus:
        00:e5:67:24:76:71:22:0e:6b:f3:c3:f1:f1:7b:e3:
        63:46:e4:ba:6d:9a:da:8f:74:cb:bc:90:d2:a4:7b:
        f0:15:cc:81:85:f7:85:18:05:26:93:1d:d3:34:92:
        7e:9c:79:1c:48:1f:19:b0:ba:cb:28:62:a5:ad:c0:
        58:92:fa:6d:d6:90:bb:0d:ba:43:a8:38:86:4b:9b:
        40:8f:05:7a:4f:c3:ee:fa:46:cd:a4:92:a9:7e:14:
        2d:c6:38:2d:43:a2:c3:d4:be:61:27:2a:8c:de:22:
        70:44:47:f1:73:93:c5:cd:7b:6e:06:4e:72:d9:4c:
        f8:e7:28:2a:d5:85:92:28:9a:fe:0b:6c:d5:4c:11:
        cc:19:45:ab:f6:99:9b:b1:6f:c3:65:d5:12:a6:b9:
        9f:90:d1:92:86:38:f6:a8:93:46:da:1b:92:ec:a5:
        92:6d:f8:c8:cb:f0:17:23:5e:90:a8:c5:92:aa:70:
        90:cf:88:62:f6:71:74:9f:68:f3:66:c3:df:74:0a:
        cb:a9:42:d8:ed:49:bc:2d:e7:50:9b:5f:de:ee:1a:
        05:64:bb:f2:47:0c:32:14:81:08:8b:ec:ee:eb:58:
        4e:be:90:3c:5a:a3:ee:5f:93:b1:46:1f:b7:e3:8d:
        82:e0:91:5a:45:37:2b:d3:71:2a:f2:c7:33:26:88:
        48:06:1a:8d:da:38:e8:2e:19:a9:58:69:4e:70:08:
        61:3d:3a:39:e6:0e:22:f7:f8:52:0b:3b:b4:0e:cd:
        0f:1a:86:34:8f:26:d8:a1:43:1b:2b:2f:c1:69:f1:
        d9:69:7e:fd:38:b5:21:0b:3b:2a:ff:17:15:b5:96:
        eb:94:d9:da:f1:90:de:ab:eb:e2:bc:02:3c:68:db:
        40:71:22:48:15:d6:cb:0f:6b:73:90:a4:bc:38:56:
        86:3c:ee:4b:07:c0:d8:14:81:a8:f0:81:d5:a1:36:
        a8:d7:08:f6:6d:51:86:67:78:1e:92:57:42:91:e3:
        f7:ee:22:56:ca:59:d2:de:b9:dd
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      Authority Information Access:
        CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
        OCSP - URI:http://ocsp.tsp.zetes.com
      X509v3 Subject Key Identifier:
        A5:64:90:F1:BC:8F:CC:FF:D7:D9:24:BD:FB:84:04:4D:B0:AB:D2:71
      X509v3 Basic Constraints: critical
        CA:FALSE
      X509v3 Authority Key Identifier:
        keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45
      qcStatements:
        070.....F..0+.....F..0!0...https://pds.tsp.zetes.com..en
      X509v3 Certificate Policies:
        Policy: 1.3.6.1.4.1.47718.2.1.2.50
        CPS: https://repository.tsp.zetes.com
        User Notice:
          Explicit Text:
      X509v3 CRL Distribution Points:
        Full Name:
          URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl
      X509v3 Key Usage: critical
        Digital Signature
      X509v3 Extended Key Usage: critical
        Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
    0b:87:f0:74:3a:4d:df:d8:8f:6d:74:4d:c1:a3:a5:87:6b:c7:
    b4:33:bb:bf:83:2e:2a:c5:61:b3:da:c8:b6:ee:dd:6b:e8:4c:
    d7:52:bf:ba:08:11:47:90:4a:07:6d:54:cc:67:e6:aa:4a:c6:
    12:f4:b0:ff:29:a8:dd:68:fa:42:4a:1a:0a:88:ca:69:b8:95:
    eb:be:3d:d8:4b:f1:87:31:41:d9:f8:81:49:c2:d5:16:7c:f2:
    c1:e0:29:cb:ec:47:c4:37:ae:4e:da:5d:d9:06:61:0f:8d:78:
    5a:10:81:43:13:c8:f9:d3:86:b4:60:bf:a2:29:da:ef:ce:3c:
    03:d2:0e:7b:31:5b:a4:75:56:44:a0:23:5e:2d:32:4c:7b:e5:
    3a:10:12:0b:17:65:bc:e5:e7:1b:6e:0c:9d:0e:6f:c2:c5:b0:
```

```
38:08:87:94:20:d1:bf:3a:d2:aa:5a:bd:3a:9f:bd:d5:17:88:
34:cd:00:3a:28:ea:3f:99:05:e3:91:71:04:e9:9b:9b:68:c0:
30:52:ba:a7:a4:1b:a2:bf:32:bf:c7:06:e5:53:9b:d4:c9:40:
14:48:08:dc:3c:65:09:8f:14:41:c9:33:3b:20:79:a0:05:f5:
83:69:94:6c:ef:cf:84:28:0f:f3:99:c6:2e:61:9d:5f:bc:57:
ba:5f:ad:db:ac:8c:0b:76:2a:0e:e4:6a:05:4b:ea:b5:85:fa:
36:bb:de:a8:c1:fc:70:4c:dd:9b:4f:4d:74:bb:ae:22:ce:f8:
d6:4a:38:eb:ca:79:81:d9:9a:99:27:8a:ec:58:33:12:3d:87:
b3:b3:ae:b9:d1:af:c9:a6:26:8d:53:a8:4f:88:5d:1a:91:a2:
d6:42:70:3f:03:ba:39:ba:c8:8b:86:18:6e:44:ae:d2:22:e0:
c3:82:3a:92:08:01:ba:0b:e9:5d:53:43:33:a4:02:b9:6f:1e:
a0:41:10:1e:94:74:68:4d:b3:d3:02:b3:4a:d9:81:28:31:dc:
75:41:35:cd:d4:dd:e0:21:c6:c6:00:88:02:0d:b6:a5:52:e2:
f8:83:ad:2d:f8:61:fa:14:b5:b5:50:36:19:20:ec:02:fa:50:
20:00:b9:b3:9a:93:8a:46:2e:6d:b0:7d:bf:cd:c3:ec:33:44:
f7:a0:e2:3f:aa:87:f7:a4:90:be:7f:6a:dd:52:c2:10:b7:16:
86:55:40:42:a3:59:c3:ed:7b:5e:9e:dd:04:9e:19:6e:8f:f4:
76:43:57:ce:eb:83:cf:95:98:46:76:16:61:e4:e9:e5:3e:91:
66:68:e8:50:53:2c:b0:dc:0b:36:b8:bb:db:5a:d1:33:66:7a:
fa:0a:5c:00:bd:af:9b:bf
-----BEGIN CERTIFICATE-----
MIH0ZCCBS0gAwIBAgIIH1bNdCQvbnAwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAAoMG1pFVEVTFIENBChWQVRCSR0wNDANdI1NjI2KTEMAoG
A1UEBRMDMDAxMSEwHwYDVQDDbHARVRFUyBUU1AgQ0EGRk9SIFRTQSAwMDEwHhCN
MTkwnZnEyMDcyNDQ3W3hcnmJmUwNzEyMDcyNDQ3W3BamQswcQYDVQGEwJCRTEkMCIG
A1UECgwbWVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSUwIwYDVQDDbHARVRF
UyBUU1AgU1NBIFFFIYwXpZml1ZCBU1UyMIIBojANBgkqhkiG9w0BAQEFAAOCAy8A
MIIBigCAYEASWckdnEiDmvzw/Hxe+NjRuS6bZraj3TLvJDSPHvFcyBhfeFGAUm
kx3TNJj+nHkcsB8ZsLrLKGKlrcBYkvptlpC7DbbDqDiGS5tAjwV6T8Pu+kbNpJKp
fhQtXjgtQ6LDL1L5hJyqM3iJwREfxc5PFzXtuBk5y2Uz45ygg1YWSKJr+C2zVTBHM
GUWR9pmbS/W/D2dUSprmfkNGShjj2qJNG2huS7KWSbfjIy/AXI16QqMWSgnCQz4hi
9nF0n2jzZsPfdArLqULY7Um8LedQm1/e7hoFZLvYRwvyFIEIi+zu61hOvpA8WqPu
X50xRh+3442C4JfArTcr03Eq8sczJohIBhqn2jj0LhmpWG10cAhhPT055g4i9/hS
Czu0Ds0PG0Y0jybU0MbKy/BafHZA790LUhCzsq/xCVtZbrlNna8ZDeq+vivAI8
anTAcSJI FdbLD2tZkKS0FaGP05LB8DYFIgo8IHVoTao1wj2bVGGZ3gekldCkeP3
7iJWylN3rndaGMBAAggJ5MIICdTbWBggrBgEFBQCBAQRkMG1wOQYIKWYBBQUH
MAKGLWh0dHA6Ly9jcNQuHhNwLnpldGVzLmNvbS9aRVRFU1RTUFRtQUNBMDAxLmNy
dDA1BggrBgEFBQCwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4E
FgQUUpWSQ8byPzP/X2SS9+4QETbCr0nEwDAYDVR0TAQH/BAIwADAFBgNVHSMEGDAW
gBQtUUt2J2QtSE0r6AU4U6nlvh+3RTBFBggrBgEFBQCBAWQ5MDcwCAAYBACORgEB
MCsGBGQAJkYBbTAHb8WGW0dHBz0i8vcGRzLnRzcC56ZXRLcy5jb20TAmVUMIIB
AgYDVRO0gBIH3MIH0BgwrBgEEAYL0ZgIBAJIwgeMwLAYIKWYBBQUHAGEWIGH0
dHBz0i8vcMwVb3NpdG9yeS50c3AuemV0ZXMuY29tMIGYBggrBgEFBQCcCAjCBPr6B
ogBaAEUAVABFAFMAIABUAFMAUAAgAFEAQBHAGwAaQBmAGkAZQBkACAAYWBLAHIA
dABpAGYAAQBJAGEAABLABAAZgBvAHIAIAB0AGkAbQBLAC0AcwB0AGEAbQBWAGKA
bgBnACAAYWbVAG0AcABsAGkAYQBvAHQAIAB3AGkAdAB0ACAARQBUAFMAFMAQAFQA
UwAgADMAQAA5ACAANAAYADEALjA+BGNVHR8ENzAlMD0gMaAvhi1odHRwOi8vY3Js
LnRzcC56ZXRLcy5jb20vWkVURVNUU1BUU0FDQTAwMS5jcmmwDgYDVRO0PAQH/BAQD
AgeAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBWIMMA0GCSqGSIb3DQEBCwUA4ICAQAL
h/B00k3f2I9tdE3Bo6WHA8e0M7u/gy4qxWGZ2si27t1r6EzXUr+6CBFHkEoHbVTM
Z+aqSsYS9LD/KajdaPpCShoKiMppuJXrvj3YS/GHMHUHZ+IFJwUWfPLB4CnL7EfE
N650213ZBmEPjXhaEiFDE8j504a0YL+iKdrvjwD0g57MVukdVZEoCNeLTJMe+U6
EBILF2W85ecbbgydDm/CxbA4CieUING/OtKgWr06n73VF4g0zQA6K0o/mQXjkXEE
6ZubaMAWUrqnpBuivzK/xwblU5vUyUAUSAjcpGUJjxRByTM7IHmgBfWdaZRs78+E
KA/zmcYUz1fvFe6X63brIwLdio05GoFS+qlhfo2u96owfxwTN2bT010u64izvJw
SjjrynB2ZqZJ4rSWMSPYezs6650a/JpiaNU6hPiF0akaLWQnA/A705usiLhhu
RK7S1uDDgjSCAG6C+ldU0MzpAK5bx6gQRAelHR0TbPTArNK2YEOmdxlQTXN1N3g
IcbGAIGcDbalUuL4g60t+GH6FLW1UDYZIOwC+lAgALmzmpOKRi5tsH2/zcPsM0T3
oOI/qof3pJC+f2rdsUQtXaGVUBCoInD7Xtent0Enhluj/R2Q1f064PP1ZhGdh2h
5On1PpFmaOhQUyyw3As2uLvbWtEzZnr6ClwAva+bvv==
-----END CERTIFICATE-----
```

### 8.2.3 ZETES TSP EC Qualified TSU3

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      3b:2d:48:07:68:95:d3:9d
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: May 16 10:19:03 2018 GMT
      Not After : May 13 10:19:03 2030 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP EC Qualified TSU3
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:d1:f1:89:64:6c:91:89:3e:87:4d:74:f0:ce:12:
        fc:96:e4:6f:98:1e:dc:37:1b:e6:17:1d:02:a2:02:
        f7:34:e7:69:b2:63:95:bb:43:d4:8d:09:81:70:d8:
        31:3c:be:d5:b5:04:ff:d2:56:2e:02:ca:13:b4:2c:
        89:fd:59:04:0e
      ASN1 OID: prime256v1
      NIST CURVE: P-256
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      FE:A8:6A:0E:97:91:94:19:6A:6E:6C:74:B8:30:19:00:81:B4:4E:57
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    qcStatements:
      070.....F..0+.....F..0!0...https://pds.tsp.zetes.com..en
    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com
      User Notice:
        Explicit Text:

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
      87:71:c3:ef:cc:40:77:9e:22:3d:84:e2:c9:c8:56:46:0a:64:
      6c:6c:88:03:ed:2d:10:76:56:26:5a:ab:f9:d9:14:4b:f9:56:
      81:eb:a8:64:4e:ba:ab:9f:35:14:5c:d3:dd:e7:59:2d:e2:db:
      90:7d:23:bb:52:5e:8c:e1:36:83:56:11:0c:d9:b5:d7:3d:36:
      ea:4b:52:c8:d8:a7:82:84:25:18:4e:18:5b:fd:9e:04:d3:b9:
      37:ef:30:a8:b8:05:3a:a2:d8:57:7a:c3:54:e9:b1:65:e9:ed:
      22:4b:10:cc:11:38:ea:a4:32:6c:71:ee:4b:c4:53:11:db:56:
      f8:99:61:ef:37:64:40:02:fe:82:ee:8e:fe:25:18:61:0b:cb:
      61:56:d4:13:a7:63:be:a5:be:a6:53:47:b4:5a:5a:74:59:7a:
      a0:20:5d:b6:f9:91:17:be:eb:1e:7c:31:14:9f:27:eb:d9:96:
      e9:7b:8c:5c:00:1a:71:89:e2:78:83:f3:9b:b8:54:de:48:6d:
      98:ee:e1:b0:4c:61:48:4d:db:a4:d6:4d:c0:61:5f:72:2c:1c:
      19:c1:50:a0:82:8c:78:e1:e3:7a:82:84:3c:38:d9:94:8c:b0:
      29:e8:77:55:ee:97:16:e9:1a:d6:93:85:ab:16:63:b9:9b:0f:
      6f:b8:aa:e5:a6:19:76:37:b3:a0:18:70:77:29:1a:4a:86:bb:
      87:a6:69:51:f0:43:c2:55:9a:b0:c5:eb:1e:93:28:42:c9:b7:
      96:72:8e:1b:40:06:fe:9f:d6:fb:a7:68:e9:6f:8f:3e:9c:a9:
      ca:42:16:44:ab:28:81:e8:1b:04:33:30:cc:82:ea:d6:53:a5:
      fd:75:e3:56:fc:b1:b0:9b:1b:96:6c:55:bb:db:bf:74:64:92:
      71:32:7e:4e:02:b7:e3:13:14:9e:6e:f7:81:00:9a:2b:91:bf:
      b2:88:2c:38:ef:52:6e:3e:9a:36:bc:78:2c:6e:1d:f5:b2:86:
      4c:25:e5:7a:07:2a:09:44:3b:e2:5f:28:60:29:08:44:8a:94:
      6d:82:25:9c:a2:a1:f1:e1:6a:3b:77:2a:00:52:98:e3:81:cd:
      61:02:a2:65:79:ce:a7:75:68:1a:65:d5:70:d8:4f:53:d7:3c:
      55:43:ca:50:fe:75:92:85:48:5f:09:95:43:69:fe:18:54:c6:
      17:53:10:cf:b3:e1:5f:cc:79:f9:c3:f2:01:9c:5f:0d:00:90:
      46:3b:ac:0b:17:75:db:b6:2c:ae:8b:83:8c:47:ce:2b:0c:11:
      2a:34:eb:f2:05:d3:d5:8f:08:34:1f:43:e6:86:6a:63:18:b3:
      e8:9f:96:82:b8:76:68:42
```



