AKD QTSA
TIME-STAMP POLICY AND PRACTICE STATEMENT

Edition 1.1

Effective from May 1st, 2020.

TABLE OF CONTENT

Document name

Code:	PRO-I-94-01
Name:	AKD QTSA Time-stamp policy and practice statement
Short name:	AKD TSP/PS
Edition:	1.1/2020-05-01
Publication date:	01.05.2020.
OID:	1.3.6.1.4.1.43999.5.7
Document type:	Time Stamp Policy, TSA Practice Statement
Available at:	http://id.hr/cps

Document revisions

Edition	Date	Description
1.0	14.02.2018.	Version 1.0 of the AKD QTSA Time-stamp policy and practice statement
1.1	01.05.2020.	Error corrections. TSU certificate profile updated.

Contact information

AKD Contact info:	AKD d.o.o Mailing Address: Savska cesta 31, 10000 Zagreb, Hrvatska Web site: http://akd.hr e-mail: akd@akd.hr
AKD QTSA Contact Info	AKD d.o.o - PMA Mailing Address: Savska cesta 31, 10000 Zagreb, Hrvatska Web site: http://id.hr/tsa e-mail: pma@akd.hr Customer service: Helpdesk-kID@akd.hr

Introduction

Agencija za komercijalnu djelatnost, d.o.o. (hereinafter: AKD) is a legal person that acts as a qualified trust service provider pursuant Regulation (EU) No 910/2014 [1].

AKD issues qualified electronic time stamps, certificates for electronic identification and qualified certificates for electronic signature. The service of AKD that issues electronic time-stamps is AKD QTSA or AKD Qualified Time-Stamping Authority.

This document deals with qualified electronic time stamp (hereinafter: time-stamp) that makes it possible to verify electronic signature and proves that:

1) an information existed before a certain time, and certainty at the moment when electronic signature was created and
2) an electronic signature was generated before the time and date contained in the time-stamp.

This is particularly important in the following circumstances:

- before the expiration of the validity of certificate, should the signer's certificate be revoked before the end of its validity, which may indicate that the signer's private key is compromised and
- after the validity period of the signer's certificate when the electronic signature has to still be valid, and when CA is not mandated to provide revocation status information beyond the end of the validity period of the certificates they have issued.

AKD's Time-Stamping Units (TSUs) issue qualified electronic time stamps that meet the requirements set out in Regulation (EU) No 910/2014 [1].

The public keys of the AKD TSUs as well as the public key of certification authority the KIDCA that issues the AKD TSUs certificates are listed in the Trusted List published by the central government body responsible for the economy in the Republic of Croatia.

1. Scope

This document, AKD TSA Time-stamp Policy and TSA practice statement (hereinafter AKD TSP/PS) specifies security requirements and organizational and technical measures that AKD QTSA implements in the course of providing time stamping service.

AKD TSP/PS is made pursuant "Time-stamp Policy" and "TSA practice statement" that are defined in ETSI EN 319 421 [11] and the content and the structure of the document are laid out in accordance with this standard.

AKD TSP/PS is meant for:

- subscribers and relying parties who need detailed information on their rights and obligations, as well as the rights and obligations of the Trust Services Provider,
- the Trust Services Provider in order to set the rules and procedures for providing services and to ensure implementation of security requirements in practice and
- the conformity assessment bodies and supervisory bodies for evaluation of capability of AKD to provide time-stamping service and to have a status of qualified service provider.

AKD has established the AKD Policy Management Authority (PMA) that has overall responsibility for maintaining and approving this document as well as all AKD PKI policies and practices. AKD management has responsibility to ensure that policies and practices approved by PMA are properly implemented and enforced.

This AKD TSP/PS should be read in conjunction with the AKD PKI Certificate Policy (CP) [23] and KIDCA Certification Practice Statement (CPS) [24], (hereinafter AKD CP/CPS).

AKD will inform the public of changes it intends to make in the AKD TSP/PS and, following approval defined in section 1.5 of AKD CP/CPS, make the revised AKD TSP/PS immediately available to the subscribers and relying parties.

2. Reference

[1] 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.

[2] Act on the Implementation of 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 (Official gazette 62/17).

[3] Act on Obligatory Rights (Official gazette 35/05, 41/08, 125/11, 78/15).

[4] Consumer Protection Act (Official gazette 41/14, 110/15).

[5] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.

