KIDCA

Certification Practice Statement Lite

Edition 1.6

Effective from July 1st, 2023.

Version for Public Release

Content:

1. Introduction

1.1. Overview

A root certification authority called AKDCA Root has been established within the AKD that issues certificates to itself and to subordinate certification authorities.

The KIDCA is a subordinate certification body that issue certificates to natural and legal persons and issues certificates used for AKD qualified electronic time-stamping service and OCSP service.

The subordinated KIDCA also issues qualified certificates for which the corresponding private keys are stored and used solely in AKD mPotpis service for remote digital signature creation in remote QSCD and managed by AKD on behalf of the signer.

This document, *"KIDCA Certification Practice Statement"* (*hereinafter: CPS or KIDCA CPS*) corresponds to the document called "*Certification Practice Statement CPS*" according to IETF RFC 3647 [36]. The structure and the contents of this document are stringently harmonized with the requirements of this standard.

This CPS specifies organizational and technical measures which are applied by the KIDCA in practice when determining identity of persons, issuing certificates on QSCD and managing their life-cycle.

Also, this CPS specifies organizational and technical measures which are applied by the KIDCA in practice when determining identity of persons, issuing certificates and managing their life-cycle, managing private keys and eID means used in AKD mPotpis service that operates remote QSCD device and private keys for remote qualified signature creation on behalf of the signer and remote qualified seal on behalf of the creator of seal (*Trustworthy system supporting server signing –TW4S*) and is harmonized with requirements of *" SSASC CP (Server Signing Application Service Component Practice Statement)"* according to ETSI TS 119 431-1 [23] and CEN EN 419 241-1 [32].

Detailed technical specifications and certificate profiles can be set out in other internal documents.

KIDCA CPS is made available to conformity assessment bodies and supervisory bodies and serves as a basis for assessing the abilities of the AKD to provide qualified trust services and has a right to bear the status of a qualified service provider.

A simplified version of the CPS, titled "*KIDCA Certification Practice Statement Lite*", does not contain confidential business information can be published on the website, and allows persons and relying parties to assess the suitability of the certificate for a particular purpose.

The terms, used in this document, set out in Annex 1 to this document, are taken from the EU Regulation No. 910/2014 [1] and corresponding standards.

The strict requirements for qualified trust service providers and qualified trust services that they provide, are defined by EU Regulation No. 910/2014 (EU) [1].

Providing time-stamping services is not in scope of certification services according to this CPS and time-stamping policy and practice statements are defined in the document AKD QTSA Policy and Practice Statement for providing time-stamping services (*hereinafter: TSP/PS*) [54].

In case of contradiction, provisions of the following documents are applied and in the following order (from the most significant):

a) ETSI EN 319 400 series provisions for QCP-n-qscd, NCP+ and QCP-l-qscd
b) CP of certification authority,
c) KIDCA CPS.

1.2. Document name and identification

1.2.1. *Document name*

Code:	PRO-IV-301-01
Name:	KIDCA Certification Practice Statement Lite
Edition:	1.6
Publication date:	24th May 2023
Effective from:	July 1st, 2023
Author:	AKD d.o.o
Document type:	Certification Practice Statement
Availability:	https://www.certilia.com

History of the amendments to the document is included in Annex 4 to this document.

1.2.2. *Identification code*

The OID, reserved by the AKD is 1.3.6.1.4.1.43999. AKD assigned No. 5 to the OID for PKI services.

The following table contains identification codes for individual's and TSU certificates.

Table 1: OID Identifiers

KIDCA personal certificates		
Name	Code	OID
Personal signing certificate KID1	kID QCP-n-qscd-ksign	1.3.6.1.4.1.43999.5.4.2.1.2.1
Personal identification certificate KID2	kID NCP+ kident	1.3.6.1.4.1.43999.5.5.2.1.2.2
Personal certificate for remote signing KID3	kID QCP-n-qscd-ksign	1.3.6.1.4.1.43999.5.4.6.1.2.1
KIDCA certificates for electronic seal		
Name	Code	OID
Certificate for electronic seal	kID QCP-l-qscd-kseal	1.3.6.1.4.1.43999.5.4.2.2.3.4
Certificate for remote electronic seal	kID QCP-l-qscd-krseal	1.3.6.1.4.1.43999.5.4.6.2.3.4
KIDCA certificates used for AKD TSA service		
Name	Code	OID
KIDCA TSU certificate	kID QCP-l-scd-tsa	1.3.6.1.4.1.43999.5.4.1.2.2.8

According to the section 5.3 of the ETSI EN 319 411-2 [16], the rules, according to which personal signing certificates KID1 and KID3 are issued, pursuant to rules of **QCP-n-qscd**, whose identification code is:

Itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd (2)

According to the section 5.3 of the ETSI EN 319 411-1 [15], the rules, according to which personal identification certificates KID2 are issued, pursuant to rules of **NCP+**, whose identification code is:

itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)

According to the section 5.3 of the ETSI EN 319 411-2 [16], the rules, according to which certificates for qualified electronic seal are issued, pursuant to rules of **QCP-l-qscd**, whose identification code is:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal-qscd (3).

According to the section 5.2, Anex A.2, ETSI TS 119 431-1 , the rules, according to which AKD implements AKD mPotpis which operates remote QSCD for remote digital signature creation on behalf of the signatory or seal creator (*AKD mPotpis service*), pursuant to rules of **EUSCP: EU SSASC Policy** whose identification code is:

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3).

1.3. PKI participants

In the context of this document, AKD PKI participants include:

a) Certification Authority – CA
b) Server Signing Application Service Provider - SSASP
c) Policy Management Authority – PMA,
d) Registration Authority – RA,
e) Persons,
f) Relying party, and
g) Others.

Responsibilities of all AKD PKI participants are set out in section 9.6.

1.3.1. *Certification Authority - CA*

Certification Authority (hereinafter: certification service provider or CA) is an authority established within the AKD, which is authorized by the PMA to issue certificates in accordance with the CP [53] and CPS.

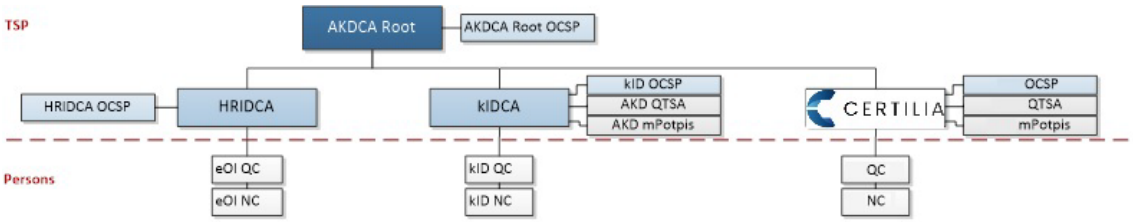
The CA provides the following trust services:

a) **Certificate generation service**: it creates and signs certificates on the basis of data gathered through registration service.
b) **Revocation service management**: it performs the certificate revocation and provides information on the certificate's status.
c) **Revocation status service**: it informs the relying parties on the status of the certificate and enables the verification through the CRL or OCSP.

d) **Dissemination service**: it informs persons and relying parties on the terms and certification conditions and other information related to certificates and certification services.

The PKI infrastructure established by the AKD PKI is arranged hierarchically so that it comprises of the root CA (AKDCA Root) that issues the certificate to itself, and of a subordinate CA that issues certificates to end-users.

Figure 1: AKD PKI hierarchical model



The subordinated KIDCA issues certificates to natural and legal persons for commercial purposes.

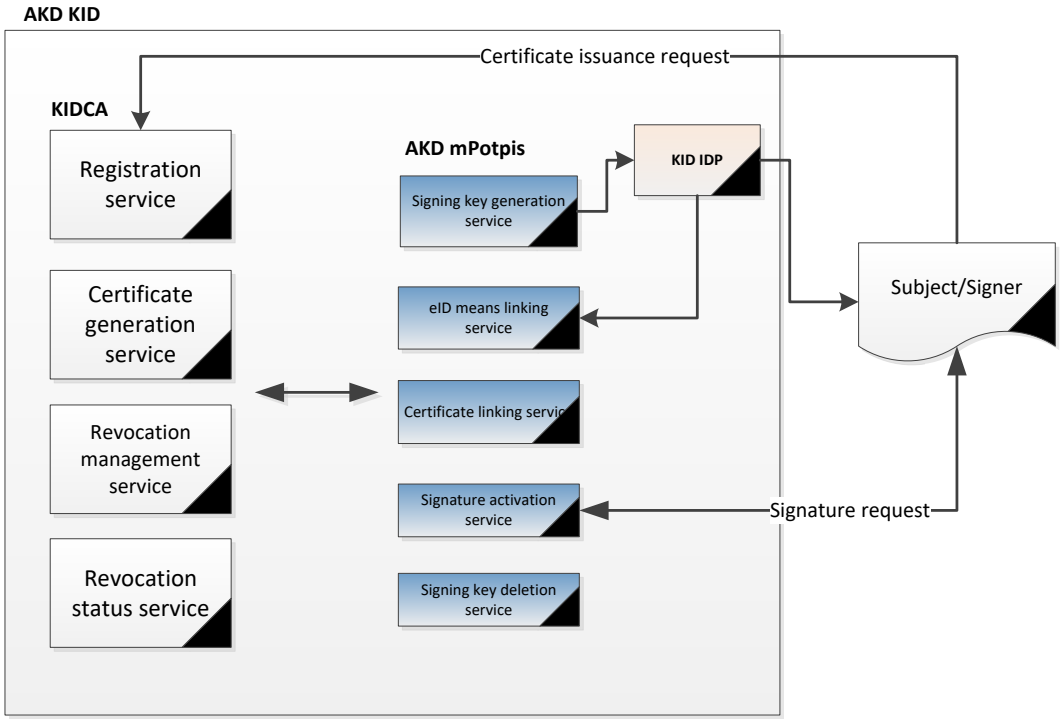
1.3.2. *Server Signing Application Service Provider – SSASP*

AKD implements and manages AKD mPotpis service for remote qualified signature and remote qualified seal creation. Certificates for remote signing and certificates for remote electronic seal used in AKD mPotpis service are issued and managed by KIDCA.

AKD mPotpis service provides the following services:

a) **Signing key generation service** – generates signing keys in the remote device. The proof of possession of generated signing keys are passed to the KIDCA RA.
b) **Certificate linking service** - links the certificates generated by the KIDCA with the corresponding signing keys.
c) **eID means linking service** - links eID means references with the corresponding signing keys in order to provide sole control. Only KID IDP registered eID means are used.
d) **Signature activation service** - verifies the signature activation data and activates the corresponding signing key in order to create a digital signature.
e) **Signing key deletion service** - destroys signing keys in a way that ensures that the signing keys cannot be used anymore.
f) **eID means provision service** - makes eID means available to the signers. Only KID IDP registered two-factor eID means are used.

Figure 1a: AKD mPotpis (SSASC)



1.3.3. *Policy Management Authority - PMA*

The AKD is a trust service provider in which persons and relying parties trust and which bears the overall responsibility for all trust services, regardless whether the services are provided independently or in collaboration with third parties.

Policy Management Authority (hereinafter: PMA) manages the provision of the trust services and operation of the AKD PKI in its entirety, and it prescribes and monitors the implementation of the security requirements that are defined in this document.

The PMA is responsible for defining, introducing and administering the CP, CPS, Security Operating Procedures and implementing documents related to the operation of the AKD PKI and provision of the trust services.

The PMA comprises several members who possess specialized knowledge related to cryptography and information security as well as knowledge related to regulatory, business, legal, formal and technical aspects of the provision of certification services.

In order to ensure the implementation of the CP and CPS in circumstances when trust service are realized in collaboration with third parties, the PMA is responsible for defining the provisions within the agreements that are concluded with third parties.

1.3.4. *Registration Authority - RA*

AKD provides registration services (hereinafter: registration service provider or RA) for the purpose of the registration of persons or verifies identities and identification data of a person under which the KIDCA issues, renews, revokes and suspends certificates.

The AKD may:

a) Carry out the activities of the RA independently, or
b) Delegate the implementation of all or some of the affairs of the RA to the third party.

The affairs of the RA include:

a) Informing persons on procedures for registration and issuance of the certificate,
b) Receiving applications for issuance and requests revocation and suspension of certificates,
c) Identity, status and affiliation validation of persons,
d) The conclusion of the conditions for providing certification services,
e) Delivering of the QSCD with certificates and private keys,
f) eID means linking and provision for AKD mPotpis service for remote digital signature and seal creation.

AKD provides registration services in AKD RA office and via on-line electronic services. AKD also provides service at location of client (mobile RA office).

AKD implements AKD RA information system which is used for registration services. Access to AKD RA system is limited to authorized persons (RA officers) – employees of AKD or employees of delegated third party. All persons are obligatory to attend the education for providing KIDCA registration services and training course for AKD RA system usage. Only authentication with KIDCA identification certificate on smartcard to AKD RA system is allowed.

In the event that all or some RA affairs are delegated to the third party, the third party must undertake to fulfil the requirements set out in this CPS, especially sections 3, 5.3 and 5.5.2. AKD and third party conclude the business contract, with provisions ensuring the compliance with CP [53] and this CPS.

1.3.5. ***Persons***

Certification subject

Certification subject (hereinafter: Subject) is natural person named in *"Subject"* field of certificate, fields *„CommonName", „GivenName"* and *„Surname",* and identified with personal identification number, field *„serialNuber".* Subjects are natural persons to whom the certificate has been issued, who have received the certificate on the QSCD and/or activation data for using certificate in AKD mPotpis service for remote signature or remote seal and which have accepted the conditions for providing certification services for natural and/or legal persons and organizations (AKD *PKI Disclosure Statement*; hereinafter: PDS) with the AKD in accordance with CP [53] and CPS.

Subscribers

Subscriber is a natural or legal person who submitted the valid certification services application, and is owner of the issued certificates. If the Subscriber and Subject are different natural/legal persons and Subscriber is an organization and requirements specified in section 3.2.3.1 f) and 3.2.3.1. g) are fulfilled, the organization name and identification number may be

contained in *„Subject“* field of the certificate e.g. field „organizationName“ and „organizationIdentifier“.

Creator of seal

Creator of seal represents a legal person who creates an electronic seal and which is named in *Subject”* field of certificate, fields *„*organizationName*“, „*organizationIdentifier*“* and whose name, commonly used to represent itself, is in the field “commonName”.

Authorized representative

Natural person authorized legally or person with legal authorization of legal representative of legal person, for representing the creator of seal. Authorized representative represents the creator of seal in the issuance process and other processes regarding the certification services. Authorized representative accepts on behalf the creator of seal the conditions for providing certification services for legal persons (PDS) and is in possession of QSCD with certificate for electronic seal and/or activation data for using the certificate for remote electronic seal in AKD mPotpis service.

Certificate application can be submitted by any person whose identity can be verified. Certificate applications are submitted to registration authority via: RA offices, RA mobile office or available on-line services under conditions set out in this CPS.

Person’s identity is verified if the person possesses a valid personal identification document (ID or passport), issued in accordance with the national or EU legislation and regulations.

Identification documents on foreign languages (other than ID or passport) are accepted if the person presents valid documentation or certificates issued by official Croatian bodies in other official procedures which require physical identification of person (e.g. HR VAT number issuance). If a person does not presents valid documentation or certificates issued by official Croatian bodies in other official procedures, identification documents (other than ID or passport) must be translated and certified by national sworn court interpreter for specific foreign language.

When submitting certificate issuance request via on-line electronic service, person must authenticate with eID mean that demonstrates high level of identity assurance and is notified eID scheme under eIDAS (EU or national level). AKD accepts eID means with identification certificate issued by KIDCA or HRIDCA.

Certificate issuance requests submitted via on-line electronic service or e-mail must be digitally signed with qualified certificate.

Certificates are issued according to the following rules:

a) Solely identification certificate may be issued to the persons above 5 years and under 18 years of age.
b) Identification certificate, as well as signing certificate, may be issued to adults above 18 years of age.
c) Certificates for electronic seal may be issued to legal persons.

Certificates on QSCD are delivered to persons or authorized representative.

Certificates used for remote digital signature or remote digital seal creation are delivered to persons or authorized representative in AKD mPotpis service operating remote QSCD.

1.3.6. *Relying parties*

The relying parties are natural or legal persons who provide on-line services and operate on the basis of reasonable reliance in a certificate and the trust service provider.

The certificate allows linking the public key and electronic signature with the person or it allows a verification of the person's identity and validation of the electronic signature to the relying party.

1.3.7. *Others*

Other participants are natural or legal persons who do not provide or use certification services, but they participate in various processes which can affect trust services, such as suppliers of HSM crypto devices, suppliers of PKI related products, services and solutions.

QSCD device used by qualified trusted service provider for managing electronic signature creation data on behalf of the certification subject or creator of seal in AKD mPotpis service is HSM device supplied by the manufacturer and supplier of the HSM crypto devices.

Remote QSCD meets the requirements set out in ISO IEC 15408 [43] *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5* and rules set out in Annex II *Regulation (EU) No. 910/2014* [1].

AKD is the manufacturer of the secure cryptographic device QSCD which is delivered to persons in possession.

QSCD meets the requirements set out in ISO IEC 15408 [43] *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5, ALC_DVS.2* and rules set out in Annex II *Regulation (EU) No. 910/2014* [1].

In accordance with the CP [53] and CPS, manufacturer provides the following affairs:

a) preparation and production of QSCD's for persons,
b) generating pairs of the cryptographic keys of persons and their entry to the QSCD,
c) distribution of the QSCD to the persons directly or using the services of RA and
d) ensuring that the QSCD is a qualified means for the creation of electronic signature/seal (*Qualified Electronic Signature Creation Device - QSCD*) according to CC EAL4+.

1.4. Certificate usage

All PKI participants must use the certificates in compliance with the CP [53], KIDCA CPS, KIDCA PDS and national and/or EU legislations and regulations.

1.4.1. *Appropriate certificate uses*

1.4.1.1. *kID NCP+ kident Personal identification certificate (1.3.6.1.4.1.43999.5.5.2.1.2.2)*

Persons and relying parties should be aware of the terms of use for personal identification certificate:

a) The high level of security attributed to the personal identification certificate is substantiated with the criteria set out in the Commission Implementing Regulation EU No. 2015/1502 [5] in order to:
   - it provides a high level of assurance of natural person's identity,
   - it provides protection against copying and unauthorized alteration by the attacker with high attack potential,
   - the person to whom it has been delivered is able to reliably protect it from the use by other persons,
   - it is delivered solely to the natural person - certification subject,
   - it has a highly reliable authentication mechanism, and
   - it is issued by the service provider with an established effective information security management practice.

b) Personal identification certificate is issued on the qualified electronic signature creation device (QSCD) meeting the requirements set out in Annex II to the *Regulation (EU) No. 910/2014* [1] as defined in Commission Implementing *Regulation (EU) 2019/650* [6].

c) A natural person is named in the personal identification certificate and this person may use it either for private purposes or for business purposes.

d) Identification certificate is used for authentication on on-line services.

e) In the event of confirmed affiliation of the person and organization, data about organization can be specified in the *„Subject" field* of the certificate, *„organizationName" and „organizationIdentifier"*.

Personal identification certificate is appropriate for authentication on AKD mPotpis service for remote signature and seal creation.

1.4.1.2. *kID QCP-n-qscd-ksign Personal signing certificate (1.3.6.1.4.1.43999.5.4.2.1.2.1)*

Persons and relying parties should be aware of the rules of use of a personal signing certificate:

a) Personal signing certificate is a qualified certificate for electronic signature, which meets requirements set out in Annex I to the *EU Regulation No. 910/2014* [1].

b) The issuer of the personal signing certificate is a qualified trust service provider and which had been granted a qualified status by the supervisory body.

c) The conformity assessment body referred to in paragraph 13 of Article 2 of the Regulation (EC) No. 765/2008 [9] performs the conformity assessment of the qualified trust service provider in order to confirm the fulfilment of the requirements of the *Regulation (EU) No. 910/2014* [1].

d) Personal signing certificate is issued on the QSCD, which is a qualified electronic signature creation device and which meets the requirements set out in Annex II to

the *Regulation (EU) No. 910/2014* [1] and as by implementation of Judgment of the Court (Grand Chamber) (EU) 2016/650 [6].

e) A natural person, certification subject, is named in the personal signing certificate and this person uses it for private and for business purposes. Personal signing certificate serves as a support in qualified electronic signature creation, as specified in Article 3, paragraph 12 of the *Regulation (EU) No. 910/2014* [1].

f) In the event of confirmed affiliation of the person and organization, data about organization can be specified in the *„Subject" field* of the certificate, *„organizationName" and „organizationIdentifier"*.

g) Unless provided with the special agreement or otherwise, the overall responsibility of the AKD towards persons and relying parties that reasonably rely on the certificate is limited with the amount of the insurance policy in accordance with the section 9.8.