## 8.2.4 ZETES TSP EC Qualified TSU4

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      7d:bf:1c:7f:e9:83:90:b5
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: May 16 10:19:47 2018 GMT
      Not After : May 13 10:19:47 2030 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP EC Qualified TSU4
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:ec:e4:4f:3d:25:d2:64:03:75:dc:07:08:58:fc:
        8b:7c:fa:bc:8d:22:a9:ed:87:fd:b2:fa:fc:bc:12:
        f9:43:e9:eb:de:5b:12:7c:f1:fd:f9:ed:64:1a:08:
        ab:0a:3f:4f:f5:b3:c6:37:60:06:a7:c7:f4:0a:73:
        4f:77:c0:39:32
      ASN1 OID: prime256v1
      NIST CURVE: P-256
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      4C:97:D4:09:D8:CD:94:53:80:10:4C:D0:46:F5:5D:1F:C7:43:23:03
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    qcStatements:
      070.....F..0+.....F..0!0...https://pds.tsp.zetes.com..en
    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com
      User Notice:
        Explicit Text:

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
    0b:1b:8c:ba:f8:9f:53:5c:66:c0:52:e0:94:54:a8:19:43:27:
    19:88:18:30:c0:f5:e4:62:82:a3:3d:cb:fa:8a:d2:cc:f9:6e:
    86:65:f6:61:1a:c1:1c:d0:d9:2f:cb:65:d6:78:5b:37:c5:53:
    15:47:34:29:1b:3b:b5:97:ea:c0:da:c7:b2:11:29:0e:82:eb:
    db:f5:c7:5c:76:18:e0:a9:5c:b2:87:f3:ba:3f:d4:c5:52:93:
    d4:fb:5a:67:1e:3a:47:e8:23:e0:68:fc:4c:c6:78:fb:03:86:
    90:e2:2d:0d:5c:de:78:37:f3:79:29:0f:33:b7:e5:4f:b5:b4:
    af:e7:f6:72:9b:35:5e:10:e8:53:2c:82:72:81:6c:dc:4d:e7:
    49:d2:6b:0f:17:aa:cd:3c:c2:eb:e6:57:5d:b7:0d:e7:be:75:
    36:77:eb:21:54:1e:51:c0:5a:df:ac:5d:79:7d:9c:85:4d:fd:
    aa:5c:2e:15:b0:cb:5d:8f:7b:0b:e2:6d:0b:fe:62:60:40:f9:
    53:ec:fb:88:80:43:b1:c4:d0:58:b7:cd:d3:94:d9:58:39:ba:
    1e:7f:36:0e:47:39:62:12:a0:e1:16:f5:a4:87:b4:f5:6e:2a:
    4b:0a:84:37:56:96:29:21:1a:c2:d1:43:94:cb:4c:22:3c:d4:
    9a:00:b5:09:13:2d:93:09:45:21:d3:bb:38:17:15:41:e8:cb:
    05:fd:13:4f:04:b6:c1:3a:0a:68:91:24:19:95:4c:9f:96:bb:
    35:be:6e:3f:17:1c:65:7c:e6:be:5d:1e:d1:51:07:3d:a9:ef:
    c1:51:2e:62:59:98:c1:d7:46:1c:26:04:4f:b3:2f:cf:f8:3b:
    6a:52:87:bd:ae:c7:1d:df:82:e7:71:40:29:c5:7e:84:29:be:
    06:48:cc:0b:fe:cd:6e:8d:d3:c5:e8:64:ae:7f:73:92:fd:38:
    0b:cc:47:5c:35:6d:0b:26:b2:46:88:ba:ad:3a:0f:05:b3:7f:
    44:9a:fc:a0:38:16:70:59:50:31:6c:ed:12:8d:c2:57:cb:ac:
    13:0c:85:9b:53:60:df:9f:14:7e:88:6a:a1:77:36:a1:c5:4f:
    33:66:bc:51:0d:46:4f:71:dc:47:b6:c2:af:b5:b7:25:22:e6:
    5a:7c:1d:ad:82:cc:fe:f9:e2:08:6c:88:30:5c:3a:43:5c:39:
    bc:b9:f3:50:18:f4:c2:6f:77:59:a7:19:2d:73:78:8c:fe:2f:
    a4:67:6d:85:30:a7:e0:8d:6b:4c:5f:88:95:05:d7:08:b7:6d:
    8f:af:68:58:a4:bf:df:a7:a9:46:80:15:9a:8d:78:31:ac:4e:
    1a:a2:7e:7d:9d:6a:ad:6e
```

-----BEGIN CERTIFICATE-----  
MIF7jCCA9agAwIBAgIIIfb8cf+mDkLUwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE  
BhMCQkUxJDAiBgNVBAoMG1pFVEVTFIFNBICHWQVRCSR0wNDA4NDI1NjI2KTEMMMAoG  
A1UEBRMDMDAxMSEwHwYDVQDDbHARVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN  
MTgwNTE2MTAxOTQ3WmczAwNTEzMTAxOTQ3WjBZMQswCQYDVQQGEwJCRTEkMCIG  
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSQwIgYDVQDDbHARVRF  
UyBUU1AgRUMgUXVhbG1maWVkiFRITVTVQWWTATBgqhkJOPQIBBgqhkJOPQMBBwNC  
AATs5E89JdJkA3XcBwhY/It8+ryNIqnth/2y+vy8Ev1D6eveWxJ88f357WQaCKsK  
P0/1s8Y3Yaax/KKc093wDkyo4ICeDCCANQwCAyIKwYBBQUHAQEEDBIMdkGCCsG  
AQUFBzACh1odHRwOi8vY3J0LnRzcC56ZXR1cy5jb20vWkVURVNUU1BUU0FDQTAW  
MS5jcncwJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXR1cy5jb20wHQYD  
VR0BBYEFeyX1AnYzZRTgBBM0EblXR/HQYMDMAwGA1UdEwEB/wQCMAAwHwYDVR0j  
BBgwFoAULVFLSduELbBNK+gFOFOp5b4ft0UwRQYIKwYBBQUHAQMEOTA3MagGBGQA  
jkyBATArBgYEAI5GAQUwITAfFhlodHRwczovL3Bkcy50c3AuemV0ZXMUy29tEwJ1  
bjCCAQEGA1UdIASB+TCB9jCB8wYkYBBIL0ZgIBAjIwgeMwLAYIKwYBBQUHAgEw  
IGh0dHBzOi8vcvcmVwb3NpdG9yeS50c3AuemV0ZXMUy29tMIGYBggrBgEFBQcCAjCB  
pr6BogBaAEUAVABFAFMAIABUAFMAUAAgAFEdQBhAGwAaQBMAGkAZQBkACAAyWb1  
AHIAAdABpAGYAaQBJAGEAdABlACAAZgBvAHIAIAB0AGkAbQBlAC0AcwB0AGEAbQBW  
AGkAbgBnACAAyWbVAG0AcABsAGkAYQBuAHQAIAB3AGkAdABoACAAARQBUAFMASQAg  
AFQAUwAgADMAMQA5ACAANAyADEALjA+BGNVHR8ENzA1MD0gMaAvh1odHRwOi8v  
Y3J0LnRzcC56ZXR1cy5jb20vWkVURVNUU1BUU0FDQTAWMS5jcmwDgYDVR0PAQH/  
BAQDAgeAMBYGAIUdJQEB/wQMMAAoGCCsGAQUFBwMIMA0GCSqGSIb3DQEBEwUAA4IC  
AQAIG4y6+J9TXGbaUuCUVKgZQycZ2BgwwPXkYOKjPcv6itLM+W6GZf2hGsEc0Nkv  
y2XWfS3xVMVRzQpGzu1l+rA2seyESK0guvb9cdcdhggVyyh/06P9TFUPU+1pn  
HjpH6CPgaPxMxnj7A4aQ4i0NXN54N/N5KQ8zt+VpTbSv5/ZymzVeEOhTLIJyGwzc  
TedJ0msPF6rNPMLr5lddtw3nvnU2d+shVB5RwFrfrF15fZyFTf2qXC4VsMtdj3sL  
4m0L/mJgQP1T7PuIgEOxxNBt83TlN1YOboefzYORz1iEqDhFvWkh7T1bipLCoQ3  
VpYpIRrC0UOUy0wiPNSaALUJEy2TCUUh07s4FxB6MsF/RNPBLbOgpkosSQZ1Uyf  
lrs1vm4/Fxx1f0a+XR7RUQc9qe/BUS5iWZjB10YcJgRPsy/P+DtqUoe9rscd34Ln  
cUApXX6EKb4GSMwL/s1ujdPF6GSuf3OS/TgLzEdcNW0LJrJG1LqtOg8Fs39Emvyg  
OBZwWVaxb00SjcJXy6wTDIwU2DfnxR+iGghdzahxU8zZrxRDUZPcdxHtsKvtbcl  
IuZafB2tgsz++eI1bIgwXDpDXDm8ufNQGPtCb3dZpxktc3iM/i+kZ22FMKfgjWtM  
X4iVBdcIt22Pr2hYpL/fp6lGgBWajXgxRE4aon59nWqtbg==  
-----END CERTIFICATE-----

## 8.2.5 ZETES TSP RSA TSU5

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      25:45:01:d5:ce:7a:f4:63
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: May 16 10:21:06 2018 GMT
      Not After : May 14 10:21:06 2024 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP RSA TSU5
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (3072 bit)
      Modulus:
        00:a4:ad:f0:09:d7:55:b3:ad:4b:03:6e:55:39:d7:
        7e:3e:14:33:da:58:ef:27:e4:02:49:b4:67:12:c9:
        8e:3f:19:f9:60:88:0f:b4:a9:a3:35:12:6c:08:a2:
        76:35:5c:0e:4a:7e:42:e0:94:26:34:df:29:be:d9:
        fb:c0:14:c7:fa:0b:65:56:88:63:ee:96:fb:18:87:
        ce:1e:25:10:fd:d4:c1:64:33:29:44:d4:74:52:63:
        38:a8:20:b9:22:03:ec:85:3a:71:86:cf:a8:47:a0:
        29:08:35:cd:37:9a:e6:66:55:c0:8b:5e:27:3a:af:
        48:86:01:8c:0b:dd:78:50:c4:61:1b:4d:8a:7a:1b:
        0a:15:ce:63:38:4e:69:89:16:c1:a6:e8:80:4c:aa:
        14:66:ad:fe:0d:75:e5:f1:d7:8e:f2:5e:52:e7:09:
        23:bd:ee:6b:99:07:3f:d5:9f:ab:7b:7f:27:4d:59:
        7b:6f:86:3e:89:6c:aa:2f:ea:ca:ce:5f:86:91:6c:
        57:74:b2:0d:ea:56:87:47:6f:63:33:d6:62:be:f1:
        42:34:cd:9b:8f:2b:6c:68:c6:00:e8:5d:1b:b3:ef:
        af:de:a6:f1:28:94:7c:74:49:5a:54:b0:c8:6c:04:
        a0:eb:82:0b:2a:81:da:86:b6:ff:b2:a6:bb:7b:ce:
        9e:6d:9a:e4:e0:e5:bf:16:a3:d2:51:e4:6b:1b:c1:
        54:3e:86:78:fb:34:54:cd:a8:14:ee:e6:88:59:1d:
        a3:7a:fd:60:41:e4:01:15:11:c9:9b:81:80:ff:d6:
        84:e7:d8:75:32:73:37:20:3f:8c:c9:a6:9e:d4:68:
        f3:31:ef:a6:2c:d1:5a:77:25:28:50:79:3e:86:28:
        b1:39:81:38:87:67:53:1c:0b:2a:bb:f3:39:a5:11:
        31:f0:5e:96:f9:57:31:89:70:78:7b:c6:4a:3f:2f:
        54:17:c6:04:93:fe:08:61:11:37:bc:dc:d1:e1:a1:
        af:f6:2a:ac:12:ca:af:50:4b:31
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      7F:6A:CE:17:C9:37:57:38:EF:FE:C0:EA:52:FF:08:8F:77:11:7F:C8
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
      20:74:9c:ac:0c:d2:77:56:c0:cb:1c:2f:b1:03:93:ce:8f:32:
      56:78:0a:71:12:be:30:18:54:97:5f:9a:10:51:c5:81:01:ce:
      08:20:df:93:b4:ce:c8:b1:96:57:b3:5b:4f:53:fe:cd:2c:94:
      2d:92:3b:00:55:f1:e6:86:61:f0:93:cf:59:88:5d:14:a3:04:
      2e:98:16:5b:0b:51:d5:74:c1:c7:8b:17:26:3a:86:f7:e6:47:
      b8:c9:c5:de:4f:99:31:67:00:f9:2c:12:9e:39:31:b6:7c:ba:
      a5:bd:ec:27:69:a2:e6:c6:03:d3:dd:b5:53:4e:08:10:01:ac:
      d6:70:30:fa:a7:ae:20:70:83:a4:0f:a3:40:24:24:6a:85:22:
      98:de:c2:11:a8:d7:be:3f:ac:df:de:22:79:e7:7f:a7:ad:94:
      a3:54:2c:b3:c2:63:78:ba:96:c3:2d:bc:2b:e2:8e:39:f8:5e:
      27:14:45:e2:e2:82:8d:3f:cb:d3:c8:49:f0:fe:83:e2:6b:f2:
      ce:2b:ec:48:05:02:dc:2a:97:26:d9:32:1a:ff:25:af:96:80:
      83:84:89:2b:4d:ed:8d:95:89:d0:e4:16:35:43:5c:49:43:2f:
```





## 8.2.6 ZETES TSP RSA TSU6

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      6e:af:d7:1e:5d:ef:99:50
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: May 16 10:21:35 2018 GMT
      Not After : May 14 10:21:35 2024 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP RSA TSU6
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (3072 bit)
      Modulus:
        00:a6:c0:59:92:49:74:ca:9d:55:29:aa:20:f9:2e:
        91:74:1b:da:d9:88:1b:61:f1:33:19:14:9a:9d:1d:
        b7:04:aa:de:10:7b:c6:ea:b3:26:22:a1:82:cf:25:
        7f:d3:9c:fa:c5:b5:ef:9d:48:ca:66:7e:45:12:05:
        ab:a6:d7:7f:cd:fd:ff:99:c4:c7:f8:ba:76:84:52:
        0a:61:af:53:0d:ec:e1:a2:2d:5e:94:30:d4:e2:28:
        04:95:ba:a0:53:3c:fd:1f:bc:ab:85:a8:e3:a8:36:
        1a:3d:21:59:43:1e:f1:68:c9:b3:dd:35:67:dd:46:
        e7:7f:fe:e3:ae:b2:01:e1:34:de:33:50:aa:3d:99:
        53:34:21:22:76:e1:4a:10:1d:c6:b7:83:c3:52:e3:
        b0:2b:07:fc:cb:e3:b2:d5:05:04:c5:e0:84:a7:f5:
        ad:36:53:b2:c2:21:76:6b:44:21:03:9d:60:3d:fa:
        ab:77:df:8b:cb:a8:d6:05:b3:78:5f:d1:cf:07:25:
        12:6b:ba:ca:79:18:1c:ab:2d:e7:38:a9:9f:b1:96:
        d0:7a:3c:8b:48:1a:15:c4:2e:92:bd:8d:f4:60:c4:
        cd:03:53:f1:28:70:34:79:cc:c7:b9:a8:d6:42:aa:
        16:4b:0a:23:09:62:a6:bb:32:b0:2d:f6:ca:d7:18:
        cf:68:16:e7:22:1b:24:b7:a9:a1:75:6f:20:f2:d5:
        9a:1b:81:97:8e:cb:71:49:36:d3:f5:bd:e0:e2:24:
        75:7f:be:e4:fe:95:25:9e:e7:b1:b3:8c:88:a6:11:
        7d:67:fe:b1:38:f6:83:07:69:d1:7c:8e:30:db:47:
        d0:19:5e:89:72:4e:7b:3a:7f:96:85:5e:22:89:da:
        44:5c:4b:8c:e8:21:85:ae:f8:e8:4a:1b:72:86:ce:
        fa:48:a5:29:23:61:44:f5:e9:43:69:65:73:f2:c8:
        8e:ff:a4:cf:aa:d4:a1:78:af:1b:94:82:1c:93:be:
        d0:2f:55:ff:4d:4e:61:07:92:19
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      9A:DA:0A:52:E9:7A:5C:7C:80:0A:71:34:61:4C:7A:AA:CE:4D:3B:F4
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
      38:b2:59:a9:51:3b:23:cc:ad:3d:3e:e0:75:ef:b2:39:f4:b2:
      02:66:07:b4:7a:f4:99:12:ae:a6:e8:27:dd:45:5a:52:a4:51:
      d4:0c:8b:f3:b4:17:64:08:46:1d:d8:0f:0a:98:7c:ff:e4:49:
      9c:8b:f5:4a:56:6b:64:87:22:e2:fd:76:84:1c:cc:3f:82:61:
      f8:ad:91:f8:a7:3b:55:92:f5:16:82:cf:2c:78:60:6a:3f:c9:
      e1:d0:a1:27:83:ed:1f:a4:30:8b:dd:30:dd:aa:d1:ad:ab:10:
      ab:fb:91:15:dc:70:8f:07:be:20:18:72:5a:97:be:dc:37:fa:
      ad:5d:d4:25:91:5f:e5:ba:ca:01:89:0c:fd:b0:12:aa:47:91:
      a6:0e:c9:e2:cc:3a:5d:b9:3c:dd:4a:14:d2:f6:a1:ce:bc:cf:
      58:66:26:ac:16:fc:9f:6c:5a:3e:47:c4:2e:25:5d:07:1e:9c:
      3d:1b:95:37:bb:f7:99:69:6c:6f:8c:c4:df:a9:f6:df:d4:44:
      b2:97:d6:52:af:6c:45:c7:fb:f3:3e:c4:88:4b:d3:66:e5:76:
      ab:80:1e:77:d1:ce:06:af:7c:c9:a9:12:a8:8c:2c:e1:15:ca:
```

## TSA PRACTICE STATEMENT AND TIME-STAMP POLICY