[6] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".

[7] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".

[8] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[9] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

[10] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2; Requirements for trust service providers issuing EU qualified certificates".

[11] ETSI EN 319 421: " Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".

[12] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".

[13] ETSI EN 319 122-1: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".

[14] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

[15] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".

[16] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".

[17] CEN TS 419 261:2015: "Security Requirements for Trustworthy Systems Managing certificates and time-stamps ".

[18] ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".

[19] ISO/IEC 27001:2013: " Information technology — Security techniques — Information security management systems — Requirements".

[20] ISO/IEC 27002:2013: "Information Technology – Security Techniques – Code of practice for information security management".

[21] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".

[22] ISO/IEC 9001:2015: "Quality management systems - Requirements".

[23] CP: AKD PKI Certificate Policy.

[24] CPS: KIDCA Certification Practice Statement.

3. Definitions and abbreviations

3.1. Definitions

General definitions of the terms used in this document are listed in the AKD CP/CPS.

For the purposes of this document the definitions of the terms are as follows:

Time-stamp policy/Practice Statement (TSP/PS): named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements and describes the practices employed in issuing time-stamp.

TSA Disclosure statement (TSDS): Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, e.g. to meet regulatory requirements.

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 6]. For most practical purposes UTC is equivalent to mean solar time at the prime meridian (0°).

NOTE: More specifically, UTC is a compromise between the highly stable atomic time (Temps Atomique International - TAI) and solar time derived from the irregular Earth rotation (related to the Greenwich mean sidereal time (GMST) by a conventional relationship) (see annex C for more details).

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.

Electronic time stamp: data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time.

Qualified electronic time stamp: an electronic time stamp which meets the following requirements:

(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

(b) it is based on an accurate time source linked to Coordinated Universal Time; and

(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

Time-stamping service: Trust service for issuing time-stamps.

Time-Stamping Authority (TSA): TSP which issues time-stamps using one or more time-stamping units.

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time.

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 ±100 ns.

3.2. Abbreviations

General abbreviations used in this document are listed in the AKD CP/CPS.

For the purposes of this document the definitions of the terms are as follows:

BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
GMT	Greenwich Mean Time
IERS	International Earth Rotation and Reference System Service

IT	Information Technology
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4. General concepts

4.1. General policy requirements concepts

The concept of time-stamping service is based on general policy for trust services providers pursuant ETSI EN 319 401 [8] and specific rules for time stamp pursuant ETSI EN 319 421 [11].

Time stamp that is issued pursuant AKD TSP/PS is qualified electronic time stamp. Applied technology of time-stamp is based on the use of public key cryptography, X 509 certificates and reliable time source.

4.2. Time-stamping services

The provision of time stamping services is broken down into the following components:

a) **Time-stamping provision service** covers technical components necessary for generating time-stamp, i.e. issuing Time Stamp Token (TST).
b) **Time-stamping management service** covers the services that monitor and control the operation of time-stamping services including the installation and de-installation of technical components of the system, synchronization with reference time source (UTC) and implementation of all procedures as defined in this AKD TSP/PS.
c) **Time-stamping information service** covers the publishing of the AKD TSP/PS and AKD TSDS, and informing subscribers and relying parties about issuing time-stamps and using AKD QTSA services.

AKD QTSA follows Best practices of Time Stamp Policy (BTSP) and standards that are referenced in section 2 of this document in order to ensure the quality and increase the trustworthiness of the time-stamping service.

4.3. Time-stamping Authority - TSA

Time-stamping Authority (hereinafter: TSA) is the authority incorporated by AKD that provides time-stamps services identified in section 4.2 of this document and which operates in accordance the rules and procedures that are described in this AKD TSP/PS.

TSA is responsible for operations of TSU and issuing TST and maintains overall responsibility for meeting the requirements defined in the present document.

The responsibilities of TSA are specified in section 6.1 of this document.

4.4. Subscribers

Subscribers are legal or natural persons who conclude agreements to use time-stamping services with TSA, to whom time-stamps are issued and who accept their duties and responsibilities as defined in AKD TSDS and in section 6.2 of this document.

When the subscriber is a legal person that comprises several end users or an individual end-user and some of the obligations as defined in section 6.2 of this document that apply to that organization will have to apply as well as to the end-users. In any case the legal person will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such a legal person is expected to suitably inform its end users.

