ZETESCONFIDENS

TSA PRACTICE STATEMENT AND TIME-STAMP POLICY

TSA Practise Statement and Time-Stamp Policy

Publication date :	**24/12/2018**		
Effective date :	**31/12/2018**		
TSA Practice Statement OID: **Time-Stamp Policy OID :**	**1.3.6.1.4.1.47718.2.2.1.50** **1.3.6.1.4.1.47718.2.2.2.50** **1.3.6.1.4.1.47718.2.2.2.51**		
Version :	**1.0**	**24/12/2018**	**Approved by PMA**

Table of Content

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
Zetes NV(*)	**Zetes SA**(*)	**Zetes SA**(*)
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

Document Version History

Version	Publication Date	Effective Date	Information about this Version
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

Certificate	**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.**
Certificate Revocation List (CRL)	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.
Coordinated Universal Time (UTC)	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
Hardware Security Module (HSM)	An electronic device offering secure key pair generation and storage, and implementing cryptographic operations using the stored key pairs.
Qualified time-stamp	Electronic time-stamp which meets the following requirements: • Binds the date and time to data so as to reasonably prevent the possibility of any undetected change of the data • It is based on an accurate time source that can be traced to UTC(k) It is signed using an advanced electronic signature of the qualified trust service provider, or some equivalent method.
Relying party	Recipient of a time-stamp who relies on that time-stamp.
Subscriber	Legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations.
Time-stamp	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.
Time-stamp Authority (TSA)	TSP providing time-stamping services using on re more time-stamping units.
Time-stamp Service (TSS)	Trust service for issuing time-stamps
Time-Stamp Token (TST)	Data object that binds a representation of a datum to a particular time with a digital signature, thus establishing evidence.
Time-Stamping Unit (TSU)	A set of hardware and software which is managed as a unit and has a single private signing key active at a time
Trust Service Provider (TSP)	Entity which provides one or more trust services
TSA system	Composition of IT products and components organized to support the provision of time-stamping services
UTC(k)	Time-scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100ns.

3.2 Abbreviations

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

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

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

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 rechtshandhavingsbepalingen 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 expiration of the certificate for the e-key ceases to be valid.

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 - BSY

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 - BSY

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	Common Name	Validity	Key	Serial Number
TSU1	ZETES TSP RSA Qualified TSU1	16/05/18–14/05/24	RSA3072	26:8F:D0:6A:48:57:6B:95
TSU2	ZETES TSP RSA Qualified TSU2	16/05/18–14/05/24	RSA3072	12:F1:4F:71:65:8E:79:16
TSU3	ZETES TSP EC Qualified TSU3	16/05/18–13/05/30	ECC256	3B:2D:48:07:68:95:D3:9D
TSU4	ZETES TSP EC Qualified TSU4	16/05/18–13/05/30	ECC256	7D:BF:1C:7F:E9:83:90:B5
TSU5	ZETES TSP RSA TSU5	16/05/18–14/05/24	RSA3072	25:45:01:D5:CE:7A:F4:63
TSU6	ZETES TSP RSA TSU6	16/05/18–14/05/24	RSA3072	6E:AF:D7:1E:5D:EF:99:50
TSU7	ZETES TSP EC TSU7	16/05/18–13/05/30	ECC256	34:A2:7C:04:14:FB:23:C1
TSU8	ZETES TSP EC TSU8	16/05/18–13/05/30	ECC256	0D:13:C8:6E:1E:2A:C5:56

