AKD PKI
CERTIFICATE POLICY

Edition 2.4

Effective from May 1st, 2020

CONTENT

Foreword

AKD d.o.o (hereinafter: AKD) is a legal person, acting as a trust service provider within the meaning of the Regulation (EU) No. 910/2014 [1].

AKD, individually or jointly in cooperation with third parties, provides following trust services:

- Registration service
- Certificate generation service
- Revocation management service
- Revocation status service
- Dissemination service
- Subject device provision service
- Time-stamp issuing service and
- Remote signature creation service.

AKD is a qualified trust service provider that was granted a qualified status by the supervisory body, the ministry responsible for Economy of the Republic of Croatia, based on the favourable report by the conformity assessment body.

AKD has been providing trust services since 2015 when it began issuing electronic identity cards for Croatian citizens and certificates stored on them and issued by HRIDCA. Since 2017 AKD is issuing certificates for commercial purposes from KIDCA system. Since 2018 AKD is issuing qualified time-stamps and providing remote signature and seal creation service AKD mPotpis implementing and managing remote QSCD device for signature creation on behalf of the signatory or creator of a seal.

AKD promotes the use of the electronic identity card and contributes to the building of trust into e-commerce as a whole, which is a key factor for the economic development of the society and the well-being of the wider community.

1. Introduction

1.1. Overview

1.1.1. *Structure of document*

This document, the "AKD PKI Certificate Policy" (CP), specifies a set of rules according to which AKD provides trust services.

According to the IETF RFC 3647 [37], the CP corresponds to the document called "Certificate Policy – CP", due to which the structure and the content of the document are in strict compliance with the requirements of mentioned standard.

In case of conflict between the Croatian original document and the English translation the Croatian original shall prevail.

This document contains:

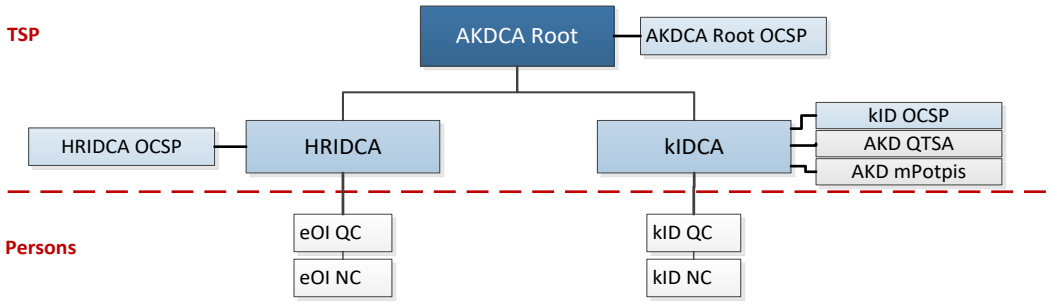
- Chapter 1: Data on the participants and the use of a certificate,
- Chapter 2: Information published by the trust service provider,
- Chapter 3: Processes for verifying the identity and identification information of the person,
- Chapter 4: Processes relating to the issuance and the management of the certificate's life-cycle,
- Chapter 5: Management, operational and facility controls and processes implemented in order to protect the certification system,
- Chapter 6: Technical security controls of the certificate, private key and information systems,
- Chapter 7: The facts contained in certificates and CRL,
- Chapter 8: Control and verification of compliance that is conducted over the provision of certification services and
- Chapter 9: Other business and legal provisions related to the certification services and trust service provider.

1.1.2. *Scope of document*

The Rules set forth in this document apply to the whole hierarchical infrastructure based on the root certification authority called AKDCA Root.

AKDCA Root issues certificates to HRIDCA and KIDCA subordinate.

Figure 1: Hierarchical model AKD PKI



AKD issues qualified (QC), normalized electronic certificates (NC), issues qualified electronic time-stamps using AKD QTSA service and provides AKD mPotpis service for remote signature creation on behalf of the signatory or creator of a seal.

HRIDCA and KIDCA are subordinate issuing CAs.

HRIDCA issues certificates exclusively for Croatian eID purpose.

KIDCA issues certificates for commercial purposes and certificates solely used for AKD QTSA time-stamping service.

KIDCA also issues certificates which are used in AKD mPotpis service implementing and managing remote QSCD device for remote signature and seal creation on behalf of the signatory or creator of seal.