When the subscriber is a natural person/end-user, the end-user will be held directly responsible if its obligations defined in section 6.2 of this document are not correctly fulfilled.

4.5. Relying Parties

The relying parties are legal or natural persons who receive time stamp and who act based on reasonable trust in time-stamp and in time-stamping authority. The relying party may or may not be end user.

4.6. TSA Policy and Practices

This document "*AKD QTSA Time-Stamp Policy and Practice Statement (AKD TSP/PS)*" unites and merges *Time-Stamp Policy* that defines WHAT has to be implemented and *TSA Practice Statement* that defines HOW to implement it.

This AKD TSP/PS is based on and additionally extends AKD's policy and practice of providing certification services described in documents *AKD PKI Certificate Policy* [23] and *KIDCA Certification Practice Statement* [24] that are available on AKD's KIDCA web site: http://id.hr/cps.

The policy and practice stated in this document are based on AKD's documentation of the management system and internal rules that more detail define technical, organizational, and implementation procedures applied by the AKD QTSA. Those documents contain confidential information or business secretes that are not publicly available.

5. Introduction to time-stamp policies and general requirements

5.1. General

The policy and practice of issuing time-stamp meet the requirements of ETSI EN 319 421 [11] and the time-stamp protocol and profile of TSU certificates are harmonized with IETF RFC3161 [15] and ETSI EN 319 422 [12].

Time-stamp issued by AKD QTSA has the following characteristics:

- uses a reliable time-source,
- each TST includes accurate time value that matches the time of issuing a time-stamp,
- contains information on the accuracy UTC time that is embedded in the TST,
- contains a unique AKD TSA policy identifier,
- contains a unique serial number identifying TST,

- contains hash od the information required for the time-stamp with a unique algorithm identifier used to compute the hash,
- includes additional information in TST, if asked by the subscriber, which allows linking the request to issue time stamp with TST,
- it can only be issued if the time stamp request was submitted in the correct format,
- does not check the correctness of the hash information but only checks whether the length of the hash information matches the length that is expected for the specified algorithm,
- does not include any data that may identify the sender of the request for issuing of time-stamp,
- it is signed with a private key of a TSU unit that is used only for time stamping, as indicated in the extension of the TSU certificate and
- meets all requirements for qualified electronic time stamp according in article 42 of Regulation (EU) No 910/2014 [1].

AKD QTSA uses TSUs that issue qualified time-stamps. TSUs of the AKD QTSA do no issue non-qualified time stamps, nor does it use private key of TSU units for any other purpose other than stamping qualified electronic time-stamps.

In order to ensure highest level of quality and to ensure credibility of time-stamping service, AKD QTSA acts pursuant Best practices Time-Stamp Policy (BTSP) and the norms that are referenced in section 2 of this document so that UTC time data that is incorporated in the time-stamp with the accuracy of less than +/- 1 second.

5.2. Identification

The object identifier (OID) that is covered by AKD TSP/PS and pursuant which time-stamp is issued is 1.3.6.1.4.1.43999.5.7.

Those rules are equivalent to the best practice for time-stamp, i.e. ETSI BSTP that are identified by 0.4.0.2023.1.1.

5.3. User community and applicability

AKD TSA provides public time-stamping services or time-stamp services used within a closed community.

The subscriber and relying party can use qualified time-stamps issued by AKD TSA whenever there is a need to prove that data or electronic signature of data existed at the moment of issuing time-stamp, i.e. when there is a need to preserve long term validity of electronic signature and conformity with ETSI EN 319 122 [13].

It is not allowed to use time-stamp for data and content that violate the rights of other persons and that act contrary to the laws and morals of the society.

5.4. Conformance

The presence of the identifier for the time-stamp policy mentioned in section 5.2. of this document in the field *"Policy"* od the Time-stamping response (see 7.7.1.3) indicates that AKD QTSA applies all the policy and practice stated in section 7 of this document and that it meets all the obligations defined in section 6.1. of this document.

In order to demonstrate its compliance with this AKD TSP/PS, Regulation (EU) No 910/2014 [1], the relevant ETSI standards EN 319 401 [8], EN 319 421 [11] and EN 319 422 [12] as well as the standards ISO/IEC 9001 [22] and 27001 [19], AKD QTSA is subject to periodic independent internal and external reviews and conformity assessment.