1.4.1.3. ***kID QCP-n-qscd-krsign Personal certificate for remote signing (1.3.6.1.4.1.43999.5.4.6.1.2.1)***

Persons and relying parties should be aware of the rules of use of a personal signing certificate:

a) Personal signing certificate is a qualified certificate for electronic signature, which meets requirements set out in Annex I to the *EU Regulation No. 910/2014* [1].

b) The issuer of the personal signing certificate is a qualified trust service provider and which had been granted a qualified status by the supervisory body.

c) The conformity assessment body referred to in paragraph 13 of Article 2 of the Regulation (EC) No. 765/2008 [9] performs the conformity assessment of the qualified trust service provider in order to confirm the fulfilment of the requirements of the *Regulation (EU) No. 910/2014* [1].

d) Personal remote signing certificate is issued by KIDCA in AKD mPotpis service on the remote QSCD, which is a qualified electronic signature creation device and which meets the requirements set out in Annex II to the *Regulation (EU)* No. *910/2014* [1] and as by implementation of Judgment of the Court (Grand Chamber) (EU) 2016/650 [6]. Remote QSCD meets the requirements *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented by AVA_VAN.5*.

e) A natural person, certification subject, is named in the personal signing certificate and this person uses it for private and for business purposes. Personal signing certificate serves as a support in remote qualified electronic signature creation, as specified in Article 3, paragraph 12 of the *Regulation (EU) No. 910/2014* [1].

f) In the event of confirmed affiliation of the person and organization, data about organization can be specified in the *„Subject" field* of the certificate, *„organizationName" and „organizationIdentifier"*.

g) Unless provided with the special agreement or otherwise, the overall responsibility of the AKD towards persons and relying parties that reasonably rely on the certificate is limited with the amount of the insurance policy in accordance with the section 9.8.

1.4.1.4. *kID QCP-l-qscd-kseal Certificate for electronic seal (1.3.6.1.4.1.43999.5.4.2.3.3.4)*

Persons and relying parties should be aware of the rules of use of a certificate for electronic seal:

a) Certificate for electronic seal is a qualified certificate for electronic seal, which meets requirements set out in Annex I to the *EU Regulation No. 910/2014* [1].

b) The issuer of the certificate for electronic seal is a qualified trust service provider and which had been granted a qualified status by the supervisory body.

c) The conformity assessment body referred to in paragraph 13 of Article 2 of the Regulation (EC) No. 765/2008 [9] performs the conformity assessment of the qualified trust service provider in order to confirm the fulfilment of the requirements of the *Regulation (EU) No. 910/2014* [1].

d) Certificate for electronic seal is issued on the QSCD, which is a qualified electronic signature creation device and which meets the requirements set out in Annex II to the *Regulation (EU) No. 910/2014* [1] and as by implementation of Judgment of the Court (Grand Chamber) (EU) 2016/650 [6].

e) A legal person, creator of seal, is named in the certificate for electronic seal and this person uses it for business purposes. Certificate for electronic seal serves as a support in qualified electronic seal creation, as specified in Article 3, paragraph 27 of the *Regulation (EU) No. 910/2014* [1].

f) Unless provided with the special agreement or otherwise, the overall responsibility of the AKD towards persons and relying parties that reasonably rely on the certificate is limited with the amount of the insurance policy in accordance with the section 9.8.

1.4.1.5. *kID QCP-l-qscd-krseal Certificate for remote electronic seal (1.3.6.1.4.1.43999.5.4.6.3.3.4)*

Persons and relying parties should be aware of the rules of use of a certificate for electronic seal:

a) Certificate for remote electronic seal is a qualified certificate for electronic seal, which meets requirements set out in Annex I to the *EU Regulation No. 910/2014* [1].

b) The issuer of the certificate for remote electronic seal is a qualified trust service provider and which had been granted a qualified status by the supervisory body.

c) The conformity assessment body referred to in paragraph 13 of Article 2 of the Regulation (EC) No. 765/2008 [9] performs the conformity assessment of the qualified trust service provider in order to confirm the fulfilment of the requirements of the *Regulation (EU) No. 910/2014* [1].

d) Certificate for remote electronic seal is issued by KIDCA in AKD mPotpis service on the remote QSCD, which is a qualified electronic signature creation device and which meets the requirements set out in Annex II to the *Regulation (EU) No. 910/2014* [1] and as by implementation of Judgment of the Court (Grand Chamber) (EU) 2016/650 [6]. Remote QSCD meets the requirements *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented by AVA_VAN.5*.

e) A legal person, creator of seal, is named in the certificate for remote electronic seal and this person uses it for business purposes. Certificate for electronic seal serves as

a support in qualified electronic seal creation, as specified in Article 3, paragraph 27 of the *Regulation (EU) No. 910/2014* [1].

f) Unless provided with the special agreement or otherwise, the overall responsibility of the AKD towards persons and relying parties that reasonably rely on the certificate is limited with the amount of the insurance policy in accordance with the section 9.8.

1.4.2. *Prohibited certificate uses*

Any use of the certificate, except for those specified in section 1.4.1, is prohibited.

Persons and relying parties must be aware of the limitations concerning the certificate's use:

a) Certificates are not intended for data encryption.

b) When a personal identification certificate is used as a support to the electronic signature, such signature is not considered as a qualified electronic signature.

c) The signing certificate may not be used for any other purpose other than to support the electronic signature or a qualified electronic signature.

d) Certificate for electronic seal may not be used for any other purpose other than to support the electronic seal or a qualified electronic seal.

1.5. Document administration

1.5.1. *Organization administering the document*

The PMA, which operates within the AKD, is responsible for the creation and administration of the document.

1.5.2. *Contact information*

Mailing address:

AKD d.o.o
Policy Management Authority
Savska cesta 31
HR-10000 Zagreb
Croatia
e-mail: pma@akd.hr
web page: https://www.certilia.com

1.5.3. *Person determining CPS suitability for the policy*

The PMA is responsible for the conformity assessment of the document with the:

- national and EU regulations related to the electronic identification and trust services,
- technical specifications, standards and procedures related to the electronic identification and trust services, and

- internal security rules and operating procedures relating to the implementation of actions and activities of the certification service provider.

Should a need to amend the document be determined, the PMA starts the procedure of harmonisation of the documentation and determine the commencement of the application of the new rules for the provision of services.

1.5.4. *CPS approval procedures*

Before the issuance of the CP and CPS and their commencement of the application, as well as following every amendment, the PMA gives the consent for the suitability and publication of the document.

General Manager (CEO) approves publication of the CP and CPS.

1.6. Definitions and acronyms

Definitions of terms and acronyms, used in this document, which are set forth in Annex 1 and Annex 2 to this document, are in line with the *Regulation (EU) No. 910/2014* [1], ETSI EN 319 411-1 [15], ETSI EN 319 411-2 [16] and other mandatory normative documents.

2. Publication and repository responsibilities

2.1. Repositories

The AKD provides certificate's status verification service and makes all the information needed for the certificate's status verification (Table 2) available to the public.

Table 2: Repository data

Information	AKDCA Root	KIDCA
CRL: HTTP protocol	http://crl1.eid.hr/akdcaroot.crl http://crl2.eid.hr/akdcaroot.crl	http://crl1.id.hr/kidca.crl http://crl2.id.hr/kidca.crl
OCSP service	http://ocsp.eid.hr/akdcaroot	http://ocsp-kidca.id.hr/kidca
CA certificates	http://eid.hr/cert/akdcaroot.crt	http://id.hr/cert/kidca.crt

Data for the certificate's status verification are contained in the certificate, fields *„CRL Distribution Points„* and/or *„Authority Info Access*".

2.2. Publication of certification information

All information that persons and relying parties may need to use the trust services are published on the web portal of the trust service provider KIDCA https://www.certilia.com and RA offices.

The public section of the web portal, https://www.certilia.com, is made available to the public, where the following information is published:

a) Rules for providing certification services – Certificate Policy (CP) [53],
b) Rules for certification procedure – Certification practice statement (CPS, SSASC PS),
c) Policy disclosure statement (PDS),
d) Notifications related to the provision of certification services,
e) Other information relevant to persons and relying parties, and
f) Contact information for user support.

The CA establishes a private section of web portal where persons, registered subjects of certification, have access to.

The following information and services are published in the private section of the web portal:

a) application and instructions necessary for the installation and use of the QSCD,
b) on-line services for certificate's status verification, suspension/withdrawal of a certificate,
c) personal contact information of the subject of certification,
d) managing the eID means for authentication to AKD mPotpis service, and
e) AKD mPotpis service for remote signature and remote seal creation.

2.3. Time or frequency of publication

The following rules apply:

a) The information on the web portal is available immediately following their formal approval.
b) All contents on the web portal are in Croatian, and a portion of the content may be available in English.
c) CP [53], CPS (this document) and terms and conditions for providing certification services are available in Croatian and English.
d) In case of inconsistence between Croatian and English version of documents, Croatian version is considered valid.
e) The data in the repository is published immediately after their issuance.
f) Information on the certificate’s status is available under the conditions specified in section 4.10.
g) The CA provides a continuous availability of the repository 24 hours a day, 7 days a week in accordance with the best business practices.
h) Following the system failure or other factors that are out of the CA’s control, all available measures are undertaken in order to ensure a system recovery within the shortest time possible.

2.4. Access controls on repositories

The following rules apply:

a) Basic information on the web portal is available to the public without restrictions and according to standard service availability.
b) Additional information and services on the web portal are available only to registered persons.

c) The CA does not set any restrictions in relation to the use of the CRL and OCSP services.
d) Certificates of the persons are not available for the public search. Certificates may be available for the public search in case of valid relaying parties' technical requirements and solely if the consent of the person is provided.
e) The CA reserves the right to take appropriate measures to protect the repository and web portal from the misuse.

3. Identification and authentication

3.1. Naming

3.1.1. *Types of names*

The name of the certificate or unique set of data that undoubtedly represents the subject of certification or legal person or creator of seal is entered in the "*Subject*" field of each certificate.

The name of certificate is determined according to Recommendation ITU-T X.520 [50] or IETF RFC 5280 [38]. *"Subject"* field is determined according to Recommendation ITU-T X.501 [51].

There are following types of names:

a) personal certificates that name a natural person, subject of certification, signatory,
b) certificates for electronic seal that name a legal person – creator of seal, and
c) CA certificates, TSU certificates and OCSP service certificates that name the KIDCA or AKD QTSA service or KIDCA OCSP service as a legal person.

3.1.2. *Need for names to be meaningful*

In case of CA certificates, TSU certificates and OCSP service certificates, the "*Subject*" field is formed from:

commonName:	Name of the CA certificate or OCSP service or AKD QTSA service
organizationIdentifier:	Legal person identifier or VAT number
organizationName:	Name of the legal person – qualified trust service provider
countryName:	Code of the country in which the legal person is established

In case of certificates of persons, the "*Subject*" field is formed from:

commonName:	Name and surname of the natural person
serialNumber:	Serial number

givenName:	Name of the natural person
Surname:	Surname of the natural person
organizationalUnitName:	Type of the certificate (RSignature for remote signature, Sigature for signature or Identification for identification)
organizationName (Optional):	Name of organization, in case of person's affiliation with organization
organizationIdentifier(Optional):	Organization identifier or VAT number (according to section 5 of the ETSI EN 319 412-1 [i.4], čl. 5 [17]), in case of person's affiliation with organization
countryName:	Code of the country

In case of certificates for electronic seals, the "*Subject*" field is formed from:

commonName:	Name commonly used by creator of seal to represent itself
organizationalUnitName:	Type of the certificate
organizationName:	Name of legal person, seal creator
organizationIdentifier:	Legal person identifier or VAT number
countryName:	Code of the country of the legal person

3.1.3. *Anonymity or pseudonyms of subscribers*

Not supported.

3.1.4. *Rules for interpreting various name forms*

The "Subject" field in all of the certificates, issued by the certification service provider, is formed in accordance with IETF RFC 5280 [38] and recommendation of the ETSI EN 319 412-2 [18] or ETSI EN 319 412-3 [19].

Rules for interpreting various name forms are indicated in Table 3.

The value of column „Presence / Content"is interpreted as follows:

1.) Presence
   - M (*Mandatory*) – the value must be present in the field
   - O (*Optional*) – the value may or may not be present in the field

2.) Content
   - Fixed – the value is predetermined
   - Variable – the value is determined using data that are not related to person's personal data (natural or legal person)
   - Holder Variable – the value is determined using person's personal data (natural or legal person)

Table 3: Rules for interpreting various name forms

Natural persons

Field	Value	Presence / Content	Note
commonName (cn)	Name Surname	M/Holder Variable	Represents the name and the surname of the natural person
serialNumber	Natural person identifier	M/Holder Variable	3 characters for a person's identity reference type, two-letter ISO country code, "-" identification number ", e.g.: PNOHR-OIB, according to point 5.1.3 of ETSI EN 319 412-1 [17]
givenName (g)	Name	M/Holder Variable	Represents the name of the subject of certification
Surname (sn)	Surname	M/Holder Variable	Represents the surname of the subject of certification
organizationalUnitName (OU)	Identification or Signature Or Rsignature	M/ Variable	Specifies the type of certificate (RSignature for remote signature, Sigature for signature or Identification for identification)
organizationName (O)	ORGANIZATION NAME D.O.O	O/Holder Variable	Name of the organization that the natural person is affiliated to.
organizationIdentifier	VATHR-1234567890	O/Holder Variable	VAT indicates a legal person HR is the code of the country A minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) 1234567890 is an identification number of the organization, for natural persons affiliated with an organization.
countryName (C)	Two-letter ISO country code	M/Holder Variable	The ISO code of the country of the subject of certification.

Legal persons (CA, OCSP, QTSA)			
Field	Value	Presence / Content	Note

commonName (cn)	AKDCA Root KIDCA	M/Fixed	Represents the name of the CA
	AKDCA Root OCSP KIDCA OCSP AKD QTSA	M/Fixed	Represents the name of the OCPS system/TSA service
organizationIdentifier	VATHR-58843087891	M/Fixed	VAT indicates a legal person, HR is the code of the country, A minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) 58843087891 is a tax identification number of the AKD (legal person)
organizationName (O)	AKD d.o.o	M/Fixed	AKD d.o.o is the name of a legal person
countryName (C)	HR	M/Fixed	HR is the code of the country of the legal person

Legal persons (electronic seal)			
Field	Value	Presence / Content	Note
commonName (cn)	Seal name	M/Holder Variable	Name commonly used by the legal person - creator of seal to represents itself.
organizationIdentifier	VATHR-1234567890	M/Holder Variable	VAT indicates a legal person, HR is the code of the country, A minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) 1234567890 is a tax identification number of legal person (OIB for HR, VAT for foreign legal persons)
organizationalUnitName (OU)	Seal Rseal	M/ Variable	Specifies the type of certificate
organizationName (O)	PRAVNA OSOBA d.o.o.	M/Holder Variable	Registered name of legal person – creator of seal
countryName (C)	Two-letter ISO country code	M/Holder Variable	Two-letter ISO code of the country in which legal person is registered

3.1.5. *Uniqueness of names*

Unique information on the natural person or legal person (when the natural person is affiliated to organization, for CA certificates, TSU certificates, for certificates of OCSP service and certificates for electronic seal) to whom/which the certificate is issued, is entered into the "*Subject*" field of each certificate.

The uniqueness of the natural person's name is provided with the "*serialNumber*" attribute, while the uniqueness of the legal person's name of the issuer is provided with the "*organizationIdentifier*" attribute in the *"Issuer"* field.

If the natural person is affiliated with organization, the uniqueness of the organization's name is provided with the *„organizationIdentifier"* attribute in the *"Subject"* field.

The uniqueness of the legal person's (creator of seal) name for the certificates for electronic seal is provided with the "*organizationIdentifier*" attribute in the *"Subject"* field.

3.1.6. *Recognition, authentication, and role of trademarks*

Not applicable.

3.2. Initial identity validation

3.2.1. *Method to prove possession of private key*

Private keys of the personal certificates and certificates for electronic seal (QCP-n-qscd-ksign, QCP-l-qscd-kseal i NCP+ kident) are generated in the HSM device and are entered on to a qualified electronic signature creation device (QSCD) in a secure environment of the manufacturer.

Private keys of certificates used for remote signature or remote electronic seal creation (QCP-n-qscd-krsign and QCP-l-qscd-krseal) are generated and used in the HSM device operated by qualified trust services provider AKD and mPotpis service. Remote HSM device is QSCD device and meets the requirements set out in ISO IEC 15408 [43] *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5* and rules set out in Annex II *Regulation (EU) No. 910/2014* [1].

Private keys and corresponding certificates for remote signature or seal are generated in AKD mPotpis service only if subject of certification or authorized representative is authenticated to AKD mPotpis service using two-factor authentication means registered in KID IDP system, using reference and authorization codes received after certificate request approval on SMS or e-mail provided in the registration process and setting the PIN for activating the private key. Delivery of certificate and control over the private key is confirmed by signatory in AKD mPotpis service by activating the key with previously set PIN.

In the process of users key generation AKD as the qualified provider of trust services applies the appropriate measures and procedures to ensure and verify the relation of natural person

or creator of seal with the public key for which the certificate is issued and also to ensure that natural person or authorized representative has full control over the private key.

Private keys of the OCSP certificate (NCP-l-scd-ocsp) are generated in the HSM device in a secure environment of the CA which performed an authorization of the natural person – administrator of the certificate to take care of the HSM device and the corresponding private key.

3.2.2. *Authentication of legal person identity*

Authentication of organization identity is carried out when certificates are issued to:

a) natural person who is subject of certification and that person is affiliated with the organization (legal person) and organization's name is specified in the certificate's *„Subject“* field, and
b) legal persons for the certificates for electronic seal.

3.2.2.1. *Collection of information on legal persons*

For the purpose of identity validation on legal persons/organization, the following information and documents are collected:

a) Basic information about the legal person includes, but are not limited to:
   - current name of the legal person,
   - personal identification number or VAT number or other unique identifier of legal person,
   - country of the legal person’s headquarter.
b) When necessary, the legal person may be requested to provide:
   - Current headquarters address of the legal person,
   - additional contact information: e-mail, phone number, etc.
c) Evidence accepted for the purpose of validation of natural person affiliation with legal person, legal person’s name, status and existence are:
   a. An excerpts from official registers of Republic of Croatia or
   b. an extract or a print of an electronic record from the parent registry in the country of the EU, translated into Croatian language and verified by certified court interpreter in Republic of Croatia.
d) Documents accepted for the purpose of validation of natural person affiliation with legal person, legal person’s name, status and existence are:
   a. Signed and certified document issued by organization to which natural person is affiliated to.
e) In the event of modification of name, status or existence of organization during the validity period of the certificates issued by certification service provider, legal person is obligated to provide the certification service provider with valid documents and excerpts regarding the modification.

Collection of information on legal persons can be performed using on-line electronic services provided by official national or EU registers, or through AKD RA system.

In case of inconsistency between data provided in documentation and application forms and data acquired from official registers via on-line services, AKD RA accepts data acquired from official register via on-line service as valid and informs the authorized representative of legal person.

3.2.2.2. *Information verification on legal persons*

The verification process includes, but is not limited to:

a) verification of legal person's status and existence in the official registers via available on-line services and/or verification of enclosed documents provided as evidence of legal person's status and existence,

b) verification of legal person's name, for the purpose of establishing that legal person's name indicated in the certificate application is equal to the name that legal person's is using in transactions, and

c) verification of legal person's identification number via available national on-line OIB service, for the purpose of establishing that legal person's identification data (identification number or vat number or other relevant identification data) indicated in the certificate application is equal to the identification data in correspondence with organization or legal person name.

Information verification on legal persons can be performed using on-line electronic services provided by official national or EU registers, or through AKD RA system.

In case of inconsistency between data provided in documentation and application forms and data acquired from official registers via on-line services, AKD RA accepts data acquired from official register via on-line service as valid and immediately informs the authorized representative of legal person.

3.2.3. *Authentication of individual identity*

3.2.3.1. *Collection of information on natural persons*

Collection and verification of data on persons are carried out in accordance with the AKD RA operating instructions [55].

For the purpose of identity validation of the natural persons, the following information and documents are collected:

a) Basic information about the subject of certification including:
   - full name and surname,
   - type and number of personal identification document,
   - personal identification number or national identification number found in valid personal identification document,
   - place and address of residence,
   - date of birth.

b) Appropriate documents or information for the verification of the name, identity and the basis for the issuance of certificate are required.

c) Public documents (national or EU) that are considered as relevant evidence of the natural persons' identity include:
   - valid personal identity card,

- valid passport.

d) If the natural person (subject of certification) is affiliated with organization, additional information and documents are required:
   - proof of legal existence, name and legal status of organization,
   - proof that natural person's affiliation with organization,
   - proof that natural person is legally authorized representative.

e) Documents that are considered as relevant evidence of person's affiliation with the organization include:
   a. Signed and certified document issued by organization to which natural person is affiliated to.

f) Documents (national or EU) that are considered as relevant evidence of natural persons authorized representative status of legal person:
   a. An excerpts from official registers of Republic of Croatia:
      i. Companies - excerpt or electronic record from the Court Registry or,
      ii. Crafts - excerpt or electronic record from Crafts register or,
      iii. Chambers - the statute and parent law or,
      iv. Freelancers - excerpt or electronic record from the parent Chamber and the decision of the Tax Administration,
   b. An extract or a print of an electronic record of the parent registry in the EU MS, translated into Croatian and verified by certified court interpreter in Republic of Croatia.
   c. In addition with Excerpts from f) a. or f) b., legal authorization of the person named in Excerpt as the legal representative of legal person.