Providing time-stamping services is not in scope of certification services according to this CP and time-stamping policy and practice statements are defined in the document AKD QTSA Policy and Practice Statement for providing time-stamping services (hereinafter: AKD QTSA TSP/PS) [56].

1.1.3. *Purpose of document*

This document is intended for:

- Persons, to gain detailed information about their rights and obligations as well as about the rights and obligations of trust service provider,
- Relying parties, to determine the suitability of the particular type of a certificate for the particular purpose, a group of persons and/or online service,
- Trust service provider, which, on the basis of the document, produces the rules of Procedure on Certification Procedures (or *Certification Practice Statement – CPS*, *[54] and [55]* hereinafter: CPS) that specify organisational and technical measures which ensure the implementation of these security requirements in practice,
- Conformity assessment bodies and supervisory bodies, to assess the ability of AKD to provide qualified trust services and its status as a qualified service provider.

Security requirements, defined in this document, are harmonised with the strict requirements for qualified trust service providers and qualified trust services that they provide, which are prescribed by the Regulation (EU) No. 910/2014 [1] and Act Implementing the Regulation (EU) No. 910/2014 [2].

1.2. Document name and identification

1.2.1. *Document name*

Code:	PRO-I-90-02
Name:	AKD PKI CP
Edition:	2.4
Publication date:	1st May 2020
Author:	AKD d.o.o.
Document type:	Certificate Policy
Availability:	http://eid.hr/cps and http://id.hr/cps

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.

Personal **qualified** certificates are issued according to the rules that are equivalent to the **QCP-n-qscd** rules, according to the chapter 5.3 of the ETSI EN 319 411-2 [17], and which are applied for the EU qualified certificates for natural persons with the private key on the qualified electronic signature creation device (QSCD).

Identification code of these certificates is:

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

Personal **normalized** certificates are issued according to the rules that are equivalent to the **NCP+** CPS, according to the chapter 5.3 of the ETSI EN 319 411-1 [16], and which are applied for the certificates of general purpose with the private key on the secure cryptographic device.

Identification code of these certificates is:

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

Qualified certificates for electronic seal are issued to legal persons according to the **QCP-l-qscd** rules, according to the chapter 5.3 of the ETSI EN 319 411-2 [17], and which are applied for the EU qualified certificates for legal persons with the private key on the secure cryptographic device.

Identification code of these certificates is:

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

The following table contains identification codes of OCSP and TSU certificates.

Table 1: Identification code of OCSP and TSU certificates

Name	Identifier	OID
AKDCA Root OCSP certificate	AKD NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.0.1.2.1.9
HRIDCA OCSP certificate	eOI NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.2.1.2.1.9
KIDCA OCSP certificate	KID NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.5.1.2.1.9
KIDCA TSU certificate	KID QCP-l-scd-tsa	1.3.6.1.4.1.43999.5.4.1.2.2.8

Identification codes and rules for certificate issuance are set out in the corresponding CPS, [54] and [55].

Rules and practice statements for issuing qualified time-stamps (AKD QTSA) are set out in the TSP/PS [56].

Rules and practice statements for AKD mPotpis service operating a remote QSCD for remote signature and seal creation are set out in the KIDCA CPS [55].