6. Policies and practices

6.1. Risk Assessment

AKD carries out risk assessment pursuant ISO/IEC 27001 [17] taking into consideration business and technical aspect related to service provision and issuing time stamp and this particularly refers to the requirements stated in clause 5 of ETSI EN 319 401 [8].

6.2. Trust Service Practice Statement

This AKD TSP/PS and AKD CP/CPS that this document is based upon are available on AKD's KIDCA web site http://id.hr/cps.

This AKD TSP/PS contains all necessary information defined in clause 6.2. of ETSI EN 319 421 [11] as well as in the clause 6.1 of ETSI EN 319 401 [8].

6.3. Terms and conditions

The subscribers and relying parties are informed of terms and conditions before entering into a contractual relationship with the AKD QTSA.

The terms and conditions of time-stamping service (AKD TSDS) is available on AKD's KIDCA web site at: http://id.hr/cps.

AKD TSDS contains all necessary information for subscribers and relying parties as required in clause 6.2 of ETSI EN 319 401 [8].

AKD QTSA may charge a fee for providing a time-stamp service.

6.4. Information Security Policy

Information security policy is carried out pursuant ISO/IEC 27001 [19] and specific requirements defined in clause 6.3 of ETSI EN 319 401 [8].

Organizational and operational practices of information security policy are specified in detail in AKD's internal rules and procedures.

6.5. TSA Obligations

6.5.1. *General*

The obligations and responsibilities contained in this section form an integral part of the AKD TSDS. Obligations of the certification authority of KIDCA issued by the TSU certificate and relying parties are specified in detail in sections 9.6.1. and 9.6.4 of the AKD CP/CPS.

Obligations and responsibilities of the service provider, subscribers and relying parties are additionally laid down in the Act on Obligatory Rights [3], Consumer Protection Act [4] and Directive 93/13 / EEC [5].

6.5.2. *TSA obligations towards subscribers*

AKD as a timestamp services provider undertakes:

- to provide timestamp services in accordance with AKD TSP/PS and AKD TSDS and will operate in accordance with AKD CP/CPS, that will be published on the http://id.hr/cps,
- to ensure that the time data embedded in the time-stamp have an accuracy of +/- 1 second of UTC or better,
- to ensure a continuous 24/7/365 access and maximum availability of its services, except in the case of planned technical interruptions and causes defined in section 6.6 of this document,
- to provide expert staff and sufficient financial resources to ensure the expected quality and continuity of timestamping service,
- to operate in accordance with Regulation (EU) No. 910/2014 [1] and the Act on the Implementation of Regulation (EU) No. 910/2014 [2],
- to implement legitimate processing and protection of personal data as well as protection all of other confidential business information and
- to carry out periodic independent internal and external reviews and conformity assessment to ensure compliance with regulatory requirements, this AKD TSP/PS as well as other AKD's internal rules and procedures.

6.5.3. *Subscriber obligations*

Obligations of the subscribers:

- to verify the signature of the time-stamp token (TST),
- to verify the issuer of the TSU certificate and validity of all certificates in the certification path,
- to verify that the TSU certificate used to sign TST has been valid and has not been revoked at the moment of signing TST,
- to use reliable cryptographic functions for time-stamping requests and
- to inform its end users and relying parties about correct use of time-stamps and the conditions of the AKD TSDS, AKD TSP/PS and AKD CP/CPS.

The TSU certificate is included in the time stamp response. For information on how to verify the TSU certificate and the certification path, see section 9.6.4 of the AKD CP/CPS.

More information on how to verify a TST and placing a signature at a particular point in time are available at IETF RFC 3161 [15] and its update in IETF RFC 5816 [16].

6.5.4. *Relying party Obligations*

Obligations of the relying parties:

- prior to using the services, get acquainted with AKD TSDS and AKD TSP/PS and about their responsibilities and obligations and the acceptable way of using time-stamping services,
- to verify that time-stamp token TST has been correctly signed before relying on a time-stamp and that the private key used to sign the time-stamp has not been compromised until the time of the verification, as indicated in section 9.6.4 of the AKD CP/CPS,
- to check the status of TSU certificate during its validity period, by using the data contained in it and

- to take into account any limitations and precautions prescribed, especially in case of production of long term time-stamps.

If this verification takes place after the end of the validity period of the TSU certificate, the relying party should follow the guidance denoted in Annex D of ETSI EN 319 421 [11].