```

47:fd:f0:f4:9c:e2:d3:31:1a:22:de:f5:42:07:8b:96:5c:02:
c7:9f:f3:91:d8:31:06:80:be:d1:46:8a:0e:67:8f:6c:f5:c0:
52:0a:0b:72:a7:bd:21:1a:ea:cd:e6:34:3b:15:2e:45:89:18:
79:bc:d9:a8:cf:36:be:44:9f:ca:1f:46:5d:a0:58:68:b1:33:
af:f6:80:f9:5b:95:74:a:51:27:ba:91:a0:2e:ec:c3:1f:b4:c1:
fd:04:64:01:c9:6d:67:13:21:f4:cc:29:b3:22:61:70:c3:e6:
af:44:74:19:eb:e8:16:b9:74:36:a1:61:30:36:7b:0c:1f:53:
c5:28:8a:c9:1c:66:0d:ad:f9:53:6b:1f:86:d5:2a:01:cc:97:
34:07:8c:c0:8a:94:0e:2f:09:7b:23:98:80:b8:41:ca:36:20:
36:d5:ee:09:3a:44:f6:e5:5b:89:04:fe:10:16:6d:63:d3:b3:f4:
ef:50:39:17:73:da:99:25:59:de:c7:0a:a3:97:63:ba:0c:de:
cf:56:54:0e:42:18:a0:76:36:7c:bb:24:8e:bd:fd:43:85:fd:
94:6d:3f:1d:ec:1f:72:56:a3:07:9d:a5:55:ad:d9:16:e4:6d:
2d:93:4b:e1:53:1e:82:64:53:0e:e4:19:88:ef:84:aa:90:b7:
69:25:b0:a2:93:e5:93:ff:14:a3:33:af:3a:ea:8a:66:4d:db:
c7:20:b0:fa:b2:ae:74:15

-----BEGIN CERTIFICATE-----
MIIGLjCCBBAGABIBAgIIBq/XHl3vmVawDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDA1BgNVBAOMG1pfVEVtY1FBNiChwQVCRSOWNDAand1NjI2TEMMAAG
A1UEBRMDXAMSEWhvY2N0Q2BhARVFYyBUU1AgQ0EgRk9S1FRTQSAWDELWwHcnM
TgWnTE2MTAyMTEwYjYjQWNTQ0TAAyMTY1YjBQMxQScQYDVQVQwECJCRTEKICG
A1UECgwbWkVURVWgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMrswGQYDVQVQwDDBJaRVRF
UyBUU1AgU1N1FRTVYwggG1MA0GCSqGSIb3DQEBAQUAA4IbBgAwGQKAgQ1BggQcm
wFmSSXTknUpqId5LPf0G9G2i8th8TM2FQjdghBct4Q8BjsgyIoYLPXj/vnTrF
te-dSMPmfKUSBaum13/N/f+ZxMf4unaEUpghr1MN70G1VL6UMNT1KASVgBTTPP0f
vKuFG0Oonho9IvLDHvFoybPdNwfdRud//u0usghGn4ZUko9mVMOISJ240Qhca3
g8NS47ArB/zL47LVBQTf4ISn9a02U7LCIXZRCDENWA9+qt334vLqNYFs3hf0c8H
JRjursp5GbyrLec4zq+xl186PttIGhELPk9jFrXqM0DgU/EocDR5lme5NcZqhZL
CiMJYga7MrAt9sXGM9OfuciG93qaf1byDyL2obgZeOy3FJnt1P5edJiHV/vnTrF
1SWe57GzjIimEX1n/EA49mHAdF8jJdbR9AZXKfYtNs6f5aFXiKJZrKcS4zoIYwu
+OhKG3KGzVpIskYjYUT16UNpZGXPyI7/pm+qX1KfYrUghyTvtAvf9NtMEhkKk
AEwAAAC0AxyVpghYMHAGCCSAgGFwBEEBhGQwYjA5BrguGBEFBQCAoYA0tR0Dov
L2Nydc50c3AuemV0ZXMx29tL1pFVEVTVFNQBOEwMDUe3J0MCJUGCCSAGQAF
BzABhhl0dHRwO18vb2NzY25tL3AuemV0ZXMx29tNBQO1UdDgQWBSA2gcs5Xpc
fIAKcTRhTHqqzk079DAMBgmVHRMBAf8EAjAAMB8GA1UdIwQYMBAAFC1RS0nbhC2w
TSv0BthTqH+H7fMEGAG1UdIARMBDMgYQLKwYBBIL0cyIbAJ1JLjASBvgrGBEF
BQCARYGa8rChm6f1ly9y2Xbvc21l0b3J5LnRZc65EXRkL1z0g3b20WpJ9D0FBCD
NTAz0DgSL4YtAHR0cDovL2Nydc50c3AuemV0ZXMx29tL1pFVEVTVFNQBOEw
MDUe3J0GA1UdDwEBlwYEAuIHgDABwYMBHUSBAf8EDDAKBggrGBEFBQCCDNDAN
BgkqhkiG9w0BAQsFAAOCAgEAOIJZqV7I8ytPT7gde+yOfSyAmYHr0mRKupugn
3UvAUqRr1AYL87QXZ4GHgdGPcph8+RjUn1s1ZsrZiCi4v12hB2MP4Jh+K2R+Kc7
VZL1FoRLPHhgaj/J4dCh9J4PtH6qG190w3carRasqg/vrUdXwvje+IbHyWpe+3DF6
rv3UJZfF5brKAYKm/bASgkeRpg7J4s6w6Xbk83UoU0vafzr3PwGmYrBb8n2xaPKE
LiVdBx6cPRUvN7v3mw1sB4ze36n239p5PwUq9s9c7h72EiEvT4K2D4a9H0
Bg98yqAG8y4sRXKR/3w9Jzi0eZaIt7fQGLlwcX5/zkdgsBoC+0daKdodvPKA
UoLcqe9JrRazgeY00xUuYfYebzQmK2vksf9hGxAbYfEzP+/AA+VvUelEnUpG
Luwxr7TB/QRKaeZiXmJ9MwpsYJhcMCPR0G0vGoFrlOnGfH2p27BFtXsKixRxm
Da35U2sftUAgAcyXNAEMwIguD18JeyOyGhLbyYgNtX3CtXp9E+VbjiQT+EGPWPBp0
71a5F73PamSVZ3sc0s5dsuge/FZUDUdIYoH4d2Lskjr39Q491NY/HwKfzlaB52l
Va3FzUrtLZNL4VMegvthw+QziO+EqpC3ASwwoP1k/8UozOvUqGHeZ3bxyCw+rKu
dBU=

-----END CERTIFICATE-----

```

## 8.2.7 ZETES TSP EC TSU7

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      34:a2:7c:04:14:fb:23:c1
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: May 16 10:22:10 2018 GMT
      Not After : May 13 10:22:10 2030 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP EC TSU7
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:9c:e0:02:c9:ec:6d:64:68:83:10:07:db:f8:7d:
        f3:16:d8:66:30:cd:a6:6c:c6:5f:4c:b6:b7:76:a8:
        af:36:f2:dd:36:5e:8c:77:1b:8d:0f:a2:de:99:79:
        53:b3:5b:cb:dc:58:7e:83:dc:e4:50:ff:62:17:89:
        cf:df:81:53:08
      ASN1 OID: prime256v1
      NIST CURVE: P-256
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      C8:CC:CF:14:F7:FC:66:0A:9C:F4:65:B1:77:57:BE:96:B3:DE:73:1D
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
    1b:a0:6a:a5:9e:af:fd:60:30:8c:1d:47:5f:93:51:a7:12:68:
    29:25:1e:73:63:78:e6:39:cd:f2:cf:24:64:f5:4b:74:73:de:
    62:22:1c:2f:45:85:8e:3e:06:6e:4b:70:a2:3a:2c:2f:72:68:
    c2:61:ca:f3:cc:52:09:60:84:36:9d:f9:11:be:72:02:ff:06:
    f5:d5:90:c9:11:84:18:f8:ce:7a:9c:6f:ef:c0:fc:2d:d2:77:
    21:43:05:57:71:a8:ca:97:1a:44:ed:d4:d8:95:bb:30:c7:7d:
    6f:9a:40:dd:44:8d:25:65:80:5c:cf:5d:80:74:24:bf:9c:1e:
    5a:13:e2:11:1b:6c:bb:75:ea:43:f2:0e:e1:bc:18:ec:46:82:
    cc:56:bb:e2:9a:13:72:8d:5a:ec:a5:93:67:ff:44:e3:db:0a:
    79:22:36:c1:8b:25:d7:0c:ab:4e:52:11:8e:81:05:0f:72:ba:
    58:e0:5d:62:b4:5a:c3:71:b8:bb:27:c8:03:95:74:09:a3:47:
    cc:50:aa:80:b0:f1:54:bf:08:cd:c8:05:5f:df:40:ec:c0:a2:
    25:4d:c4:84:aa:05:09:e4:8c:2f:5a:fc:63:79:ec:c1:f5:86:
    b7:d5:3b:ef:90:48:c1:28:66:06:f4:c8:6d:d4:a8:b2:bc:16:
    ae:f4:a2:ab:92:5a:64:ab:b2:c8:d0:5e:8b:b0:c5:a3:ff:44:
    4b:42:19:0d:a0:1a:af:97:51:be:61:78:d5:7a:88:ac:10:6e:
    06:ac:6b:3c:91:47:c6:2a:ff:b0:60:9a:4a:ca:c7:92:38:87:
    c8:d9:5e:eb:e3:9f:81:87:ad:d5:29:79:ce:8d:59:2c:16:f3:
    f5:86:57:80:3b:9a:6a:75:5f:ae:75:f1:69:4f:9f:d0:48:2b:
    26:7c:d3:f9:21:ba:2d:ab:c3:51:b2:a1:b6:c4:7d:d8:60:b8:
    88:3c:74:9a:51:1a:43:09:7f:14:57:b4:7a:57:af:85:6a:20:
    67:2f:70:8d:4c:d7:ff:53:a6:21:a9:91:30:12:58:8e:e3:e6:
    87:f4:b2:54:8d:9a:47:72:81:2f:b1:0c:6d:ad:51:b6:87:4a:
    45:54:85:f0:eb:51:2f:65:46:38:2e:3c:0a:a9:a8:3e:09:0c:
    85:ae:3f:aa:0e:21:c0:17:03:bb:c6:d2:2d:f1:03:fd:80:b3:
    b5:50:15:f8:b8:6a:dd:92:cf:6a:13:8f:ef:04:12:57:06:bb:
    82:6d:b2:b2:7f:1b:fa:03:a5:85:22:5b:ae:38:85:41:aa:68:
    c0:65:db:62:20:ee:77:f0:96:2f:cc:52:d7:97:9c:13:06:78:
    08:97:68:9c:82:d5:be:31
  -----BEGIN CERTIFICATE-----
  MIIe4jCCAsqgAwIBAgIINKJ8BBT7I8EwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
  BhMCQkUxJDAiBgNVBAoMGlpFVEVTFjFNBChWQVRCRS0wNDA4NDI1NjI2KTEMMaOG
  A1UEBRMDMDAxMSEwHwYDQDDBBhARVRfUyBUU1AgQ0EgRk9SIFRTQSAAwMDEwHhcN
  1805161022102018GMT+0200Z
  -----END CERTIFICATE-----
```

MTgwNTE2MTAyMjEwWbcNMzAwNTEzMTAyMjEwWjBPMQswCQYDVQGEwJCRTEkMCIG  
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMR0wGAYDVQDDBFaRVRF  
UyBUU1AgRUMgVFNVNzBZMBMGBYqGSM49AgEGCCqGSM49AwEHA0IABJzgAsnsbWRo  
gxAH2/h98xbYzjDNpmzGX0y2t3aorzby3TZeJHcbjQ+i3p15U7Nby9xyfoPc5FD/  
YheJz9+BUwjjggf2MIIBcjBwBggrBgEFBQcBAQRkMG1wOQYIKwYBBQUHMAKGLWh0  
dHA6Ly9jcncQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRtQUNBMDAxLmNydDA1Bggr  
BgEFBQcWAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4EFgQUyMzP  
FPf8Zgqc9GWxdle+lrPecx0wDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAwBQtUUTJ  
24QtsE0r6AU4U6nlvh+3RTBIBgNVHSAEQTA/MD0GCysGAQSC9GYCAQIyMC4wLAYI  
KwYBBQUHAgEWIGh0dHBzOi8vcmlvbnRpdG9yeS50c3AuemV0ZXMuY29tMD4GA1Ud  
HwQ3MDUwM6AxcCGLWh0dHA6Ly9jcmlwudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRt  
QUNBMDAxLmNydDA0BGNVHQ8BAf8EBAMCB4AwFgYDVR01AQH/BAwwCgYIKwYBBQUH  
AwgwdQYJKoZIhvcNAQELBQADggIBABugaqWer/lgMIwdr1+TUacSaCklHnNjeOY5  
zfLpJGT1S3Rz3mIiHC9FhY4+Bm5LcKI6LC9yaMJhyvPMUglghDad+RG+cgL/BvXV  
kMkRhBj4znqcb+/A/C3SdyFDBVdxqMqXGkTt1NiVuzDHfW+aQN1ejSVlgFzPXYB0  
JL+cHl0t4hEbbLt16kPyDuG8G0xGgsxWu+KaE3KNWuylk2f/ROPbCnkiNsGLJdcM  
q05SEY6BBQ9yuljgXWK0WsNxuLsnyAOVdAmjR8xQqoCw8VS/CM3IBV/fQOzAoiVN  
xISqBQnkjC9a/GN57MH1hrfVO++QSMEOZgb0yG3UqLK8Fq70oquSWmSrssjQXouw  
xaP/REtCGQ2gGq+XUb5heNV6iKwQbgasazyRR8Yq/7BgmkRkx5I4h8jZXuvjn4GH  
rdUpec6NWSwW8/WGV4A7mmp1X6518W1Pn9BIKyZ80/khui2rw1GyobbEfdhguIg8  
dJpRGkMJfxRXtHpxr4VqIGcvcI1M1/9TpiGpkTASWI7j5of0slSNmkdygS+xDG2t  
UbaHSkVUhfDrUS91rjguPAqpqD4JDIWuP6oOIcAXA7vG0i3xA/2As7VQFfi4at2S  
z2oTj+8EE1cGu4JtsrJ/G/oDpYUw644hUGqamBL22Ig7nfwli/MuteXnBMGeAiX  
aJyC1b4x  
-----END CERTIFICATE-----