Collection of information on natural persons can be performed using on-line electronic services provided by official national or EU registers, or through AKD RA system, and from a qualified electronic signature of the application form received via the electronic online service.

In case of inconsistency between data provided in documentation and application forms and data acquired from official registers via on-line services, AKD RA accepts data acquired from official register via on-line service as valid and informs the person.

3.2.3.2. *Information verification on natural persons*

The following rules apply:

a) The RA (offices) collects and verifies information and documents in order to ensure that each information, contained in the certificate, is verified and confirmed.

b) Processes for identifying and verifying the identity of natural persons and person's affiliation with organization and/or person's status of legal representative of the legal person, are conducted in accordance with the national and EU identification practice and also with national and EU acts for data exchange interoperability.

The verification process includes, but is not limited to:

a) direct verification of the existence and identity of the natural person with the direct identification and the physical presence of a person on the basis of the enclosed document,

b) verification of existence and identity of the natural person subject of the certification by identification in the physical presence of the person, carried out at the Notary Office, based on the presented Application for certification, in accordance with Article 60. Identification and Article 77 Verification of signature of the Public Notaries act [10], and which fulfils the requirements of Article 24 (1) (a) of Regulation (EU) No 1095/2010. 910/2014 [1],

c) indirect verification that provides the same level of verification of the existence and identity as direct identification and the physical presence of a person,

d) indirect verification of the existence and identity of the person is conducted by verifying person's certificate used for creating qualified electronic signature issued upon direct verification of the existence and identity of the person,

e) indirect verification is used by using electronic identification means of level 'substantial' or 'high', pursuant to Article 8 of the *Regulation (EU) No. 910/2014* [1], used for issuing qualified certificates,

f) verification of organization's existence, name and status on the basis of the enclosed documents or excerpts,

g) verification of person's affiliation with organization on the basis of the enclosed documents,

h) verification of person's authorized representative status in relevant parent registers and, if required, on the basis of the enclosed documents or excerpts,

i) verification assessing whether collected information correspond to those stated in the enclosed documents,

j) authenticity verification for the enclosed documents and excerpts,

k) determining whether there is a basis for the issuance of identification certificate and/or signing certificate,

l) verification on accepting the Policy Disclosure Statement and conditions for providing certification services.

Information verification on natural persons can be performed using on-line electronic services provided by official national or EU registers, or through AKD RA system.

In case of inconsistency between data provided in documentation and application forms and data acquired from official registers via on-line services, AKD RA accepts data acquired from official register via on-line service as valid and immediately informs the person.

3.2.4. *Non-verified subscriber information*

Persons can be asked for common name that legal person - creator of seal will represent itself.

The RA (offices) does not verify mobile phone number, e-mail address and additional contact information, as a person is responsible for their accuracy. E-mail address or mobile phone number can be verified when accessing private web portal when signatory or authorized representative is using AKD mPotpis service for remote signature creation.

3.2.5. *Validation of authority*

If natural person's affiliation with organization is indicated in application for issuing certificates to natural persons, RA officers must verify in the official register in charge for the organizations

or legal persons, that signatory on the enclosed document issued by the organization (see section 3.2.3.1, g.) is the same person that is certified and legal representative of organization.

When application for issuing certificates for electronic seal is received, the signatory's on the enclosed documents identity is determined and verified according to sections 3.2.3.1 and 3.2.3.2, in order to check if the signatory is the same person that is certified as authorized representative of legal person.

Additionally, authorization of authorized representative is checked in the parent register for legal persons. If the person authorized representative is not the person named as authorized legal representative in the parent register, the legal authorization is required for authorized representative person is required.

Identity of persons with legal authorization is established and verified using the same procedures as used for the legal representative.

Validation of authority can be performed using on-line electronic services provided by official national or EU registers, or through AKD RA system.

In case of inconsistency between data provided in documentation and application forms and data acquired from official registers via on-line services, AKD RA accepts data acquired from official register via on-line service as valid and immediately informs the representative of legal person.

3.2.6. *Criteria for interoperation*

No stipulation.

3.3. Identification and authentication for re-key requests

3.3.1. *Identification and authentication for routine re-key*

Rules of identification and verification of the identity upon issuance of the new pair of keys referred to in section 3.3.2 are applied.

3.3.2. *Identification and authentication for re-key after revocation*

Upon issuance of the new pair of keys, the following security measures and procedures apply:

a) The rules for identity validation upon issuance of the new pair of keys are the same as the rules of initial identity validation (section 3.2.3).
b) Information's and documents collected in the initial identity verification may be used upon issuance of the new pair of keys.
c) Persons submitting requests due the name or surname or organization name modification must provide public personal identification document or excerpt with the modified name or surname or organization name, which person is obliged to use in legal transactions. Modifications of name or surname or organization name can be verified using on-line electronic services provided by official national or EU registers, or through AKD RA system.

3.4. Identification and authentication for revocation request

Identity verification of the person is carried out upon submitting a request for revocation. With the identity verification of person submitting the request also the authorization of person submitting the request is determined.

If a revocation request is submitted at the RA office identity of person is established with the direct identification and the physical presence of a person on the basis of the adduced personal identity document.

When submitting revocation requests for certificates for electronic seal and certificates issued to persons affiliated with organization when the person who is submitting the request is not the subject of certification, identity verification of authorized or legal representative is carried out.

Identity verification and authentication of persons can be carried out by validating and verifying qualified electronic signature of the person or authorized representative created when the request is signed and submitted in electronic form.

Upon submitting a request for certificate suspension, the identity verification may be carried out remotely, by electronic means using the appropriate method of authentication.

The acceptable remote method of authentication includes authentication to private part of web portal and verification of requested action via link provided in the e-mail. With successful authentication to web portal and verification of requested action the person has submitted a valid request for certificate suspension.

Data for authentication to web portal are delivered to the user according to section 6.4.

Identity of person submitting the request in electronic form may also be established and verified by validating and verifying person's qualified electronic signature created when signing request in electronic form.

4. Certificate life-cycle operational requirements

4.1. Certificate Application

4.1.1. *Who can submit a certificate application*

Application can be submitted by adult natural person who is a certification subject, legal representative of the organization (subscriber) on behalf of certification subject that is affiliated with organization and authorized representative on behalf of the legal person – creator of seal for certificates for electronic seal.

4.1.2. *Enrolment process and responsibilities*

Information about the enrolment process and submitting a certificate application is available to public on the web portal https://www.certilia.com and in RA offices.

The following rules are prescribed:

a) The certificate application is submitted via RA: at RA offices or via on-line service.
b) The certificate application is submitted on the prescribed form which is available in the RA offices, web portal https://www.certilia.com or via on-line service.
c) The persons are required to confirm that the personal identification data at the time of submission of an application are complete and accurate by signing the certificate application.
d) By submitting the certificate application, the natural persons and/or legal person representatives confirms the acceptance of conditions for providing certification services (PDS).
e) Confirmation of payment fees for requested services is required, except in the case of application for certificates for remote signing that are issued to adult eOI users in accordance with the amendments to the Identity Card Act (Official Gazette 144/2020) [54].

4.2. Certificate application processing

4.2.1. *Performing identification and authentication functions*

The following rules apply:

a) The identity of natural persons is confirmed in the procedures specified in point 3.2.3.
b) Identification and authentication of the RA officers and CA personnel is performed as defined in section 3.2.5.
c) The procedures related to the verification of RA officers and CA personnel are defined in section 5.3.
d) RA may verify the person's data indicated in certificate application via on-line services provided by official national registers, or through AKD RA system, of which persons are informed promptly. In case of inconsistency of data indicated in certification application and the data acquired from the on-line service RA may use the latter personal data as valid.
e) In the event of data inconsistency, as described above (section 4.2.1 c), RA may replace personal data indicated in certificate application, specified in section 3.2.3 and 3.2.2, with the personal data acquired on-line from official national registers.

4.2.2. *Approval or rejection of certificate applications*

The RA or on-line service decide on the approval or rejection of the certificate application.

Certificate application will be rejected if:

a) there is a suspicion that the information gathered about natural or legal persons are not accurate, complete or reliable,
b) information verification process concerning natural persons cannot be successfully carried out according to the section 3.2.3.2,
c) information verification process concerning legal persons cannot be successfully carried out according to the section 3.2.2.2,
d) information verification process concerning legal persons, when person is affiliated with organization, cannot be successfully carried out according to the section 3.2.2.2,
e) person or representative of legal person does not accept data acquired via on-line service, or through AKD RA, from official national registers as valid,
f) the certificate application has been retroactively withdrawn, or
g) it has been determined subsequently following the submission of the application that certificate application has not been authorized.

If the certificate application has been rejected, the Subscriber enquires orally about the reasons for the rejection of the application.

Certificate application is approved if the identity of the natural person is confirmed according to the section 3.2.3, and/or the identity of the legal person is confirmed according to the section 3.2.2.

All submitted applications are entered into the information system of the RA which meets the security requirements set out in sections 6.5 and 6.6.

Forms, contracts and all printed documentation that are collected during the application procedure are stored and kept in accordance with the rules set out in section 5.5.2.

Applications submitted in electronic form via on-line service are stored and kept in AKD RA system in accordance with the rules set out in section 5.5.2.

The protection of the personal data collected in the registration process of natural persons is carried out in accordance with the rules set out in section 9.4.

4.2.3. *Time to process certificate applications*

Certificate applications are processed within 7 work days from the submission of application.

4.3. Certificate issuance

4.3.1. *CA actions during certificate issuance*

a) Certificates may be issued to natural and legal persons solely after all data has been validated and verified and certificate application has been authorized and entered in to the AKD RA system.

b) After the entering the certificate application in the information system of the RA, data necessary to complete the application is sent to the CA through a secure communication channel.

c) The CA does not verify the completeness, accuracy and uniqueness of the received data for the issuance of the certificates, but it relies on the verification carried out in the RA.

d) Certificates may be issued to persons solely on the basis of the certificate application received from the RA.

e) When certificates are issued on the QSCD and the QSCD is issued to natural person or authorized representative the manufacturer produces the QSCD with a chip and a printed design or installs the certificate and primary key on a certified QSCD owned by the subject of certification.

f) The process of producing and issuing of a certificate and generating pairs of keys and their entry into the remote QSCD, their storage and usage when the qualified trusted service provider manages electronic signature creation data on behalf of the signatory or creator of seal, is carried out in a secure environment of AKD mPotpis service which meets the security requirements set out in sections 6.5 and 6.6.

g) The profile of the issued certificate must be in accordance with the requirements set out in section 7.1.

h) The CA keys, that are used to sign the certificates and keys of the person offer protection using measures and procedures, prescribed in section 6.2.

4.3.2. *Notification to subscriber by the CA of issuance of certificate*

Notifications to natural person or authorized representative about the date of issuance of certificate, collection of QSCD or delivery of certificates for remote signature creation in ADK mPotpis service are as follows:

a) direct notification by the RA officers in the RA office at the time of submitting the certificate application,

b) notification to the e-mail address or mobile phone number indicated in certificate application.

4.4. Certificate acceptance

4.4.1. *Conduct constituting certificate acceptance*

a) The certificates are delivered to the natural person – subject of certification or Authorized representative.

b) Subject of certification or authorized representative must verify the content of the certificate immediately upon receiving the certificate. If found that content of certificate is not as intended and certificate is not accepted, the person must inform AKD without delay.

c) When the certificates are delivered on QSCD, it is deemed that the person (certification subject) or authorized representative has accepted the private key and the certificate at the time of delivery of the QSCD.

d) At the time the QSCD is being collected, the person is informed of the conditions applicable for the use of the certificate and has already accepted the conditions for providing certification services (PDS) according to the section 4.1.2.

e) If the person fails to collect the QSCD with certificate within 120 days, it is deemed that the certificate was not accepted.

f) When the qualified trusted service provider manages electronic signature creation data on behalf of the signatory or creator of seal, it is deemed that the certificate is accepted at the time of first usage of certificate in AKD mPotpis service. Certificate is accepted after completion of following procedure:

   a. Signatory or authorized representative receives reference and authorization codes for generation and activation of private key and corresponding certificate. Codes are generated in AKD mPotpis service and sent to e-mail or SMS provided in certificate application.

   b. Signatory or authorized representative must authenticate to AKD mPotpis service using two-factor eID means registered in KID IDP.

   c. Certificate is registered in AKD mPotpis service by using reference and authorization code in AKD mPotpis service and setting the PIN for private key activation.

   d. Signatory or authorized representative must perform first activation of private key with PIN in AKD mPotpis service.

   e. If the signatory or authorized representative fails to perform procedure described above, a) to d), within 120 days, it is deemed that the certificate was not accepted.

g) Certificates that have not been accepted are revoked in line with the procedure described in section 4.9.3.

4.4.2. *Publication of the certificate by the CA*

Certificates of the person are not available in the public directory for the public search. AKD reserves the right to subsequently make available public search of certificates of the person, if required and under commercial terms.

4.4.3. *Notification of certificate issuance by the CA to other entities*

The information that the certificate has been issued and that the QSCD has been produced or remote certificate has been accepted in AKD mPotpis service the CA sends to the AKD RA information system through a secure communication channel.

The CA does not inform other entities regarding the certificate issuance.

The persons may deliver its certificate to other entities, when necessary.

4.5. Key pair and certificate usage

4.5.1. *Subscriber private key and certificate usage*

When the person is in the possession of key pair on QSCD and manages the keys the following rules apply:

a) An undamaged security envelope containing registration data for the web portal and the QSCD activation is delivered to the persons (certification subject) or authorized representatives.
b) Registration data for web portal and/or QSCD activation can be delivered to the persons (certification subject) or authorized representatives via e-mail or SMS provided in certificate application, if indicated in application form.

The QSCD contains:

a) signing certificate, which is a qualified certificate and is intended for the electronic signature creation,
b) certificate for electronic seal, which is qualified certificate and intended for electronic seal creation, and/or
c) identification certificate, which is an electronic identification means of high level of security and is intended for the authentication on electronic services.

When the person is in control of key pair on remote QSCD in AKD mPotpis service and keys are managed by AKD on behalf of person, the following rules apply:

a) Registration data for web portal and registration codes for certificate registration and acceptance are delivered to the persons (certification subject) or authorized representatives via e-mail or SMS provided in certificate application.

The remote QSCD can contain:

a) signing certificate, which is a qualified certificate and is intended for remote electronic signature creation, and/or
b) certificate for electronic seal, which is qualified certificate and intended for remote electronic seal creation.

Certificates issued to natural persons are the property of a subscriber and are used by certification subject for private purposes, and also for business purposes when the affiliation of the natural person to organization is verified.

Certificates issued to legal persons are the property of creator of seal and are used by authorized representative for business purposes.

Persons accepted the conditions for providing certification services (PDS) are obligated to fulfil the responsibilities indicated in section 9.6.4.

Conditions for providing certification services include:

a) Information's about certification service provider, scope of provided services and rules for providing the services,
b) Information's about certificate types, appropriate and prohibited certificate usage and certificate status related services,
c) Information's about authentication and private key activation data usage in AKD mPotpis service,
d) Representations and warranties of natural and legal persons, certification services provider and relying parties,
e) Information's regarding liability, prices, conclusion and termination of contract, etc.,
f) Data protection and confidentiality provisions,

g) Communication, complaint and dispute resolution procedures, and
h) Applicable laws and supervision procedure of certification service provider.

4.5.2. *Relying party public key and certificate usage*

The relying parties using certificates and certification services are obligated to act in accordance with conditions for providing certification service and fulfil the following responsibilities:

a) to enquire on the web portal about conditions for providing certification services, and the appropriate manner to use the certification services,
b) to independently assess and determine the appropriateness of the certificate use for the appropriate purpose,
c) to establish, before exercising trust in the certificate, that the certificate has not expired and that it is not revoked, all according to the data contained in the certificate,
d) that the verification of the certificate validity is carried out using an authorized source and reliable equipment, and
e) to verify the certificate's status of the persons and of all certificates in the certification path according to the procedures indicated in IETF RFC 5280 [38] and IETF RFC 3739 [37].

4.6. Certificate renewal

4.6.1. *Circumstance for certificate renewal*

The certificate must be renewed if the period of validity has expired.
Any renewal of the certificate means issuing of a new pair of keys (refer to section 4.7.1).

4.6.2. *Who may request renewal*

The rules indicated in section 4.1 apply.

4.6.3. *Processing certificate renewal requests*

The rules indicated in section 4.2 apply.

4.6.4. *Notification of new certificate issuance to subscriber*

The rules indicated in section 4.3 apply.

4.6.5. *Conduct constituting acceptance of a renewal certificate*

The rules indicated in section 4.4.1 apply.

4.6.6. *Publication of the renewal of certificate by the CA*

The rules indicated in section 4.4.2 apply.

4.6.7. *Notification of certificate issuance by the CA to other entities*

The rules indicated in section 4.4.3 apply.

4.7. Certificate re-key

4.7.1. *Circumstances for certificate re-key*

A new pair of keys and a new certificate is issued:

a) If the certificate must be renewed (refer to section 4.6), or
b) If the certificate must be modified (refer to section 4.8), or
c) In the case of certification revocation (refer to section 4.9).

The CA does not it reactivate the revoked certificate, but a new pair of keys and a new certificate is issued to person.

4.7.2. *Who may request certification of a new public key*

The rules indicated in section 4.1 apply.

4.7.3. *Processing certificate re-keying requests*

The rules indicated in section 4.2 apply.

4.7.4. *Notification of new certificate issuance to subscriber*

The rules indicated in section 4.3 apply.

4.7.5. *Conduct constituting acceptance of a re-keyed certificate*

The rules indicated in section 4.4.1 apply.

4.7.6. *Publication of the re-keyed certificate by the CA*

The rules indicated in section 4.4.2 apply.

4.7.7. *Notification of certificate issuance by the CA to other entities*

The rules indicated in section 4.4.3 apply.

4.8. Certificate modification

4.8.1. *Circumstances for certificate modification*

Circumstances for certificate modification include:

a) There was a modification of data contained in the certificate,
b) It was found that the information, contained in the certificate, are incorrect, or
c) Permanent loss of PIN for private key activation in AKD mPotpis service.

Any modification of the certificate means issuing of a new pair of keys (refer to section 4.7.1).

4.8.2. *Who may request certificate modification*

The rules indicated in section 4.1 apply.

4.8.3. *Processing certificate modification requests*

The rules indicated in section 4.2 apply.

4.8.4. *Notification of new certificate issuance to subscriber*

The rules indicated in section 4.3 apply.

4.8.5. *Conduct constituting acceptance of modified certificate*

The rules indicated in section 4.4.1 apply.

4.8.6. *Publication of the modified certificate by the CA*

The rules indicated in section 4.4.2 apply.

4.8.7. *Notification of certificate issuance by the CA to other entities*

The rules indicated in section 4.4.3 apply.

4.9. Certificate revocation and suspension

4.9.1. *Circumstances for revocation*

The certificate is revoked under the following circumstances:

a) An authorized request for the certificate revocation has been submitted.
b) A modification in certificate data contained in the attributes of the „Subject“ field has been reported, e.g. name or identification number of natural or legal person or certificate name.
c) Errors in certificate data or on body of QSCD are discovered during application processing, certificate issuance, QSCD personalization, security envelope personalization or other activities during certification services providing, before the delivery or acceptance of certificates.

d) A loss or malfunction of QSCD has been reported.

e) A misuse or unauthorized use of the QSCD has been reported, private key or activation data is not in solely possession of the subject of certification or authorized representative or whenever the private key compromising is possible. Private key activation PIN for remote signature creation used in AKD mPotpis service is permanently loss.

f) A cessation of previously established affiliation of the subject of certification with subscriber (organization) has been reported.

g) A cessation of validity of the certificate has been established before the expiration of the period for which the certificate has been issued for due to the death of a person or if there are no grounds according to which the certificate was issued.

h) Exceptional circumstances and an instance of force majeure occurred, including weather-related and natural disasters, landslides, floods, fire, war, acts of war, terrorism, intrusion into physical space, intrusion in an information system or civil disorders.

i) The court, public prosecution or institutions that conduct judicial or criminal investigation request a certificate revocation in order to prevent a crime.

j) It was found that the private key does not match the public key in the certificate or it was found that the data in the certificate are incorrect.

k) It was found that the certificate application was not authorized or it was retroactively withdrawn.

l) It has been established that the eOI user who, in accordance with the amendments to the Identity Card Act Official Gazette 144/2020) [54] was issued a remote certificate for signature, had his certificates revoked more than 45 days ago or a new eOI was issued with new certificates.

m) It was found that the certificate was not issued in accordance with the CPS or CP.

n) The CA certificate was revoked.

The CA certificate is revoked under the following circumstances:

a) It is prescribed by a mandatory regulatory request or standard that the technical and security characteristics of the certificate, such as a cryptographic algorithm and key length, represent an unacceptable risk for all participants indicated in section 1.3.

b) The CA private key compromising has been established.

c) When the certification service provider, due to technical, contractual or any other reason, ceases to issue certificates or ceases to provide certification services.