The relying parties should:

- to verify that the private key TSU has not been compromised at any time until the time the relying party verifies the time-stamp,
- to verify that the hash algorithms used in the time-stamp exhibits no collisions at the time of verification, and
- to verify that the length of the cryptographic keys and the incorporated cryptographic algorithms or parameters used to create a time-stamp are not outdated and are still suitable at the time of verification.

The validity of a time-stamp over a long period of time can be achieved by reapplying a time-stamp to protect the integrity of a previously created time-stamp. Before reapplying the timestamp, it is necessary to verify and confirm that the previously created time-stamp is valid.

The relying parties should be aware that the KIDCA certification authority that issued TSU certificate does not obligatory to providing revocation status information for expired certificates.

6.6. Limitation of liability

AKD warrants that what it is as a provider of time stamp issuing is responsible, and it is explicitly stated that the liability of the AKD in point 6.5.2.

AKD has secured the risk of liability for damage arising from the provision of trust services.

The amount of total financial responsibility for transactions based on trust in the timestamp is limited to the amount of 80,000 kn for the subscribers and relying parties who use the timestamping services properly.

AKD is not liable for:

- damages caused by inappropriate use of time-stamping services,
- damages caused by malfunctions or errors in the software or hardware of the subscriber or a relying party,
- damages caused intentionally or by negligently by the subscriber or a relying party that that do not fulfil their obligations or fail to act in accordance with their obligations and
- damages that may arise from the using of the time stamp.

AKD is not responsible for any loss that may arise as a result of force majeure and other circumstances beyond the control of the AKD including weather-related and natural disasters, landslides, floods, fire, explosion, war, acts of war, terrorism, intrusion into physical space, intrusion in an information system or civil disorders, power interruption, failure of the hardware, software or communications infrastructure, or other disturbances that are not under the exclusive control of AKD.

7. TSA management and operation

7.1. Introduction

AKD ensures that the establishment, implementation, maintenance and continuous improvement of the quality management and information security management system is carried out in accordance with best business practices and applicable norms.

More detailed information on physical, organizational-management and technical protection measures can be found in sections 5.1, 5.2 and 6 of the AKD CP/CPS.

7.2. Internal organization

The AKD has established a system of responsibilities and has set the limitation of trust in time-stamp. The subscribers and relying parties are informed of their obligations and responsibilities and of the terms under which the AKD provides time-stamping services.

AKD has the financial stability and AKD TSA has sufficient human and financial resources to meet its obligations and provide uninterrupted service in accordance with the AKD TSP/PS.

AKD have appropriate liability insurance to cover liabilities arising from provision of trust services.

More detailed information on the service provider's business operations can be found in the AKD CP/CPS, and more specifically in section 9 of this document.

7.3. Personnel

The AKD applies the principles of segregation of duties and other organizational and management measures of protection in accordance with section 5.2 of the AKD CP/CPS.

Selection, employment, training and education, verification and information of personnel participating in the implementation of the activity of issuing time-stamps are carried out in accordance with section 5.3 of the AKD CP/CPS.

7.4. Asset management

AKD ensures an adequate level of protection of its assets that are used in the process of providing time-stamping services. AKD maintains an inventory of assets and conducts the classification of data in order to meet this requirement.

Security measures have been implemented pursuant clause 8 of ISO/IEC 27002 [20] in order to ensure adequate management and protection of assets and to prevent unauthorized disclosure, modification, transfer or destruction of information stored on the media.

7.5. Access control

Security measures are enforced in order to prevent unauthorized access to IT resources and network, pursuant sections 6.5 and 6.7 of the AKD CP/CPS.

7.6. Cryptographic controls

7.6.1. *General*

The management of cryptographic keys and HSM devices is carried out pursuant clause 10 of the ISO/IEC 27002 [20], and as detailed in sections 6.1, 6.2, 6.3 and 6.4 of the AKD CP/CPS.

7.6.2. *TSU Key Generation*

The procedure for TSU key generation is done by authorized personnel in assigned trusted roles, in a physically secure environment in a high security area according to a defined procedure and a previously prepared technical script.

Cryptographic keys of TSU units are generated, used, and stored in a HSM device that is compliant with the FIPS PUB 140-2 level 3 [7].

Each TSU unit has its own certificate and uses its cryptographic key to sign a time-stamp. TSU key is 2048 bits long, RSA algorithm.