8.2.1 ZETES TSP RSA Qualified TSU1

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            26:8f:d0:6a:48:57:6b:95
    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 10:13:24 2018 GMT
            Not After : May 14 10:13:24 2024 GMT
        Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP RSA Qualified TSU1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                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: 1.3.6.1.4.47718.2.1.2.50
                  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
         82:2e:49:31:99:7e:02:0f:bf:91:77:c4:0b:95:2f:28:51:cd:
         4a:eb:00:ee:7b:20:f0:8d:bd:bd:69:64:32:8d:a0:c5:d7:1f:
         f2:34:2a:a8:d0:f2:2a:f5:71:f2:96:06:16:53:11:8b:d1:6b:
         1d:bf:60:4c:f3:17:fa:34:91:e8:7b:23:11:44:ef:fe:3c:b0:
         69:42:10:dc:8f:a6:75:d4:73:37:e1:46:20:8d:c7:cc:2b:90:
         42:f3:10:cf:0d:c9:82:ec:46:50:6b:76:e0:40:d1:65:a3:80:
         60:6c:31:5d:4b:92:3b:fb:06:9e:02:e2:65:f9:e5:18:ef:25:
         b1:29:7a:ca:86:47:96:ff:ba:a9:87:ff:05:58:98:96:d0:96:
         0d:fc:af:b1:4e:0d:3b:08:e2:45:6e:6f:d3:ba:92:26:2c:e4:
         ed:8a:59:54:c1:d0:8f:f8:c7:77:87:78:36:9e:b8:dd:0f:fb:
         f2:a8:00:8a:40:c6:2c:32:fd:1f:24:f9:de:bb:be:49:3b:11:
         c6:8f:b1:dc:ad:f5:9b:ed:92:d4:16:94:8e:79:ee:2e:d7:3e:
         f7:7d:a5:f9:44:69:4b:0a:c5:6a:41:02:68:80:e0:50:4d:64:
         cd:60:89:74:b1:7a:fc:57:c7:6d:fb:b7:69:17:e5:a1:d7:02:
         cd:b8:60:5f:90:fb:ac:75:ae:72:f8:d9:72:77:a5:a5:cc:4b:
         00:ed:e4:5d:97:89:8b:0d:b7:57:30:6b:21:66:79:57:c7:72:
         79:4b:a6:34:eb:2b:f3:6b:37:7e:b0:81:35:5d:64:a5:0b:4c:
         3c:4c:43:ae:1f:8d:61:2a:81:fb:13:ea:f0:8e:af:c5:66:de:
         2f:20:de:a0:2d:dd:34:cf:b3:57:43:a7:b2:d3:ff:55:e6:5a:
         70:05:6a:06:6a:4d:38:86:f9:af:3a:c7:8c:9e:9a:eb:7d:f7:
         88:fd:6a:10:f7:9d:dc:5e:e4:88:40:c0:4e:d2:0e:cc:3d:4c:
         fe:0b:a1:d1:b8:08:50:73:bf:74:95:14:62:61:4a:d4:76:02:
         9d:4f:5a:2c:8f:16:af:ed:6b:91:73:a9:05:1d:7d:26:f8:ec:
         2b:b2:27:49:5a:23:c3:b4:46:8f:9a:dc:60:85:c1:c1:49:83:
         e8:77:59:81:3c:0c:66:90:9c:67:3c:83:15:56:af:11:95:f7:
         e0:5e:12:eb:df:7a:f6:f9:1f:06:21:33:ef:3b:2c:fb:75:b3:
         10:d6:c8:42:6a:ec:79:31:b0:5e:c5:3d:7a:03:7c:1b:f9:aa:
         a7:eb:2c:44:31:a3:9b:fb:4f:be:59:60:8c:a6:e8:f0:1e:44:
         7f:46:73:4d:af:98:16:98
-----BEGIN CERTIFICATE-----
MIIHOjCCBSKgAwIBAgIIJo/QakhXa5UwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
MTgwNTE2MTAxMzI0WhcNMjQwNTE0MTAxMzI0WjBaMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSUwIwYDVQQDDBxaRVRF
UyBUU1AgU1NBIFF1YWxpZmllZCBUU1UxMIIBojANBgkqhkiG9w0BAQEFAAOCAY8A
MIIBigKCAYEAtSnqXY5vaXpOoyZ95QEicHpfP8Jpplz6KH7oTm7Dvla1DLTsIN69
51VBLYu80qfZ9dwxiP9iyzPWgvTWyewa9cVUlGVW2oRBqVyEaxVZxRXFcCpHHwba
4vAM90PFgbu0fAuibtnCx9hHwlXCEeKTaqWlrkmJv9iDX1uUO5+7IQ1D0ajjZd3e
af2ws1G9aTZtDQXiuIZF1H3xhlQXy46ueWi4vD7O8eOacmQYXay0F4oDUGAyHmr4
RGD+6/utl9bRWr9botWwJvVkElCHrPlIxfX9VO22KGUCUpWmFOskvgEtG1Bcj1zu
BHgwhYugYZXI9+pX96jAueXc0SkB4DJIFUzA4NCsfP/zj8wtv+Z7CIZiZWfB4zvP
0hnEYvL0dHvsnVUqoaSo3hHKC5725Ojtw5AS7gdRaRff1Mu+cXwsOPfJURtlkcEU
Hdzi9xvIXE69MaRAl43bMMTf9bjxVZuGCHnGBuzyIfbsguRNfdyw2D/iPLTdrl5d
FKYCHWqKaYH1AgMBAAGjggJ4MIICdDBwBggrBgEFBQcBAQRkMGIwOQYIKwYBBQUH
MAKGLWh0dHA6Ly9jcnQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRTQUNBMDAxLmNy
dDAlBggrBgEFBQcwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4E
FgQUbcBzbgntxmuP0eEc/ZLxM919WjAwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAW
gBQtUUtJ24QtsE0r6AU4U6nlvh+3RTBFBggrBgEFBQcBAwQ5MDcwCAYGBACORgEB
MCsGBgQAjkYBBTAhMB8WGWh0dHBzOi8vcGRzLnRzcC56ZXRlcy5jb20TAmVuMIIB
AQYDVR0gBIH5MIH2MIHzBgsrBgEEgvRmAgECMjCB4zAsBggrBgEFBQcCARYgaHR0
```