## 8.2.8 ZETES TSP EC TSU8

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      0d:13:c8:6e:1e:2a:c5:56
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: May 16 10:22:32 2018 GMT
      Not After : May 13 10:22:32 2030 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP EC TSU8
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:42:84:dc:85:fe:c0:00:b6:3b:4d:0d:2e:b0:fc:
        bd:21:13:e2:cc:d3:49:bd:b8:b9:f1:95:aa:f2:e0:
        d0:38:68:b8:86:25:12:ab:14:f2:30:90:96:c5:08:
        c7:c2:08:dd:16:e9:a4:22:8f:06:02:88:4d:55:ce:
        01:bd:6a:ee:dd
      ASN1 OID: prime256v1
      NIST CURVE: P-256
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      F3:44:11:10:00:E2:5C:D2:DD:7C:E7:47:B9:22:52:DE:4D:A1:B6:2E
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
      0a:6d:f6:6f:5a:c5:c3:05:24:90:c1:45:8b:b5:b7:b0:d0:35:
      bc:bf:bc:1a:e6:cb:7b:5d:b4:51:12:35:40:cd:df:0f:66:88:
      6a:30:d5:60:fe:36:03:e8:a7:48:23:df:e5:2b:c0:ad:60:b4:
      9b:6d:25:32:08:a2:30:9a:bf:e0:4c:13:46:86:74:66:4b:66:
      9c:04:54:cd:f7:0d:ae:77:0a:7c:f0:12:bd:01:a2:11:83:95:
      19:ce:a5:97:af:6f:ee:d5:ec:d2:12:21:32:28:71:34:e9:da:
      3c:31:f7:e6:3f:08:1a:ba:27:4e:ad:c1:9f:c5:2e:e2:79:85:
      3a:ee:76:e4:0d:07:3e:3b:49:c5:c3:6d:3e:83:de:06:af:8d:
      f7:93:1d:9e:ed:12:5e:e0:bd:fb:53:35:42:71:eb:f4:1a:f7:
      1e:23:ab:c3:a6:9b:20:24:de:c0:fc:5d:09:2c:e3:08:dd:73:
      cd:b5:2b:02:00:9f:2b:9b:c2:9b:d3:68:00:d8:51:06:de:ab:
      ef:46:fc:4e:d5:4a:b4:1d:2c:41:4d:a4:cd:db:00:3a:c5:c1:
      d2:0d:02:ac:6f:cf:89:e2:56:78:89:9c:4a:2b:8a:c6:62:a7:
      bb:bd:51:c3:59:94:7a:3b:60:17:b4:73:ef:12:aa:57:ea:02:
      59:67:3a:bb:af:fc:43:5c:db:d0:05:d3:28:76:07:9d:7b:ab:
      04:91:a5:00:cf:99:80:80:1e:67:91:35:5a:c2:07:30:a9:7f:
      71:a1:a0:1f:75:63:80:27:dd:83:49:22:85:8c:4f:96:f8:ed:
      39:7c:b8:c8:70:e7:e6:39:26:6e:dd:58:88:a2:78:13:85:1a:
      91:0e:83:1a:ee:4a:16:7a:2c:1c:b3:1a:9c:11:58:d2:69:e6:
      6a:4c:e3:94:10:5b:a8:22:92:60:59:32:17:69:49:77:ee:98:
      f8:30:dc:6a:84:21:4a:a8:32:2b:cb:e9:c7:19:0f:45:60:00:
      7e:fb:5b:d5:d4:29:9a:91:e4:67:7d:03:53:e9:7b:e4:79:75:
      6c:bf:7c:87:ec:87:d3:45:ee:06:65:0a:25:fd:84:75:de:58:
      ce:3d:eb:c5:bb:80:d4:23:23:81:7f:6f:5b:86:71:26:75:8b:
      68:7e:aa:22:3a:6a:82:57:61:72:27:23:e7:be:52:ba:ee:02:
      a5:b7:93:30:b9:9c:37:04:ab:09:ff:e9:0b:a9:89:00:e8:70:
      04:fc:24:2f:10:ad:bf:52:00:02:1f:7f:c9:a0:d8:e7:9d:e9:
      e6:7e:c7:fd:73:a8:e0:cb:41:d6:18:3c:78:90:bb:64:ce:df:
      6d:02:ce:72:78:16:f2:60
  -----BEGIN CERTIFICATE-----
  MIIe4jCCAsqgAwIBAgIIDRPIbh4qxVYwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
  BhMCQkUxJDAiBgNVBAoMGlpFVEVtIFNBICBhWQVRCS0wNDA4NDI1NjI2KTEMMAAoG
  A1UEBRMDMDAXMSEWHDYVQDDbBhARVRfUyBUU1AgQ0EgRk9SIFRtQSAAWMEWHhCN
```

MTgwNTE2MTAyMjMyWhcNMzAwNTEzMTAyMjMyWjBPMQswCQYDVQGEwJCRTEkMCIG  
A1UECgbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMRowGAYDVQDDBFaRVRF  
UyBUU1AgRUMgVFNvODBZMEMGByqGSM49AgEGCCqGSM49AwEHA0IABEKE3IX+wAC2  
O00NLRd8vSET4szTSb24ufGVqvLg0DhouIYlEqsU8jCQ1sUIx8II3RbpbCKPBgKI  
TVX0Ab1q7t2jggF2MIIBcjBwBggrBgEFBQcBAQRkMG1wOQYIKwYBBQUHMAKGLWh0  
dHA6Ly9jcnQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRtQUNBMDAxLmNydDA1Bggr  
BgEFBQcAwYyZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAuBgNVHQ4EFgQU80QR  
EADiXNldfOdHusJS3k2hti4wDAYDVROTAQH/BAIwADAfBgNVHSMEGDAWgBQtUUTJ  
24QtsE0r6AU4U6nlvh+3RTBIBgNVHSAEQTA/MD0GCysGAQSC9GYCAQIymC4wLAYI  
KwYBBQUHAgEWIGh0dHBzOi8vcmluZS8uY29udG9yeS50c3AuemV0ZXMuY29tMD4GA1Ud  
HwQ3MDUwM6AxcC+GLWh0dHA6Ly9jcmwudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRt  
QUNBMDAxLmNybDA0BqNVHQ8BAf8EBAMCB4AwFgYDVRO1AQH/BAwwCgYIKwYBBQUH  
AwgwdQYJKoZIhvcNAQELBQADggIBAapt9m9axcMFJJDBRYult7DQNby/vBrmy3td  
tFESNUdN3w9miGow1WD+NgPop0gj3+UrwK1gtJttJTIIojCav+BME0aGdGZLZpwE  
VM33Da53CnzwEr0BohGD1RnOpZevb+7V7NISITIOcTTP2jwx9+Y/CBq6J06twZ/F  
LuJ5hTruduQNBz47ScXDdt6D3gavjfeTHZ7tE17gvftTNUJx6/Qa9x4jq8OmmyAk  
3sD8XQks4wjdc821KwIAnyubwpvTaADYUQbeq+9G/E7VSRQdLEFNpm3bAdRfwdIN  
Aqxvz4niVniJnEorisZip7u9UcNZ1Ho7YBe0c+8Ssq1fqA1lnOruv/ENc29AF0yh2  
B517qwSRpQDPmYCAHmeRNVrCBzCpf3GhoB91Y4An3YNJIoWMT5b47T18uMhw5+Y5  
Jm7dWiiieBOFGpEOgxruShZ6LByzGpwRWNJp5mpM45QQW6gikmBZMhdpsXfumPgW  
3GqEiUqomivL6ccZD0VgAH77W9XUKZqr5Gd9A1Ppe+R5dWy/fifsh9NF7gZ1CiX9  
hHXeWM4968W7qNqjI4F/bluGcSZ1i2h+qiI6aoJXYXInI+e+UrruAQW3kzC5nDcE  
qwn/6QupiQDocAT8JC8Qrb9SAAIff8mg2Oed6eZ+x/1zqODLQdYYPHiQu2T032OC  
znJ4FvJg  
-----END CERTIFICATE-----

## 8.2.9 ZetesConfidens RSA Qualified TSU9

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
1d:c8:f3:c3:43:d4:47:f9  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001  
Validity  
Not Before: Jul 12 07:27:44 2019 GMT  
Not After : Jul 12 07:27:44 2022 GMT  
Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZetesConfidens RSA Qualified TSU9  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public-Key: (2048 bit)  
Modulus:  
00:ab:a8:95:af:a2:a4:ea:21:cd:2c:c5:ea:ce:32:  
cf:94:9f:84:82:02:81:dd:06:bd:99:c8:3b:60:ba:  
d4:38:11:7f:7b:05:32:c2:80:01:3d:63:cb:c7:e1:  
2a:7f:00:96:82:15:8e:8b:32:54:6a:c7:a9:27:24:  
dd:7b:60:e0:69:eb:b8:29:9e:fe:21:25:4e:7a:9e:  
bd:5d:85:a1:d9:4a:fd:0e:6a:d2:a7:04:46:58:f7:  
3f:41:44:34:25:21:ee:fb:92:18:19:e0:a2:9b:ab:  
80:a3:06:c3:b9:9f:cb:cd:c8:59:45:ae:58:bf:1f:  
e3:53:cc:e3:11:55:80:cb:13:36:a4:a5:2e:44:eb:  
ad:d2:3a:f8:37:d1:7e:27:04:30:12:38:41:6b:19:  
41:6c:6f:51:9d:4d:a9:80:6a:5a:08:27:f4:91:8d:  
47:33:e6:ed:6a:6c:63:6f:fa:e3:a3:85:f1:1b:22:  
e9:81:43:af:0d:4f:28:00:63:a2:c2:5c:1d:4d:7c:  
5d:46:4b:67:11:c1:6c:5b:ea:83:c3:f8:7b:96:58:  
11:e2:1b:84:42:23:c2:c6:45:b7:e0:d9:c8:17:33:  
42:5e:e4:0c:10:7b:d4:93:82:ba:b6:d1:92:42:44:  
52:5d:34:d4:e1:02:6d:5a:ca:40:84:e3:92:85:53:  
3f:65  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
Authority Information Access:  
CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt  
OCSP - URI:http://ocsp.tsp.zetes.com  
  
X509v3 Subject Key Identifier:  
22:2F:17:65:7B:1B:7C:E0:EE:65:D8:E1:DD:E9:EC:E9:B3:C6:EC:0A  
X509v3 Basic Constraints: critical  
CA:FALSE  
X509v3 Authority Key Identifier:  
keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45  
  
qcStatements:  
070.....F..0+.....F..0!0...https://pds.tsp.zetes.com..en  
X509v3 Certificate Policies:  
Policy: 1.3.6.1.4.1.47718.2.1.2.50  
CPS: https://repository.tsp.zetes.com  
User Notice:  
Explicit Text:  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl  
  
X509v3 Key Usage: critical  
Digital Signature  
X509v3 Extended Key Usage: critical  
Time Stamping  
Signature Algorithm: sha256WithRSAEncryption  
52:66:8d:32:18:0f:bd:a3:e3:32:a5:bc:25:d2:28:ef:b4:9a:  
ee:55:43:2e:7b:3e:83:27:aa:41:43:64:2d:a8:80:ad:7a:49:  
a6:37:78:2b:19:5a:bf:3a:12:90:57:eb:08:ec:78:8d:b2:b9:  
7a:eb:9b:f0:74:60:40:9b:96:41:56:81:0a:1f:e6:7e:30:6c:  
68:c9:a7:ea:95:31:b6:25:2b:e9:a5:a4:c7:a6:ec:57:68:ed:  
f3:d2:dd:b2:25:34:46:a5:02:0b:e4:39:4c:1f:96:e3:09:c1:  
de:e5:bd:9f:a4:16:b9:1b:2a:26:77:8b:dd:1b:df:a5:64:cb:  
c1:d4:6a:8d:61:39:cb:c6:71:c5:40:03:4e:32:4e:a4:02:6c:  
d3:e0:e1:fc:3c:b9:fe:93:ef:be:02:f6:c8:85:95:00:d2:8c:  
ba:4b:46:1c:3a:bd:75:c1:d8:c9:f7:09:ed:83:a7:0c:ad:37:  
7e:91:36:6f:bc:d8:59:f1:43:2b:26:cd:5c:23:a7:ad:e6:a7:  
b6:9e:9a:a7:b3:a2:3f:5a:de:eb:ae:62:7b:d2:63:b9:bd:e1:  
bf:3f:0f:6a:e7:eb:9b:ba:18:72:7f:be:7a:78:9d:04:b6:10:  
67:f1:aa:f7:57:a3:a6:a4:8d:d6:41:11:04:b2:e2:d7:2b:44:  
6a:6d:de:50:7a:b9:8e:9e:e9:e2:36:30:ad:a0:26:bf:89:58:  
e0:ba:ef:0b:23:a8:5c:61:c9:a6:ba:45:0c:85:ef:93:bd:4d:  
29:b9:97:8d:0c:b5:66:19:85:70:80:ca:cb:21:28:25:df:0d:

06:f2:e8:49:57:10:cd:3b:bc:1a:18:0c:58:a2:e4:f6:11:d8:  
70:20:ff:9a:be:05:fe:ee:ac:bf:dc:47:a6:58:1f:9c:70:8b:  
43:cc:2a:ca:9b:58:ec:49:94:c4:56:dd:b2:9f:ea:74:4b:3e:  
46:c9:b6:7c:eb:f9:b2:9a:e1:2b:43:4b:ab:dc:47:0b:13:c7:  
53:7a:2f:19:a1:fd:4c:12:83:ca:62:5c:33:14:fc:43:9d:86:  
86:f2:21:d7:82:97:73:56:f0:2d:db:bf:8d:0a:d7:4c:16:27:  
52:cb:a2:cb:a7:36:c1:f8:92:06:7c:0c:7c:ac:9d:e6:a4:0f:  
4a:98:ea:8e:7e:53:1f:4f:39:ce:c8:c3:28:77:42:38:f7:fd:  
c3:17:a0:4b:4f:29:30:67:bf:45:7b:64:5e:0c:0f:8d:ac:1e:  
a6:87:79:d3:59:27:e2:a8:d1:f7:9b:20:cb:78:5e:9b:27:13:  
f2:e2:41:55:fb:12:52:0b:86:4f:31:e7:65:a8:ff:dd:67:fe:  
c6:52:a4:d1:3b:b7:f8:81  
-----BEGIN CERTIFICATE-----  
MIIGWDCBBKigAwIBAgIIHcjzw0PUR/kwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE  
BhMCQkUxJDAlBgNVBAoMG1pFVEVTFIFNBICHWQVRCSR0wNDA4NDI1NjI2KTEMMAoG  
A1UEBRMDMDAxMSEwHwYDVQDDbHArVRfUYBUU1AgQ0EGRk9SIFRTQSAwMDEwHhcN  
MTkwnZyEyMDcyNzQ0W0hcnmJiWnZyEyMDcyNzQ0WjBfMQswCQYDVQGEwJCRTEKMCIG  
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSowKAYDVQDDCFaZXRRL  
c0NvbWZpZGVucyBU0EgUXVhbGlmawVWkIFRFTVTKwggEiMA0GCSqGSIb3DQEBAQUA  
A4IBDwAwggEKAoIBAQCrcqJWvoqTqIc0sXerOMs+Un4SCAoHdBr2ZyDtqutQ4EX97  
BTLcGAE9Y8vH4Sp/AJaCFY6LMlRqx6knJN17YOBp67gpnv4hJU56nrl1dhaHZSv00  
atKnBEZY9z9BRDQ1Ie77khgZ4KKbq4CjBs05n8vNyFlFrli/H+NTzOMRVYDLEzak  
pS5E663S0vg30X4nBDASOEFRGUFSb1GdTamAaloIJ/SrjUcz5u1qbGNv+u0jhFEb  
IumBQ68NTYgAY6LCXB1NfF1GS2cRwWxb6oPD+HuWBBHIG4RCI8LGRbfq2cgXM0Je  
5AwQe9STgrq20ZJCRFjdNNThAmlaykCE45KFUz91AgMBAAGgggJ5MIICdTBwBggr  
BgEFBQcBAQRkMG1wOQYIKwYBBQUHMAKGLWh0dHA6Ly9jcnQudHNwLnpldGVzLmNv  
bs9ArVRVFU1RTUFRFQUNBMDAxLmNydDALBggrBgEFBQcwAYYZaHR0cDovL29jc3Au  
dHNwLnpldGVzLmNvbsTAdBgNVHQ4EFgQUiI8XZXSbfODuZdjh3ens6bPG7AowDAYD  
VR0TAQH/BAIwADAFBgNVHSMEGDAWgBQtUUTJ24QtsE0r6AU4U6n1vh+3RTBFBggr  
BgEFBQcBAQw5MDcWCAyGBACORgEBMCsGBgQAJkYBBTAhMB8WGW0dHBz0i8vcGRz  
LnRzcC56ZXRlcy5jb20TAmVuMIIBAgYDVROgBiH6MIH3MIH0BgwrBgEEAYL0ZgIB  
AjIwgeMwLAYIKwYBBQUHAgEWIGH0dHBz0i8vcvVwb3NpdG9yeS50c3AuemV0ZXMu  
Y29tMIGYBggrBgEFBQcCAjCBPr6BogBaAEUAVABFAFMAIABUAFMAUAAgAFEAAdQBh  
AGwAAQBMAGkAZQBkACAAYwB1AHIAAdABpAGYAaQBJAGEAdABlACAAZgBvAHIAIAIB0  
AGkAbQBlAC0AcwB0AGEAbQBWAGkAbgBNACAAyBvBvAG0AcABsAGkAYQBuAHQAIAIB3  
AGkAdABoACAARQBUAUFMASQAGAFQAUwAgADMAMQA5ACAANAyADEALjA+BgNVHR8E  
NzA1MDogMaAvh1lodHRWoi8vY3JsLnRzcC56ZXRlcy5jb20vWkVURVNUU1BUU0FD  
QTAmMS5jcmwwDgYDVROPAQH/BAQDAgeAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMI  
MA0GCSqGSIb3DQEBCwUAA4ICAQBSZo0yGA+9o+MyPbw10ijvtJruVUMuez6DJ6pB  
Q2QtqICtekmN3grGVq/OhKQV+sI7HiNsrl665vwdGBAm5ZBVoEKH+Z+MGxoyafq  
1TG2JSvppaTHpuxXa03z0t2yJTRGpQIL5DlMH5bjCcHe5b2fpBa5Gyomd4vdG9+1  
ZMvBlGqNYTnLnHFQANOMk6kAmzT4OH8PLn+k+++AvbIhZUA0oy6S0YcOr11wdjJ  
9wntg6cMrTd+kTzvvNhZ8UMrJs1cI6et5qe2npqns6I/Wt7rrmJ70m05veG/Pw9q  
5+ubuhhyf756eJ0EthBn8ar3V6OmpI3WQREESuLXK0Rqbd5QermOnuniNjCtoCa/  
iVjguu8Li6hcXcmuKUMhe+TvU0puZeNDLVmGYVwgMrLISgl3w0G8uhJVxDNO7wa  
GAxYouT2EdhWIP+avgX+7qy/3EemWB+ccItDzCrKmljsSZTEVT2yn+p0Ssz5GybZ8  
6/mymuErQ0ur3EcLE8dTei8Zof1MEoPKYlwzFPxDnYaG8iHXgpdzVvAt27+NCTdM  
FidSy6LlpzbB+JIGfAx8rJ3mpA9KmoQOf1MfTznOyMMod0I49/3DF6BLTykwZ79F  
e2ReDA+NrB6mh3nTWSfiqNH3myDLeF6bJxPy4kFV+xJSC4ZPMed1qP/dZ/7GUqTR  
07f4gQ==  
-----END CERTIFICATE-----



## 8.2.10 ZetesConfidens RSA Qualified TSU10

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
59:c5:4c:a5:fc:6e:f5:89  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001  
Validity  
Not Before: Jul 12 07:29:39 2019 GMT  
Not After : Jul 12 07:29:39 2022 GMT  
Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZetesConfidens RSA Qualified TSU10  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public-Key: (2048 bit)  
Modulus:  
00:aa:51:c4:d0:d0:e0:30:c0:e6:8f:f3:4d:ca:d5:  
01:d0:99:d3:e1:26:f6:8e:a7:93:a8:9d:21:ef:f2:  
a3:92:79:df:59:b6:c2:60:c9:7e:58:fa:41:d5:ef:  
81:c6:13:fd:a1:91:83:c7:79:97:8e:fc:50:bb:c8:  
c4:23:b0:10:a2:c5:47:da:b6:d0:a6:7b:e9:61:9f:  
69:b9:a1:e8:47:ef:8e:74:c9:f7:89:20:ff:69:84:  
2b:29:71:27:23:34:0a:90:2f:c9:63:76:08:87:35:  
6b:b4:6e:ea:45:d4:f0:c4:d0:85:1f:12:f6:f6:b1:  
0f:4b:32:2a:5d:f7:fe:49:64:bd:dc:18:65:20:5c:  
8e:63:aa:e4:fb:4b:d0:38:69:dc:8b:e5:2a:96:d3:  
0e:9b:ec:ea:6f:0e:dd:90:81:4f:74:02:15:6d:9e:  
93:3c:2a:13:4e:a2:4e:27:b8:83:6d:b9:d2:a1:41:  
14:25:5a:9b:84:10:d0:b9:ad:c9:74:d2:d8:a0:ab:  
f7:28:26:b8:3a:a6:f0:d9:b0:d9:b7:59:6e:d7:46:  
f2:c5:e5:d9:07:1b:22:bc:fe:d2:df:44:7c:1f:42:  
c2:fc:5d:37:a7:e0:ad:88:e6:50:59:3f:82:df:25:  
67:a4:14:48:97:a0:78:a3:ec:a8:6c:c0:5b:59:27:  
88:ed  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
Authority Information Access:  
CA Issuers - URI:<http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt>  
OCSP - URI:<http://ocsp.tsp.zetes.com>  
  
X509v3 Subject Key Identifier:  
5E:19:D1:DB:23:13:EA:46:A7:FC:1C:FE:C7:04:97:18:9A:CB:04:49  
X509v3 Basic Constraints: critical  
CA:FALSE  
X509v3 Authority Key Identifier:  
keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45  
  
qcStatements:  
070.....F..0+.....F..0!0...<https://pds.tsp.zetes.com..en>  
X509v3 Certificate Policies:  
Policy: 1.3.6.1.4.1.47718.2.1.2.50  
CPS: <https://repository.tsp.zetes.com>  
User Notice:  
Explicit Text:  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI:<http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl>  
  
X509v3 Key Usage: critical  
Digital Signature  
X509v3 Extended Key Usage: critical  
Time Stamping  
Signature Algorithm: sha256WithRSAEncryption  
88:bb:89:92:7a:d5:b4:fb:44:fa:c0:5b:6e:44:31:00:42:25:  
e7:75:e1:56:e3:86:fd:bc:74:25:d6:c1:73:54:76:65:87:5a:  
57:b9:0d:24:0b:48:a1:52:50:9c:cf:d8:ab:99:65:84:e8:6a:  
b3:69:fb:6e:89:92:ff:73:f4:3f:eb:0f:31:90:3e:3d:b5:56:  
b3:39:ac:48:47:58:87:dc:8d:c3:a6:ae:64:ce:9a:ff:25:8f:  
10:fe:af:b2:cc:80:c2:db:6d:47:da:17:32:8c:8b:f9:f8:d2:  
f2:0a:78:d0:70:5c:25:da:da:13:8a:1d:72:55:73:18:f6:f2:  
76:66:87:b5:c6:9f:a0:39:f1:3d:f2:c1:28:1a:63:a2:0b:f9:  
8d:65:11:73:25:a5:1b:bc:70:eb:fd:24:27:d3:4e:a8:05:6c:  
f3:ef:d8:14:84:b5:60:9f:dc:83:0a:22:0f:32:29:99:5a:d4:  
f1:a3:39:03:05:37:62:ba:8e:66:21:c3:dc:5d:e3:ea:cb:d5:  
1c:8d:e1:9a:c1:02:b9:97:7b:9f:c5:23:23:5c:85:e3:f9:25:  
f9:be:11:ce:8e:fd:62:b8:5b:bd:73:4a:91:4e:8f:34:c6:28:  
79:b9:db:1e:80:f5:82:9a:f4:dc:bf:9c:a6:db:c3:55:c0:3c:  
93:03:f9:f8:13:29:ea:6a:bd:c0:af:43:9f:c9:82:04:ce:3b:  
ee:03:97:20:43:df:3d:06:db:4f:3b:02:0b:e1:a1:30:87:88:  
4e:2c:77:bd:84:0e:15:9e:98:12:22:3c:de:27:b6:ff:51:aa:

```
1b:5b:a9:a6:12:c8:09:61:9c:8f:65:3d:5f:be:29:f4:a8:30:
71:ec:8b:5a:50:9f:c5:67:f6:3c:88:3f:88:82:e7:67:1e:32:
99:ae:0f:33:5b:39:d0:28:7d:f7:4a:cc:e2:2c:1b:99:32:b1:
a3:54:20:75:ef:f9:0a:c9:f7:2e:88:3b:a3:48:07:b0:ee:79:
96:84:a6:37:00:37:ac:7a:81:30:fd:0f:2e:e4:16:3e:d2:3c:
22:f1:b6:4b:b1:44:98:48:ab:34:b5:9b:1b:aa:d9:4f:a4:d2:
14:d7:06:2f:62:a1:0a:0c:9f:3a:2b:74:c8:54:fc:ac:54:1a:
1c:e9:6d:49:8c:a1:c3:da:e0:9c:33:95:ef:83:e6:d0:cc:71:
de:2a:f9:a4:80:e8:15:81:ec:59:07:a6:50:42:15:a7:e4:fa:
b1:24:39:99:37:c2:b8:ca:35:cd:64:8e:40:00:f8:ea:1e:ae:
b2:d5:d1:7a:39:c6:95:5d:1e:0c:b0:e0:d6:a3:90:ec:a0:f4:
ce:8a:07:8b:46:34:88:81
-----BEGIN CERTIFICATE-----
MIIGWTCBKMgAwIBAgIIWcVMpfXu9YkwdQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTFIFNBICHWQVRCSR0wNDA4NDI1NjI2KTEMMAAOG
A1UEBRMDMDAxMSExWYDVQQDDbHARVRfUyBUU1AgQ0EGRk9SIFRTQSAwMDEwHhcN
MTkwNzEyMDcyOTM5W5hcnmJwNzEyMDcyOTM5WjBGMQswCQYDVQGEwJCRTEKMCIG
A1UECgwbWkVURVMyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRL
c0NvbmZpZGVucyBSU0EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIBGCKCAQEAqlHEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/Kjknf
WbbCYM1+WppB1e+BxhP9oZGDx3mXjvxQu8jEI7AQosVH2rbQpnpvY29puaHoR++O
dMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRdTwNCFHxL29rEPSzIqXff+SWS9
3Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6TPCoTTqJOJ7iDbbns
oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyI
KwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3Nw
LnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYI
KwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bk
cy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYC
AQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVz
LmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++OdMn3iSD/aYQrKXEnIzQKkC/JY3YIhzVrtG7qRd
TwNCFHxL29rEPSzIqXff+SWS93Bh1IFyOY6rk+0vQOGnci+UqltMOM+ZqbW7dkIFPdAIVbZ6
TPCoTTqJOJ7iDbbns oUEUJvqbhBDQua3JdNLYoKv3KCa40qbw2bDZt1lul0byxeXZBxsivP7S30R8H0LC
/F03p+CtioZQWT+C3yVnpBRIL6B4o+yobMBbWSeI7QIDAQABo4ICeTCCANUwCAyIKwYBBQUHAQEEDDBiMDkGCCsGAQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRLcy5j
b20wWkVURVNUU1BUU0FDQTAwMS5jcncWJQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXRLcy5jb20wHQYDVRO0BBYEFf4Z0dsjE+pGp/wc/scElxiaywRJMAG
A1UdEwEB/wQCMAAwHwYDVR0jBBGwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAGBGBGQAjkyBATArBgYEA15GAQUwITafFh1odHRwcZovL3Bkcy50c3AuemV0ZXMuY29tEwJlbjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsGAQUFBwIBFiBodHRwcZovL3JlCG9zaXRvcnkudHNwLnpldGVzLmNvbTBjCBsgYIKwYBBQUHAgiwgaUegaIAWgBFAFQARQBTACAABABTAFAAIAABRAHUA
YQBsAGkAZgBpAGUAZAAGAGMAZQBIAHQAAQBMAGkAYwBhAHQAZQAgAGYAbwByACAA
dABpAG0AZQATAHMAABhAG0ACABpAG4AZwAgAGMAbwBtAHAABABpAGeAbgB0ACAA
dwBpAHQAaaAAGAEUAVABTAekAIABUAFMAIAAzaDEAOQAQADQAMgAxAAC4wPgYDVROf
BDcWNTAzODGg14YtaHR0cDovL2Nybc50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNb
Q0EwMDEuY3J0LnRzcC56ZXRLcy5jBGMQswCQYDVQGEwJCRTEKMCIGA1UECgwbWkVURV
MyU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSswKQYDVQDDCJaZXRRLc0NvbmZpZGVucyBSU0
EgUXVhbG1maWVkJFRVTVEwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIBGCKCAQEAql
HEONdGMMdmj/NNytUB0JnT4Sb2jqtTgJ0h7/KjknfWbbCYM1+WppB1e+BxhP9oZGDx3mXj
vxQu8jEI7AQosVH2rbQpnpvY29puaHoR++
```

## 8.2.11 ZetesConfidens EC Qualified TSU11

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
02:cf:13:87:c6:2c:85:bc  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001  
Validity  
Not Before: Jul 12 07:31:08 2019 GMT  
Not After : Jul 12 07:31:08 2025 GMT  
Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZetesConfidens EC Qualified TSU11  
Subject Public Key Info:  
Public Key Algorithm: id-ecPublicKey  
Public-Key: (256 bit)  
pub:  
04:f8:8b:9a:93:80:57:63:b7:5c:9f:b2:b0:d6:4d:  
23:80:76:d3:c9:22:78:ad:0b:e5:c7:27:d0:07:50:  
57:35:89:a0:f5:40:f7:ab:e6:7d:4a:11:88:88:fb:  
df:c8:cf:b4:0f:8b:ff:f5:d9:51:10:b4:8b:3c:0b:  
3f:27:bd:99:c2  
ASN1 OID: prime256v1  
NIST CURVE: P-256  
X509v3 extensions:  
Authority Information Access:  
CA Issuers - URI: <http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt>  
OCSP - URI: <http://ocsp.tsp.zetes.com>  
  
X509v3 Subject Key Identifier:  
E7:8F:26:86:6E:36:1D:B0:FB:51:20:12:FF:AE:7C:9D:58:17:25:15  
X509v3 Basic Constraints: critical  
CA:FALSE  
X509v3 Authority Key Identifier:  
keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45  
  
qcStatements:  
070.....F..0+.....F..0!0...https://pds.tsp.zetes.com..en  
X509v3 Certificate Policies:  
Policy: 1.3.6.1.4.1.47718.2.1.2.50  
CPS: <https://repository.tsp.zetes.com>  
User Notice:  
Explicit Text:  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI: <http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl>  
  
X509v3 Key Usage: critical  
Digital Signature  
X509v3 Extended Key Usage: critical  
Time Stamping  
Signature Algorithm: sha256WithRSAEncryption  
69:d1:e1:1a:4e:2b:9a:88:1c:69:59:e1:9d:ff:45:e1:46:e3:  
ce:8c:3d:a5:2e:30:eb:bb:12:fa:e4:e9:76:2e:d2:22:09:aa:  
73:bd:f1:92:7a:d0:59:41:76:b6:b4:49:7f:4d:32:29:87:01:  
59:75:ec:2e:da:59:fd:3e:46:a3:21:60:30:77:85:08:23:47:  
2b:2a:d7:f9:14:89:ce:ca:96:41:84:d7:19:0a:c4:5d:a0:a5:  
d3:82:cf:68:40:34:65:fc:03:83:37:e9:aa:b6:ba:58:ac:a2:  
7f:f9:93:f0:ba:02:d2:f9:3a:28:3f:1f:96:35:41:b6:ce:e3:  
25:f6:0c:6d:17:7c:0f:b1:34:c1:a8:d6:6d:ae:e1:07:1e:76:  
a2:31:4c:fd:55:a4:81:c7:77:74:ea:39:8f:0d:38:02:af:d5:  
a7:36:91:75:49:64:c2:ef:b1:4e:2c:d8:20:b2:7c:4e:62:61:  
ad:b7:5f:8b:41:8b:c2:f9:64:5f:97:ac:ec:57:bd:e4:a9:8f:  
45:15:58:39:a8:cd:12:55:2a:34:e0:60:bc:ec:2c:7c:21:d9:  
9e:4c:ce:ff:60:e3:43:c2:bd:e8:aa:15:a6:4c:1c:5c:9a:8e:  
18:11:d5:de:fd:b0:e6:51:65:20:cc:ef:30:f3:74:2d:d0:35:  
d0:aa:e3:1f:96:f6:b5:d6:dc:52:8b:a0:85:38:36:5c:88:1f:  
99:d6:46:c4:93:b0:f5:e8:10:53:ea:ec:44:7c:f6:0f:79:41:  
73:3d:26:2a:33:7e:88:fa:35:08:7c:c6:93:60:1e:22:69:e1:  
1d:d6:8b:35:6a:03:ef:c7:9a:53:34:7d:1f:f0:19:1c:11:13:  
7e:e1:78:47:b8:dc:f2:da:a1:0b:3d:a7:b0:27:86:60:05:1c:  
fc:a8:ec:a5:77:5e:1f:33:a1:4b:4f:68:e3:cd:56:92:fd:2e:  
47:85:e8:02:7d:f5:e2:f8:eb:36:11:80:21:d0:d1:8b:9e:37:  
e1:0d:31:59:dc:b4:7a:d8:39:07:73:00:24:34:b7:5d:67:0b:  
ba:c8:65:cb:1d:c1:f9:3e:e9:b6:b7:2b:a1:f6:d9:41:28:23:  
b7:03:e9:2d:7b:be:8d:00:aa:51:82:28:5d:60:cd:78:0d:51:  
e7:fa:4e:01:63:96:6c:0f:21:04:56:27:e8:a0:e9:9b:62:b6:  
1e:78:12:70:a2:08:eb:12:0c:3b:a4:38:f7:eb:99:3b:e4:84:  
1e:80:57:a9:06:01:d1:15:20:5c:f2:b8:71:cf:d2:db:56:4a:  
26:ea:cf:3e:b0:d4:ad:a2:f3:83:08:b7:01:6e:b1:41:bf:f6:  
97:8b:5e:ba:63:5d:d2:23

-----BEGIN CERTIFICATE-----  
MIIF9TCCA92gAwIBAgIIAs8Th8YshbwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE  
BhMCQkUxJDAiBgNVBAoMG1pFVEVETIFNBICWQVRCSR0wNDA4NDI1NjI2KTEMMMAoG  
A1UEBRMDMxMSEwHwYDVQDDbHVRVUFyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN  
MTkwNzEyMDczMTA4WncNMjUwNzEyMDczMTA4WjBfMQswCQYDVQGEwJCRTEkMCIG  
A1UECgbWkVURVWU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSowKAYDVQDDCFaZXR1  
c0NvbWZpZGVucyBFQyBRdWFSaWZpZWQgVENVMTEwWTATBgqhkhjOPQIBBggqhkhjO  
PQMBBwNCAAT4i5qTgFdtlyfsrDWTSoAdtPJInitC+XHJ9AHUFC1iaD1QPer5n1K  
EYiI+9/Iz7QPi//12VEQtIs8Cz8nvZnCo4ICeTCCAnUwcAYIKwYBBQUHAQEEDBi  
MDkGCCsGAQUFBzAChilodHRwOi8vY3J0LnRzcC56ZXR1cy5jb20vWkVURVNUU1BU  
U0FDQTAwMS5jcnQYIKwYBBQUHMAGGWh0dHA6Ly9vY3NwLnRzcC56ZXR1cy5j  
b20wHQYDVVR0OBBYEFOePJoZuNh2w+1EgEv+ufJlYFYUVMawGAlUdEwEB/wQCMAAw  
HwYDVR0jBBgwFoAULVFLSduELbBNK+gFOFOp5b4ft0UwRQYIKwYBBQUHAQMEOTA3  
MAGGBgQAJkYBATArBgYEAISGAQUwITAfPhlodHRwcovL3Bkcy50c3AuemV0ZXMu  
Y29tEwJlbnjCCAQIGA1UdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsG  
AQUFBwIBFiBodHRwcovL3JlcG9zaXRvcnkudHNwLnpldGVzLmNvbTCBsgYIKwYB  
BQUHAgiWgaUegaIAWgBFARQBTACAABABTAFAAIABRAHUAYQBsAGkaZgBpAGUA  
ZAAgAGMAZQBByAHQAaQBMAGkAYwBhAHQAQAgAGYAbwByACAAdABpAG0AZQAtAHMA  
dABhAG0AcABpAG4AZwAgAGMAbwbTAHAABABpAGeAbgB0ACAAdwBpAHQAaAAgAEUA  
VABTAekAIABUAFMAIAAzADEAQAgADQAMgAxAC4wPgYDVVR0fBDCwNTAzoDGG14Yt  
aHR0cDovL2NybcC50c3AuemV0ZXMuY29tLlplFVEVTVFNQVFNBOEwMDEuY3JsMA4G  
A1UdDwEB/wQEAWIHgDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDANBgkqhkiG9w0B  
AQsFAAOCAgEAAAdHhGk4rmogcaVnhnf9F4Ubjzow9pS4w67sS+uTpd17SIgmqc73x  
knrQWUF2trRJf00yKYcBWXSLtpZ/T5GoyFgMHeFCCNHKyrX+RSJzsqWQYTXGQrE  
XaCl04LPaEA0ZfwDgzfpqra6WKyif/mT8LoC0vk6KD8fljVBts7jJfYMBrd8D7E0  
wajWba7hBx52ojFM/VWkgcd3d0o5jw04Aq/VpzaRdUlkWu+xTizYILJ8TmJhrbdf  
i0GLwv1kX5es7Fe95KmPRRVY0ajNElUgNOBgvOwsfCHZnkzO/2DjQ8K96KoVpkwc  
XJqOGBHV3v2w5lF1IMzvMPN0LdA10KrjH5b2tdbcUoughTg2XIgfmdZGxJOW9egQ  
U+rsRH2D3lBcz0mKjN+iPolCHzGk2AeImnhHdaLNWod78eaUzR9H/AZHBETfuF4  
R7jc8tqhC2nsCeGYAUc/KjspXdeHzOhS09o48lWkv0uR4XoAn3l4vjrnHGAIdDR  
i5434Q0xWdy0etg5B3MAJDS3XWcLushlyx3B+T7ptcrofbZQSgjtWpPLXu+jQCq  
UYIoXWDNeAlR5/pOAWOWbA8hBFYn6KDpm2K2HngScKII6xIMO6Q49+uZO+SEHoBX  
qQYB0RUgXPk4cc/S2lZKJurPPrDuraLzgwI3AW6xQb/2l4teumNd0iM=  
-----END CERTIFICATE-----

## 8.2.12 ZetesConfidens EC Qualified TSU12

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
5a:c7:28:39:ec:de:ae:05  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001  
Validity  
Not Before: Jul 12 07:32:42 2019 GMT  
Not After : Jul 12 07:32:42 2025 GMT  
Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZetesConfidens EC Qualified TSU12  
Subject Public Key Info:  
Public Key Algorithm: id-ecPublicKey  
Public-Key: (256 bit)  
pub:  
04:c8:66:d3:00:58:1d:b6:51:22:3f:f8:9a:0d:8b:  
44:87:e2:2d:e6:a1:e8:b2:5b:82:b3:97:ff:36:c1:  
fd:35:b6:7f:dd:24:88:52:ab:5f:1b:b8:01:c2:92:  
13:6e:b9:47:af:94:ea:83:14:96:6a:9b:81:94:47:  
4d:8a:ed:09:4c  
ASN1 OID: prime256v1  
NIST CURVE: P-256  
X509v3 extensions:  
Authority Information Access:  
CA Issuers - URI: <http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt>  
OCSP - URI: <http://ocsp.tsp.zetes.com>  
  
X509v3 Subject Key Identifier:  
60:5F:58:F1:B0:03:3E:D5:CC:8E:5B:45:69:C6:54:A8:88:03:52:D2  
X509v3 Basic Constraints: critical  
CA:FALSE  
X509v3 Authority Key Identifier:  
keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45  
  
qcStatements:  
070.....F..0+.....F..0!0...https://pds.tsp.zetes.com..en  
X509v3 Certificate Policies:  
Policy: 1.3.6.1.4.1.47718.2.1.2.50  
CPS: <https://repository.tsp.zetes.com>  
User Notice:  
Explicit Text:  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI: <http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl>  
  
X509v3 Key Usage: critical  
Digital Signature  
X509v3 Extended Key Usage: critical  
Time Stamping  
Signature Algorithm: sha256WithRSAEncryption  
0d:8e:fd:44:c7:88:46:30:7e:30:e9:fb:d6:a7:72:8e:5d:55:  
1d:b0:de:b5:c7:b9:f1:61:26:ca:a1:51:0c:30:fd:07:40:91:  
ab:f7:7c:82:01:d5:d5:ed:44:57:27:96:76:74:58:f6:63:43:  
76:27:bc:ac:2a:14:b4:6d:08:a8:f4:26:fa:24:fb:95:4e:64:  
b0:07:85:67:3d:0a:ba:bd:c9:34:a6:95:b7:25:8a:b7:95:25:  
63:7e:94:49:59:88:3e:2f:9e:e5:b7:e6:fb:7f:08:4f:d3:2c:  
f8:9c:f7:d2:3d:c9:1e:b6:47:68:56:f8:aa:d6:b2:1d:25:e4:  
51:b0:ed:ce:94:ea:e0:e0:8f:e2:dd:9e:f3:8f:43:d6:5d:19:  
b2:6e:c4:0e:1e:e5:82:33:42:f7:24:1a:59:7f:2a:5e:a9:0f:  
40:2f:a4:84:44:bd:a5:ba:54:4b:ee:1e:3f:a1:8a:94:51:5a:  
d4:5a:f1:e2:bb:33:36:81:10:b3:cb:b2:b7:cc:69:b8:73:43:  
2d:b0:f8:81:26:45:fc:d2:a2:9e:71:d7:ca:18:6a:e2:b0:f4:  
f7:35:c5:1d:48:2c:27:da:fb:9e:8b:e0:a2:49:a2:ae:a6:c2:  
2b:85:42:49:36:6a:e9:54:80:e4:57:27:0c:08:65:81:e1:12:  
56:43:21:0b:53:88:41:f0:de:c3:7b:52:a3:ce:28:bd:2f:6d:  
3e:a9:8b:f8:6a:70:7c:85:40:4b:38:f8:da:cd:22:fb:d0:32:  
f5:85:0a:30:75:28:2f:ea:a1:47:03:7d:7d:ce:65:09:17:28:  
48:5f:a7:39:19:2e:26:c0:6c:7a:04:45:af:19:2e:c7:e0:53:  
12:99:f2:f3:6d:96:92:62:b6:7a:5d:f2:3a:bf:2e:b4:0a:02:  
19:79:c5:7a:75:55:0d:cb:6e:5a:30:b3:a8:f5:83:df:65:17:  
66:dc:48:6d:96:b2:c4:d0:e4:78:b3:f4:51:c6:4c:08:a9:22:  
ef:b1:7a:0a:9a:15:db:3b:40:b4:51:bd:2d:93:c8:23:40:79:  
19:a9:be:8d:3d:79:e8:a6:fc:d0:ed:84:c4:94:c3:01:bf:0d:  
db:3a:aa:b4:40:cb:c9:f5:b1:79:97:25:ae:95:15:85:38:3c:  
17:b0:df:bb:53:41:5d:8c:0c:fe:9d:df:55:65:f5:3d:e3:2d:  
97:be:a2:94:9f:72:41:38:5c:3e:62:9a:22:0f:c0:41:fb:b9:  
18:11:2f:c9:20:ab:54:31:91:1a:f9:cf:8e:4a:dd:7d:a3:4a:  
fd:d2:f7:00:ab:eb:81:0e:ad:ad:5d:79:3f:af:cd:93:ef:07:  
5e:c7:8a:e9:d2:c5:cb:58

-----BEGIN CERTIFICATE-----  
MIIF9TCCA92gAwIBAgIIWscOeZergUwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE  
BhMCQkUxJDAiBgNVBAoMG1pFVEVtIFNBIChtWQVRCSR0wNDA4NDI1NjI2KTEMAAOG  
A1UEBRMDMxMSEwHwYDVQDDbHVRVUFyBUU1AgQ0EgRk9SIFFRTQSAwMDEwHhcN  
MTkwNzEyMDczMjQyWncNMjUwNzEyMDczMjQyWjBfMQswCQYDVQGEwJCRTEkMCIG  
A1UECgwBwKwURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSowKAYDVQDDCFaZXRl  
c0NvbWZpZGVucyBFQyBRdWFSaWZpZWQgVFNVMtIwWTATBgqhkhjOPQIBBggqhkhjO  
PQMBBwNCAATIZtMAWB22USI/+JoNi0SH4i3moeiyW4Kz1/82wf01tn/dJiHsq18b  
uAHCKhNuuUev1OqDFJZqm4GUR02K7Q1Mo4ICeTCCAnUwAYIKwYBBQUHAQEEDBi  
MDkGCCsGAQUFBzAChilodHRwOi8vY3J0LnRzcC56ZXR1cy5jb20vWkVURVNUU1BU  
U0FDQTAwMS5jcnQYIKwYBBQUHMAAGGWh0dHA6Ly9vY3NwLnRzcC56ZXR1cy5j  
b20wHQYDVDR0OBByEFGbFWPGwAz7VzI5bRWNvGKkiIAlLSMAwGAlUdEwEB/wQCMAAw  
HwYDVR0jBBgwFoAULVFLSduELbBNK+gFOFOP5b4ft0UwRQYIKwYBBQUHAQMEOTA3  
MAGGBGQAJkYBATArBgYEAISGAQUwITAfFh1odHRwcovL3Bkcy50c3AuemV0ZXMu  
Y29tEwJlBjCCAQIGAlUdIASB+jCB9zCB9AYMKwYBBAGC9GYCAQIyMIHjMCwGCCsG  
AQUFBwIBF1BodHRwcovL3JlcG9zaXRvcnkudHNwLnpldGVzLmNvbTCBsgYIKwYB  
BQUHAhIwgaUegaIAWgBFAFQARBTACAABVABTAFAAIABRAHUAYQBSAGkAZgBpAGUA  
ZAAgAGMAZQBByAHQAaQBMAGkAYwBhAHQAQAGAGYAbwByACAAdABpAG0AZQAtAHMA  
dABhAG0AcABpAG4AZwAGAGMAbWBTAAHAAABAPAGEAbgB0ACAAdwBpAHQAaAAgAEUA  
VABTAekAIABUAFMAIAAZADEAQAGADQAMgAxAC4wPgYDVDR0fBDCwNTAzoDGG14Yt  
aHR0cDovL2NybcC50c3AuemV0ZXMuY29tLlplFVEVtVFNQVFNBOEwMDEuY3JsMA4G  
A1UdDwEB/wQEAWIHgDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDANBgkqhkiG9w0B  
AQsFAAOCAgEADY79RMeIRjB+Mon71qdyj11VHbDetce58WEmyqFRDD9B0CRq/d8  
ggHV1e1EVYeWdnRY9mNDdie8rCoUtG0IqPQm+iT7lU5ksAeFZz0Kur3JNKAvtYWK  
t5Uly36USVmPi+e5bfm+38IT9Ms+Jz30j3JHrZHaFb4qtayHSXkUBDtztTq40CP  
4t2e849D110Zsm7EDh71gJNC9yQaWX8qXqkPQC+khES9pbpUS+4eP6GK1FFa1FrX  
4rszNoEQs8uyt8xpuHNDLbD4gSZF/NKinnHXyhhq4rD09zXFHUGsJ9r7novgokmi  
rqBCK4VCSTZq6VSA5FcdAhlgeESVkhMhC1OIQfDew3tSo84ovS9tPqML+GpwfIVA  
Szj42s0i+9Ay9YUKMHUoL+qhRwN9fc51CRcoSF+nORkuJsBsegFrXkux+BTEpny  
822WkmK2el3yOr8utAoCGXnFenVVDctuWjCzqPWD32UXZtxIbZayxNDkeLP0UcZM  
CKki77F6Cpov2ztAtFG9LZPII0B5Gam+jT156Kb8002ExJTDAb8N2zqqEDLyfWx  
eZclrPUVhTg8F7DfulNBXYwM/p3fVWX1PeMt176ilJ9yQThcPmKaIg/AQfu5GBEv  
ySVCVDGRGvnpJkrdfANK/dL3AKvrgQ6trV15P6/Nk+8HXsek6dLFy1g=  
-----END CERTIFICATE-----

### 8.2.13 ZetesConfidens RSA TSU13

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
46:97:be:e8:42:72:7f:b0  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001  
Validity  
Not Before: Jul 12 07:35:44 2019 GMT  
Not After : Jul 12 07:35:44 2022 GMT  
Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZetesConfidens RSA TSU13  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public-Key: (2048 bit)  
Modulus:  
00:b8:0b:f0:66:18:84:46:4c:20:fb:50:72:fc:05:  
ad:7c:ec:45:8f:a0:69:80:7b:d8:8a:c7:49:76:7d:  
86:75:d9:15:26:42:b2:6b:cb:2e:f6:c0:d8:34:d0:  
d0:12:fc:7b:6c:33:24:73:4e:6d:b6:f9:61:a9:96:  
39:d0:e9:2c:fd:a8:8b:7a:cd:99:be:24:a0:a7:ff:  
8d:1d:7f:ba:2f:3e:0b:ad:2f:29:26:94:7b:ac:a0:  
7f:13:01:18:66:42:19:8c:81:52:82:2c:15:11:21:  
01:07:c7:7b:35:bb:41:75:6c:a7:c3:8a:96:cb:cc:  
cf:8f:23:f9:0d:a2:f0:be:ab:74:65:16:67:24:81:  
22:d0:13:72:73:1e:c7:8f:de:33:7e:6c:b0:3d:6d:  
43:b1:95:f3:96:fb:e8:b0:35:0f:7b:23:f5:49:59:  
19:43:31:71:07:ce:7a:d2:7b:6e:ac:53:9e:e5:21:  
ff:fb:f8:bf:6d:45:b3:2d:aa:aa:2d:88:7f:56:1b:  
65:ab:66:99:b5:3c:b6:2e:43:58:85:e0:e1:2a:0c:  
7f:21:b8:36:29:4b:45:66:48:55:de:be:5a:61:f5:  
c4:9f:48:41:16:8d:72:e1:53:59:9e:45:26:bb:f1:  
04:87:10:d0:43:5e:62:04:0b:16:26:15:2a:44:fc:  
61:0b  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
Authority Information Access:  
CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt  
OCSP - URI:http://ocsp.tsp.zetes.com  
  
X509v3 Subject Key Identifier:  
EE:F5:85:41:C0:73:94:17:13:95:8F:8D:5E:C7:62:A1:C1:15:63:78  
X509v3 Basic Constraints: critical  
CA:FALSE  
X509v3 Authority Key Identifier:  
keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45  
  
X509v3 Certificate Policies:  
Policy: 1.3.6.1.4.1.47718.2.1.2.50  
CPS: https://repository.tsp.zetes.com  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl  
  
X509v3 Key Usage: critical  
Digital Signature  
X509v3 Extended Key Usage: critical  
Time Stamping  
Signature Algorithm: sha256WithRSAEncryption  
48:c1:31:f4:aa:f9:c9:4b:34:73:dd:c3:59:b0:31:84:21:8d:  
8d:ed:f5:b2:fa:10:97:00:e8:f3:c4:0d:ad:80:54:20:32:a4:  
2a:76:f9:b8:b5:f7:73:28:0e:4b:1f:0f:a5:87:42:ca:0b:98:  
aa:3a:2c:d5:81:6e:f6:5d:6e:59:f1:f3:9f:19:43:d8:22:76:  
12:e1:33:36:c7:04:ac:36:6c:87:ec:ef:14:09:87:48:bc:b8:  
47:9d:89:4b:4d:e7:20:39:f5:3a:47:59:a2:9e:1e:d2:07:56:  
a5:69:d7:17:72:69:3f:92:8b:06:04:d4:06:90:46:b3:b0:83:  
79:15:0b:07:c0:75:ea:bb:8c:e6:cf:a9:ff:a6:b8:1b:el:4f:  
fc:c5:59:40:0d:aa:ff:b2:e6:14:d8:d4:da:9a:c6:f3:93:2d:  
f1:d2:d5:c2:71:35:71:db:33:5f:82:77:d6:bf:6b:03:d4:f1:  
30:4c:9e:7a:69:1e:08:90:58:9c:f7:6f:a4:04:18:84:90:81:  
8a:3f:d9:85:ab:05:75:93:b7:b9:85:50:82:61:c3:a3:b3:33:  
c7:bb:7c:a9:b7:7a:ec:b2:c2:6a:06:cb:3f:a3:03:5e:8f:07:  
75:70:d8:67:29:0b:e0:93:b7:f1:e7:67:a4:27:2c:eb:42:63:  
19:c4:e6:ee:1f:c6:ad:61:e3:5d:7b:2e:0f:fc:47:ba:2a:c8:  
93:99:aa:f3:28:fa:52:ee:4c:ec:07:78:52:7f:36:83:eb:6c:  
3a:b9:c6:e0:02:22:45:a8:da:23:ff:57:86:68:47:b7:82:68:  
0b:12:81:bb:75:5e:f8:2a:b1:f0:c1:53:b4:5e:19:f9:cf:73:  
66:d0:ed:c2:48:2e:51:14:9b:f2:54:5c:09:37:3c:1a:c4:6e:  
c1:5e:78:dd:7c:fa:e0:2f:a8:45:cf:cc:c7:45:5b:28:el:71:  
8d:81:40:b4:3f:0b:40:af:69:d1:45:4c:41:f1:64:eb:54:c7:





## 8.2.14 ZetesConfidens RSA TSU14

Certificate:  
Data:  
Version: 3 (0x2)  
Serial Number:  
69:d8:11:e7:e1:a2:b5:1b  
Signature Algorithm: sha256WithRSAEncryption  
Issuer: C = BE, O = ZETES SA (VATBE-0408425626), serialNumber = 001, CN = ZETES TSP CA FOR TSA 001  
Validity  
Not Before: Jul 12 07:37:05 2019 GMT  
Not After : Jul 12 07:37:05 2022 GMT  
Subject: C = BE, O = ZETES SA (VATBE-0408425626), CN = ZetesConfidens RSA TSU14  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
RSA Public-Key: (2048 bit)  
Modulus:  
00:e6:be:44:d2:ec:b0:95:4a:ac:24:c6:65:b3:74:  
58:7b:4e:ef:a4:a3:39:88:92:e2:c7:96:c1:38:0c:  
93:e7:a1:28:69:c5:6b:cc:52:be:67:97:b2:30:23:  
5e:df:51:e2:3b:34:94:d3:42:00:a2:9a:dd:37:ec:  
31:fd:7e:54:85:f3:b5:da:20:65:e7:5c:03:12:f6:  
ac:58:18:fe:b9:70:47:de:d1:b5:83:42:7c:ae:69:  
60:33:de:14:d5:92:c1:83:ce:f7:67:d6:dc:3d:8c:  
79:a0:fc:f4:fc:d4:6e:91:97:76:28:6a:d3:79:d5:  
9b:75:38:98:33:fb:87:97:fe:d8:9c:7b:6e:b3:48:  
7e:5d:7a:96:24:6a:04:ff:27:bd:aa:43:9e:81:f0:  
86:43:dc:75:0c:9e:6c:39:05:8d:0b:df:4f:f9:0d:  
5e:d4:35:c4:63:b6:c2:a4:29:dc:1f:15:e5:a3:0d:  
6f:89:29:6e:91:0b:15:78:11:d0:74:cf:d4:78:58:  
12:3a:76:02:7d:e8:72:4e:af:00:a3:b4:df:b1:e8:  
75:d0:41:b6:b7:7d:9f:ec:d5:66:63:9b:29:c5:41:  
8c:8f:32:1c:cf:07:51:1f:f4:a3:1f:87:ef:5f:ca:  
58:27:cc:30:77:31:d0:10:87:88:21:ea:9f:ef:56:  
e5:83  
Exponent: 65537 (0x10001)  
X509v3 extensions:  
Authority Information Access:  
CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt  
OCSP - URI:http://ocsp.tsp.zetes.com  
  
X509v3 Subject Key Identifier:  
90:D6:65:9F:E2:3B:02:E4:4B:C2:5B:98:2E:9E:47:56:0D:60:14:37  
X509v3 Basic Constraints: critical  
CA:FALSE  
X509v3 Authority Key Identifier:  
keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45  
  
X509v3 Certificate Policies:  
Policy: 1.3.6.1.4.1.47718.2.1.2.50  
CPS: https://repository.tsp.zetes.com  
  
X509v3 CRL Distribution Points:  
  
Full Name:  
URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl  
  
X509v3 Key Usage: critical  
Digital Signature  
X509v3 Extended Key Usage: critical  
Time Stamping  
Signature Algorithm: sha256WithRSAEncryption  
13:aa:14:98:71:d5:51:ae:f9:c6:b8:52:eb:5a:96:1d:01:ba:  
71:0b:05:5c:91:ac:25:ff:37:13:93:01:25:a9:c2:8f:29:33:  
bf:95:07:a9:fc:a0:74:a7:e9:1f:9e:cc:9f:68:7f:9b:ab:95:  
ea:8b:15:75:b2:5c:a5:7d:5f:9a:46:57:c9:e4:f6:f9:36:e3:  
66:3a:05:d0:6c:10:8e:ce:e1:f6:31:91:e3:13:2f:2f:d9:11:  
74:e2:9d:4e:68:7c:7b:af:d4:fe:ed:53:2e:86:ad:ee:a4:a2:  
85:d7:a6:ba:91:cd:bb:3b:fe:6a:ff:02:02:b8:84:e3:3f:89:  
49:4a:07:08:4f:06:78:e3:cc:85:b4:cb:ae:33:0c:b4:b5:65:  
07:2a:71:f6:91:b5:8a:d0:53:b6:3b:55:67:00:f5:e0:4f:d7:  
29:52:be:53:dc:f0:f5:c1:69:4d:fd:08:4b:1f:e5:1b:e9:77:  
04:af:e1:13:c0:84:2e:47:d0:4e:e4:be:2d:13:fd:96:84:72:  
18:ef:df:2d:0d:e9:85:d6:50:dd:14:b5:cf:39:ff:d9:1a:0e:  
bd:c2:3c:49:13:6d:13:60:1c:30:3d:4c:4e:11:f4:ca:c8:8a:  
76:62:f0:cd:5f:bf:de:74:af:ed:cd:fa:af:cc:ea:0c:17:dc:  
01:a0:3d:a4:85:7f:de:72:1b:90:21:4f:de:69:c4:31:ad:cb:  
2d:57:b4:19:88:7a:6c:9f:5d:c9:22:85:79:63:9b:ed:93:bf:  
bd:31:84:75:0e:63:16:a4:4c:88:72:71:47:29:f4:05:0b:08:  
7f:0c:c4:3b:20:a3:1b:de:4a:4d:5b:2c:64:93:73:f8:1f:60:  
1a:0a:0e:c1:f1:37:80:39:13:38:62:8f:b6:64:f1:e4:8c:e1:  
34:5e:ec:4d:66:ab:ab:dc:d0:1e:7b:ff:6a:7c:31:22:e5:59:  
8a:5c:6b:74:3f:fe:c2:f0:3e:a3:28:84:5d:0b:1d:69:b1:00:

```
5d:35:28:4c:50:9c:b7:44:0d:53:58:9a:5f:73:07:50:f9:67:
be:98:76:31:5a:3b:a1:74:2e:a0:24:b5:fb:c2:35:25:b1:8a:
cd:de:82:f7:12:4f:ab:52:98:58:32:6c:1f:c1:ef:aa:8f:91:
09:ce:ee:82:32:fd:8f:49:ed:73:41:64:11:49:58:aa:9f:db:
cb:5b:d4:fa:51:57:34:10:9f:b4:30:1a:be:af:3c:1f:c8:47:
d3:8b:30:e3:2e:ec:8d:a8:5e:e7:26:f5:88:4b:35:e8:b7:43:
cc:fa:f0:f3:26:9b:8a:b1:10:30:6e:a7:bd:ed:d4:b3:bb:5e:
ad:0f:f2:7d:f5:f7:b6:90
-----BEGIN CERTIFICATE-----
MIIFtTCCA52gAwIBAgIIadgR5+GitrswDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVtIFNBIChtWQVRCSR0wNDA4NDI1NjI2KTEMMMAoG
A1UEBRMDMDAxMSEwHwYDVQDDbHARVRVUyBUU1AgQ0EgRk9SIFRtQSAwMDEwHhcN
MTkwNzEyMDczNzA1WhcNMjIwNzEyMDczNzA1WjBWMQswCQYDVQGEwJCRTEkMCIG
A1UECgwbWkVURVVGU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSEwHwYDVQDDbHARVRVUy
c0NvbWZpZGVucyB3U0EgVFNVMtQwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQMvKTS7LCVSqwkxmWzdFh7Tu+kozmIkuLHlsE4DJpNoShpxWwMUR5n17Iw
I17fUeI7NJTtQgCimt037DH9f1SF87XaIGXnXAMS9qxYGP65cEfe0bWQDnyuaWAz
3hTVksGDzvdn1tw9jHmg/PT81G6R13YoatN51Zt10Jgz+4eX/tice26zSH5depYk
agT/J72qQ56B8IzD3HUMnmw5BY0L30/5DV7UNCRjtsKkKdwfFeWjDw+JKW6RCxV4
EdB0z9R4WBI6dgJ96HJOrwCjtn+x6HXQQba3fZ/s1WZjmynFQYyPMhzPB1Ef9KMf
h+9fy1gnzDB3MdaQh4gh6p/vVuWDAgMBAAGjggF3MIIbCzBwBggrBgEFBQcBAQRk
MGIIwOQYIKwYBBQUHMAKGLWh0dHA6Ly9jcncudHNwLnpldGVzLmNvb39aRVRFU1RT
UFRtQUNBMDAxLmNydDA1BggrBgEFBQcwAYYZaHR0cDovL29jc3AudHNwLnpldGVz
LmNvbTAuBgNVHQ4EFgQUkNZLn+I7AuRLwluYLP5HVglgFDcWDAYDVR0TAQH/BAIw
ADAfBgNVHSMEGDAwBgQcUUtJ24QtsE0r6AU4U6n1vh+3RTBJBgNVHSAEQjBAMD4G
DCsGAQQBgvrRmAgECmJAuMCwGCCsGAQUFBwIBFiBodHRwczovL3JlcG9zaXRvcnkud
HNwLnpldGVzLmNvbTAuBgNVHR8ENzA1MD0gMaAvhilodHRwOi8vY3JsLnRzcC56
ZXR1cy5jb20vWkVURVNUU1BUU0FDQTAwMS5jcmmwDgYDVR0PAQH/BAQDAgeAMBYG
A1UdJQEBe/wQMMMAoGCCsGAQUFBwMIMA0GCSqGSIb3DQEBCUAA4ICAQATqhsYcdVR
rvnGuFlrWpYdAbpxCwVckawl/zcTkWE1qcKPKTO/lQep/KB0p+kfnisyfaH+bq5Xq
ixV1sl1fV+aR1fJ5Pb5NuNmOgXQbBCOzuH2MZHjEy8v2RF04p1OaHx7r9T+7VMu
hq3upKKF16a6kc270/5q/wICuITjP41JSgcITwZ448yFtMuuMwy0tWUHKH2kbWK
0FO201VnAPXgT9cpUr5T3PD1wW1N/QhLH+Ub6XcEr+ETwIQuR9B05L4tE/2WhHIY
798tDemF11DdFLXPOf/ZGg69wjxJE20TYBwwPUxOEfTKyIp2YvDNX7/edK/tzfqv
zOoMF9wBoD2khX/echuQIU/eacQxrcstV7QZiHpsn13JIoV5Y5vtk7+9MYR1DmMW
pEyIcnFHKfQFCwh/DMQ7IKMb3kpNWyxkk3P4H2AaCg7B8TeAORM4Yo+2ZPHkjOE0
XuxNZqur3NAee/9qfDEi5VmKXGt0P/7C8D6jKIRdCx1psQbDnShMUJy3RA1TWJpf
cWdQ+We+mHYxWjUhdC6gJLX7wJUlSyrN3oL3Ek+rUphYmMwFwe+qj5EJzu6CMv2P
SelzQWQRSViqn9vLW9T6UVc0EJ+0MBq+rzwfyeFTizDjLuyNqF7nJvWISzXot0PM
+vDzJpuKsRAwbqe97dSzu16tD/J99fe2kA==
-----END CERTIFICATE-----
```

## 8.2.15 ZetesConfidens EC TSU15

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      2f:f7:15:65:be:21:b5:a0
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: Jan 22 13:33:38 2019 GMT
      Not After : Jan 20 13:33:38 2025 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZetesConfidens EC TSU15
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:9e:75:ce:0a:72:c5:a0:8a:8d:ec:a3:cb:e3:dd:
        04:92:15:91:34:71:5c:d1:81:cc:c5:07:7f:f8:6a:
        df:4b:c7:36:42:ed:d6:6e:03:4c:80:35:c9:88:a3:
        a6:14:25:b6:b2:0c:6c:aa:05:b4:a5:44:18:41:96:
        05:43:52:1b:aa
      ASN1 OID: prime256v1
      NIST CURVE: P-256
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      91:94:DE:D5:24:03:E7:69:DE:A8:22:4B:7F:C4:42:4A:E5:26:79:F6
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
    28:de:aa:06:63:2a:c7:00:a1:77:77:5d:10:47:9b:7a:47:4b:
    79:82:fd:c4:64:1f:5d:2e:4e:c1:13:f5:c2:55:63:df:64:98:
    3b:be:c7:66:b2:8a:e1:f9:88:db:f0:49:5b:c2:29:47:07:18:
    9b:fa:bb:04:33:b0:3b:62:82:f7:b8:78:2b:2e:a6:14:dd:97:
    3b:73:67:7f:44:9d:1f:9d:c4:0a:10:e0:bc:45:11:20:28:82:
    7e:e3:04:99:39:7c:92:8e:93:7a:84:3f:51:ee:a9:37:85:6f:
    ef:dd:06:c1:31:69:88:24:fe:4e:d4:ab:ce:80:db:01:81:9c:
    ae:5d:43:12:de:ed:54:89:d5:86:b5:06:cc:d0:5b:ee:d8:d9:
    57:3e:c8:41:38:f5:70:87:0b:c6:5f:05:12:61:f2:f7:8a:8d:
    01:75:54:b3:3e:8f:1a:13:40:4c:1e:8b:02:f6:cd:49:8f:46:
    e3:69:4c:e8:4d:b2:5e:42:35:1e:9e:c9:60:6b:33:ee:2a:9a:
    76:82:42:d8:35:47:c6:cf:30:bd:53:de:ce:35:50:a5:d6:a3:
    94:77:59:c0:3c:e0:86:f0:53:17:26:25:12:a1:ad:d8:58:63:
    76:1e:b8:b3:18:ea:eb:01:c5:ad:8a:2b:3c:51:41:ff:a4:eb:
    02:1d:37:9a:58:f3:3f:40:49:63:76:02:0a:d7:1a:de:1b:55:
    3e:3c:32:26:40:ab:0c:73:3f:ae:c8:bd:45:ba:08:e8:ac:2e:
    7e:14:5b:3c:55:5d:89:6d:02:be:11:fc:36:b3:72:f5:c5:30:
    7f:46:13:6d:31:53:a9:13:f4:97:47:97:ea:21:be:6f:ed:94:
    f4:17:5c:e8:e0:cc:05:07:57:ee:42:8f:f4:cc:12:d8:cd:2f:
    41:66:dc:6e:dd:eb:90:19:ab:f5:5a:f5:5f:75:23:fe:10:ae:
    dd:7b:d0:bf:28:2c:6e:57:af:64:da:35:4b:a1:70:23:2b:19:
    eb:c2:ec:dd:07:0b:d8:ce:b1:50:53:b8:00:3a:14:5a:26:ac:
    9f:1e:90:d6:25:49:55:4a:93:d7:c8:31:32:c5:31:5c:8e:1e:
    74:84:21:54:d4:b3:8b:ef:88:04:03:d0:90:5f:9b:e8:34:8a:
    da:19:21:9f:d0:b1:06:99:ed:46:f0:43:bc:27:33:e1:45:9c:
    ec:94:9a:31:10:36:88:da:3f:58:07:fe:93:ba:b1:33:0a:0a:
    09:ba:a4:e4:fc:e5:d9:4e:40:18:de:c7:fc:cd:9a:9f:c0:34:
    75:05:4d:91:fe:10:b5:46:6c:a8:5a:42:7e:86:02:db:25:0a:
    ff:b0:de:6c:01:92:7b:7b
  -----BEGIN CERTIFICATE-----
  MIIe6DCCAtCgAwIBAgIIL/cVZb4htaAwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
  BhMCQkUxJDAiBgNVBAoMGlpFVEVTFIFNBICWhQVCRS0wNDA4NDI1NjI2KTEMMMAoG
  A1UEBRMDMDAxMSEwHwYDQDDBBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAAwMDEwHhcN
```