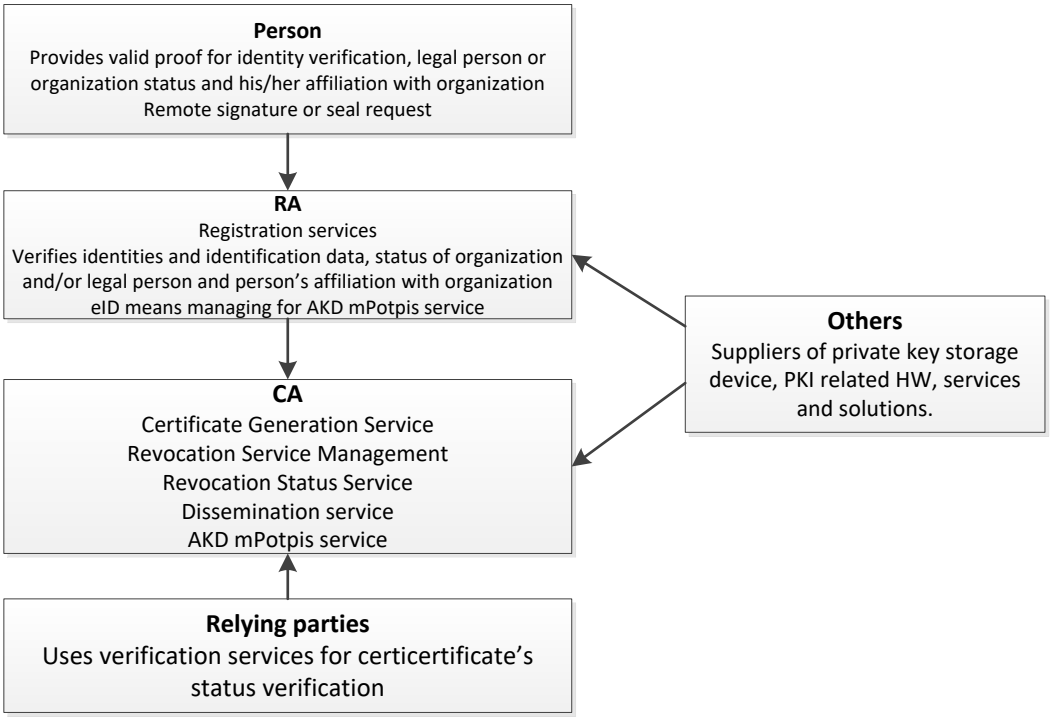
1.3. PKI participants

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.

The participants and the services that they provide are shown in the following layout.

Figure 2: The relationship between the participants



Responsibilities of all AKD PKI participants are set out in section 9.6 and in the corresponding CPS, [54] and [55].

Responsibilities of AKD as Server Signing Application Service Provider (SSASP) regarding the providing of AKD mPotpis service for remote signature creation are set out in KIDCA CPS [55].

1.3.1. *Certification Authority*

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

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 is 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**.**

1.3.3. *Policy Management Authority – PMA*

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 prescribed with 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.

1.3.4. *Registration Authority – RA*

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

The affairs of the RA include:

a) Informing persons on procedures for registration and issuance of the certificate,
b) Receiving requests for issuance, revocation and suspension of certificates,
c) Identity, status and association validation of persons and applicants,
d) The conclusion of the Agreement on certification services,
e) Delivering of the device with the private key (QSCD).

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.

In the event that all or some affairs are delegated to the third party, the third party must ensure to fulfil the following requirements under a contract:

a) To ensure that the identity of the personnel, authorised to perform the registration, is undoubtedly established and that the person is reliable and conscientious,
b) To perform controls related to the personnel, authorised to perform the registration in accordance with section 5.3,
c) To keep the documentation in accordance with section 5.5.2,
d) To carry out registration in a manner described in section 3,
e) To undertake to abide by the CP and CPS or provide their own documented procedures pursuant to which the supervisory bodies are able to perform control and verification of the compliance with the requirements of the standards.

The affairs of RA can include other activities in the scope of services provided by subordinated CA, set out in corresponding CPS, [54] and [55].

1.3.5. ***Persons***

Person can be a natural person or legal person.

The natural person that is named as the Subject of certification in the certificate may be:

a) A natural person, acting on his/her own behalf, or
b) A natural person affiliated with an organizational entity.

Whenever a natural person is the subject of certification he/she shall accept responsibilities and warranties from section 9.6.4.

Whenever a natural person is named in the certificate that is identified in affiliation with an organizational entity, and requirements from section 3.2.2 of the corresponding CPS, [54] and [55], are fulfilled, organizational entity shall also accept responsibilities and warranties from section 9.6.4.

For certificates for electronic seal issued to legal persons, legal person is named in the Subject of certificate.

Legal person who creates an electronic seal is a creator of seal.

Creator of seal is represented by authorized representative. Authorized representative accepts on behalf of the creator of seal the conditions for providing certification services (PDS).

Authorized representative is in possession of QSCD with certificate for electronic seal and/or registration codes for certificate registration a setting the activation data for private key in AKD mPotpis service.

Subscriber can be a natural or legal person who submits certificate application. If the Subscriber is a different person from a Subject, Subscriber is a certificate owner.

1.3.6. *Relying parties*

The relying parties are natural or legal persons who provide online 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 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 [44] *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 [44] *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 and CPS, [54] and [55], manufacturer provides the following affairs:

a) The preparation and production of secure cryptographic devices (cards or QSCD) for persons,
b) Generation of the cryptographic key pairs for a person and their entry into the secure cryptographic devices,
c) Distribution of the devices to the persons, 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+.