```
cHM6Ly9yZXBvc2l0b3J5LnRzcC56ZXRlcy5jb20wgbIGCCsGAQUFBwICMIGlHoGi
AFoARQBUAEUAUwAgAFQAUwBQACAAUQB1AGEAbABpAGYAaQB1AGQAIABjAGUAcgB0
AGkAZgBpAGMAYQB0AGUAIABmAG8AcgAgAHQAaQBtAGUALQBzAHQAYQBtAHAAaQBu
AGcAIABjAG8AbQBwAGwAaQBhAG4AdAAgAHcAaQB0AGgAIABFAFQAUwBJACAAVABT
ACAAMwAxADkAIAA0ADIAMQAuMD4GA1UdHwQ3MDUwM6AxoC+GLWh0dHA6Ly9jcmwu
dHNwLnpldGVzLmNvbS9aRVRFU1RTUFRTQUNBMDAxLmNybDAOBgNVHQ8BAf8EBAMC
B4AwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwDQYJKoZIhvcNAQELBQADggIBAIIu
STGZfgIPv5F3xAuVLyhRzUrrAO57IPCNvb1pZDKNoMXXH/I0KqjQ8ir1cfKWBhZT
EYvRax2/YEzzF/o0keh7IxFE7/48sGlCENyPpnXUczfhRiCNx8wrkELzEM8NyYLs
RlBrduBA0WWjgGBsMV1Lkjv7Bp4C4mX55RjvJbEpesqGR5b/uqmH/wVYmJbQlg38
r7FODTsI4kVub9O6kiYs5O2KWVTB0I/4x3eHeDaeuN0P+/KoAIpAxiwy/R8k+d67
vkk7EcaPsdyt9ZvtktQWlI557i7XPvd9pflEaUsKxWpBAmiA4FBNZM1giXSxevxX
x237t2kX5aHXAs24YF+Q+6x1rnL42XJ3paXMSwDt5F2XiYsNt1cwayFmeVfHcnlL
pjTrK/NrN36wgTVdZKULTDxMQ64fjWEqgfsT6vCOr8Vm3i8g3qAt3TTPsldDp7LT
/1XmWnAFagZqTTiG+a86x4yemut994j9ahD3ndxe5IhAwE7SDsw9TP4LodG4CFBz
v3SVFGJhStR2Ap1PWiyPFq/ta5FzqQUdfSb47CuyJ0laI8O0Ro+a3GCFwcFJg+h3
WYE8DGaQnGc8gxVWrxGV9+BeEuvfevb5HwYhM+87LPt1sxDWyEJq7HkxsF7FPXoD
fBv5qqfrLEQxo5v7T75ZYIym6PAeRH9Gc02vmBaY
-----END CERTIFICATE-----
```

8.2.2 ZETES TSP RSA Qualified TSU2

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:f1:4f:71:65:8e:79:16
    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 10:14:19 2018 GMT
            Not After : May 14 10:14:19 2024 GMT
        Subject: C=BE, O=ZETES SA (VATBE-0408425626), CN=ZETES TSP RSA Qualified TSU2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                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: 1.3.6.1.4.47718.2.1.2.50
                  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
         4f:2b:4c:52:4a:91:32:26:40:66:07:25:a2:fd:ab:7c:a9:25:
         30:66:4f:42:f5:54:9b:a6:b9:69:8f:a6:a8:77:5f:c6:dc:1b:
         21:68:26:c7:ee:b7:bc:9f:26:56:5f:61:d4:f5:81:3a:d3:bb:
         0a:43:77:88:e3:4c:3c:0b:a4:53:c3:38:90:dc:62:15:c1:d2:
         09:b5:0a:8f:69:0d:38:60:67:3d:b2:67:c2:d3:e9:0e:f9:c7:
         31:55:89:d5:61:d8:e9:b6:c3:30:22:3e:e6:c8:95:eb:1b:4e:
         44:b1:8c:d1:ab:68:7f:bf:46:14:61:1e:65:ae:68:6c:7e:3e:
         49:27:5f:3a:4a:52:5e:66:35:32:c4:f8:06:89:a1:f8:b0:d4:
         88:83:10:5a:24:eb:44:e9:62:6e:b3:66:6a:9c:9e:e4:e0:51:
         38:7f:fe:17:c5:72:ee:e1:c8:64:e2:53:bf:79:ce:71:11:2e:
         67:13:b6:df:9a:7a:2e:5c:3f:22:c7:a6:4d:73:c9:03:97:06:
         4d:44:80:06:66:ba:2b:49:1f:e9:b4:43:ac:b4:2f:f0:47:55:
         fa:04:4c:7c:37:51:da:b6:e1:ca:cb:74:71:71:f6:09:dc:9a:
         3f:07:b7:b5:5e:2c:fc:0d:0c:51:36:d0:3b:03:54:f8:a4:88:
         48:fc:68:d8:90:19:d6:ad:13:1f:dd:08:af:36:a6:af:34:2c:
         69:4c:a1:59:bc:2d:02:bd:64:18:a6:54:d6:a8:66:74:08:cd:
         89:2b:46:e9:3f:9f:43:76:f1:a5:93:78:bc:de:9a:dc:69:df:
         85:65:c4:40:b9:ea:11:28:fc:a2:4e:19:31:fa:44:18:e0:1b:
         e3:e2:44:19:39:2a:ca:9d:1a:88:6d:67:62:0d:f2:70:f0:f1:
         28:ab:de:f2:d5:a4:e9:74:c9:0b:92:74:89:2a:34:68:6d:c8:
         77:f2:37:9f:af:77:5f:2e:d6:7f:da:45:09:fb:36:88:f3:f4:
         5e:95:5a:2e:14:8d:ee:41:24:2c:6e:90:b5:ab:88:3b:ca:cb:
         5a:a3:52:3f:4d:1c:f0:33:37:b5:24:11:e4:44:f0:43:8d:3b:
         77:ce:ce:02:cc:cb:17:6d:02:2d:24:36:e8:08:c7:b6:db:ec:
         46:24:cb:fd:90:b3:5a:8d:98:d0:a4:64:cc:24:68:69:a2:72:
         a7:d5:4e:d1:10:50:43:87:14:ad:eb:5e:90:b4:fe:61:ae:64:
         19:1a:01:3c:85:fd:76:ca:f4:51:4e:e0:df:3f:47:0d:2e:09:
         c2:a1:50:3d:62:44:54:ba:20:16:78:83:7b:b5:14:f0:59:d4:
         15:2c:bb:5c:e4:8d:2e:2f
-----BEGIN CERTIFICATE-----
MIIHOjCCBSKgAwIBAgIIEvFPcWWOeRYwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
MTgwNTE2MTAxNDE5WhcNMjQwNTE0MTAxNDE5WjBaMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSUwIwYDVQQDDBxaRVRF
UyBUU1AgU1NBIFF1YWxpZmllZCBUU1UyMIIBojANBgkqhkiG9w0BAQEFAAOCAY8A
MIIBigKCAYEA5WckdnEiDmvzw/Hxe+NjRuS6bZraj3TLvJDSpHvwFcyBhfeFGAUm
kx3TNJJ+nHkcSB8ZsLrLKGKlrcBYkvpt1pC7DbpDqDiGS5tAjwV6T8Pu+kbNpJKp
fhQtxjgtQ6LD1L5hJyqM3iJwREfxc5PFzXtuBk5y2Uz45ygq1YWSKJr+C2zVTBHM
GUWr9pmbsW/DZdUSprmfkNGShjj2qJNG2huS7KWSbfjIy/AXI16QqMWSqnCQz4hi