4.9.2. *Who can request revocation*

The certificate revocation for the certificates issued to natural persons may be requested by:

a) The natural person named as certification subject or his/her legal representative, for circumstances indicated in section 4.9.1, points a) to b) and d) to g),

b) Legal representative on the behalf of the subscriber, for circumstances indicated in section 4.9.1, points a) to b) and d) to g),

c) Authorized RA/LRA personnel, for circumstances indicated in section 4.9.1 points a) to g) and l),

d) Authorized CA personnel and approved by the PMA for circumstances indicated in section 4.9.1 points i) to o),
e) PMA, for circumstances indicated in section 4.9.1 and
f) CA, TSU and OCPS revocation request is initiated and approved by the PMA.

The certificate revocation for the certificates issued to legal persons may be requested by:

a) Authorized representative on the behalf of creator of seal, for circumstances indicated in section 4.9.1, points a) to b) and d) to g),
b) Authorized RA/LRA personnel, for circumstances indicated in section 4.9.1, points a) to g),
c) Authorized CA personnel and approved by the PMA, for circumstances indicated in section 4.9.1. points i) to o),
d) PMA, for circumstances indicated in section 4.9.1, and
e) CA, TSU and OCPS revocation request is initiated and approved by the PMA.

4.9.3. *Procedure for revocation request*

The following procedures for the certificate revocation request are applied:

a) Clear instructions concerning procedures to be taken in case of occurrence of the reason for the certificate revocation available on the web portal are indicated in section 4.1.9.
b) Certificate revocation request is submitted:
    a. in the RA offices during work hours,
    b. on-line on the private web portal for submitting certificate suspension requests, according to procedure specified in section 4.9.15 . Service is available 24/7 or
    c. via other electronic communication channels by which identity validation and verification of person submitting the request can be determined, according to rules set out in section 3.4.
c) The certificate revocation request is accepted only if the identity of the applicant is determined in accordance with the rules for identity validation in line with the section 3.4.
d) Accepted revocation requests are entered in AKD RA system by RA officers.
e) Revocation requests are forwarded from AKD RA system for further processing to the CA.
f) CA, TSU and OCSP revocation request is initiated and approved by the PMA.

4.9.4. *Revocation request grace period*

The certificate revocation request should be submitted within the shortest time possible from the occurrence of the reason for revocation.

If there was a modification of the data named in the certificate (e.g. name or identification number of natural or legal person), the person, creator of seal or authorized representative or

subscriber is required to request a revocation within the shortest time possible from the date the modification occurred.

4.9.5. *Time within which CA must process the revocation request*

The following rules are applied:

a) Immediately after having received the information on the occurrence of the reason for the certificate revocation, an investigation of the problem commences, and a decision concerning certificate revocation or some other activity to be carried out is reached within 24 hours.

b) In reaching a decision concerning certificate revocation the following is considered:
   - authenticity and reliability of the received information concerning the occurrence of the reason for the revocation,
   - number of certificate revocation requests,
   - relevance and authorization power of the revocation request's source,
   - legal obligations, and
   - consequences that may result during certificate revocation or its non-revocation.

c) If the decision on acceptance of the revocation request has been reached, the CA processes the request within 60 minutes and publicly publishes the information concerning certificate revocation.

d) If there is no possibility for the revocation request to be accepted within 24 hours, the certificate's status changes.

e) The system for the certificate revocation has a reliable source of time and it provides a valid record of the date and time that is synchronized with the UTC at least once a day.

f) The CA provides a secure environment in which the certificate revocation procedure is performed, as indicated in sections 6.5, 6.6 and 6.7.

g) Revoked certificates cannot be reactivated and their status cannot be modified or changed.

4.9.6. *Revocation checking requirement for relying parties*

The relying party should check the status of the certificate before trusting the certificate.

Information verification services concerning the certificate's status are available on-line (pursuant to clauses 4.9.9 and 4.9.10 herein).

Should the relying party, for any reason at a particular moment, fail to obtain information concerning the certificate's status, and then it is obligated to either reject the use of the certificate or assume risk and responsibilities, and bear consequences for the use of a certificate whose status has not been confirmed.

4.9.7. *CRL issuance frequency*

The CRL is issued according to the following rules:

a) KIDCA obliges to issue a CRL at least 1-time within 24 hours.

b) The new KIDCA CRL list is issued at least 10 minutes before the expiration of the validity of the CRL.

c) Under regular work conditions, the KIDCA generates and issue the CRL every 12 hours.
d) The period of the validity for KIDCA CRL is 24 hours from the time of the issuance of the CRL.
e) AKDCA CRL is valid for 90 days after the CRL issuance.
f) In the case of the CA certificate revocation, the CRL list is issued within 24 hours.
g) If the validity period of the certificate that is revoked and present on the CRL list expires, the certificate may be removed from the CRL list.
h) In order to ensure the availability of the CRL in accordance with the rules set forth in this chapter, the timeliness for CRL issuance is monitored.

4.9.8. *Maximum latency for CRL*

The maximum allowed latency from the moment of CRL issuance to the moment of CRL publication in the public directory or on-line is 10 minutes.

4.9.9. *On-line revocation/status checking availability*

AKD PKI enables on-line verification of certificate status through the OCSP service.

The AKD OCSP service is available over HTTP at the address published in the Authority Information Access field of each certificate.

The OCSP response is consistent with IETF RFC 6960 [35] and IETF RFC 5019 [40].

4.9.10. *On-line revocation checking requirements*

The on-line certificate's status verification via OCSP service is enabled according to the following rules:

a) The KIDCA refreshes the information that is published via OCSP at least every 24 hours.
b) Under regular work conditions, the KIDCA refreshes the information that is published via OCSP immediately following receipt of the certificate revocation request.
c) The validity of the response by the KIDCA OCSP service is a maximum of 24 hours.
d) The AKDCA refreshes the information that is published via OCSP at least every 90 days.
e) In the event of the certificate revocation of the subordinate CA, the AKDCA refreshes the information that is published via OCSP within 24 hours.
f) Every response of the OCSP service is signed electronically by the certificate which is issued by the same CA that issued the certificate for which the certificate's status verification is requested.
g) If the OCSP service receives a request for the certificate's status verification, which has not yet been issued, it does not respond with a status "good".
h) In order to ensure the availability of the service in accordance with the rules set forth in this chapter, the operation of the OCSP service is continuously monitored.

4.9.11. *Other forms of revocation advertisements available*

The AKD provides the certificate's status verification to the registered persons in the private section of the web portal, which is available on-line at the address https://www.certilia.com.

The AKD may provide OCSP service, with higher level of availability, to interested parties with separate contract and under commercial terms.

4.9.12. *Special requirements re-key compromise*

The CA, in accordance with section 4.9.1, revokes the certificate if the private key has been confirmed as compromised.

4.9.13. *Circumstances for suspension*

Circumstances for suspension of certificate include:

a) An authorized request for the certificate suspension has been submitted.
b) A disappearance of the QSCD has been reported or suspicion of cessation of possession of the private key and/or activation data.
c) There is a possibility that the submitted certificate revocation request is retroactively withdrawn.
d) There is no possibility for the certificate revocation request to be submitted in a timely manner for any reason, indicated in section 4.9.1.
e) There is no possibility for the decision concerning certificate revocation to be reached when the consequences, which may result due to the certificate non-revocation, are significant.
f) In case of non-fulfilment of contractual obligations by the recipient of the certification services.

Circumstances for the withdrawal of the suspension of the certificate include:

g) An authorized request for the withdrawal of the suspension of the certificate has been submitted,
h) QSCD has been found or cessation of circumstances for suspension indicated in point b)
i) Cessation of the circumstances due to which a suspension of the certificate has been requested.

4.9.14. *Who can request suspension*

Request for suspension or withdrawal of the suspension of a certificate may be submitted by:

a) Person subject of certification (or his/her legal representative) or authorized representative or legal representative of legal person or organization,
b) Others – any natural or legal person via RA.

4.9.15. *Procedure for suspension request*

Clear instructions concerning procedures to be taken in case of occurrence of the reason for the certificate suspension available to persons on the web portal are indicated in section 4.9.13.

The following rules are applied:

a) The subjects of certification submit suspension request for their certificate:
   - in the RA offices during work hours, or
   - remotely using electronic on-line services for the certificate suspension.

b) Other persons submit suspension request for their certificate:
   - in the RA offices during work hours.

c) The electronic on-line service for the certificate suspension is available continuously 24/7. Authentication with two-factor eID means registered in KID IDP is required.

d) The certificate suspension request submitted by subject of certification or authorized representative or legal representative is accepted only if the identity of the applicant is determined in accordance with the rules for identity validation in line with section 3.4.

e) The certificate suspension request submitted in RA office by any other person is accepted only if QSCD is presented to RA officers.

f) The maximum amount of time that can elapse between receiving the request for suspension or withdrawal of the suspension of a certificate and the publication of the status is 24 hours.

g) If the revocation request is granted, it is forwarded for further processing by the CA.

h) The maximum amount of time that can elapse between receiving the request for suspension or withdrawal of the suspension of a certificate and the publication of the status is 24 hours.

i) The system for the suspension or withdrawal of the suspension of a certificate has a reliable source of time and it provides a valid record of the date and time that are synchronized with UTC at least once a day.

j) The CA provides a secure environment in which the procedure for the suspension or withdrawal of the suspension of a certificate is performed.

4.9.16. *Limits on suspension period*

In the event of cessation of the circumstances for the suspension of a certificate, indicated in section 4.9.13, it is possible to request the withdrawal of a request for certificate suspension within 8 days.

If the withdrawal of the suspension of a certificate is not requested within 8 days from the submission of the request for suspension, the suspended certificate is revoked.

4.10. **Certificate status services**

4.10.1. *Operational characteristics*

The following rules are applied:

a) The CA provides on-line CRL verification services via HTTP protocol and OCSP service for the certificate's status verification.
b) The information concerning revoked certificates with the expired validity (Expiry Date) is deleted from the publicly available CRL services, but remains archived at the CA and available via OCPS service.
c) Public address for status verification using the OCSP service: http://ocsp-kidca.id.hr/kidca.
d) Public addresses to retrieve the CRL on the web server: http://crl1.id.hr/kidca.crl and http://crl2.id.hr/kidca.crl.
e) In case of differences in certificate status, the OCSP service response is more up-to-date and accurate and should be implemented.

4.10.2. *Service availability*

The KIDCA provides:

a) AKD provides an uninterrupted provision of its services and availability of its critical services 24 hours a day, 7 days a week. This includes:
   - on-line service for certificate application,
   - revocation, suspension of certificate and suspension withdrawal service,
   - verification of the current certificate's status,
   - AKD mPotpis service for remote signature creation, and
   - dissemination services.
b) The response time for CRL and OCSP verification of the current certificate's status in a maximum of 10 seconds.
c) In order to shorten the processing time and certificate's status verification it is recommended to use the OCSP protocol.
d) In the case of system failure, the service is available within the shortest time possible and in accordance with the positive business practices.

Other KIDCA services are available during work hours of RA offices.

4.10.3. *Optional features*

Not foreseen.

4.11. **End of subscription**

The period of the certificate validity is set out in section 6.3.2.

The certificate ceases to be valid before the expiration of the validity if revoked at an earlier time.

If the subscriber cancels the certification agreement before the certificate expires, AKD will revoke all certificates to which this agreement applies.

4.12. **Key escrow and recovery**

The CA does not escrow or recover the private keys of persons.

4.12.1. *Key escrow and recovery in AKD mPotpis Service*

Private keys used for remote signature creation are stored in secure environment of remote QSCD in AKD mPotpis service which meets the requirements ISO IEC 15408 [43] *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5* and rules set out in Annex II *Regulation (EU) No. 910/2014* [1].

Recovery of private keys in AKD mPotpis service is not available to persons.

5. Facility, management, and operational controls

5.1. Physical controls

The AKD has a documented and implemented policy of physical security, and controls the physical access to all data and components related to the provision of the trust services.

Activities of assessment and combating the risk are conducted, and in order to prevent the failures and interferences in the provision of services, and an unauthorized physical access to the facility, areas and information, security measures are established in accordance with the section 11 of the ISO/IEC 27002 [46].

5.1.1. *Site location and construction*

The information system of the CA, the environment used for managing the electronic signature creation data on behalf of the signatory and the manufacturing facilities where the QSCD (smartcard) are produced and individualized and remote QSCD used in AKD mPotpis service is operated are located within a business complex of the AKD.

The AKD's facilities are massive structures, and the gate, the main entrance and vulnerable points (windows, roofs, fences, accesses for vehicles and delivery) are constructed to provide an adequate protection against unauthorized access.

According to the type, purpose and significance of the activity which is being carried out there, all AKD's activities are organized into security zones: access, administrative, limited, active and secure zone.

Security zones are separated by physical barriers, and protection measures that are being applied in the security zones are proportional to risk factors.

The CA systems and production facilities are located in active and secure zone (high-security area) where the most stringent physical, technical and procedural protection measures are being applied.

5.1.2. *Physical access*

Sophisticated technical protection measures are implemented to provide the protection of the perimeter and the interior areas. The protection measures include physical barriers, video surveillance, access control, fire protection system and anti-robbery protection.

Security guards are always be present at the facility 24/7, and the whole business complex of the AKD is being continuously monitored from the central control system 24/7.

All information systems functioning as the service providers are located in the computer room in the high-security area, and access to the areas are limited to the authorized personnel carrying out administrative activities and supervision.

Access control to facilities and areas of the AKD is granted using the ID card.

Physical access to the high-security areas is granted using biometric identification methods.

Physical access to the information system of the CA is carried out solely with the dual control.

The technical protection information system records all activities of the access rights usage and any changes to the access control system.

Methods of assigning access rights to the areas are carried out in accordance with the documented internal rules.

5.1.3. *Power and air conditioning*

The computer room area where the information infrastructure is located is properly conditioned. All equipment is connected to the source of uninterrupted power supply, and in the case of a power failure in the city's energy network for a longer period of 48 hours, a standby generator is provided.

Air conditioning system and power supply are monitored and regularly maintained, and the system's capacities are sufficient for the implementation of the operational activities.

5.1.4. *Water exposures*

Facilities and areas where the information infrastructure is located and where the provision of certification services is carried out are located in a place that is secure against flooding.

5.1.5. *Fire prevention and protection*

In the area of the secure zone, the adequate fire protection measures are implemented in accordance with the current legislation.

The fire protection system consists of:

a) automated systems for fire detection and firefighting,
b) fire extinguishers for the firefighting of the initial fires,
c) hydrant network, and
d) ancillary equipment and devices for the evacuation and rescue.

5.1.6. *Media storage*

All media are properly labelled and stored in security containers, and their handling is defined by the internal security rules.

The physical access to the security containers and all of the physical equipment associated with the cryptographic activities such as media, cryptographic devices, physical keys, smart cards, tokens, passwords etc. is carried out solely under the dual control.

In order to prevent an unauthorized disclosure, modification, relocation or destruction of the information stored on the media, security measures are established in accordance with the chapter 8 of the ISO/IEC 27002 [46].

©AKD 2023

5.1.7. *Waste disposal*

All print and electronic media for which the need for archiving in a secure manner is not required are destroyed according to the methods providing reasonable assurance that the destroyed data cannot be recovered.

The destruction of the cryptographic media is carried out by the commission in the presence of at least 2 persons.

The destruction of the physical equipment associated with cryptographic activities is carried out using shredding machines.

The security level of the shredding machines used for the destruction is determined according to the degree of the data confidentiality for which it is used, and which is determined according to the internal procedures.

5.1.8. *Off-site backup*

Backups are kept on dislocated sites in the areas and security containers that comply with the same or higher security requirements.

5.2. Procedural controls

5.2.1. *Trusted roles*

The authorized employees who are involved in the implementation of the certification activities are granted the appropriate trusted roles with clearly defined responsibilities and authorizations pursuant to the ETSI EN 319 401 [13], CEN TS 419 261 [31] and ETSI TS 119-431-1 [23], CEN EN 419-241-1 [32].

The trusted roles include, but are not limited to:

a) **Security administrators** are responsible for the implementation and enforcement of the security rules in practice.
b) **RA officers** are responsible for verification of data and data preparation that must be carried out when issuing certificates and granting approval for certificate applications.
c) **Revocation officers** are responsible for the implementation of the change of status of certificates.
d) **Information system administrator** is responsible for the installation, configuration and maintenance of information systems.
e) **Operators** are responsible for the performance of the daily activities on information systems and to save and restore data when needed.
f) **System Auditors** are responsible for the daily review of the reports concerning the operation of the system, audit logs and archives when needed.

Trusted roles related to the management of the cryptographic keys include:

g) **Key Custodians** are responsible for all activities related to the management of the cryptographic keys.

h) **Key Managers** are responsible for keeping the cryptographic key components and other security materials and media they are entrusted with.

5.2.2. *Number of persons required per task*

In order to protect security-sensitive functions and information, the following principles are strictly complied with:

a) Split knowledge: each out of two or more different persons have only one component of data (e.g. of the cryptographic key) so that no person is able to independently access or use the information.

b) Dual control: two or more different persons must perform an activity together so that no person is able to independently perform a security-sensitive function.

The principle of the dual control is applied on the logical and physical level.

5.2.3. *Identification and authentication for each role*

All information equipment is configured in such manner which enforces a strict compliance with the documented internal security rules and prevents the implementation of the activities without prior authentication of authorized persons.

The authentication is achieved with at least a user account and password, and always when necessary or when a technical support is available, a multi-factor authentication is made whenever possible.

Identification and authentication of the RA officers and CA personnel are carried out according to the following rules:

RA officers:

a) Before assigning tasks to the RA officers, verification is made, as well as the unambiguous validation of the identity and reliability of the officers.

b) Two-factor authentication (identification certificate on smartcard issued by KIDCA) is used in the authentication process of the officers in the information system of the AKD RA.

c) In order to prevent conflict of interest, the signatory and the officers of RA must not be the same person. The RA officer who require the certificate, do not identify himself/herself nor enter the request for the issuance of his/her own certificate in the information system of the RA.

CA personnel:

a) Upon assigning trusted roles to the CA personnel, it is verified whether the candidates are reliable and suitable and whether they are permanently employed at the CA.

b) During the ceremony of generating the CA key, the public notary conducts a formal process of identification of all participants of the ceremony and the physical presence of a person on the basis of the adduced document.

c) When issuing certificates for CA, TSU or OCSP service, it is verified in collaboration with the human resources, whether the administrator of the cryptographic key is permanently employed at the CA.

©AKD 2023

d) The access to the information system of the CA is enabled solely with the dual control.
e) A software module that performs an automated collection, verification and sending of the requests to be processed, authenticates itself to the information system of the CA using SSL client authentication.

5.2.4. *Roles requiring separation of duties*

Upon assigning trusted roles, the principles of segregation of duties are strictly complied with in order to prevent a potential conflict of interest and misuse of the authority.

The following rules are applied:

a) The person who authenticates himself/herself as a security administrator or an officer for the revocation or an RA officer may not have the authorizations of a System Auditor.
b) The person who authenticates himself/herself as an information system administrator or System Operator may not have the authorizations of a System Auditor or a security administrator.
c) The person who authenticates himself/herself as an RA officer or a System Auditor may not have the authorizations of a security administrator, an information system administrator or an operator.
d) The security administrator, information system administrator or System Operator may have the rights for the reading of audit logs that are assigned to the System Auditor if necessary.

5.3. Personnel controls

5.3.1. *Qualifications, experience, and clearance requirements*

When employing, the AKD conducts a strict selection procedure, and standard procedure of employment including the following verification:

a) professional qualifications,
b) previous employments,
c) criminal records,
d) medical fitness, and
e) credit/financial capacity in accordance with legal regulations.

All employees sign an employment contract and undertake to comply with the established security rules.

Members of PMA and all authorized persons to whom a trusted role are been assigned to and which are involved in the implementation of the CA's activities are permanently employed at the AKD and have no business relationship with other certification service providers.

5.3.2. *Background check procedures*

When assigning roles and selecting employees that will be involved in the implementation of the certification activity, a formal process to assess the suitability of the employee for a specific role are performed according to the predefined criteria is carried out.

The employee is not entrusted with the implementation of the certification activity if one of the following facts is determined:

a) misrepresentation or falsification of data,
b) unfavourable or unreliable data on professional qualifications,
c) established criminal activity or criminal conviction,
d) lack of financial responsibility, and
e) acting contrary to internal security rules.

When selecting employees for roles related to the management of cryptographic keys, it is strictly considered that the employees are employed in various organizational units of the AKD.

5.3.3. *Training requirements*

All employees to whom a trusted role is been assigned to and who is involved in the implementation of the CA's activities have relevant qualifications, knowledge and experience, necessary to perform the role entrusted to them.

The AKD ensures necessary expert knowledge, experience and qualification related to understanding the concepts of the PKI infrastructure, cryptographic algorithms and devices, and information security.

The AKD provides professional training for its employees in order to obtain an adequate knowledge needed to perform the business functions of the employees.

In addition, employees who are involved in the implementation of certification activities are adequately informed about the rules of conduct before they assume their obligations.

The aim of the informing includes the following:

a) to provide an understanding of the security requirements and internal security rules,
b) to ensure awareness to the employees concerning their role and responsibilities in the business process,
c) to enable the identification of the security problems and incidents and responding in accordance with the needs of the business function, and
d) to ensure the implementation of the plan of continuity of business.