AKD is the manufacturer of the QSCD devices which are delivered to persons in possession.

1.4. Certificate usage

1.4.1. *Appropriate certificate uses*

The root CA issues a certificate to itself and to the subordinate CA, while the subordinate CA issues certificates to persons.

The CA certificates are also used for the issuance of the associated CRL and for the issuance of the OCSP certificate.

According to usage, certificates are grouped:

a) **CA Certificates** are used for the issuance of the associated CRL, issuance of the certificate to persons and for the issuance of the OCSP certificate, as follows:
   - **AKD Root CA** certificate used to for signing subordinate CA: HRIDCA and KIDCA,
   - **HRIDCA** certificate used for certificates issued to natural persons for eOI and
   - **KIDCA** certificate used for certificates issued to natural and legal persons for commercial purposes.

   Corresponding private keys of CA certificates are securely stored on secure cryptographic device.

b) **OCSP** certificate used for signing OCSP replies. Every CA issues its own OCSP certificate. Corresponding private key is securely stored on secure cryptographic device.

c) **TSU** certificate used for signing AKD QTSA service replies. TSU certificates are used solely by AKD QTSA service and are issued by KIDCA solely for AKD QTSA.

   Corresponding private keys of OCSP and TSU certificates are securely stored on secure cryptographic device.

d) **eOI** certificates are issued by HRIDCA to end users, according to eID law [13]. Appropriate usage of certificates is defined in CPS HRIDCA [54].

e) **KID** certificates are issued by KIDCA to end users. Appropriate usage of certificates uses is defined in CPS KIDCA [55].

Certificate's usage is defined in X.509 v3 certificate's extensions: „KeyUsage", „Extended Key Usage" (see section 7).

1.4.2. *Prohibited certificate usages*

Any usage of the certificate, not specified in section 1.4.1, is prohibited.

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

When verifying the certificate validity, described in section 9.6.5 of this document, the relying parties should verify the OID of the certificate in *Table 1* in order to reach a valid decision on the approval or rejection of the certificate for a particular purpose.

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 this 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

webpage: http://eid.hr, http://id.hr

1.5.3. *Person determining document suitability*

The PMA is responsible for the conformity assessment of the document with the national and EU regulations and the technical specifications, standards and procedures related to the electronic identification and trust services.

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. *CP 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 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 [16], ETSI EN 319 411-2 [17] and ETSI EN 319 422 [23] .

2. Publication and repository responsibilities

2.1. Repositories

The CA makes the information, necessary to verify the certificate's status, available to the public, which includes:

a) Information on the certificate's status that are available as the OCSP service ,
b) Last issued CRL for the root and subordinate CA and
c) CA certificates.

Every end user certificate contains addresses where CA certificate, CRL and OCSP service are available.

The certificates, issued by the root and subordinate CA, are contained in the structure of the public directory, and may be available to the public under the conditions set forth in section 2.4.

2.2. Publication of certification information

All information that persons and relying parties may need in order to use the trust services are published on the web portals of the trust service provider, http://eid.hr for certificates issued by HRIDCA and http://id.hr for certificates issued by KIDCA.

The basic information that is published on the web portal includes, but is not limited to:

a) Rules for providing certification services - Certificate policy (CP), http://eid.hr/cps; http://id.hr/cps
b) Rules for certification procedure - Certification practice statement (CPS, [54] and [55]), http://eid.hr/cps; http://id.hr/cps
c) Conditions/Agreement for providing certification services - PKI disclosure statement (PDS),
d) Notifications related to the provision of certification services, and
e) Other information relevant to persons and relying parties.

The CA provides additional information and services to the registered persons, such as:

a) Information and applications for the device (QSCD) usage,
b) Information and applications for using the AKD mPotpis service and managing two-factor eID means for authenticating to AKD mPotpis service, and
c) On-line services for certificate's status verification and the suspension of a certificate.