9nFOn2jzZsPfdArLqULY7Um8LedQm1/e7hoFZLvyRwwyFIEIi+zu61hOvpA8WqPu
X5OxRh+3442C4JFaRTcr03Eq8sczsJohIBhqN2jjoLhmpWGlOcAhhPTo55g4i9/hS
Czu0Ds0PGoY0jybYoUMbKy/BafHZaX79OLUhCzsq/xcVtZbrlNna8ZDeq+vivAI8
aNtAcSJIFdbLD2tzkKS8OFaGPO5LB8DYFIGo8IHVoTao1wj2bVGGZ3gekldCkeP3
7iJWylnS3rndAgMBAAGjggJ4MIICdDBwBggrBgEFBQcBAQRkMGIwOQYIKwYBBQUH
MAKGLWh0dHA6Ly9jcnQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRTQUNBMDAxLmNy
dDAlBggrBgEFBQcwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4E
FgQUpWSQ8byPzP/X2SS9+4QETbCr0nEwDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAW
gBQtUUtJ24QtsE0r6AU4U6nlvh+3RTBFBggrBgEFBQcBAwQ5MDcwCAYGBACORgEB
MCsGBgQAjkYBBTAhMB8WGWh0dHBzOi8vcGRzLnRzcC56ZXRlcy5jb20TAmVuMIIB
AQYDVR0gBIH5MIH2MIHzBgsrBgEEgvRmAgECMjCB4zAsBggrBgEFBQcCARYgaHR0
cHM6Ly9yZXBvc2l0b3J5LnRzcC56ZXRlcy5jb20wgbIGCCsGAQUFBwICMIGlHoGi
AFoARQBUAEUAUwAgAFQAUwBQACAAUQBlAGEAbABpAGYAaQBlAGQAIABjAGUAcgB0
AGkAZgBpAGMAYQB0AGUAIABmAG8AcgAgAHQAaQBtAGUALQBzAHQAYQBtAHAAaQBu
AGcAIABjAG8AbQBwAGwAaQBhAG4AdAAgAHcAaQB0AGgAIABFAFQAUwBJACAAVABT
ACAAMwAxADkAIAA0ADIAMQAuMD4GA1UdHwQ3MDUwM6AxoC+GLWh0dHA6Ly9jcmwu
dHNwLnpldGVzLmNvbS9aRVRFU1RTUFRTQUNBMDAxLmNybDAOBgNVHQ8BAf8EBAMC
B4AwFgYDVR0lAQH/BAwwCgYIKwYBBQUHAwgwDQYJKoZIhvcNAQELBQADggIBAE8r
TFJKkTImQGYHJaL9q3ypJTBmT0L1VJumuWmPpqh3X8bcGyFoJsfut7yfJlZfYdT1
gTrTuwpDd4jjTDwLpFPDOJDcYhXB0gm1Co9pDThgZz2yZ8LT6Q75xzFVidVh2Om2
wzAiPubIlesbTkSxjNGraH+/RhRhHmWuaGx+PkknXzpKUl5mNTLE+AaJofiw1IiD
EFok60TpYm6zZmqcnuTgUTh//hfFcu7hyGTiU795znERLmcTtt+aei5cPyLHpk1z
yQOXBklEgAZmuitJH+m0Q6y0L/BHVfoETHw3Udq24crLdHFx9gncmj8Ht7VeLPwN
DFE20DsDVPikiEj8aNiQGdatEx/dCK82pq80LGlMoVm8LQK9ZBimVNaoZnQIzYkr
Ruk/n0N28aWTeLzemtxp34VlxEC56hEo/KJOGTH6RBjgG+PiRBk5KsqdGohtZ2IN
8nDw8Sir3vLVpOl0yQuSdIkqNGhtyHfyN5+vd18u1n/aRQn7Nojz9F6VWi4Uje5B
JCxukLWriDvKylqjUj9NHPAzN7UkEeRE8EONO3fOzgLMyxdtAi0kNugIx7bb7EYk
y/2Qs1qNmNCkZMwkaGmicqfVTtEQUEOHFK3rXpC0/mGuZBkaATyF/XbK9FFO4N8/
Rw0uCcKhUD1iRFS6IBZ4g3u1FPBZ1BUsu1zkjS4v
-----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
```

```
-----BEGIN CERTIFICATE-----
MIIF7jCCA9agAwIBAgIIOy1IB2iV050wDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
MTgwNTE2MTAxOTAzWhcNMzAwNTEzMTAxOTAzWjBZMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSQwIgYDVQQDDBtaRVRF
UyBUU1AgRUMgUXVhbGlmaWVkIFRTVTMwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNC
AATR8Y1kbJGJPodNdPDOEvyW5G+YHtw3G+YXHQKiAvc052myY5W7Q9SNCYFw2DE8
vtW1BP/SVi4CyhO0LIn9WQQOo4ICeDCCAnQwcAYIKwYBBQUHAQEEZDBiMDkGCCsG
AQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRlcy5jb20vWkVURVNUU1BUU0FDQTAw
MS5jcnQwJQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnRzcC56ZXRlcy5jb20wHQYD
VR0OBBYEFP6oag6XkZQZam5sdLgwGQCBtE5XMAwGA1UdEwEB/wQCMAAwHwYDVR0j
BBgwFoAULVFLSduELbBNK+gFOFOp5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAgGBgQA
jkYBATArBgYEAI5GAQUwITAfFhlodHRwczovL3Bkcy50c3AuemV0ZXMuY29tEwJl
bjCCAQEGA1UdIASB+TCB9jCB8wYLKwYBBIL0ZgIBAjIwgeMwLAYIKwYBBQUHAgEW
IGh0dHBzOi8vcmVwb3NpdG9yeS50c3AuemV0ZXMuY29tMIGyBggrBgEFBQcCAjCB
pR6BogBaAEUAVABFAFMAIABUAFMAUAAgAFEAdQBhAGwAaQBmAGkAZQBkACAAYwBl
AHIAdABpAGYAaQBjAGEAdABlACAAZgBvAHIAIAB0AGkAbQBlAC0AcwB0AGEAbQBw
AGkAbgBnACAAYwBvAG0AcABsAGkAYQBuAHQAIAB3AGkAdABoACAARQBUAFMASQAg
AFQAUwAgADMAMQA5ACAANAAyADEALjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8v
Y3JsLnRzcC56ZXRlcy5jb20vWkVURVNUU1BUU0FDQTAwMS5jcmwwDgYDVR0PAQH/
BAQDAgeAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMA0GCSqGSIb3DQEBCwUAA4IC
AQCHccPvzEB3niI9hOLJyFZGCmRsbIgD7S0QdlYmWqv52RRL+VaB66hkTrqrnzUU
XNPd51kt4tuQfSO7U16M4TaDVhEM2bXXPTbqS1LI2KeChCUYThhb/Z4E07k37zCo
uAU6othXesNU6bFl6e0iSxDMETjqpDJsce5LxFMR21b4mWHvN2RAAv6C7o7+JRhh
C8thVtQTp2O+pb6mU0e0Wlp0WXqgIF22+ZEXvusefDEUnyfr2Zbpe4xcABpxieJ4
g/ObuFTeSG2Y7uGwTGFITduk1k3AYV9yLBwZwVCggox44eN6goQ8ONmUjLAp6HdV
7pcW6RrWk4WrFmO5mw9vuKrlphl2N7OgGHB3KRpKhruHpmlR8EPCVZqwxesekyhC
ybeWco4bQAb+n9b7p2jpb48+nKnKQhZEqyiB6BsEMzDMgurWU6X9deNW/LGwmxuW
bFW72790ZJJxMn5OArfjExSebveBAJorkb+yiCw471JuPpo2vHgsbh31soZMJeV6
ByoJRDviXyhgKQhEipRtgiWcoqHx4Wo7dyoAUpjjgc1hAqJlec6ndWgaZdVw2E9T
1zxVQ8pQ/nWShUhfCZVDaf4YVMYXUxDPs+FfzHn5w/IBnF8NAJBGO6wLF3Xbtiyu
i4OMR84rDBEqNOvyBdPVjwg0H0PmhmpjGLPon5aCuHZoQg==
-----END CERTIFICATE-----
```