5.3.4. *Retraining frequency and requirements*

The program of the professional training of employees is carried out continuously, especially in the event of significant changes.

Informing the employees about the rules of conduct is carried out during the introduction of the new internal rules and in the event of significant changes, at least once a year.

5.3.5. *Job rotation frequency and sequence*

The employees to whom trusted roles have been assigned in relation to the management of cryptographic keys are subjected to the suitability re-assessment every three years according to the section 5.3.2.

5.3.6. *Sanctions for unauthorized actions*

A strict disciplinary action is taken against employees who do not comply with the established and documented procedures.

5.3.7. *Independent contractor requirements*

Independent contractors do not participate in the implementation of the CA's activities and are assigned no trusted roles.

The requirements for the visitors, consultants and independent contractors involved in the implementation of the system maintenance are described in internal procedures.

5.3.8. *Documentation supplied to personnel*

The documentation necessary to perform everyday tasks, including internal security rules, procedures and work instructions as well as the specific manufacturer's instructions for the system administration and maintenance are made available to all employees involved in the implementation of the activities by CA.

5.4. Audit logging procedures

5.4.1. *Types of events recorded*

Audit logs are generally available in electronic form, and information systems create them automatically. Where it is not possible to provide audit logs in electronic form, written evidence of the fulfilment of the security requirements, set forth in this document, are provided.

Types of audit logs include:

a) logs on the management of the certificate's life-cycle, which include, but are not limited to:
   - user registration,
   - access to on-line service for application request submitting,
   - certification services,
   - certificate registration in AKD mPotpis service,
   - data preparation and QSCD creation,
   - delivery of registration and activation data by e-mail or SMS,
   - access to AKD mPotpis service,
   - revocation, suspension, withdrawal of the suspension of a certificate, and
   - issuance and publication of the CRL.

b) logs on the management procedures of the cryptographic keys in KIDCA systems and AKD mPotpis service, which include, but are not limited to:
   - key generation,
   - key activation,
   - key distribution,
   - key loading,
   - key storage,
   - key usage,
   - key backup/recovery and
   - key destruction.

c) logs on the system administration and maintenance, which include, but are not limited to:
   - application starting and stopping,
   - monitoring the system's operation (alerts, alarms, downtimes, errors, use of resources, etc.),
   - configuration changes of critical systems,
   - rescue and recovery of data,
   - data access rights, etc.

Audit logs are sufficient in order to perform the monitoring or in order to adequately investigate the unauthorized use of the information system, should the need arise.

Audit logs contain at least the following data:
- user identification,
- type of the event,
- date and time of the event,
- successful and unsuccessful events,
- the origin of the event, and
- data, system components or resources that have been accessed.

5.4.2. *Frequency of processing log*

Storage, protection and processing of audit logs are carried out in real time with automatic alarming for the occurrences of security events for all critical activities.

Periodic control is carried out for less critical activities.

5.4.3. *Retention period for audit log*

Audit logs for all critical systems are copied, protected and kept on-line for at least three months.

Audit logs related to activities of system administration and maintenance are kept for at least one year.

Audit logs related to the management of the certificate's life-cycle and the management of cryptographic keys are archived in accordance with the archiving rules, described in section 5.5.

5.4.4. *Protection of audit log*

Audit logs are adequately protected and credible and may be presented as material evidence in possible subsequent court proceedings. This includes at least the following protection mechanisms:

a) All system clocks and times are mutually harmonized so that audit logs contain a valid record of the date and time.
b) Confidential data are exempt or are masked so that they do not be included in the audit logs.
c) A cryptographic protection of integrity of all critical audit logs is implemented to be protected from any kind of modification or deletion.
d) Unauthorized access to the audit logs is prevented.
e) System configuration that deactivates the centralized log management system is enabled.
f) System administrators are not be allowed to modify or delete less critical audit logs that are not be included in the log management system.

5.4.5. *Audit log backup procedures*

Regular and automated activities related to the creation of the audit log backups are established.

Different methods for the creation of backups are applied on a daily, weekly, quarterly or annual basis.

The procedure of recovering data from the backup is familiar, tested and reliable and provides data recovery within a reasonable time.

5.4.6. *Audit collection system (internal vs. external)*

The log management system that performs an automatic storage, protection and processing of audit logs in real time are established.

Audit logs of all critical systems are included in the log management system, while less critical logs are collected by manual or partly manual procedures.

5.4.7. *Notification to event-causing subject*

The log management system performs an automatic processing of audit logs in real time and it performs automatic alarming in the case of the occurrences of security events for all critical activities.

The AKD shall, if necessary, notify the entities that caused the recording of the audit log in the information system.

5.4.8. *Vulnerability assessments*

A system vulnerability analysis is performed using approved software tools for all information systems in high-security areas.

An external vulnerability analysis is performed periodically, and internal analysis is performed in the event of significant configuration changes.

Immediately after the discovery of the vulnerability, activities are undertaken to address them.

5.5. Records archival

5.5.1. *Types of records archived*

All activities related to the management of the certificate's life-cycle are archived, which include, but are not limited to:

a) data on persons collected in the registration process and accompanying documentation,
b) certificates and information on certificate application processing procedures,
c) data on the procedure of production, distribution and delivery of the QSCD,
d) data on procedure of generation and distribution of registration codes and activation data,
e) records of authentication to on-line service for submitting certificate application request,
f) records of authentication to on-line service for certificate management,
g) records of certificate registration and private key activation in AKD mPotpis service,
h) records of revoked certificates and data on the application processing procedures for revocation, suspension and withdrawal of the suspension of a certificate,
i) data on the issuance and publication of the OCSP,
j) audit logs related to the management of the certificate's life-cycle, and
k) audit logs related to the management of cryptographic keys, and.

5.5.2. *Retention period for archive*

All archived data and documentation stated in the section 5.5.1 are kept for at least 10 years after the expiry of certificate validity.

5.5.3. *Protection of archive*

The following measures of protection are applied:

a) The archival media are stored in an adequately secured place, and the access right to archival data is granted only to authorized persons.
b) Log integrity protection against any kind of modification, such as cryptographic protection and storage on the write-once media are implemented.
c) Protection measures from the media being deleted are implemented, and at least 2 copies of the media, that are stored in different locations, are created.
d) Media with archival data are checked from time to time and copied to other media in order to ensure protection against ageing or technological obsolescence.

The AKD, as the creator and owner of the public archival and registry material, acts in accordance with the provisions of the Archival Materials and Archives Act (Official Gazette 61/2018).

5.5.4. *Archive backup procedures*

Archive backup procedures are performed in the protected area, and backup archives are stored in another location.

5.5.5. *Requirements for time-stamping of records*

Not applicable.

5.5.6. *Archive collection system (internal or external)*

Archive collection is performed internally regarding the types of records.

The collection and archiving of data and documentation that is generated in the registration process of persons in the external RA are regulated by the separate contract.

5.5.7. *Procedures to obtain and verify archive information*

The procedures to obtain the data from the archive are managed by the professionally qualified employee in charge of the archives.

Verification of the data from the archives is carried out depending on the method applied for the data integrity protection.

5.6. Key changeover

Before the expiry of the validity period of the CA certificate, the certification authority ceases to issue certificates, change the CA key and start to issue certificates using the new changed CA key.

The change of the CA key is planned and carried out in a timely manner, taking into account:

- that the validity period for each certificate issued is always be shorter than the validity period of the CA certificate that issued the latter, and
- that the cryptographic algorithms and parameters is always be suitable for use and in accordance with the recommendations referred to in the ETSI TS 119 312 [21].

The procedure concerning the change of the CA key is carried out according to the procedure of generating the key, which is set forth in section 6.1.1.

The new CA key is available to all participants of the certification procedure in the manner described in section 6.1.4.

All participants of the certification procedure are informed on generating a new pair of the CA keys, and the CA certificate is delivered to them in the same manner as the existing CA certificate, and which is described in section 6.1.4.

The trust service provider takes into account that the process of generating a new pair of CA keys does not cause any inconveniences or downtimes for persons, relying parties and other participants which are related to the provision of certification services.

5.7. Compromise and disaster recovery

5.7.1. *Incident and compromise handling procedures*

The AKD has a defined and well-documented business process and prescribed formal responsibilities in order to ensure a prompt and effective response in the event of an incident occurrence.

The incidents that are recorded and processed include corruptions of computing resources, software and/or data, and in cases of the compromise of computing resources, software and/or data, the incidents are classified and treated as security events according to the defined internal procedure.

5.7.2. *Computing resources, software, and/or data are corrupted*

Corruptions of computing resources, software and/or data that are recorded and processed include, but are not limited to:

- failure of hardware and software,
- malfunctions,
- capacity overload or service degradation,
- vulnerability and detected weaknesses in the system, and
- unavailability of the service, network or application, etc.

The AKD has an established information system that manages incidents so that they provide evidence that the incidents are being recorded and that a response to them is timely and adequately provided.

The incident management procedure is carried out through the following phases: notification, classification, escalation, investigation, resolution and clearing of the incident.

Procedures for resolving incidents include system recovery, the procedure of recovering data from the backups and replacement of the equipment when necessary.

5.7.3. *Entity private key compromise procedures*

In cases of the compromise of computing resources, software and/or data, processing procedures of security events are carried out in accordance with the internal security rules.

In the event that a compromise of the CA key has occurred, the following is followed:

a) certification of the compromised CA system shall be ceased,
b) the CA certificate revocation procedure shall be initiated,
c) person's certificate revocation procedure, issued by the compromised CA, shall be initiated,
d) persons and relying parties shall be informed via the web portal,
e) competent national and supervisory bodies and other interested parties shall be informed,

f) in the case of the suspicion of elements of a crime, the latter shall be reported to the police in order to initiate an investigation process, and
g) the process of generating a new CA key shall be initiated.

5.7.4. *Business continuity capabilities after a disaster*

The AKD has the established, documented, implemented and maintained plans and procedures in order to ensure the business continuity in the event of downtime of the IT system as well as in the case of natural disasters, accidents, large equipment failures and deliberate actions.

All employees with a defined role and responsibility for the business continuity are made familiar with their functions and obligations related to the implementation of the recovery plan.

AKD ensures high availability and continuous operation of following services:

- revocation management service,
- verification of the current certificate's status,
- dissemination services, and
- AKD mPotpis service for remote signature creation.

5.8. **CA or RA termination**

In the event of the termination of the KIDCA certification services, AKD will act according to Act on the Implementation of Regulation (EU) No. 910/2014 [2] and consult the competent national authorities on further actions to be taken related to the cessation of certification services, at least three months before planned cessation of service.

Termination procedures include, depending of the type of service that will be terminated, at least:

a) informing users and relying parties regarding possible planned cessation of certification services or specific certification service or AKD mPotpis service,
b) arrange continuation of service at another service provider, if possible,
c) withdrawal of authorizations and termination of the agreement,
d) submission of the collected documentation and archival materials,
e) cessation of certificate issuing or cessation of specific certification service or AKD mPotpis service, and
f) proper destruction of cryptographic keys and data.

6. **Technical security controls**

6.1. **Key pair generation**

6.1.1. *Key pair generation*

The following rules apply:

a) The process of initial generating of the pair of CA keys is carried out in a formal ceremony of generating CA keys organized and supervised by the PMA.
b) The ceremony is carried out in a physically secure environment in the high-security area according to defined procedures and pre-prepared technical script.
c) The ceremony is attended by employees entrusted with the roles (section 5.2), internal and external auditors, public notary and other invited witnesses.
d) Before the start of the ceremony in the presence of a public notary, a formal identification of persons and the assignment of devices, security envelopes and forms of storage are carried out.
e) The process of generating the CA key is carried out according to a pre-prepared technical script that includes the inspection of the equipment, cables, security settings and equipment parameters and every command that is entered into the information system during the implementation process.
f) The ceremony includes the creation of backup of the CA keys and other data and storage of the cryptographic materials and other contents to the defined locations.
g) During the ceremony, the records of the contents in the safe cabinets with stored cryptographic materials on primary and backup locations are certified.
h) During the ceremony, the internal and external auditors certify the technical script and the printout of the certificate by CA (certification authority) (with the public key) confirming that the process of generating the key has been carried out correctly and that the integrity of the generated keys has been ensured.
i) After the ceremony, the public notary certifies the record of implementation of the ceremony with the confirmed identity and statements of participants.
j) The certified technical script signed by all participants of the ceremony, a printout of the CA certificate, a record of the implementation of the ceremony and a video of the ceremony of generating the CA key are stored in the archives.
k) The process of generating the keys of persons and certificates for electronic seal and their entry in the QSCD is performed by the manufacturer in the physically secure environment in a high-security area.
l) The CA keys and keys of persons are generated, used and stored in the HSM module that implement standards and control functions as specified in the section 6.2.1.
m) Keys for certificates for the remote electronic signature and remote electronic seal are generated and used in HSM module that implement standards and control functions as specified in the section 6.2.1, in a secure environment of AKD mPotpis service for remote electronic signature creation on behalf of signatory or creator of seal.
n) When generating keys, care is taken that cryptographic algorithms and parameters are always suitable for use and in accordance with the recommendations of ETSI TS 119 312 [21].

6.1.2. *Private Key delivery to subscriber*

The QSCD with private keys are delivered to subject of certification or authorized representative of the creator of seal after identity validation by the direct identification in the physical presence of a person. The QSCD with private keys can be delivered to subject of

certification or authorized representative of the creator of seal by delivery service with proof of person's identity validation by the direct identification in the physical presence of a person.

For certificates for remote electronic signature and certificates for remote electronic seal private keys are kept in a secure environment of AKD mPotpis service for electronic signature creation on behalf of the signatory. Subject of certification or authorized representative access the AKD mPotpis service using authentication eID means and procedures which guarantees to persons full control over their private key.

Control over the private key and activation of private key is as follows:

a) Signatory or authorized representative receives reference and authorization codes for generation and activation of private key and corresponding certificate. Codes are generated in AKD mPotpis service and sent to e-mail or SMS provided in certificate application.
b) Signatory or authorized representative must authenticate to AKD mPotpis service using two-factor eID means registered in KID IDP.
c) Certificate is registered in AKD mPotpis service by using reference and authorization code in AKD mPotpis service and setting the PIN for private key activation.
d) Signatory or authorized representative must perform first activation of private key with PIN in AKD mPotpis service.
e) Procedures and controls that are used are described in section 6.2.8.1.

6.1.3. *Public Key delivery to certificate issuer*

Immediately after generating the keys of persons, the manufacturer or AKD mPotpis service obtains a certificate from the KIDCA using electronic service.

The manufacturer or AKD mPotpis service sends the public key of the person using the PKCS#10 format of the application, and the KIDCA returns it within the issued certificate.

The authentication of the manufacturer and AKD mPotpis service is carried out using a client certificate, and in order to ensure the protection of the integrity and authenticity of the public key, a secure communication channel (SSL/TLS) is used.

6.1.4. *CA Public Key delivery to relying parties*

The AKDCA Root and KIDCA public keys are available in the certificates on the web portal (refer to the section 2.2).

The integrity verification of the CA certificate is carried out using a summary of the certificate which is available on the web portal, and which may be delivered through a secure channel at the request of the relying party.

6.1.5. *Key sizes*

The AKDCA Root and KIDCA keys are 4096 bits long with the RSA algorithm.

The OCSP and TSU keys are 2048 bits long with the RSA algorithm.

The keys of natural persons and certificates for electronic seal are 2048 bits long with the RSA algorithm.

6.1.5.1. *Key sizes used in AKD mPotpis*

The keys of certificates issued by KIDCA and used in AKD mPotpis service for remote signature creation are 2048 bits long with the RSA algorithm.

Transport keys used for transfer the activation data from client to ADK mPotpis service are 1024 bits long with the RSA algorithm.

Key sizes used in AKD mPotpis service are described in section 6.2.8.1.

6.1.6. *Public key parameters generation and quality checking*

The CA keys, OSCP keys as well as keys of persons are generated on the HSM device using random number generator. Public key parameters of RSA algorithm are in accordance with the FIPS 186-4 [42] or other equivalent standard approved by the PMA.

In general, in order to generate the CA keys and keys of persons, cryptographic algorithms and parameters are used in accordance with the ETSI TS 119 312 [21].

6.1.7. *Key usage purposes (as per X.509 v3 key usage field)*

The X.509 v3 certificates are issued in accordance with IETF RFC 5280 [38], and their purpose are defined by the value of the “keyUsage” field.

For the CA certificates, “keyUsage” is: Certificate Signing, Off-line CRL Signing and CRL Signing.

For the OCSP certificates, “keyUsage” is: Digital Signature.

For the TSU certificates, “keyUsage” is: Digital Signature and “extendedKeyUsage” is: Time Stamping.

For the identification certificate of the person, “keyUsage” is: Digital Signature.

For the signing certificate of the person, “keyUsage” is: Non-Repudiation.

For certificates for electronic seal, “keyUsage” is: Non-Repudiation.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. *Cryptographic module standards and controls*

The following rules apply:

a) The CA keys, TSU keys OCSP keys as well as keys of persons are generated in HSM module that demonstrates the compliance with the FIPS PUB 140-2 level 3 [41] standard.

b) The initialization of the HSM device and generation of the CA keys is performed during the ceremony of generating the CA keys as described in the section 6.1.1.

c) The access to the HSM device and all management procedures of the cryptographic keys, including the generation, usage, loading, storage, recovery and destruction of the cryptographic keys are carried out solely in the secure zone under the dual control.

d) In order for activities related to the HSM devices and cryptographic keys to be carried out in accordance with defined security rules, a trusted role of a coordinator of management of the cryptographic keys are assigned to individual persons.

e) Management procedures of the cryptographic keys are documented and proper records providing evidence on the implementation of activities in accordance with the security requirements are kept.

f) When the private keys are delivered in possession of subject of certification or authorized representative, following the generation they are entered in the QSCD, which as a qualified electronic signature creation device, meet the requirements of the EAL 4+ according to the ISO/IEC 15408 [43] and demonstrate the compliance with the forms of protection of the series EN 419 211 [25], [26], [27], [28], [29] and [30].

g) When the qualified trusted service provider manages the electronic signature creation data on the behalf of the signatory i.e. subject of certification or creator of seal, signature creation data is generated in HSM module i.e. remote QSCD in AKD mPotpis service that meets the requirements *EAL4+ augmented with AVA_VAN.5* ISO/IEC 15408 [43] and rules set out in Anex II of *Regulation (EU) No. 910/2014* [1].

h) AKD monitors the certification status of QSCDs used for issuing of certificates to persons, and will take appropriate measures in the event that change in status of used QSCDs occurs before the end of the validity period of issued certificates.

6.2.2. *Private Key (n out of m) multi-person control*

Management procedures of the cryptographic keys are carried out in strict compliance with the principle of split knowledge which means that the regeneration of the cryptographic key requires n out of total m of the cryptographic components (n out of m).

Individuals, to whom a trusted role of the administrator is assigned, are appointed, and each administrator is given only one cryptographic component.

To access and implement any activity on the HSM device, a dual control is needed that is carried out between the coordinator of management and administrator of the cryptographic key, and in order to regenerate the cryptographic key, a presence of two or more administrators of the cryptographic key is required.

6.2.3. *Private Key escrow*

The rules for storage of private keys of the CA, TSU and OCSP service are the following:

a) After they are generated, the private keys of the CA, TSU and OCSP service remains stored in the HSM device that demonstrates the compliance with the FIPS PUB 140-2 level 3[41].

b) A system that manages the AKDRoot CA private key is not connected to a computer network and remains inactive (offline) the entire time, and it is activated only when necessary.

c) A system that shall manage the KIDCA private key shall be constantly available and shall be used solely for the signing of the certificates of persons and CRL. The same shall apply to OCSP system which signs the replies to enquiries regarding the certificate's status.

d) The cryptographic keys outside the HSM device may only be in the encrypted form and in accordance with the rules specified in section 6.2.6.

The rules for storage of the private keys of persons delivered on QSCD in person's possession:

a) The AKD does not provide a permanent storage of the keys of persons.
b) The individual private keys of persons are encrypted immediately following generation using the cryptographic keys whose strength is equal or greater than the key that is protected.
c) In addition, private keys are encrypted within the shared file which is transferred to the manufacturer in its centre for individualization.
d) The decrypting of the private key of a person is carried out in the manufacturer's safe area and only within the minimum time necessary for their entry into the QSCD chip.
e) The keys that are used to encrypt/decrypt the private keys of persons in the production, are also be stored in the HSM device that demonstrates the compliance with the FIPS PUB 140-2 level 3 [41] standard.
f) Immediately following the individualization of the QSCD, the private keys of persons are deleted.

6.2.3.1. *Private Key escrow in AKD mPotpis service*

The rules for storage of the private keys managed by qualified trusted service provider on behalf of the certification subject or creator of seal in AKD mPotpis service:

a) The individual private keys of persons are generated, used and stored in remote QSCD device that meets the requirements *EAL4+ augmented with AVA_VAN.5* ISO/IEC 15408 [43] and rules set out in Anex II of *Regulation (EU) No. 910/2014* [1].
b) The individual private keys are encrypted immediately following generation using the keys generated with cryptographic mechanisms provided by implemented remote QSCD device and as described in section 6.2.8.1.
c) The AKD does not provide a permanent storage of the private keys in AKD mPotpis service.