The TSU certificate is 5 years. The certificate is valid from the date of issue (the "*Valid from*" field of validity) until the expiration date of the validity period (the "*Valid to*" certificate).

The validity period of the TSU private key is 2 years as defined in the field *"Private Key Usage Period"* of TSU certificate.

The purpose of the TSU certificate is defined through the value of the *"Key Usage"* extension that has "Digital Signature" and "*Non-Repudiation"* values.

The TSU certificate has an additional extension "Extended Key Usage" that has the value "Time Stamping (1.3.6.1.5.5.7.3.8)"

"Key Usage" and *"Extended Key Usage"* extensions have been identified as critical extensions.

AKD QTSA takes into account that cryptographic algorithms, cryptographic key lengths, and TSU key periods are consistent with ETSI TS 119 312 [14].

7.6.3. *TSU private key protection*

The private keys of TSU units are held and used within HSM device after their generation and under at least dual person control.

The Private Key Protection of the TSU Unit is done in accordance with sections 6.2, 6.3 and 6.4 of the AKD CP/CPS.

7.6.4. *TSU certificate*

Public keys of TSA units are available to subscribers and relying parties in the certificate. Certificates of TSU units are issued by the certification authority KIDCA and published on their portal http://id.hr/cert.

Information that is required for verification of TSU certificate and certification path are contained in the TSU certificate.

The TSU certificate profile is in compliance with the requirements of ETSI EN 319 422 [12] and IETF RFC 3161 [15] as well as with section 7 of the AKD CP/CPS.

The TSU certificate profile is shown in the following table:

Table 1: Profile of TSU certificate

Field	Value
BASIC FIELDS	
Version	X.509 V3
Serial Number	Unique positive number with 32-bit entropy
Signature Algorithm	SHA256RSA
Issuer DN	CN = KIDCA, 2.5.4.97 = VATHR-58843087891, O = AKD d.o.o., C = HR
Valid from	utcTime
Valid to	utcTime (Valid from +5 years
Subject DN	CN = AKD QTSA < year of issue > 1, 2.5.4.97 = VATHR-58843087891, O = AKD d.o.o., C = HR CN = AKD QTSA <year of issue> 2, 2.5.4.97 = VATHR-58843087891, O = AKD d.o.o., C = HR
Subject Public Key	Subject Public Key, RSA (2048 Bits)
Signature Value	Signature of the certificate issuer
EKSTENZIJE	
Key Usage*	Digital Signature
Extended Key Usage*	Time Stamping (1.3.6.1.5.5.7.3.8)
Basic Constraints	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	Derived using the SHA-1 hash of the public key.
Private Key Usage Period	utcTime (Valid from +2 years
Authority Info Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://id.hr/cert/kidca.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp-kidca.id.hr/kidca
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.4.1.2.2.8 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://id.hr/cps
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.id.hr/kidca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.id.hr/kidca.crl
qcStatements	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://id.hr/cps/KIDCA-pds1-0-en.pdf language=en PdsLocation: url= https://id.hr/cps/KIDCA-pds1-0-hr.pdf language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-eseal (2) (0.4.0.1862.1.6.2)

* Critical extension

7.6.5. *Rekeying TSU's key*

Prior to the expiration of the TSU private key validity period, AKD QTSA will replace the private TSU key and a new certificate will be issued to the TSU unit. TSU units will refuse to sign a times-stamp if the TSU private key expires.

7.6.6. *Life cycle management of signing cryptographic hardware*

The standards and control functions of the cryptographic module that are defined in section 6.2.1 of the AKD CP/CPS are applied.

7.6.7. *End of TSU key life cycle*

During the TSU key life cycle, the AKD QTSA takes care that the process of generating and reissuing the TSU key is completed before the expiration of the TSU key's validity period in order to prevent service delivery delays.

When issuing a new private TSU key, the old TSU private key is permanently destroyed and can no longer be used.

The certification authority KIDCA that issued TSU certificate ensures that the TST certificate status verification information is available during the TSU validity period.

7.7. Time-stamping

7.7.1. *Time-stamp issuance*

7.7.1.1. *General*

AKD QTSA provides a time-stamping service by using time-stamp protocols via a standard HTTP as described in IETF RFC 3161 [15].

Prior to submitting the request, the AKD QTSA subscribers shall be authenticated using a digital certificate (two-way TLS) or other authentication method according to the instructions published on the AKD QTSA Portal http://id.hr/tsa.