MTkwMTIyMTMzMzM4WhcNMjUwMTIwMTMzMzM4WjBVMQswcQYDVQQGEWJCRTEkMCIG  
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSAwHgYDVQDDbDdaZXRl  
c0NvbWZpZGVucyBFQyBUU1UxNTBZMBMBYqGSM49AgEGCCqGSM49AwEHA0IABJ51  
zgpyxaCKjeYjy+PdBJIVkTRxXNGBzMUHf/hq30vHNkLtlm4DTIAlyYijphQltrIM  
bKoFtKVEGEGWBUNSG6qjggF2MIIBcJBwBggrBgEFBQcBAQRkMGiwoQYIKWYBBQUH  
MAKGLWh0dHA6Ly9jcncQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRtQUNBMDAxLmNy  
dDA1BggrBgEFBQcwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4E  
FgQUkZt1SQD52neqCJLf8RCSuUmeFYwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAW  
gBQtUUtJ24QtsE0r6AU4U6nlvh+3RTBIBgNVHSAEQTA/MD0GCysGAQSC9GYCAQIy  
MC4wLAYIKWYBBQUHAgEWIgh0dHBzOi8vcvcmVwb3NpdG9yeS50c3AuemV0ZXMuY29t  
MD4GA1UdHwQ3MDUwM6Axc+CGLWh0dHA6Ly9jcmwudHNwLnpldGVzLmNvbS9aRVRF  
U1RTUFRtQUNBMDAxLmNybdAOBgNVHQ8BAf8EBAMCB4AwFgYDVR0LAQH/BAwwCgYI  
KWYBBQUHAgwDQYJKoZIhvcNAQELBQADggIBACjeqgZjKscAoXd3XRBHm3pHS3mC  
/cRkH10uTsET9cJYV99kmDu+x2ayiuH5iNvwSVvCKUCuHGJv6uwQzsDtigve4eCsu  
phTdlztz39EnR+dxAoQ4LxFESAogn7jBjk5fJK0k3gEP1HuqTeFb+/dBsExaYgk  
/k7Uq8A2wGBnK5dQxLe7VSJ1Ya1BsZQW+7Y2Vc+yEE49XCHC8ZfBRJh8veKjQF1  
VLM+jxoTQEweiwL2zUmPRuNpTOhNs15CNR6eyWBrM+4qmnaCQtglR8bPML1T3s41  
UKXWo5R3WcA84IbwUxcmJRKhrdhYY3YeuLMY6usBxa2KKzxRQf+k6wIdn5pY8z9A  
SWN2AgrXGt4bVT48MiZAqwxzP67IvUW6COisLn4UWzxVXY1tAr4R/DazcvXFMH9G  
E20xU6kT9JdH1+ohvm/tlPQXXOjgzAUHV+5Cj/TMEtjNL0Fm3G7d65AZq/Va9V91  
I/4Qrt170L8oLG5Xr2TaNUuhcCMrGevC7N0HC9jOsVBTuAA6FFomrJ8ekNY1SVVK  
k9fIMTLFMVyOHnSEIVTUs4vviAQD0JBfm+g0i toZIZ/QsQaZ7UbwQ7wnM+FFnOyU  
mjEQNojaP1gH/pO6sTMKCGm6pOT85dlOQBjex/zNmp/ANHUFtZH+ELVGbKhaQn6G  
Ats1Cv+w3mwBknt7  
-----END CERTIFICATE-----