6.2.4. *Private Key backup*

The CA private key backup is carried out in the protected area of the secure zone in accordance with the rules set out in sections 6.2.1 and 6.2.2.

Backups of the CA private keys are stored in a secondary location where the same or higher level of protection of the private key is provided.

The rules related to a backup of the CA private key also apply for the OCSP private keys.

The private keys of persons are not copied.

Private keys used in the AKD mPotpis service for remote signing and stamping are stored in a secure environment of a remote QSCD device that complies with EAL4+ augmented with AVA_VAN.5 according to ISO / IEC 15408 [43] and according to the rules defined in Annex II of the Regulation (EU) no. 910/2014 [1].

AKD does not allow persons to recover private keys used in the AKD mPotpis service.

6.2.5. *Private Key archival*

The CA private keys are not archived.

The OCSP and TSU private keys are not archived.

The private keys of persons are not archived.

6.2.6. *Private key transfer into or from a cryptographic module*

The CA private key is transferred to another HSM device only if the new device is in accordance with the FIPS PUB 140-2 level 3 [41] standard.

When the CA private key is outside of the HSM module for the purposes of backup, the hardware protection mechanisms of the private key is used, which is provided by the manufacturer of the HSM device, and which are in accordance with the FIPS PUB 140-2 level 3 [41] standard.

Whenever the CA private key is outside of the HSM device due to the transfer to another device or due to the purposes of backup, the same or greater level of security of the private key is guaranteed.

The rules regarding the transfer of the CA key into the HSM device or from it is applied for the OCSP and TSU keys as well.

The cryptographic keys outside the HSM device may only be in an encrypted form.

The private keys of persons that are forwarded to the manufacturer of QSCD device that is delivered to person's possession are encrypted in accordance with the rules specified in section 6.2.3 and cannot be transferred between cryptographic modules.

The private keys used in AKD mPotpis service are protected by security mechanisms and cryptographic keys of implemented remote HSM that meets requirements set out in ISO IEC 15408 [43] Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5, as described in HSM Security Target.

6.2.7. *Private key storage on cryptographic module*

The unencrypted private key of the CA, TSU and OCSP service in its original readable format is only found inside the HSM device, and may be used only after the activation procedure is carried out.

After the production, the unencrypted private key of persons in its original readable format is found inside the QSCD.

The persons may use their private keys only after the activation procedure of the QSCD is carried out.

The activation of private keys on the on the QSCD in possession and remote QSCD in AKD mPotpis service is carried out in accordance with the section 6.2.8.

6.2.8. *Method of activating private key*

The activation of the private key in the HSM device:

a) The activation of the CA, TSU and OCSP private key in the HSM device is carried out solely under the dual control of authorized persons.

b) Once activated, the private key in the HSM device remains activated during the time that the HSM device is turned on.
c) After power cycling, the HSM device, activation of the private keys is carried out again.

The activation of the private key of a person on the QSCD in person's possession:

a) The activation of the private key of a person is performed one time by entering a PIN.
b) The setting of the PIN values and activation of the private keys on the QSCD is possible only following the activation of the QSCD, which is carried out in accordance with the rules specified in section 6.4.1.

6.2.8.1. *Method of activating private key in AKD mPotpis service*

The activation of the private key managed by qualified trusted service provider on behalf of the certification subject or creator of seal on remote QSCD used in AKD mPotpis service:

a) The activation of the private key is carried out solely upon authentication of subject of certification or authorized representative to AKD mPotpis service using two-factor authentication eID means registered in KID IDP.
b) Private keys are automatically deactivated after signature creation and HSM session is terminated.
c) Generated activation data is never stored in AKD mPotpis service.

Controls are established in order to protect from threats on activation data (SAD), SAD itself and private keys in AKD mPotpis service against online guessing, offline guessing, credential duplication, reply, man-in-the middle attack, credential theft, phishing, eavesdropping, spoofing, masquerading attacks.

6.2.9. *Method of deactivating private key*

The deactivation of the private key in the HSM device:

a) The private key of the CA, TSU or the OCSP service is deactivated if the HSM device or system that controls the private key is not active or is not in operation.
b) The OCSP and TSU private key is deactivated in the same way as the CA private key.

The deactivation of the private key of a person on the QSCD:

a) The private key of a person is deactivated by removing the QSCD from the reader.
b) The private key of a person may not be used if the QSCD is locked or blocked as set forth in section 6.4.2.

Private key used in AKD mPotpis service is deactivated immediately after creating remote electronic signature or remote electronic seal.

6.2.10. *Method of destroying cryptographic key*

The methods of destroying the private key of the CA, TSU or OCSP service:

a) The destruction of the CA private key or TSU private key or OCSP service is carried out:
   - if the HSM device is taken out of the secure zone for repair or equipment replacement, or
   - after the expiry of the validity period of the certificate, or
   - after the CA, AKD QTSA or OCSP termination.

b) When the need arises, the destruction of the private key on the HSM device is carried out using a secure method that is provided by the manufacturer of the HSM device, which guarantees that the destroyed private key is able to be recovered or reused in any way.

c) The destruction of cryptographic keys is carried out by the commission in the presence of at least 2 persons to whom trusted roles have been assigned and record of destruction is provided.

d) The method of destruction of cryptographic keys is carried out in a safe manner, in the areas of the secure zone as described in detail in the documented internal procedures.

e) Destruction of backups and archive of the private key is carried out using the method described in section 5.1.7.

The method of destroying the private keys of persons on the QSCD in possession:

a) The destruction of files with encrypted private keys of persons on the information system is carried out with an automated method, following the process of individualization and putting the private key of persons on the QSCD.

b) The destruction of the encrypted private keys on the information system is carried out using the proven safe method and provided audit log of destruction.

The method of destroying the private keys managed by qualified trusted service provider on behalf of the certification subject or creator of seal in AKD mPotpis service:

a) When the need arises, the destruction of the private key on the HSM device is carried out using a secure method that is provided by the manufacturer of the HSM device, which guarantees that the destroyed private key is able to be recovered or reused in any way.

b) The method of destruction of cryptographic keys is carried out in a safe manner, in the areas of the secure zone as described in detail in the documented internal procedures.

c) When the need arises, the destruction of the private key on the HSM device is carried out using a secure method that is provided by the manufacturer of the HSM device, which guarantees that the destroyed private key is able to be recovered or reused in any way.

d) Destruction of backups and archive of the private key is carried out using the rules set out in section 5.1.7.

6.2.11. *Cryptographic Module Rating*

It refers to the section 6.2.1.

6.3. Other aspects of key pair management

6.3.1. *Public key archival*

The public keys of all persons to whom the certificates have been issued, including the public keys of the CA, TSU and OCSP services, are an integral part of the certificate which are archived to enable the subsequent verification of electronic signatures and provide the evidence for judicial, administrative and other procedures.

The archiving rules, set forth in section 5.5, are applied.

6.3.2. *Certificate operational periods and key pair usage periods*

The validity period of the certificate is given in Table 4.

Table 4: Validity period of the certificate

Certificate	Validity period
Certificate of the root certification authority called AKDCA Root	do 2038-01-19 03:14:07+00:00
Certificate of the subordinate certification authority called KIDCA	15 years
Certificate for signing of OCSP replies	3 years
TSU certificate for signing AKD QTSA replies	5 years
Certificates for natural persons (QSCD in possession)	up to 3 years
Certificates for remote electronic signature	up to 2 years
Certificates for electronic seal (QSCD in possession)	up to 2 years
Certificates for remote electronic seal	up to 2 years

The certification authority ceases to issue certificates, change the CA key and start to issue certificates on the new CA before the expiry of the validity period according to the rules set forth in section 5.6.

The certificate is valid from the date of the issuance until the expiration of the validity and should not be used after the expiration of the validity.

Private key's validity period is equal to validity period of corresponding certificate.

Private key's validity period for TSU certificates is 2 years (extension "privateKeyUsagePeriod").

Private key of corresponding certificate must not be used after the certificate validity period is expired or certificate is suspended or certificate is revoked

During the validity period of the certificate, the certificate may be suspended or permanently revoked, whereupon it ceases to be valid and may not be used any longer.

6.4. **Activation data**

6.4.1. ***Activation data generation and installation***

The manufacturer performs the generation and installation of activation data in accordance with the following rules:

a) The activation data are generated in the HSM device and remains encrypted the whole time using a cryptographic key stored in the HSM.
b) Decryption of the activation data in the information system is carried out only through the minimum time needed to perform their entry in the QSCD or to print them out in the security envelopes or delivery by e-mail or SMS.
c) Immediately after putting the activation data of persons on the QSCD or after printing the activation data in the security envelopes or delivery by e-mail or SMS, a destruction of files with encrypted activation data are carried out.
d) The destruction of the data in the information system is carried out with an automated procedure using a safe method and provided audit log of destruction.

When the qualified trusted service provider manages the signature creation data on behalf of the subject of certification or creator of seal in the remote HSM in AKD mPotpis service:

a) Reference and authorization codes used for certificate registration in AKD mPotpis service are generated and stored in safe environment of AKD mPotpis service that operates remote HSM and are delivered to persons via e-mail or SMS.
b) Reference and authorization codes are used in AKD mPotpis service for certificate registration and for setting the PIN value used for private key activation for creating remote signature.
c) After the registration of certificate in AKD mPotpis service is successfully completed, reference and authorization codes cannot be used anymore.
d) Reference and authorization codes are valid for 120 days.

Persons perform the activation of the QSCD in accordance with the following rules:

a) The activation of the QSCD is carried out by the subject of certification or authorized representative individually after collecting the QSCD using the data for the activation in the security envelope and according to the instruction for the QSCD activation that is available on the web portal of the QSCD.
b) During the activation of the QSCD, PINs are set to protect private keys, and PUK value is set to unlock the QSCD.

When the qualified trusted service provider manages the signature creation data on behalf of the subject of certification or creator of seal private key is activated in the remote HSM device in AKD mPotpis service at the time of certificate registration, using reference and authorization

codes delivered to subject of certification or authorized representative by e-mail or SMS and setting the PIN for private key activation.

Persons are informed of their obligations related to the protection of the activation data, registration codes or PINs.

6.4.2. *Activation data protection*

When the certificates are delivered to persons on the QSCD the manufacturer undertakes the following measures for the activation of the data protection:

a) Generating the activation data, their entry into the QSCD and printing in the security envelopes are carried out under the dual control in the manufacturer's secure environment of the QSCD.
b) The security envelopes with the activation data are packed in separate packages and sent to the RA or directly to persons, regardless of the sending of the QSCD.
c) The security envelopes with the activation data are delivered to the persons via RA offices or directly.
d) Activation data can be delivered to person's e-mail or SMS provided in certificate application for which the person guarantee that only he/she can access, if indicated in application.

Persons are informed of implemented security measures for protecting QSCD and PINs for private keys on QSCD.

a) After 6 consecutive attempts of entering the wrong PIN, the QSCD locks.
b) The locked QSCD the person may unlock independently using the PUK value set during the activation of the QSCD.
c) After 6 consecutive attempts of entering the wrong PUK, the QSCD blocks.
d) The blocked QSCD may be unblocked only by the RA officer in a secure environment using the electronic service to unblock the QSCD.
e) The unblocking of the QSCD is carried out in the physical presence of the person after identity validation of said person.

6.4.2.1. *Activation data protection in AKD mPotpis service*

When the qualified trusted service provider manages the signature creation data on behalf of the subject of certification or creator of seal on remote QSCD device the following measures for the activation of the data protection are applied:

a) Registration codes (reference and authorization codes) for certificate registration and PIN setting for key activation are generated and managed in a secure environment of the AKD mPotpis service operating remote QSCD device and delivered to person's e-mail or SMS indicated in certificate application.
b) Registration codes are used only for single certificate registration and for setting the PIN used for private key activation in AKD mPotpis service. After certificate is accepted and PIN is set, the registration codes cannot be used for any other purpose.

c) Certificate acceptance process is only possible after two-factor authentication of the subject of certification or authorized representative to AKD mPotpis service.
d) Registration codes are valid for 120 days.

Activation data used for private key activation in AKD mPotpis service operating remote QSCD device are protected as described in section 6.2.8.1.

6.4.3. *Other aspects of activation data*

The AKD applies the appropriate protection measures of the activation data and registration codes against loss, modification, disclosure and unauthorized use.

In accordance with the documented internal procedures, the AKD performs:

a) Protection of the activation data during generation, installation, printing in the security envelopes, e-mail or SMS delivery and the destruction of the activation data until the transport and delivery of the security envelopes to the persons.
b) Protection of the registration codes for certificate registration and setting the PIN for private key activation in AKD mPotpis service during generation, installation, e-mail or SMS delivery and the destruction of the registration codes until certificate acceptance.

Activation data may be delivered, besides the procedures described in this CPS, also as follows:

a) by security envelope,
b) by e-mail,
c) by SMS,
d) in the LRA/RA in person, after identity of the subject of certification or authorized representative or legal representative of the natural or legal person is determined and
e) by combining procedures in a) to d).

Registration codes used for certificate registration and setting the PIN for private key activation in AKD mPotpis service are delivered to person's e-mail or SMS indicated in certificate application.

After the delivery of the security envelopes, the persons are responsible for the protection of the activation data and/or registration codes. Persons can change activation data for private keys using application for QSCD device. For private keys used for remote signature creation activation data (PIN) can be changed in AKD mPotpis service.

6.5. **Computer security controls**

6.5.1. *Specific computer security technical requirements*

Computing resources are protected by the security measures according to the ISO/IEC 27001 [45] and ISO/IEC 27002 [46] standards.

In addition, technical requirements related to the computer security are implemented according to the requirements of the ETSI EN 319 411-1 [15] and ETSI EN 319 411-2 [16] as well as according to the requirements set forth in CEN TS 419 261 [31], ETSI TS 119 431-1 [23] and CEN EN 419 241-1 [32].

This means the following:

a) Internal security standards are documented and there is a number of procedures and instructions which are regularly updated in order to be in compliance with the security requirements.
b) The organizational and management structure with clearly defined trusted roles and responsibilities are established.
c) The rules related to employees, security guards, visitors and external service personnel are defined prior and during the contractual relationship and after the expiry of the contract.
d) Measures to protect the property and data that include defining the owner, classification and operation are applied.
e) Appropriate systems for physical protection of facilities, areas and information equipment are established.
f) Management of authorizations and access rights is restrictive and dual control for the implementation of all critical operations involving the issuing, deletion or modification of the certificate or its status are established.
g) Strict rules related to the management of cryptographic keys and equipment are prescribed and implemented.
h) Regular measures to maintain the security of the network and computer equipment including protection against malicious code, management of audit logs and security testing are carried out.
i) The system is continuously monitored and alarmed in order to allow the detection, registration and timely response to unauthorized actions or irregular occurrences.
j) Backups are created and stored, and business continuity management procedures are established.
k) Management rules for incidents, modifications, problems and requirements are established.

6.5.2. *Computer security rating*

Examination, testing, verification, evaluation and assessment of the security of computing resources are carried out periodically as will their compliance with the standards set forth in section 6.5.1.

6.6. Life-cycle technical controls

In accordance with chapter 12 of the ISO/IEC 27002 [46] controls over computing resources are established, which includes:

a) The procedures are documented, trusted roles are assigned and responsibilities are established in order to ensure a correct and safe implementation of activities.
b) Organizational, business and technical modifications to the computer systems are be controlled.

c) The resources are regularly monitored, adjusted and planned in order to ensure sufficient capacities and the required system performances.
d) Risk assessment is carried out pursuant Norm ISO/IEC 27005[48], during which business and technical aspects related to provision of services are taken into consideration.
e) The development, testing and production environment are strictly separated in order to reduce risks of unauthorized access and modification to the production environment.
f) The computer systems are protected from viruses, malware and unauthorized software.
g) Backups are regularly created and are protected from damage, loss and unauthorized access in order to prevent data loss.
h) Audit logs are provided and all measures for their protection are taken.

In accordance with chapter 14 of the ISO/IEC 27002 [46] , controls over the development and life-cycle of the software are established, which includes:

a) The methodology of the software development is established, and the development process is regularly monitored and evaluated.
b) The appropriate protection of the source and the executable code is provided.
c) The software is tested and subjected to the extensive testing and evaluation prior to its implementation in a production environment.
d) In accordance with the risk assessment, the software security corrections are implemented, and the entire management process concerning versions, corrections and modifications to the software is defined and controlled.

In accordance with the chapter 15 of the ISO/IEC 27002 [46] , controls related to business relations and suppliers are established, which includes:

a) The procurement procedure and evaluation of suppliers is carried out according to the documented procedures.
b) The security requirements are defined in the agreements, and procedures related to the implementation of the agreements are monitored in order to ensure the safe delivery of equipment and implementation of services.

6.7. Network security controls

Controls over network infrastructure are established in accordance with chapter 13 of the ISO/IEC 27002 [46], CEN TS 419 261 [31], ETSI TS 119 431-1 [23] and CEN EN 419 241-1 [32].

The following network controls are established:

a) All computing resources are segmented into logically separate, specific functional units called network zones.
b) The following network zones are established:
    a. PKI CA zone, where computing resources for the implementation of the services of generating and management of certificate revocation is be located,

   b. PKI service zone, where computing resources for the implementation of the services of informing and certificate's status verification is located,
   c. Perso service zone, where computing resources for uploading cryptographic keys on QSCD in possession and printing activation data on security envelopes,
   d. DMZ where computing resources that are exposed directly to the public is located.

c) Clear rules are defined and established so that specific network zone applies the same physical, technical and procedural protection measures.
d) The equipment and hardware between the network zones are physically separated and placed into separate computer cabinets.
e) Computer cabinets are placed in areas within the adequate zone of physical security, and protected by the appropriate measures of physical security in accordance with the section 5.1.
f) Wiring and all physical points of connections and active and passive network equipment is controlled and monitored.
g) The physical access to computing resources and network equipment is limited to persons with trusted roles that are authorized to administer the software.
h) The network zones are separated by firewalls, and between network zones the network traffic according to the formally approved lists of allowed services are strictly regulated.
i) The communication between the network zones is carried out through the secure channels separated intentionally and logically and which protect the data against modification and disclosure.
j) Only the communication, necessary for the implementation of service is enabled between the network zones, and any communication other than the one explicitly granted is prohibited.
k) The limited access to the network zone may be carried out in the following way:
   a. the secure zone may be accessed only from the service and operational zone,
   b. the service and operational zone may be accessed only from the control and access zone.
l) Reports on every change to the firewall configuration are automatically generated.
m) Intrusion detection system, that monitors the network traffic in the active and service zone and alarm all suspicious activities in real time, is implemented.
n) Vulnerability testing is carried out periodically and for every major configuration change, and all critical vulnerabilities are resolved within the shortest time possible.
o) A system penetration test is carried out in the event of significant changes and at least once a year.

6.8. **Time-stamping**

All information equipment has a harmonized system clocks with UTC time so that all audit logs contain a valid record of the date and time. Ensured minimum UTC time accuracy time is +/- 1 second.

7. Certificate, CRL, and OCSP profiles

7.1. Certificate profiles

Forms (profiles) of all certificates are made pursuant IETF RFC 5280 [38] and Recommendation ITU-T X.509 [49].

Profile certificates are issued to private individuals pursuant the requirements of ETSI EN 319 412-1 [17] and ETSI EN 319 412-2 [18] as well as the requirements of EU qualified certificates pursuant ETSI EN 319 412-5[20].

Profile certificates are issued to legal persons pursuant the requirements of ETSI EN 319 412-1 [17] and ETSI EN 319 412-3 [19] as well as the requirements of EU qualified certificates pursuant ETSI EN 319 412-5[20].

Forms for CA and OCSP certificates are made pursuant ETSI EN 319 412-3[19].

Forms for TSU certificates are made pursuant ETSI EN 319 422 [22] and IETF RFC 3161 [39].

The following table contains basic certificate fields.

Table 5: Basic/General fields

Field	Value/Limits of the value
Version	X.509 V3, see section 7.1.1
Serial Number	Unique positive No. with 32 bit entropy
Signature Algorithm	SHA256RSA, see section 7.1.3.
Issuer DN	See section 7.1.4.
Valid from	utcTime
Valid to	utcTime(Valid from +period of certificate validity pursuant 6.3.2).
Subject DN	See section 7.1.4.
Subject Public Key	Subject Public Key
SignatureValue	Issuer's signature of the certificate, generated and coded according to IETF RFC 5280 [38]

7.1.1. *Version Number*

X.509 version V3 is used.

7.1.2. *Certificate extensions*

7.1.2.1. *Extensions of CA certificate*

Specified in the CP [53].

7.1.2.2. *Extensions of OCSP certificate*

Specified in the CP [53].