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:d8:18:30: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-----
MIIF7jCCA9agAwIBAgIIfb8cf+mDkLUwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
MTgwNTE2MTAxOTQ3WhcNMzAwNTEzMTAxOTQ3WjBZMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMSQwIgYDVQQDDBtaRVRF
UyBUU1AgRUMgUXVhbGlmaWVkIFRTVTQwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNC
AATs5E89JdJkA3XcBwhY/It8+ryNIqnth/2y+vy8EvlD6eveWxJ88f357WQaCKsK
P0/1s8Y3YAanx/QKc093wDkyo4ICeDCCAnQwcAYIKwYBBQUHAQEEZDBiMDkGCCsG
AQUFBzAChi1odHRwOi8vY3J0LnRzcC56ZXRlcy5jb20vWkVURVNUU1BUU0FDQTAw
MS5jcnQwJQYIKwYBBQUHMAGGGWh0dHA6Ly9vY3NwLnRzcC56ZXRlcy5jb20wHQYD
VR0OBBYEFEyX1AnYzZRTgBBM0Eb1XR/HQyMDMAwGA1UdEwEB/wQCMAAwHwYDVR0j
BBgwFoAULVFLSduELbBNK+gFOFOp5b4ft0UwRQYIKwYBBQUHAQMEOTA3MAgGBgQA
jkYBATArBgYEAI5GAQUwITAfFhlodHRwczovL3Bkcy50c3AuemV0ZXMuY29tEwJl
bjCCAQEGA1UdIASB+TCB9jCB8wYLKwYBBIL0ZgIBAjIwgeMwLAYIKwYBBQUHAgEW
IGh0dHBzOi8vcmVwb3NpdG9yeS50c3AuemV0ZXMuY29tMIGyBggrBgEFBQcCAjCB
pR6BogBaAEUAVABFAFMAIABUAFMAUAAgAFEAdQBhAGwAaQBmAGkAZQBkACAAYwBl
AHIAdABpAGYAaQBjAGEAdABlACAAZgBvAHIAIAB0AGkAbQBlAC0AcwB0AGEAbQBw
AGkAbgBnACAAYwBvAG0AcABsAGkAYQBuAHQAIAB3AGkAdABoACAARQBUAFMASQAg
AFQAUwAgADMAMQA5ACAANAAyADEALjA+BgNVHR8ENzA1MDOgMaAvhi1odHRwOi8v
Y3JsLnRzcC56ZXRlcy5jb20vWkVURVNUU1BUU0FDQTAwMS5jcmwwDgYDVR0PAQH/
BAQDAgeAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMIMA0GCSqGSIb3DQEBCwUAA4IC
AQALG4y6+J9TXGbAUuCUVKgZQycZ2BgwwPXkYoKjPcv6itLM+W6GZfZhGsEc0Nkv
y2XWeFs3xVMVRzQpGzu1l+rA2seyESkOguvb9cdcdhjgqVyyh/O6P9TFUpPU+1pn
HjpH6CPgaPxMxnj7A4aQ4i0NXN54N/N5KQ8zt+VPtbSv5/ZymzVeEOhTLIJygWzc
TedJ0msPF6rNPMLr5lddtw3nvnU2d+shVB5RwFrfrF15fZyFTf2qXC4VsMtdj3sL
4m0L/mJgQPlT7PuIgEOxxNBYt83TlNlYOboefzYORzliEqDhFvWkh7T1bipLCoQ3
VpYpIRrC0UOUy0wiPNSaALUJEy2TCUUh07s4FxVB6MsF/RNPBLbBOgpokSQZlUyf
lrs1vm4/FxxlfOa+XR7RUQc9qe/BUS5iWZjB10YcJgRPsy/P+DtqUoe9rscd34Ln
cUApxX6EKb4GSMwL/s1ujdPF6GSuf3OS/TgLzEdcNW0LJrJGiLqtOg8Fs39Emvyg
OBZwWVAxbO0SjcJXy6wTDIWbU2DfnxR+iGqhdzahxU8zZrxRDUZPcdxHtsKvtbcl
IuZafB2tgsz++eIIbIgwXDpDXDm8ufNQGPTCb3dZpxktc3iM/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:
         67:4a:a3:65:97:c6:58:05:c1:0a:8c:ba:fa:a8:35:18:31:4b:
         c6:14:8f:01:18:3d:48:74:54:0a:23:b5:9a:93:30:24:19:49:
         a4:8b:6e:46:74:a3:c6:6f:72:5a:7d:f2:27:e8:6c:1e:09:27:
         0d:0f:f5:88:50:be:9e:28:98:08:54:f5:3e:1b:71:d4:71:0f:
         48:99:13:87:aa:cb:dc:c1:a6:f8:7f:4e:90:28:22:87:c3:7e:
         de:f5:a4:9c:79:4a:cf:9e:3a:01:a3:b0:8c:c5:d5:38:74:7c:
         2d:84:67:90:f9:27:c3:1a:38:54:72:9a:fb:15:79:62:ec:f9:
         cb:90:be:c6:04:0d:c1:fe:87:99:ee:19:3e:7e:92:9e:96:35:
         64:e6:b8:cb:e0:4f:bb:2b:79:a4:3a:33:76:5d:32:29:b2:38:
         c8:b9:05:05:c3:90:c8:1d:69:fe:a6:d6:2a:99:79:d0:1f:da:
         2f:0a:c5:4e:9a:e6:b0:8c:af:89:1a:59:1e:19:94:14:09:93:
         04:47:44:db:00:05:24:73:67:c7:ea:01:94:b1:d4:39:ff:f0:
```