The AKD QTSA system will not accept a time-stamp request if the user authentication was not successful.

The AKD QTSA system will not issue a time-stamp if the time used by TSU is not obtained from the UTS laboratory or if the UTS laboratory synchronization did not achieve the accuracy declared in the response to the request for time stamp issuance.

The TSU unit uses a dedicated private key that is used exclusively for stamping a time-stamp and can only be used if it is not revoked and its validity period has not expired.

7.7.1.2. *Time-stamping request*

The time-stamping request sent by user applications must comply with clause 2.4.1 of the IETF RFC 3161 [15] as well as the ESSCertIDv2 modifications specified in clause 2.1 IETF RFC 5816 [16].

According to ETSI EN 319 422 [12] AKD QTSA supports the following fields in time-stamping request:

- *reqPolicy*,
- *nonce* and
- *certReq*.

According to Appendix A.8 of ETSI TS 119 312 [14], the hash algorithm for the time-stamp data should be one of the following:

- *sha-256 (OID: 2.16.840.1.101.3.4.2.1)*
- *sha-384 (OID: 2.16.840.1.101.3.4.2.2)*
- *sha-512 (OID: 2.16.840.1.101.3.4.2.3).*

The profile for the format of the request is listed in the following table.

Table 2: Profile for the format of the request

Field	Supported value	Description
Version	v1 (1)	Version of time stamp request
messageImprint	hashAlgorithm: hash algorithm hashedMessage: hash value of the data to be time-stamped	The hash algorithm and hash value of the data to be time-stamped
reqPolicy	1.3.6.1.4.1.43999.5.7	TSA Policy identifier under time stamp token should be provided
nonce	Integer	Data that allows connection of requests and responses
certReq	FALSE (default) TRUE	Request for TSU certificate

7.7.1.3. *Time-stamping response*

The time-stamping response sent by AKD QTSA is in accordance with clause 2.4.2 IETF RFC 3161 [15] as well as the ESSCertIDv2 modifications specified in clause 2.2 IETF RFC 5816 [16].

According to ETSI EN 319 422 [12] each time stamp response contains the following fields:

- *accuracy* and
- *nonce*. if it was supplied in time-stamping request.

In the time-stamping response, field *nonce* contains the same value that is placed in the field of the same name in the time-stamping request.

In the time-stamping response, is sealed by the TSU.

According to Appendix A.8 of the ETSI TS 119 312 [14], the algorithm used to sign time stamp tokens (*signatureAlgorithm*) is:

- *sha256-with-rsa (OID: 1.2.840.113549.1.1.11)*

The profile for the format of the response is listed in the following table.

Table 3: The profile for the format of the response

Polje	Supported values	Description
PKIStatusInfo	0 (TST is present in response) 1 (TST is present in response) Other value (TST is not present in response)	Information about the status of successful issuing a time-stamp
TimeStampToken		
version	v1 (1)	Version of time stamp response
policy	1.3.6.1.4.1.43999.5.7	TSA Policy identifier under time stamp token is provided
serialNumber	Integer	Unique identifier of TST
genTime	UTC time YYYYMMDDHHMMSS(.s…)Z	Time in which TST is created which includes seconds
accuracy	1 second	Accuracy of time
nonce	Integer, 160 bits	Data that allows connection of requests and responses (if provided in the request)

7.7.2. *Time synchronization with UTC*

AKD QTSA owns satellite receivers that receive a GPS time signal of the exact UTC time distributed by numerous UTC(k) laboratories around the world.

The UTC time information that AKD QTSA incorporates into the time-stamp has a deviation of less than +/- 1 second.

In order to achieve the stated accuracy of UTC time, the following technical and organizational security measures are taken:

- the calibration of the clocks of TSU units is made when necessary, and at least twice a day
- the system takes into account of one-second leaps that UTC applies ("*leap second*"),
- the system detects a loss of synchronization with UTC and will not issue a timestamp if the time difference/deviation is greater than the declared accuracy and
- the system records all activities and it sound an alarm in case of an error, including any deviation from the declared accuracy or inability to calibrate the clocks.

7.8. Physical and environmental security

AKD QTSA system is located on AKD business premises in the same area where AKD PKI infrastructure and KIDCA system that issues TSU certificate are situated.

Measures of physical security are implemented as described in section 5.1 of the AKD CP/CPS.