## 8.2.16 ZetesConfidens EC TSU16

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      56:8b:16:bc:77:ed:91:3a
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=BE, O=ZETES SA (VATBE-0408425626)/serialNumber=001, CN=ZETES TSP CA FOR TSA 001
    Validity
      Not Before: Jan 22 14:41:50 2019 GMT
      Not After : Jan 20 14:41:50 2025 GMT
    Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZetesConfidens EC TSU16
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)
      pub:
        04:b3:2e:a3:d0:02:d3:d5:f1:e9:77:c0:00:af:02:
        f1:b5:ec:17:12:39:ac:d4:5a:b9:47:2c:f1:b6:d1:
        b7:80:af:37:66:3b:fd:bd:05:5e:f5:18:b3:5a:0a:
        67:8b:87:e0:1b:65:01:4f:13:22:d7:4a:4d:8f:76:
        bb:aa:20:c5:6d
      ASN1 OID: prime256v1
      NIST CURVE: P-256
  X509v3 extensions:
    Authority Information Access:
      CA Issuers - URI:http://crt.tsp.zetes.com/ZETESTSPTSACA001.crt
      OCSP - URI:http://ocsp.tsp.zetes.com

    X509v3 Subject Key Identifier:
      70:79:4E:E1:5D:5E:1A:5C:46:0E:E5:0E:E9:B5:DD:DD:C0:16:CB:76
    X509v3 Basic Constraints: critical
      CA:FALSE
    X509v3 Authority Key Identifier:
      keyid:2D:51:4B:49:DB:84:2D:B0:4D:2B:E8:05:38:53:A9:E5:BE:1F:B7:45

    X509v3 Certificate Policies:
      Policy: 1.3.6.1.4.47718.2.1.2.50
      CPS: https://repository.tsp.zetes.com

    X509v3 CRL Distribution Points:

      Full Name:
        URI:http://crl.tsp.zetes.com/ZETESTSPTSACA001.crl

    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Extended Key Usage: critical
      Time Stamping
    Signature Algorithm: sha256WithRSAEncryption
      2e:4b:78:96:aa:89:8b:9e:ba:2e:56:c4:52:89:45:ee:6d:c6:
      b5:47:9f:56:c9:63:a7:fd:e2:ff:c6:12:b4:4d:fa:f2:21:98:
      94:3e:f7:78:82:ad:31:a4:74:61:08:0f:39:53:5f:46:a9:2a:
      11:e7:a9:3a:d3:e7:02:2b:0f:98:eb:c5:4a:44:17:23:e7:b9:
      60:74:aa:55:db:32:2d:c4:c3:70:1d:ac:44:a4:51:12:e8:63:
      b5:ec:b2:53:ee:ae:6a:13:e1:0d:d6:57:36:42:87:5e:2e:f7:
      1a:1d:1b:48:a6:77:21:fc:2b:87:a1:c6:54:c6:89:69:a3:57:
      9d:8c:cb:00:b1:37:66:6c:59:d4:26:da:42:09:7f:99:56:f7:
      83:16:43:8c:93:70:2d:ed:9e:64:63:52:4e:aa:46:6b:83:9e:
      6e:d1:3d:c7:63:2d:01:ec:be:76:39:6b:b7:27:1f:b0:ac:0c:
      72:37:5b:03:64:2b:4d:7c:b3:b4:54:eb:71:dc:65:94:ac:62:
      0d:57:d9:62:2f:fb:7d:d8:f3:4f:a6:8b:26:53:b0:ce:a3:db:
      4e:8b:fd:c5:00:71:dd:30:88:a5:c1:bb:4e:a6:e5:52:6a:9e:
      bb:eb:fa:b9:07:30:c0:25:a2:d9:ae:aa:9d:16:6a:a3:b0:70:
      33:09:1f:e9:be:f4:65:8c:25:1e:ac:7b:65:5e:81:e2:b1:8d:
      06:f0:9d:d5:d6:d3:11:9f:9e:4c:51:72:7c:74:02:84:8c:f6:
      57:73:c5:48:e5:43:45:5b:2a:4d:66:14:20:ad:5b:14:96:ad:
      fb:c0:cb:6f:50:52:12:b9:72:07:70:19:ed:4d:54:95:2b:88:
      9e:b9:30:83:8e:d9:fb:6f:e6:26:2d:ea:0e:f9:12:a1:70:eb:
      f1:50:cf:15:13:97:e8:5e:59:35:18:26:6c:15:26:6b:6f:f3:
      58:61:fd:b1:90:5f:7f:2f:2e:1f:80:47:f3:52:17:c7:0c:e8:
      9b:da:76:b7:c2:7c:63:59:9b:7b:c1:d5:86:d8:e6:81:c0:fa:
      17:0d:6b:28:c0:da:ce:39:32:75:2f:98:ff:5c:5b:93:c2:b9:
      59:51:51:80:44:d7:f6:ea:52:07:23:da:7d:dd:64:90:2b:6d:
      58:e4:de:b1:72:af:fb:45:f8:95:c8:91:08:3a:6e:db:ac:9e:
      d1:cf:94:04:52:77:cd:a2:dd:ec:7c:ea:99:92:76:5a:d4:5b:
      05:8b:4e:9f:6f:ee:39:9d:9e:88:d5:2b:9b:c3:69:bf:3c:ab:
      45:49:26:33:3a:e6:3b:cf:93:40:93:10:71:f0:77:19:45:3e:
      28:a9:9a:c3:a4:4c:c4:db
  -----BEGIN CERTIFICATE-----
  MIIe6DCCAtCgAwIBAgIIIVosWvHftkTowDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
  BhMCQkUxJDAiBgNVBAoMGlpFVEVTFIFNBChWQVRCRS0wNDA4NDI1NjI2KTEMMAAoG
  A1UEBRMDMDAXMSEwHwYDVQQDDDBhRVRFUyBUU1AgQ0EgRk9SIFRFTQSAWMEHhCN
```

MTkwMTIyMTQ0MTUwWWhcNMjUwMTIwMTQ0MTUwWjBVMQswcQYDVQQGEWJCRTEkMCIG  
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSAwHgYDVQDDbDdaZXRL  
c0NvbWZpZGVucyBFQyBUU1UxNjBZMBMBYqGSM49AgEGCCqGSM49AwEHA0IABLMu  
o9AC09Xx6XfAAK8C8bXsFxI5rNRauUcs8bbRt4CvN2Y7/b0FXvUYs1oKZ4uH4Bt1  
AU8TIttdKTY92u6ogxW2jggF2MIIBcjbWBggrBgEgFBQcBAQRkMGiwoQYIKwYBBQUH  
MAKGLWh0dHA6Ly9jcnQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRtQUNBMDAxLmNy  
dDA1BggrBgEgFBQcWAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4E  
FgQUChl04V1eGlxGDuU06bXd3cAWy3YwDAYDVROTAQH/BAIwADAfBgNVHSMEGDAW  
gBQcUUtJ24QtSE0r6AU4U6nlvh+3RTBIBgNVHSAEQTA/MD0GCysGAQSC9GYCAQIy  
MC4wLAYIKwYBBQUHAgEWIgh0dHBzOi8vcvcmVwb3NpdG9yeS50c3AuemV0ZXMuY29t  
MD4GA1UdHwQ3MDUwM6Axc+CGLWh0dHA6Ly9jcmwudHNwLnpldGVzLmNvbS9aRVRF  
U1RTUFRtQUNBMDAxLmNybDAOBgNVHQ8BAf8EBAMCB4AwFgYDVRO1AQH/BAwwCgYI  
KwYBBQUHAgwDQYJKoZIhvcNAQELBQADggIBAC5LeJaqiYueui5WxPKJRe5txrVH  
n1bJY6f94v/GERRN+vIhmJQ+93iCrTGkdGEIDz1TX0apKhHnqTrT5wIrD5jrxUpE  
FyPnuWB0q1XbMi3Ew3AdrESkURLoY7XsslPurmoT4Q3WVzZCh14u9xodG0imdyH8  
K4ehx1TGiWmJV52MywCxN2ZsWdQm2kIJf51W94MWQ4yTcC3tnmRjUk6qRmuDnm7R  
PcdjLQhsvny5a7cnH7CsDHI3WwNkK018s7RU63HcZSsYg1X2Wiv+33Y80+miyZT  
sM6j206L/cUAcD0wiKXBu06m5VJqnrvr+rKHMMALotmuqp0WaqOwcDMJH+m+9GWM  
JR6se2VegeKxjQbwndXW0xGfnkxRcnx0AoSM9ldzxUj1Q0VbKk1mFCCtWxSWrfvA  
y29QUhK5cgdwGe1NVJUriJ65MIO02ftv5iYt6g75EgFw6/FQzxUT1+heWTUYJmwV  
Jmtv81hh/bGQX38vLh+AR/NSF8cM6JvadrCfGNZm3vB1YbY5oHA+hcnayjA2s45  
MnUvmp9cW5PCuVlRUyBE1/bqUgcj2n3dZJArbVjk3rFyr/tF+JXIKQg6btusntHP  
lARSd82i3ex86pmSdlrUWwWLTp9v7jmdnojVK5vDab88q0VJJjM65jvPk0CTEHHw  
dxlFPiipmsOkTMTb  
-----END CERTIFICATE-----

## **9 TSA ISSUING NON-QUALIFIED AND QUALIFIED ELECTRONIC TIME-STAMPS AS PER REGULATION (EU) NO 910/2014**

---

The TSU that issues time-stamps that are claimed to be qualified electronic time-stamps as per Regulation (EU) No 910/2014 [9] do not issue non-qualified electronic time-stamps.

ZETESCONFIDENS TSA uses different TSUs identified by different subject names in their public key certificate. These TSUs shall be accessible via separate service access points.

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