```
         8c:ae:a7:c5:10:ee:91:72:8c:30:1b:68:1e:06:34:ac:18:81:
         ae:70:a9:a9:50:ed:0b:25:e6:81:39:81:27:86:c8:50:c8:13:
         09:b7:5a:9e:d8:37:4b:81:a9:29:d1:1e:3d:53:0c:7f:e5:b0:
         d3:51:a4:06:2a:fe:c4:1e
-----BEGIN CERTIFICATE-----
MIIGLjCCBBagAwIBAgIIJUUB1c569GMwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
MTgwNTE2MTAyMTA2WhcNMjQwNTE0MTAyMTA2WjBQMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMRswGQYDVQQDDBJaRVRF
UyBUU1AgU1NBIFRTVTUwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQCk
rfAJ11WzrUsDblU5134+FDPaWO8n5AJJtGcSyY4/GflgiA+0qaM1EmwIonY1XA5K
fkLglCY03ym+2fvAFMf6C2VWiGPulvsYh84eJRD91MFkMylE1HRSYzioILkiA+yF
OnGGz6hHoCkINc03muZmVcCLXic6r0iGAYwL3XhQxGEbTYp6GwoVzmM4TmmJFsGm
6IBMqhRmrf4NdeXx147yXlLnCSO97muZBz/Vn6t7fydNWXtvhj6JbKov6srOX4aR
bFd0sg3qVodHb2Mz1mK+8UI0zZuPK2xoxgDoXRuz76/epvEo1Hx0SVpUsMhsBKDr
ggsqgdqGtv+yprt7zp5tmuTg5b8Wo9JR5GsbwVQ+hnj7NFTNqBTu5ohZHaN6/WBB
5AEVEcmbgYD/1oTn2HUyczcgP4zJpp7UaPMx76Ys0Vp3JShQeT6GKLE5gTiHZ1Mc
Cyq78zmlETHwXpb5VzGJcHh7xko/L1QXxgST/ghhETe83NHhoa/2KqwSyq9QSzEC
AwEAAaOCAXYwggFyMHAGCCsGAQUFBwEBBGQwYjA5BggrBgEFBQcwAoYtaHR0cDov
L2NydC50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNBQ0EwMDEuY3J0MCUGCCsGAQUF
BzABhhlodHRwOi8vb2NzcC50c3AuemV0ZXMuY29tMB0GA1UdDgQWBBR/as4XyTdX
OO/+wOpS/wiPdxF/yDAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFC1RS0nbhC2w
TSvoBThTqeW+H7dFMEgGA1UdIARBMD8wPQYLKwYBBIL0ZgIBAjIwLjAsBggrBgEF
BQcCARYgaHR0cHM6Ly9yZXBvc2l0b3J5LnRzcC56ZXRlcy5jb20wPgYDVR0fBDcw
NTAzoDGgL4YtaHR0cDovL2NybC50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNBQ0Ew
MDEuY3JsMA4GA1UdDwEB/wQEAwIHgDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAN
BgkqhkiG9w0BAQsFAAOCAgEAIHScrAzSd1bAyxwvsQOTzo8yVngKcRK+MBhUl1+a
EFHFgQHOCCDfk7TOyLGWV7NbT1P+zSyULZI7AFXx5oZh8JPPWYhdFKMELpgWWwtR
1XTBx4sXJjqG9+ZHuMnF3k+ZMWcA+SwSnjkxtny6pb3sJ2mi5sYD0921U04IEAGs
1nAw+qeuIHCDpA+jQCQkaoUimN7CEajXvj+s394ieed/p62Uo1Qss8JjeLqWwy28
K+KOOfheJxRF4uKCjT/L08hJ8P6D4mvyzivsSAUC3CqXJtkyGv8lr5aAg4SJK03t
jZWJ0OQWNUNcSUMvZ0qjZZfGWAXBCoy6+qg1GDFLxhSPARg9SHRUCiO1mpMwJBlJ
pItuRnSjxm9yWn3yJ+hsHgknDQ/liFC+niiYCFT1Phtx1HEPSJkTh6rL3MGm+H9O
kCgih8N+3vWknHlKz546AaOwjMXVOHR8LYRnkPknwxo4VHKa+xV5Yuz5y5C+xgQN
wf6Hme4ZPn6SnpY1ZOa4y+BPuyt5pDozdl0yKbI4yLkFBcOQyB1p/qbWKpl50B/a
LwrFTprmsIyviRpZHhmUFAmTBEdE2wAFJHNnx+oBlLHUOf/wjK6nxRDukXKMMBto
HgY0rBiBrnCpqVDtCyXmgTmBJ4bIUMgTCbdantg3S4GpKdEePVMMf+Ww01GkBir+
xB4=
-----END CERTIFICATE-----
```

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:
         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:d6:8a:0e:87:6f:8c: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:
         a7:f6:80:f9:5b:95:7a:51:27:ba:91:a0:2e:ec:31:af:b4:c1:
         fd:04:64:01:c9:6d:27:13:21:f4:cc:29:b3:22:61:70:c3:e6:
         af:44:74:19:eb:e8:16:b9:74:36:a1:61:30:36:7b:05:f1:53:
         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:fb:e5:5b:89:04:fe:10:63:d6:3d:b3:f4:
         ef:50:39:17:73:da:99:25:59:de:c7:0a:a3:97:6c:ba:0c:de:
         fc:56:54:0e:42:18:a0:7e:36:7c:bb:24:8e:bd:fd:43:85:fd:
         94:d6:3f:1d:ec:1f:72:56:a3:07:9d:a5:55:ad:d9:16:e4:6d:
         2d:93:4b:e1:53:1e:82:fb:61:c3: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-----
MIIGLjCCBBagAwIBAgIIbq/XHl3vmVAwDQYJKoZIhvcNAQELBQAwZDELMAkGA1UE
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
MTgwNTE2MTAyMTM1WhcNMjQwNTE0MTAyMTM1WjBQMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMRswGQYDVQQDDBJaRVRF
UyBUU1AgU1NBIFRTVTYwggGiMA0GCSqGSIb3DQEBAQUAA4IBjwAwggGKAoIBgQCm
wFmSSXTKnVUpqiD5LpF0G9rZiBth8TMZFJqdHbcEqt4Qe8bqsyYioYLPJX/TnPrF
te+dSMpmfkUSBaum13/N/f+ZxMf4unaEUgphr1MN7OGiLV6UMNTiKASVuqBTPP0f
vKuFqOOoNho9IVlDHvFoybPdNWfdRud//uOusgHhNN4zUKo9mVM0ISJ24UoQHca3
g8NS47ArB/zL47LVBQTF4ISn9a02U7LCIXZrRCEDnWA9+qt334vLqNYFs3hf0c8H
JRJrusp5GByrLec4qZ+xltB6PItIGhXELpK9jfRgxM0DU/EocDR5zMe5qNZCqhZL
CiMJYqa7MrAt9srXGM9oFuciGyS3qaF1byDy1ZobgZeOy3FJNtP1veDiJHV/vuT+
lSWe57GzjIimEX1n/rE49oMHadF8jjDbR9AZXolyTns6f5aFXiKJ2kRcS4zoIYWu
+OhKG3KGzvpIpSkjYUT16UNpZXPyyI7/pM+q1KF4rxuUghyTvtAvVf9NTmEHkhkC
AwEAAaOCAXYwggFyMHAGCCsGAQUFBwEBBGQwYjA5BggrBgEFBQcwAoYtaHR0cDov
L2NydC50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNBQ0EwMDEuY3J0MCUGCCsGAQUF
BzABhhlodHRwOi8vb2NzcC50c3AuemV0ZXMuY29tMB0GA1UdDgQWBBSa2gpS6Xpc
fIAKcTRhTHqqzk079DAMBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFC1RS0nbhC2w
TSvoBThTqeW+H7dFMEgGA1UdIARBMD8wPQYLKwYBBIL0ZgIBAjIwLjAsBggrBgEF
BQcCARYgaHR0cHM6Ly9yZXBvc2l0b3J5LnRzcC56ZXRlcy5jb20wPgYDVR0fBDcw
NTAzoDGgL4YtaHR0cDovL2NybC50c3AuemV0ZXMuY29tL1pFVEVTVFNQVFNBQ0Ew
MDEuY3JsMA4GA1UdDwEB/wQEAwIHgDAWBgNVHSUBAf8EDDAKBggrBgEFBQcDCDAN
BgkqhkiG9w0BAQsFAAOCAgEAOLJZqVE7I8ytPT7gde+yOfSyAmYHtHr0mRKupugn
```

```
3UVaUqRR1AyL87QXZAhGHdgPCph8/+RJnIv1SlZrZIci4v12hBzMP4Jh+K2R+Kc7
VZL1FoLPLHhgaj/J4dChJ4PtH6Qwi90w3arRrasQq/uRFdxwjwe+IBhyWpe+3Df6
rV3UJZFf5brKAYkM/bASqkeRpg7J4sw6Xbk83UoU0vahzrzPWGYmrBb8n2xaPkfE
LiVdBx6cPRuVN7v3mWlsb4zE36n239REspfWUq9sRcf78z7EiEvTZuV2q4Aed9HO
Bq98yakSqIws4RXKR/3w9Jzi0zEaIt71QgeLllwCx5/zkdgxBoC+0daKDodvjPXA
UgoLcqe9IRrqzeY0OxUuRYkYebzZqM82vkSfyh9GXaBYaLEzp/aA+VuVelEnupGg
Luwxr7TB/QRkAcltJxMh9MwpsyJhcMPmr0R0GevoFrl0NqFhMDZ7BfFTxSiKyRxm
Da35U2sfhtUqAcyXNAeMwIqUDi8JeyOYgLhByjYgNtXuCTpE++VbiQT+EGPWPbP0
71A5F3PamSVZ3scKo5dsugze/FZUDkIYoH42fLskjr39Q4X9lNY/HewfclajB52l
Va3ZFuRtLZNL4VMegvthw+QZiO+EqpC3aSWwopPlk/8UozOvOuqKZk3bxyCw+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
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
```



```
MTgwNTE2MTAyMjEwWhcNMzAwNTEzMTAyMjEwWjBPMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMRowGAYDVQQDDBFaRVRF
UyBUU1AgRUMgVFNVNzBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABJzgAsnsbWRo
gxAH2/h98xbYZjDNpmzGX0y2t3aorzby3TZejHcbjQ+i3pl5U7Nby9xYfoPc5FD/
YheJz9+BUwijggF2MIIBcjBwBggrBgEFBQcBAQRkMGIwOQYIKwYBBQUHMAKGLWh0
dHA6Ly9jcnQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRTQUNBMDAxLmNydDAlBggr
BgEFBQcwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4EFgQUyMzP
FPf8Zgqc9GWxd1e+lrPecx0wDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBQtUUtJ
24QtsE0r6AU4U6nlvh+3RTBIBgNVHSAEQTA/MD0GCysGAQSC9GYCAQIyMC4wLAYI
KwYBBQUHAgEWIGh0dHBzOi8vcmVwb3NpdG9yeS50c3AuemV0ZXMuY29tMD4GA1Ud
HwQ3MDUwM6AxoC+GLWh0dHA6Ly9jcmwudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRT
QUNBMDAxLmNybDAOBgNVHQ8BAf8EBAMCB4AwFgYDVR0lAQH/BAwwCgYIKwYBBQUH
AwgwDQYJKoZIhvcNAQELBQADggIBABugaqWer/1gMIwdR1+TUacSaCklHnNjeOY5
zfLPJGTlS3Rz3mIiHC9FhY4+Bm5LcKI6LC9yaMJhyvPMUglghDad+RG+cgL/BvXV
kMkRhBj4znqcb+/A/C3SdyFDBVdxqMqXGkTt1NiVuzDHfW+aQN1EjSVlgFzPXYB0
JL+cHloT4hEbbLt16kPyDuG8GOxGgsxWu+KaE3KNWuylk2f/ROPbCnkiNsGLJdcM
q05SEY6BBQ9yuljgXWK0WsNxuLsnyAOVdAmjR8xQqoCw8VS/CM3IBV/fQOzAoiVN
xISqBQnkjC9a/GN57MH1hrfVO++QSMEoZgb0yG3UqLK8Fq70oquSWmSrssjQXouw
xaP/REtCGQ2gGq+XUb5heNV6iKwQbgasazyRR8Yq/7BgmkrKx5I4h8jZXuvjn4GH
rdUpec6NWSwW8/WGV4A7mmp1X6518WlPn9BIKyZ80/khui2rwlGyobbEfdhguIg8
dJpRGkMJfxRXtHpXr4VqIGcvcI1M1/9TpiGpkTASWI7j5of0slSNmkdygS+xDG2t
UbaHSkVUhfDrUS9lRjguPAqpqD4JDIWuP6oOIcAXA7vG0i3xA/2As7VQFfi4at2S
z2oTj+8EElcGu4JtsrJ/G/oDpYUiW644hUGqaMBl22Ig7nfwli/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
BhMCQkUxJDAiBgNVBAoMG1pFVEVTIFNBIChWQVRCRS0wNDA4NDI1NjI2KTEMMAoG
A1UEBRMDMDAxMSEwHwYDVQQDDBhaRVRFUyBUU1AgQ0EgRk9SIFRTQSAwMDEwHhcN
MTgwNTE2MTAyMjMyWhcNMzAwNTEzMTAyMjMyWjBPMQswCQYDVQQGEwJCRTEkMCIG
A1UECgwbWkVURVMgU0EgKFZBVEJFLTA0MDg0MjU2MjYpMRowGAYDVQQDDBFaRVRF
UyBUU1AgRUMgVFNVODBZMBMGByqGSM49AgEGCCqGSM49AwEHA0IABEKE3IX+wAC2
O00NLrD8vSET4szTSb24ufGVqvLg0DhouIYlEqsU8jCQlsUIx8II3RbppCKPBgKI
TVXOAb1q7t2jggF2MIIBcjBwBggrBgEFBQcBAQRkMGIwOQYIKwYBBQUHMAKGLWh0
dHA6Ly9jcnQudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRTQUNBMDAxLmNydDAlBggr
BgEFBQcwAYYZaHR0cDovL29jc3AudHNwLnpldGVzLmNvbTAdBgNVHQ4EFgQU80QR
EADiXNLdfOdHuSJS3k2hti4wDAYDVR0TAQH/BAIwADAfBgNVHSMEGDAWgBQtUUtJ
24QtsE0r6AU4U6nlvh+3RTBIBgNVHSAEQTA/MD0GCysGAQSC9GYCAQIyMC4wLAYI
KwYBBQUHAgEWIGh0dHBzOi8vcmVwb3NpdG9yeS50c3AuemV0ZXMuY29tMD4GA1Ud
HwQ3MDUwM6AxoC+GLWh0dHA6Ly9jcmwudHNwLnpldGVzLmNvbS9aRVRFU1RTUFRT
QUNBMDAxLmNybDAOBgNVHQ8BAf8EBAMCB4AwFgYDVR0lAQH/BAwwCgYIKwYBBQUH
AwgwDQYJKoZIhvcNAQELBQADggIBAApt9m9axcMFJJDBRYu1t7DQNby/vBrmy3td
tFESNUDN3w9miGow1WD+NgPop0gj3+UrwK1gtJttJTIIojCav+BME0aGdGZLZpwE
VM33Da53CnzwEr0BohGDlRnOpZevb+7V7NISITIocTTp2jwx9+Y/CBq6J06twZ/F
LuJ5hTruduQNBz47ScXDbT6D3gavjfeTHZ7tEl7gvftTNUJx6/Qa9x4jq8OmmyAk
3sD8XQks4wjdc821KwIAnyubwpvTaADYUQbeq+9G/E7VSrQdLEFNpM3bADrFwdIN
Aqxvz4niVniJnEorisZip7u9UcNZlHo7YBe0c+8SqlfqAllnOruv/ENc29AF0yh2
B517qwSRpQDPmYCAHmeRNVrCBzCpf3GhoB91Y4An3YNJIoWMT5b47Tl8uMhw5+Y5
Jm7dWIiieBOFGpEOgxruShZ6LByzGpwRWNJp5mpM45QQW6gikmBZMhdpSXfumPgw
3GqEIUqoMivL6ccZD0VgAH77W9XUKZqR5Gd9A1Ppe+R5dWy/fIfsh9NF7gZlCiX9
hHXeWM4968W7gNQjI4F/b1uGcSZli2h+qiI6aoJXYXInI+e+UrruAqW3kzC5nDcE
qwn/6QupiQDocAT8JC8Qrb9SAAIff8mg2Oed6eZ+x/1zqODLQdYYPHiQu2TO320C
znJ4FvJg
-----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----------