7.9. Operational security

The AKD QTSA information system is part of the overall AKD PKI infrastructure and implements the same controls over the computer resources and software life cycle as described in sections 6.5 and 6.6 of the AKD CP/CPS.

The AKD QTSA system is based on reliable hardware and software components, and critical system operations are supported by redundant components.

Special supervision and capacity management measures are implemented to ensure adequate efficiency and availability of the AKD QTSA system.

7.10. Network security

AKD QTSA's computer resources are separated into network zones that are protected by appropriate physical, technical and procedural security measures.

In order to ensure high availability of the service and avoid single point of failures, all network components of the AKD QTSA system, including external network connection, are redundant.

More detailed information can be found in section 6.7 of the AKD CP/CPS.

7.11. Incident management

The information and operation of the AKD QTSA system are collected and analysed in real time so that if there are any unusual and suspicious activities an alarm is sounded.

Management of incidents and malfunctions of computer resources and network is done pursuant the procedures defined in sections 5.7.1 and 5.7.2 of the AKD CP/CPS.

7.12. Collection of evidence

Procedures related to the collection, processing and the protection of records are implemented in the manner described in section 5.4 of the AKD CP/CPS.

Moreover, specific activities related to the operation of the AKD QTSA system are recorded and this includes, but is not limited to:

- activities related to generation and life cycle of TSU keys and TSU certificates,
- activities related to TSU synchronization with UTC time including regular calibration of clocks,
- activities related to the use of TSU private key and
- malfunctions and failures of the system including loss of synchronization or inability to calibrate the clocks.

Collected evidence is archived for a period of 10 years after the date of occurrence, pursuant the business practice implemented in AKD described in detail in section 5.5 of the AKD CP/CPS.

All AKD QTSA records are adequately protected and therefore, so credible, that they can be presented as material evidence in subsequent court proceedings.

7.13. Business continuity management

The procedures of business continuity management apply as defined in section 5.7. of the AKD CP/CPS.

Moreover, the procedures are implemented that are specific for AKD QTSA that include:

a) In case of compromise or suspected compromise of the TSU private key, AKD QTSA will instantly stop using the compromised TST signing key and revoke TSU certificate.
b) In case of loss of calibration of TSU units over a period longer than one day, the TSU will stop issuing time-stamps until steps necessary for system recovery are taken.
c) The AKD QTSA will inform via the portal end users and relying parties of any calibration losses that caused the delays in providing a time-stamp service
d) If it has been subsequently found that TSU has issued a time-stamp in compromising circumstances when there has been loss of calibration, AKD QTSA will, via the portal, inform end users and relying parties about TST serial numbers which are suspected or contained incorrect data.

7.14. TSA termination plan

Cessation of times-stamping services will be implemented pursuant AKD CP/CPS and pursuant the issued KID termination plan for certification services.

Additionally, in case of termination, the AKD QTSA will:

a) inform in a timely manner the supervisory bodies, end-users and relying parties on the intent of terminating time-stamping services,
b) optionally, it will enable users to receive time-stamping services by other service providers, and
c) it will revoke the certificates of all the TSU units that were used for providing time-stamping services.

7.15. Compliance

AKD QTSA provides adequate evidence that its business operations meet the applicable legal regulations.

This applies in particular to:

a) collecting a minimal set of personal identification data sufficient to allow access to the time-stamping service of the subscriber,
b) guaranteeing individuals' privacy rights and legitimate processing and protection of all personal data and
c) adequate protection and processing of all confidential business information that is collected or incurred during the process of providing time-stamping services.

The AKD QTSA time-stamp service is accessible for all persons able to act via the internet. No other ability-dependent restrictions apply.

8. Compliance with Regulation (EU) No. 910/2014

AKD QTSA is a qualified trust service provider who issues a qualified electronic time stamp as per Regulation (EU) No. 910/2014 [1] and the relevant ETSI standards EN 319 401 [8], EN 319 421 [11] and EN 319 422 [12].

Certificates of AKD TSUs that seal time-stamps are qualified and they are issued by a KIDCA certification authority that operating under ETSI EN 319 411-1 [9] and ETSI EN 319 411-2 [10].

Subscribers and relying parties may use a Trusted List to establish whether the AKD TSU and the timestamp issued by AKD QTSA are qualified.

According to ETSI EN 319 421 [11], 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.