7.1.2.3. *Extensions of TSU certificate*

Table 6a: Extensions of TSU certificate

Polje	Vrijednost
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 godina)
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 language=en PdsLocation: url= https://id.hr/cps 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 field*

7.1.2.4. ***Extensions of certificate***

Table 6b: Extensions of certificates issued to natural and legal persons

Field	Certificate type	Value	Content
Key Usage*	kID NCP+ kident	Digital Signature (80)	Fixed
	kID QCP-n-qscd-ksign	Non-Repudiation	Fixed
	kID QCP-n-qscd-krsign	Non-Repudiation	Fixed
	kID QCP-l-qscd-kseal	Non-Repudiation	Fixed
	kID QCP-l-qscd-krseal	Non-Repudiation	Fixed
Basic Constraints*	All End Entity	Subject Type=End Entity Path Length Constraint=None	Fixed
Subject Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.	Variable
Authority Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.	Variable
Authority Info Access	All End Entity	[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	Fixed
Certificate Policies	kID NCP+ kident	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.5.2.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://id.hr/cps	Fixed
	kID QCP-n-qscd-ksign	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.4.2.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:	Fixed

		http://id.hr/cps	
	kID QCP-n-qscd-krsign	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.4.6.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://id.hr/cps	Fixed
	kID QCP-l-qscd-kseal	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.4.2.2.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://id.hr/cps	Fixed
	kID QCP-l-qscd-krseal	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.4.6.2.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://id.hr/cps	Fixed
Subject Alternative Name	kID NCP+ kident	Microsoft UPN(1.3.6.1.4.1.311.20.2.3)	O / Holder variable
		RFC822Name=email@domain.tld	O / Holder variable
Extended Key Usage	kID NCP+ kident	Any Purpose (2.5.29.37.0)	M
		Id-kp-clientAuth (1.3.6.1.5.5.7.3.2)	M
CRL Distribution Points	All End Entity	[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	Fixed
qcStatements			
	kID QCP-n-qscd-ksign	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1)	Fixed

		id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://id.hr/cps language=en PdsLocation: url= https://id.hr/cps language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-esign(1) (0.4.0.1862.1.6.1)	
	kID QCP-n-qscd-krsign	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://id.hr/cps language=en PdsLocation: url= https://id.hr/cps language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-esign(1) (0.4.0.1862.1.6.1)	Fixed
	kID QCP-l-qscd-kseal	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://id.hr/cps language=en PdsLocation: url= https://id.hr/cps 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)	Fixed
	kID QCP-l-qscd-krseal	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url=https://id.hr/cps language=en PdsLocation: url= https://id.hr/cps 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)	Fixed

**Critical field*

7.1.3. *Object identifier (OID)*

Algorithms with accompanying OID identifiers that are issued in AKD PKI system based on AKD Root CA are shown in Table 7.

Table78: Algorithms and accompanying object identifiers

Algorithm	OID
Sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

7.1.4. *Types of names*

X.500 Distinguished Name is written in the fields Subject and Issuer in all certificates issued by AKD PKI system pursuant section 3.1.1. of this document.

Types of names for certificates that are issued in AKD PKI system are described in detail in sections 3.1.1 and 3.1.4 of this document.

7.1.5. *Limitations of names*

N/A.

7.1.6. *Object identifier (OID) of CP*

All certificates by AKD PKI are issued under AKD Root CA and contain extension Certificate Policies and accompanying OID as specified in section 1.2. of this document.

7.1.7. *Use of extension Policy Constraints*

N/A.

7.1.8. *Syntax and semantics of CP qualifiers*

AKD fulfils CPS identifier that indicates the appropriate CPS in all issued certificates with Certificate Policies extension. Individuals' certificates may contain additionally User Notice identifier that may indicate either an appropriate CPS or Agreement.

7.1.9. *Process semantics for critical extension Certificate Policies*

N/A.

7.2. CRL profiles

CRL profiles AKDCA Root and KIDCA/i.e. CPS of the issuer support X.509 version 2 pursuant the requirements defined in IETF RFC 5280[38]. CRL profiles for KIDCA and AKDCA Root are in the following table.

Table 8: Basic CRL fields

Field	Value/Limitation of value
Version	X.509 V2, see section 7.2.1
Signature Algorithm	SHA256RSA, see section 7.1.3.
Issuer DN	X.500 Distinguished name of the issuer of the CRL.
Effective Date	utcTime
Next Update	utcTime (thisUpdate+24h)
Revoked Certificates	A list of revoked certificates that includes serial number of the certificate that was revoked, date and reason of revoking, (keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold).

7.2.1. *Number of version*

X.509 verzija V2 is used.

7.2.2. *CRL extensions*

Table 9: Extension CRL

Field	Value/Limitation of value
authorityKeyIdentifier	Derived using the SHA-1 hash of the public key.
CRL Number	Monotonically increasing sequential number.

7.3. OCPS profile

AKD PKI makes it possible to check on line the status of certificate via OCSP service. Certificate of OCSP service (OCSP responder) issues KIDCA, i.e. AKDCA Root. Certificate of OCSP service is created pursuant IETF RFC 5019 [40] and IETF RFC 6960 [35].

AKDCA Root and KIDCA OCSP profiles are specified in CP [53].

7.3.1. *Version number*

X.509 version V3 is used.

7.3.2. *Extension of OCSP certificate*

Specified in CP [53].

8. Compliance audit and other assessments

8.1. Frequency or circumstances of assessment

The document provides an audit in order to verify the compliance with the legislation and mandatory standards.

The regular supervision by the trust service providers and conformity assessment with the *Regulation (EU) No. 910/2014* [1] is carried out every 24 months.

The regular supervision of the management system in order to verify the compliance with the ISO/IEC 9001[47], ISO/IEC 27001 [45] and ISO/IEC 14298 [44] standards are carried out at least every 12 months.

Internal assessments in order to verify the compliance with this document and internal procedures are carried out periodically according to the established plan and program.

The national supervisory body may perform an assessment or request the performance of the assessment at any given moment in order to establish whether the requirements related to the implementation of the legislative provisions are met.

8.2. Identity/qualifications of assessor

The assessment of the compliance with the *Regulation (EU) No. 910/2014* [1] will be carried out by the authority which is authorized as competent for the conformity assessment of a qualified trust service provider and qualified trust service the latter provides and accredited according to ETSI EN 319 403[14].

Supervision of the management system is carried out by the authorized audit companies, according to the ISO/IEC 9001[47], ISO/IEC 27001 [45] and ISO/IEC 14298[44].

The internal assessors must:

- have the knowledge in the field of the PKI and information security,
- have the knowledge and understanding of the ETSI EN 319 401[13], ETSI EN 319 403 [14] and ETSI EN 319 411[15], [16],
- know the provisions of the CP and CPS of Procedure on Certification Procedures,
- know the legislation in the field of e-commerce, information security and data confidentiality protection, and
- have the skills necessary for the implementation of internal assessments.

8.3. Assessor's relationship to assessed entity

The external assessors agree independent and delegated by the competent national authority or authorized external audit company.

The internal assessment within the AKD is carried out by the Information Security Advisor or other independent person appointed by the PMA.

8.4. Topics covered by assessment

External assessments of the management system include the entire business of the AKD.

The internal assessment includes, but is not limited to:

- certificate generating procedures,
- procedures of generating and protection of all private keys,
- certificate revocation management,
- implementation of the certificate's status verification service,
- implementation and operation of AKD mPotpis service,
- availability and contents of dissemination services,
- documentation and agreements related to the registration service, and
- Implementation of the prescribed procedures and protection measures in accordance with the CP and CPS.

8.5. Actions taken as a result of deficiency

In the event of non-compliance operational plan to eliminate non-compliances is produced with assigned tasks and due dates.

If a non-compliance significantly affects the security of the provision of trust services or prevents the fulfilment of the statutory requirements, AKD will cease the provision of KIDCA services, until the reason for cessation of service occurred no longer exists.

AKD will undertake all necessary actions in order to prevent the adverse impact of the cessation of the provision of service to affected parties.

AKD will continue to provide KIDCA services when the PMA establishes that the reason as to why the cessation of service occurred no longer exists.

8.6. Communication of results

The report on the performed assessment or determined non-compliance is forwarded to the PMA, the representatives of the assessed area and responsible persons in the accordance with the organizational structure of the AKD.

The AKD, in accordance with legal provisions, submits a report on conformity assessment to the supervisory body within 3 working days upon the report is received.

9. Other business and legal matters

9.1. Fees

The AKD charges fees for services provided in scope of certification services. Price and fees for services are determined by the AKD organizational sector in charge for business development.

Valid price lists and fees for certification services and the payment methods, are available to persons and relaying parties as follows:

a) The AKD publishes valid price list on-line on web portal https://www.certilia.com,

b) The AKD immediately communicates any changes of price list, fees and method of payments to RA officers,
c) RA officers inform the persons and relying parties in the RA offices.

The AKD may set the prices and fees for certification services with separate contract with client, separately from the published price list. AKD reserves the right to change the pricelist at any time.

9.1.1. *Certificate issuance or renewal fees*

Certificate issuance or renewal fees are in accordance to published price list.

The AKD may set the prices and fees for certification services with separate contract with client, separately from the published price list.

The KIDCA is not providing certificate renewal services and valid price lists do not contain fees for renewal of certificate.

9.1.2. *Certificate access fees*

Certificates of the person are not available in the public directory for the public search. AKD reserves the right to subsequently make available public search of certificates of the person, if required and under commercial terms.

The AKD may set the prices and fees for certificate search in public directory service with separate contract with client.

9.1.3. *Revocation or status information access fees*

The AKD may set fees for the revocation, suspension/withdrawal of suspension and revocation. The fees set out in valid price lists apply.

The AKD may set fees for the certificate status information access. The fees set out in valid price lists apply.

The AKD may set the prices and fees for certificate search in public directory service with separate contract with client.

9.1.4. *Fees for other services*

The AKD may set fees for other services and products provided in the scope of certification services, independently or with contracted third party:

a) RA fees for natural persons registration services,
b) Fees for smart card reader,
c) Fees for printed design of QSCD,
d) Fees for QSCD manufacturing,
e) Fees for QSCD individualization,
f) Fees for AKD mPotpis service for remote signature creation,
g) Fees for delivery of the certificates on QSCD to the location indicated in certificate application, other than location where certificate application was submitted (RA office location).

h) Fees related to usage, upgrade, lease or maintenance of hardware and software, user education, etc.

The AKD publishes fees and payment methods as set out in section 9.1 of this document.

The AKD may set the prices and fees for certification services with separate contract with client, separately from the published price list.

9.1.5. *Refund policy*

Refunds for payments are approved if the provided service or product does not meet the provisions specified or there was an unintentional error in payment caused by subscriber.

Refund policy terms and conditions regarding the certificate issuance are published on the web portal and available in RA offices.

Refund policy can be specified in the conditions for providing certification services.

9.2. Financial responsibility

9.2.1. *Insurance coverage*

The AKD establishes a system of accountability, determine the limits of reliance in certificates and clearly define the obligations of all users of certification services. The service users are informed in advance through the web portal on the conditions of provision of the certification services.

The AKD has an insured liability risk for damages arising from the provision of certification services in the amount specified in section 9.2.3 and regarding to issuing eID means and providing qualified and non-qualified services of creating, verifying and validating electronic signatures, electronic seals or time stamps and related certificates.

The AKD is liable for damages that are inflicted on any natural or legal person for failure to fulfil obligations in accordance with this document and the *Regulation (EU) No. 910/2014* [1].

The AKD is not liable for damages that occur intentionally or by negligence resulting from exceeding the limits of reliance in a certificate or due to the failure to fulfil obligations of the user.

In the event that all or some RA affairs are delegated to the third party, AKD may require that third party has a separated insured liability risk for damages (insurance policy) arising from the services which third party is providing.

The rules for the participants in the provision of certification services are regulated in accordance with the Civil Obligations Act[12].

9.2.2. *Other assets*

The AKD has sufficient financial resources at its disposal to fulfil its commitments and the undisturbed provision of services.

The information on the operation and financial affairs of the AKD is made public on the official website of the AKD: http://www.akd.hr.

9.2.3. *Insurance or warranty coverage for end-entities*

The AKD has an insured liability risk for damages arising from the provision of certification services.

The total value of the insurance policy amounts to 265.445,62 euros.

Maximum financial limit that AKD accepts per transaction is indicated in the issued certificate, it the field *"CertificatePolicies",* attribute *"PolicyIdentifier",* second last digit of the OID identifier *(e.g.* Policy Identifier = 1.3.6.1.4.1.43999.5.4.2.1.2.1)

The rules for interpretation of the identifier are set out in section 9.8.

The AKD additionally insures the property with the insurance policy that covers insurance against the risk of fire, weather-related disasters, floods, explosions, etc., and insurance against machinery breakdown (industrial fracture) and glass breakage, which covers possible damages caused by the failure or damage to installations and/or hardware.

9.3. Confidentiality of business information

9.3.1. *Scope of confidential information*

The confidential business data include all data, in any format marked as confidential or are by their nature confidential and the disclosure of which to the unauthorized person may cause harmful consequences for the participants of the certification process.

The confidential business data include, but are not limited to:

a) personal data and documentation collected in the registration process in accordance with the section 9.4,
b) databases, audit logs and archives of the service providers,
c) reports on the implementation of activities and procedures of the provision of services,
d) business communication between the participants of the certification process, and
e) other data of various types, important for the operations or interests of the participants.

A special category of the confidential business data include, but is not limited to:

f) all private keys, activation data and data for the registration on the web portal,
g) all symmetric keys, PINs, passwords, codes and all encrypted communication between participants, networks or components of the PKI infrastructure,
h) specific data related to security and implementation of the data protection measures, information systems, business cooperation, employees and location for the carrying out of the activities, and
i) protection plans and layouts of facilities and areas, and plans related to business continuity.

9.3.2. *Information not within the scope of confidential information*

The data that is not be considered as confidential business data includes, but is not limited to all business data whose disclosure is not adversely affect the business, provision of services or the interests of the participants of the certification procedure, in particular:

a) certificates, certificate revocation lists and information on the certificate's status,
b) information and documents, published on the web portal,
c) data whose disclosure would not undermine the Constitution and statutory rights and freedoms of natural and legal persons,
d) data that are published by the AKD on its official website or which they are required to publish in order to meet their obligations under the Freedom of Information Act [11],
e) other data whose unrestricted distribution is permitted or required for the realization of business goals.

9.3.3. *Responsibility to protect confidential information*

The protection of the confidential business data is carried out in accordance with the national and European legislation governing the area of data protection.

Employees and officers involved in the implementation of certification procedures, which are granted access and handle confidential business data referred to in section 9.3.1 acts in accordance with the internal rules and procedures.

The duty to keep secrets pertains to all persons and relying parties that have become aware of the confidential business data in any way.

9.4. Privacy of personal information

9.4.1. *Privacy plan*

The protection of personal data is ensured to every natural person.

Persons are informed that the AKD and RA processes personal data in order to meet statutory requirements related to the implementation of services, and to guarantee the legal treatment and processing of personal data in its possession.

The AKD and legal persons providing RA services take appropriate technical and organisational protection measures against unauthorized or unlawful processing and against accidental loss, destruction or damage to personal data.

The transfer of personal data between the legal persons delegated RA affairs and the AKD and between authenticated PKI components are carried out through encrypted communication channels that ensure the protection of the integrity and confidentiality of data.

9.4.2. *Information treated as private*

The AKD and contracted legal persons delegated RA affairs collect and processes personal data for the purpose of issuing certificates.

In order to meet the statutory requirements related to the implementation of the services, the personal data set forth in section 3.2.3 are collected in the process of registration of persons.

The personal data are retained as part of the archive and in the part of the audit logs as specified in sections 5.4.1 and 5.5.1.

9.4.3. *Information not deemed private*

The AKD keeps a register of certificates and may publish the certificates in a public directory under the conditions, defined in section 4.4.2.

The personal data of the subject of certification that is contained in the certificate is as follows: a name, surname and OIB.

If person's affiliation with organization is confirmed, as indicated in section 3.2.3.1, certificate may contain name and OIB/VAT identification number of organization.

9.4.4. *Responsibility to protect private information*

The AKD and legal person's delegated RA affairs are responsible for the protection of personal data.

A lawful processing of the personal data is ensured in accordance with the provisions of the Implementation of the General Data Protection Act [4] and related subordinate acts or the *Regulation (EU) No. 2016/679* [3].

9.4.5. *Notice and consent to use private information*

Except for the purposes of the performance of legal or contractual obligations arising from the agreements governing the certification services, the personal data are only used pursuant to the written consent of the person.

By signing the conditions for certification services providing the persons are aware of use of personal data for the purposes of keeping records and to publish certificates in a public directory.

9.4.6. *Disclosure pursuant to judicial or administrative process*

The access rights to personal data and all other information collected during the end user registracion procedure are enabled if required by legislation, or when requested by the competent court, administrative or other relevant national authority in writing for the implementation of the procedure or investigation of the irregular or illegal conduct.

9.4.7. *Other information disclosure circumstances*

There are no provisions.

9.5. Intellectual property rights

All participants are required to uphold the copyrights and intellectual property rights in accordance with applicable legal regulations.

The AKD and the Republic of Croatia, which is the owner of the AKD, owns and reserves all copyrights and intellectual property rights associated with adjustments of their own infrastructure and databases, produced websites and published publications.

The AKD is the author and owner of all documents published on the website, including CP [53], CPS, certificates and CRL, and in accordance with applicable laws of the Republic of Croatia, the AKD retain all copyright and related rights over them.

The AKD develop their own source code and owns and reserve unlimited copyrights and intellectual property rights of the application for the QSCD (AKD-eID-Card 1.0) as well as the application (middleware) for the use of the QSCD.

The AKD, as the author and owner of the aforementioned contents and applications on the web portal, have the unlimited rights of usage, and particular right of reproduction, distribution, publishing and processing.

The persons have the right to use the QSCD and the application for the use of the QSCD free of charge according to the licensing conditions for end users (*End User License Agreement – EULA*).

The software and all other goods that are used for the provision of trust services, and which are owned by the AKD, participants of the certification procedure or any third party, are used in the accordance with the EULA or other provisions concerning the right of usage.

9.6. Representations and warranties

9.6.1. *PMA representations and warranties*

The representations and warranties of the PMA include:

a) Defining, introducing and administering CP [53], CPS, security operating procedures and implementing documents related to the operation of the AKD PKI and provision of the trust services,

b) Maintaining the continuing suitability and compliance of the CP [53] and CPS with the *Regulation (EU) No. 910/2014* [1] and binding national, European or international standards.

c) Monitoring of the implementation of the security requirements, which are prescribed with the CP [53] and CPS.

9.6.2. *CA representations and warranties*

The representations and warranties of the CA include:

a) Ensuring the implementation of the *Regulation (EU) No. 910/2014* [1] and the application of the administrative and management procedures in accordance with the binding national, European or international standards.

b) Ensuring the implementation of the certificate generating services, certificate revocation management, certificate's status verification, AKD mPotpis service as well as dissemination services in accordance with this document.

c) Timely processing of applications on the basis of complete, accurate and verified data provided by the RA.

d) Provision of personnel with the necessary expertise, reliability, experience and qualifications sufficient for the implementation of the business activities and meeting the requirements set forth in this document.

e) Provision of sufficient financial resources necessary for the provision of certification services in accordance with the requirements set forth in this document.

f) Application of organizational, operational and physical security measures to protect the CA system and data in accordance with this document.

g) Recording and long-term archiving of all relevant information in relation to the data issued and received by the CA and AKD mPotpis service, especially for the purposes of submitting evidence in court proceedings and to ensure continuity of service.

h) The lawful processing of personal data in accordance with the Implementation of the General Data Protection Act [4] and related subordinate acts or the *Regulation (EU) No. 2016/679* [3].

i) Provision of the ISO/IEC 9001 [47] and ISO/IEC 27001 [45] certificates as proof of quality and security for the provision of certification services.

9.6.3. *RA representations and warranties*

The representations and warranties of the registration service (AKD and legal person's delegated RA affairs) providers include:

a) Collection and verification of data on natural person identities is in accordance with the provisions set out in this document.

b) Collection and verification of data on legal persons and organizations identities and persons affiliation with the organization is in accordance with the provisions set out in this document.

c) Receiving applications by persons, including applications for issuing the certificates, requests for revocation and suspension of the certificates and requests to unblock the QSCD and the delivery of the QSCD.

d) The direct verification and the unambiguous validation of the identity of natural persons by the direct identification in the physical presence of a person upon receiving the application by the person, as well as upon delivering the QSCD.

e) Registration of complete, accurate and verified personal identification data on natural persons and their requirements to the records of the RA.

f) The verification and approval of applications by the persons and forwarding of complete, accurate and verified data to the manufacturer of the QSCD or the CA.

g) Ensuring that registration activities are conducted solely by the reliable and conscientious RA officers whose identity can be undoubtedly established and who are adequately trained before they are granted authorization.

h) Application of organizational, operational and physical security measures to protect the RA systems and all data and documents collected in the registration process.

i) Recording and long-term archiving of data collected in the registration process and all relevant information in relation to the data issued and received by the RA, especially for the purposes of submitting evidence in court proceedings and to ensure continuity of service, at least for the period of 10 years after the expiration of related certificate.

j) The lawful processing of personal data in accordance with the Implementation of the General Data Protection Act [4] and related subordinate acts or the *Regulation (EU) No. 2016/679*[3].

k) Implementation of organization and technical measures for accessibility to its services for persons with disabilities, whenever possible.

l) Conducting activities a) to k) regarding the issuance of two-factor electronic identification means used for authentication to AKD mPotpis service.

Legal persons concluded the separate contract with AKD regarding the registration services are obliged to comply with representations and warranties indicated in this document as well as representations and warranties indicated in contract.

9.6.4. *Subscriber representations and warranties*

The person is responsible:

a) that all data submitted in the registration process are accurate and true,
b) that the personal data in the certificate are true,
c) that only the person which is indicated in the certificate or authorized representative of the creator of the seal uses the private key which match the public key in the certificate,
d) that the certificate at the time of its use has not expired and has not been revoked,
e) that the certificate is used only for legal and authorized purposes and in accordance with their intended purpose,
f) that an unauthorized person has no access to the private key on QSCD or in AKD mPotpis service,
g) that the person requests the revocation or suspension of the certificate if there is modification of data in the certificate (e.g. name of natural or legal person or identification number, cessation of affiliation of the natural person with organization, or any reason set out in section 4.9), or if the loss, theft, misuse or unauthorized use of the private key are suspected,
h) to enquire about the CP, CPS and conditions for providing certification services in case of any uncertainties and questions concerning his/her responsibilities and obligations, and the appropriate manner to use the certification services.

9.6.5. *Relying party representations and warranties*

The relying parties are responsible:

a) to enquire about the CP, CPS and conditions for providing certification services, and especially concerning their responsibilities and obligations, and the appropriate manner to use the certification services,
b) to independently assess and determine the appropriateness of the certificate use for the appropriate purpose,
c) to establish, before exercising trust in the certificate, that the certificate has not expired and that it is not revoked, all according to the data contained in the certificate,
d) that the verification of the certificate validity is carried out using an authorized source and reliable equipment,
e) to verify the certificate's status of the person and of all certificates in the certification path according to the procedures indicated in IETF RFC 5280 [38] and IETF RFC 3739 [37] and
f) to validate electronic signature or seal before relying on them.

9.6.6. *Representations and warranties of other participants*

Representations and warranties of the manufacturer include:

a) Data preparation and production of the QSCD on the basis of the application and unmodified data provided by the RA.
b) Generating a pair of keys and activation data, obtaining the certificates from the subordinate CA and their entry in the QSCD.
c) Generating data for the activation of the QSCD and registration on the web portal and production of the security envelopes, when applicable.
d) Application of organisational, operational and physical security measures to protect the information system of the manufacturer and data in accordance with this document.
e) The lawful processing of personal data in accordance with the Implementation of the General Data Protection Act [4] and related subordinate acts or the *Regulation (EU) No. 2016/679* [3].
f) Provision of the ISO/IEC 9001 [47], ISO/IEC 27001 [45] and ISO/IEC 14298 [44] certificates as proof of quality for the management of business and production of the security printing and security of information systems.
g) Ensuring the QSCD qualified electronic signature creation device, that meets the requirements of the EAL 4+ according to the ISO/IEC 15408 [43] and demonstrates the compliance with the forms of protection of the series EN 419 211 [25], [26], [27], [28], [29] and [30].

Representations and warranties of suppliers of HSM crypto devices, suppliers of PKI related products, services and solutions are defined in separate contracts which AKD concludes with specific supplier.

9.7. **Disclaimers of warranties**

The AKD is liable only for things they are responsible for as a service provider, and which are expressly stated as responsibilities of the AKD in section 9.6.

The AKD is not liable for:

a) damages caused by improper use of the certificate according to the section 1.4.2,
b) damages caused by the false or negligent use of the QSCD in the possession of person, activation data, certificate or CRL or OCSP service response,
c) damages incurred in a period from the certificate revocation to the issuance of the following CRL,
d) damages caused by malfunction and errors in the software and hardware of the person or the relying party, and
e) all damages caused intentionally or by negligence by the person or relying party that do not fulfil their obligations or fail to act in accordance with their obligations set out in sections 9.5.4 and 9.6.5.

The AKD is not responsible for the damages resulting from the provision of false information in the registration process or misrepresentation of the person during the process of identification and identity validation.

The AKD is not liable if there has been a violation of the responsibilities of other participants, especially for the use of the certificate issued by other certification service providers.

The AKD is not responsible for other indirect damages that may result from the use of the certificate.

9.8. Limitations of liability

Total financial responsibility for transactions made on the basis of reliance in the certificates, issued according to this document, shall amount up to 265.445,62 euros.

The amount of the financial responsibility for the transactions towards persons and relying parties, that use certificates in an appropriate manner, shall be limited in accordance with the recommended financial limit.

Maximum financial limit that AKD accepts per transaction is indicated in the issued certificate, it the field *"CertificatePolicies", attribute "PolicyIdentifier", second last digit of the OID identifier (e.g.* Policy Identifier = 1.3.6.1.4.1.43999.5.4.2.1.***2***.1)

The following rules apply:

Identifier	Maximum Financial limit
1	Up to 1.061,78 euros
2	Up to HRK 10.617,82 euros
3	Up to HRK 53.089,12 euros

9.9. Indemnities

Each participant that causes damage due to the non-compliance with the provisions of applicable acts, standards, CP and CPS are liable towards the affected participant.

The natural or legal person is liable towards the affected party if:

a) he/she obtains a certificate on the eOI, issued by the KIDCA, based on fraudulent information given in the certificate application, or
b) he/she operates or presents himself/herself on behalf of the other natural person.

The relying party is liable towards the affected party if:

a) they confide in the certificate without verifying its validity, or
b) they use the certificate in an inappropriate manner for the purposes for which is not intended or in spite of set limitations.

The AKD is liable should this liability be clearly established by the agreement, CP [53], CPS or the applicable legislation and regulation.

9.10. Term and termination

9.10.1. *Term*

The application of the rules outlined in this document shall commence on the date of the publication of the document on the web portal as set forth in section 2.2.

The PMA decides upon the necessary amendments to the document and suitability of the document and its publication on the web portal as set forth in sections 1.5.3 and 1.5.4. Approval of the document is as set forth in section 1.5.4.

9.10.2. *Termination*

The document ceases to be in force when replaced by a newer edition of the document or when the termination of the document is published.

Information on the termination or publication of the new edition of the document is published on the web portal.

Termination of the document does not affect the certificate validity, issued according to the CPS outlined in the previous edition of the document, and while the document was in force.

9.10.3. *Effect of termination and survival*

With the new edition of the document, the new rules, outlined therein apply.

The certificates, issued according to the rules, outlined in the earlier edition of the document continue to be in force until the expiry of the validity period of the certificate or the certificate revocation.

9.11. Individual notices and communications with participants

Informing of persons and relying parties is carried out through the web portal.

The communication with the AKD is carried out in writing or by e-mail using the contact information indicated in the Table 13.

Table 13: Contact information of the AKD

Contact information of the AKD:	
Mailing address:	AKD d.o.o Savska cesta 31 HR-10000 Zagreb Croatia
e-mail:	pma@akd.hr

9.12. Amendments

9.12.1. *Procedure for amendment*

All significant changes that affect the participants are published in the new editions of the document according to the procedure set forth in section 9.12.2.

Typing errors, minor corrections or modifications that do not affect the participants are published in the versions of the documents. It is not necessary to send prior notice and/or modify the edition of the document.

The edition of the document is marked with the first number in the edition designation of the document, while versions are marked with the second number after the full stop.

Every participant may initiate the amendment to the document using the contact information indicated in section 9.11, and the PMA considers the proposal and decide whether to accept it or reject it.

Should the PMA determine that the proposed amendment is not in accordance with the legal regulations and standards or may impair the quality of the provision of service; the proposal by the participant is rejected.

9.12.2. *Notification mechanism and period*

The participants are informed on the new edition of the document through the web portal immediately following the publication of the document.

The participants are not informed on the new version of the document.

The accepted proposals by the participants are included in the new edition of the document.

9.12.3. *Circumstances under which OID has to be changed*

Minor corrections or modifications of content of CP or CPS that do not affect significantly all participants will be published without change of OID.

In case PMA defines that a change or modification of CP or CPS is a significant one, and that it may affect the participants, then a new OID that identifies an appropriate certificate or a group of certificates will be determined.

9.13. Dispute resolution provisions

All disputes and disagreements among the participants shall endeavour to resolve amicably. Should the amicable resolution of the dispute not be achieved, the disputes shall be resolved before the competent court in Zagreb with the application of the legislation of the Republic of Croatia.

9.14. Governing law

For the interpretation of the provisions of this document, provisions of the *Regulation (EU) No. 910/2014* [1], the AKD is a qualified trust service provider, which had been granted a qualified status by the supervisory body, the Ministry of Economy of the Republic of Croatia.

9.15. **Compliance with applicable law**

This document is compliant with the applicable law as specified in section 9.14.

In accordance with the *Regulation (EU) No. 910/2014* [1] , the AKD is a qualified trust service provider, which had been granted a qualified status by the supervisory body, the ministry responsible for economy of the Republic of Croatia.

9.16. **Miscellaneous provisions**

If not in contravention of the legal regulations, provisions of the CP or CPS, the AKD may, as the trust service provider, enter into an agreement with other participants which stipulates the commitments of the contracting parties to comply with the binding legal regulations and standards set forth in the section 9.14, as well as with the CPS and CP.

ANNEX 1: Definitions

1. ‘electronic identification’ means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person;
2. ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an on-line service;
3. ‘person identification data’ means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;
4. ‘electronic identification scheme’ means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing legal persons;
5. ‘authentication’ means an electronic process that enables the electronic identification of a natural or legal person, or the origin and integrity of data in electronic form to be confirmed;
6. ‘relying party’ means a natural or legal person that relies upon an electronic identification or a trust service;
7. ‘public sector body’ means a state, regional or local body, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;
8. ‘signatory’ means a natural person who creates an electronic signature;
9. ‘creator of a seal’ means a legal person who creates an electronic seal;
10. ‘electronic signature’ means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;
11. ‘advanced electronic signature’ means an electronic signature which meets the requirements set out in Article 26 *Regulation (EU) No 910/2014* [1];
12. ‘qualified electronic signature’ means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;
13. ‘electronic signature creation data’ means unique data which is used by the signatory to create an electronic signature;
14. ‘certificate for electronic signature’ means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;
15. ‘qualified certificate for electronic signature’ means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I *Regulation (EU) No 910/2014* [1];
16. ‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;
17. ‘advanced electronic seal’ means an electronic seal, which meets the requirements set out in Article 36 *Regulation (EU) No 910/2014* [1];

18. ‘qualified electronic seal’ means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;
19. ‘electronic seal creation data’ means unique data, which is used by the creator of the electronic seal to create an electronic seal;
20. ‘certificate for electronic seal’ means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person;
21. ‘qualified certificate for electronic seal’ means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III *Regulation (EU) No 910/2014* [1];
22. ‘electronic seal creation device’ means configured software or hardware used to create an electronic seal;
23. ‘qualified electronic seal creation device’ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II *Regulation (EU) No 910/2014* [1];
24. ‘trust service’ means an on line service normally provided for remuneration which consists of:
    a. the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
    b. the creation, verification and validation of certificates for website authentication; or
    c. the preservation of electronic signatures, seals or certificates related to those services;
25. ‘qualified trust service’ means a trust service that meets the applicable requirements laid down in this Regulation;
26. ‘conformity assessment body’ means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008 [9], which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides;
27. ‘trust service provider’ means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;
28. ‘qualified trust service provider’ means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;
29. ‘product’ means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
30. ‘electronic signature creation device’ means configured software or hardware used to create an electronic signature;
31. ‘qualified electronic signature creation device’ means an electronic signature creation device that meets the requirements laid down in Annex II *Regulation (EU) No 910/2014* [1];
32. certificate: public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it

33. Certificate Policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements
34. Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer
35. Certification Authority (CA): authority trusted by one or more users to create and assign certificates

    NOTE 1: A CA can be:

    1) a trust service provider that creates and assigns public key certificates; or
    2) a technical certificate generation service that is used by a certification service provider that creates and assign public key certificates.
36. Certification Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
37. Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-RTF.460-6 [52].
38. digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient
39. high security area: specific physical location of the security area where the Root CA key is held
40. Registration Authority (RA): entity that is responsible for identification and authentication of subjects of certificates mainly

    NOTE 1: The RA assist in the certificate application process and revocation process.
41. registration officer: person responsible for verifying information that is necessary for certificate issuance and approval of certification requests
42. revocation officer: person responsible for operating certificate status changes [i.8]
43. root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)
44. secure cryptographic device: device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user
45. secure zone: area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the systems used by the TSP
46. subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
47. applicant or subscriber: natural or legal person submitting the certificate request, owner of certificate
48. subject of certification (subject): natural persons whose name and surname are indicated in certificate subject fields: Common name and/or givenname and surname, and personal identification number in field serialnumber
49. subordinate CA: certification authority whose Certificate is signed by the Root CA NOTE: A subordinate CA issues end user certificates
50. remote signature creation device: signature creation device used remotely from signer perspective and provides control of signing operation on the signer's behalf

51. server signing application service component (SSASC): TSP service component employing a server signing application to create a digital signature value on behalf of a signer
52. server signing application service provider (SSASP): TSP operating a server signing application service component
53. signature creation device (SCDev): configured software or hardware used to implement the signature creation data and to create a digital signature value
54. TSA Disclosure Statement: Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to Subscribers and Relying Parties, for example to meet regulatory requirements
55. TSA Practice Statement: Statement of the practices that a TSA employs in issuing Time Stamp Tokens
56. Time-stampimg Service: trust service for issuing time-stamps.
57. Time-Stamping Authority (TSA): Trust Service Provider which issues time-stamp using one or more time-stamping units
58. 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
59. UTC(k): time scale realized by laboratory “k” and kept in close agreement with UTC, with the goal to reach ±100ns
60. Activation data: confidential data necessary to access or activate the cryptographic module. Activation data may be a PIN, password or electronic key which the person knows or possesses
61. Registration codes: data necessary for certificate registration and setting the PIN for private key activation in AKD mPotpis service operating QSCD device for remote signature creation

©AKD 2023

ANNEX 2: Acronyms

AKD	AKD d.o.o.
AKDCA	Certification Authority AKD Root
HRIDCA	Certification Authority for issuing certificates to natural persons for the purposes of the eOI issuance
KIDCA	Certification Authority for issuing certificates to natural persons for the commercial purposes
PKI	Public Key Infrastructure
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
CP	Certificate Policy
CPS	Certificate Practice Statement
TSA CP/CPS	TSA Policy/Practice Statement
TSA	Time-Stamping Authority
EUSCP	EU SSASC Policy
SSASC	Server Signing Application Service Component
SSASC PS	SSASC Practice Statement
AKD mPotpis	AKD SSASC
SCP	SSASC Policy
SSASP	Server Signing Application Service Provider
QCP	Qualified Certificate Policy
PMA	Policy Management Authority
CA	Certificate Authority
RA	Registration Authority
LRA	Local Registration Authority
OID	Object Identifier - Identifikacijska oznaka
SCD/ SCDev	Signature Creation Device
SSCD	Secure Signature Creation Device
QSCD	Qualified Electronic Signature Creation Device
RQSCD	Remote Qualified Electronic Signature Creation Device
IdP	Identity Provider
AKD IdP	AKD Identity Provider
SAML	Security Assertion Markup Language
SMS-OTP	One Time Password sent over Short Message Service
SCD	Signature Creation Data
DTBS	Data to be Signed

SAD	Signature Activation Data
SAP	Signature Activation Protocol
SIC	Signer's Interaction Component
SSA	Server Signing Application
SCA	Signature Creation Application
SCAL	Sole Control Assurance Level
SAM	Signature Activation Module
2FA	Two-Factor Authentication
PBKDF	Password Based Key Derivation Function
NIAS	Nacionalni identifikacijski i autentikacijski sustav
CRL	Certificate Revocation List
CARL	Certification Authority Revocation List
LDAP	Lightweight Directory Access Protocol
OCSP	On-line Certificate Status Protocol
HTTP	Hypertext Transfer Protocol
UTC	Coordinated Universal Time
RSA	Rivest, Shamir and Adleman algorithm
AES	Advanced Encryption Standard
HSM	Hardware security module
FIPS	Federal Information Processing Standard
x.509v3	Public Key Infrastructure Standard
PIN	Personal Identification Number
PUK	Personal Unblocking Code
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
EULA	End User Licence Agreement
PDS	PKI Disclosure Statement
PTC	Publicly-Trusted Certificate
TSU	Time-Stamping Unit

ANNEX 3: References

EU and national acts:

[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 62/2017, 08. July 2017.).

[3] REGULATION (EU) No 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[4] Implementation of the General Data Protection Act (Official Gazette 42/2018).

[5] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of 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.

[6] COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of 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.

[7] COMMISSION IMPLEMENTING DECISION (EU) 2015/296 of 24 February 2015 establishing procedural arrangements for cooperation between Member States on electronic identification pursuant to Article 12(7) of 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.

[8] COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of 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.

[9] REGULATION (EC) No 765/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.

[10] Public Notary Act (Official Gazette 78/1993, 29/1994, 162/1998, 16/2007, 75/2009, 120/2016).

[11] Freedom of Information Act (Official Gazette 25/2013, 85/2015).

[12] Civil Obligations Act (Official Gazette 35/05, 41/2008, 125/2011, 78/2015, 29/2018).

Normative references

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

[14] ETSI EN 319 403: “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers“.

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

[16] 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“.

[17] ETSI EN 319 412-1: “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.

[18] ETSI EN 319 412-2: “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons“,

[19] ETSI EN 319 412-3: “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons“.

[20] ETSI EN 319 412-5: “Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements“.

[21] ETSI TS 119 312: “Electronic Signatures and Infrastructures (ESI); Cryptographic Suites”.

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

[23] ETSI TS 119 431-1: „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev“.

[24] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[25] CEN EN 419 211-1: “Protection profiles for secure signature creation device - Part 1: Overview“.

[26] CEN EN 419 211-2: “Protection profiles for secure signature creation device - Part 2: Device with key generation“.

[27] CEN EN 419 211-3: “Protection profiles for secure signature creation device - Part 3: Device with key import“.

[28] CEN EN 419 211-4: “Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application“.

[29] CEN EN 419 211-5: “Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application“.

[30] CEN EN 419 211-6: “Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted communication with signature creation application“.

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

[32] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements".

©AKD 2023

[33] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing".

[34] CEN 419 221-5: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".

[35] IETF RFC 6960: „X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol – OCSP (2013)“.

[36] IETF RFC 3647: “Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework”.

[37] IETF RFC 3739: “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”.

[38] IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“.

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

[40] IETF RFC 5019 (2007): „The Lightweight On-line Certificate Status Protocol (OCSP) Profile for High-Volume Environments“.

[41] FIPS PUB 140-2 (2001): “Security Requirements for Cryptographic Modules”.

[42] FIPS PUB 186-4: „Digital Signature Standard (DSS)“.

[43] ISO/IEC 15408 (parts 1 to 3): “Information technology – Security techniques – Evaluation criteria for IT security”.

[44] ISO/IEC 14298: “Graphic technology – Management of security printing processes”.

[45] ISO/IEC 27001:2013: “Information technology — Security techniques — Information security management systems — Requirements”.

[46] ISO/IEC 27002:2013: „Information Technology – Security Techniques – Code of practice for information security controls“.

[47] ISO/IEC 9001:2015: “Quality management systems – Requirements”.

[48] ISO/IEC 27005:2011: “Information technology – Security techniques – Information security risk management”.

[49] ITU-T X.509 Recommendation: “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks”.

[50] ITU-T X.520 Recommendation: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[51] ITU-T X.501 Recommendation: „Information technology – Open Systems Interconnection – The Directory: Models“.

[52] ITU-R TF.460-6 Recommendation: “Standard-frequency and time-signal emissions”.

AKD documentation

[53] AKD PKI CP.

[54] AKD QTSA CP/CPS.

[55] AKD RA user manual.

ANNEX 4: History of document amendments

Edition	Date	Reasons for amendment
0.1	14.11.2016.	Draft 1st Edition of the KIDCA Certification Practice Statement Lite
1.0	15.05.2017.	Approved Edition.
1.1	12.12.2017.	Error corrections. Harmonization with Act on the Implementation of Regulation (EU) No. 910/2014 [2]. Corrections and additions regarding the implementation of TSA service.
1.2	04.07.2018.	Error corrections. Corrections and additions regarding the implementation of issuing qualified certificates for electronic seal and issuing of certificates for remote signing and remote sealing. Harmonization with The Law on the Implementation of the General Data Protection Act. Approved Edition.
1.3	01.07.2019.	Error corrections. Update and corrections of references. Additions regarding AKD mPotpis service for remote digital signature creation on behalf of the signer in line with ETSI TS 119-431-1 [23] and CEN 419 241-1 [32]. Approved Edition. Version for Public Release. Effective from July 15th 2019.
1.4	01.05.2020.	Error corrections. Update and corrections of reference. Certificate verification status requirements for trusted parties, availability of online certificate status verification, and end of certificate use updated. The provisions regarding the escrow of the person's private key have been corrected. The added obligation and responsibility of third parties to validate the e-signature / e-stamp before establishing trust. Added procedure for initial identity validation of natural persons performed in Notary Offices.
1.5	01.07.2021.	Alignment with the Amendments to the Identity Card Act (Official Gazette 144/2020). Corrections of detected errors in the document.
1.6	24.05.2023	Alignment with the changes in ETSI ESI norms (EN 319 401, EN 319 411). Corrections of detected errors in the document.Changes in currency from HRK to EUR.