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 part of the content may be available in English.
c) CP, CPS, [54] and [55], 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 according to section 4.9.7.

f) Information on the certificate's status is available under the conditions specified in section 4.10.
g) CRL issuance frequency is according to section 4.9.7.
h) OCSP service is available according to section 4.9.10.
i) The CA is obliged to provide a continuous availability of the repository 24 hours a day, 7 days a week in accordance with the best business practices.
j) Following the system failure or other factors that are out of the CA's control, all available means have to be applied 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.
b) Additional information and services on the web portal is 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 person can be available for the public search if the consent of the person is provided. Consent for public search of person's certificates is determined according to the corresponding CPS, [54] and [55].
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 field „Subject" of each certificate contains data which represents natural or legal person name.

The name of the certificate is determined in accordance with the rules of the Recommendation ITU-T X.520 [51] or IETF RFC 5280 [39].

The field „Subject" is determined in accordance with the rules of the Recommendation ITU-T X.501 [52].

Rules applied for certificates containing the „Subject Alternative Name" field are in accordance with Recommendation IETF RFC 5280 [39].

In case of CA, OCSP and TSU certificates, the "Subject" field is formed as follows:

Field	Explanation
commonName:	Name of CA certificate, OCSP system or TSA system affiliated to legal person.

organizationIdentifier:	Identification number of the legal person – trusted service provider.
organizationName:	Name of the legal person - trusted service provider.
countryName:	2 characters ISO country code.

In case of certificates issued to natural persons, the "Subject" field is determined in accordance with the rules of the corresponding CPS, [54] and [55].

In case of commercial certificates issued to legal persons, the "Subject" field is determined in accordance with the rules of the corresponding KIDCA CPS [55].

3.1.2. *Need for names to be meaningful*

Names contained in the *„Subject"* field of certificates must be meaningful and CA must be able to identify natural or legal person with the included data.

3.1.3. *Anonymity or pseudonyms of subscribers*

Not supported.

3.1.4. *Rules for interpreting various name forms*

Rules for interpreting various name forms are indicated in tables.

Table 2: Rules for interpreting CA, TSU and OCSP certificates

Field	Explanation
CommonName (cn)	Name of CA or OCSP or TSA system.
organizationName (O)	Name of the legal person - trusted service provider.
organizationIdentifier	VATHR-OIB, where the VAT code indicates a legal person, HR means the country code, minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) and OIB means the tax identification number of the legal person.
countryName (C)	Two-letter ISO code of the country of the trusted service provider (HR).

Table 3: Rules for interpreting certificates for natural persons

Field	Type of certificate	Explanation
CommonName (cn)	All End Entity	Name Surname represents the name and the surname of the natural person from the identification document.

serialNumber	All End Entity	PNOHR-OIB, where the PNO code indicates a natural person, HR means the country code, minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) and OIB means the personal identification number
givenName (g)	All End Entity	Name represents the name of the natural person (certificate subject).
Surname (sn)	All End Entity	Surname represents the surname of the natural person (certificate subject).
organizationalUnitName (OU)	All End Entity	Type of the certificate (signing, identification).
organizationName (O)	HRIDCA End Entity	Name of the CA that issues certificates.
	KIDCA End Entity	Name of the organization affiliated with natural person.
organizationIdentifier	HRIDCA End Entity	No stipulation.
	KIDCA End Entity	VATHR-OIB, where the VAT code indicates a legal person, HR means the country code, minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) and OIB means the tax identification number of the organization affiliated with natural person.
countryName (C)	All End Entity	Two-letter ISO code of the country of natural person (certificate subject).

Table 4: Rules for interpreting certificates for legal persons (electronic seal)

Field	Type of certificate	Explanation
CommonName (cn)	KIDCA End Entity	Name commonly used by the legal person - Creator of seal to represents itself.
organizationalUnitName (OU)	KIDCA End Entity	Type of the certificate (seal, rseal)
organizationName (O)	KIDCA End Entity	Name of the legal person
organizationIdentifier	KIDCA End Entity	VATHR-OIB, VAT indicates a legal person, HR is the country code, A minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) and OIB is a tax identification number of legal person
countryName (C)	KIDCA End Entity	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 to whom 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.

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*

The following rules apply:

a) Private keys of certificates of natural or legal persons are generated in the HSM device and are entered on to a qualified electronic signature creation device (QSCD) or generated and used within remote QSCD device in a secure environment.

b) The QSCD with private keys of a person intended for persons possession must be delivered directly to the person following the identity validation.

c) Registration codes used for certificate registration and setting the activation data (PIN) in AKD mPotpis service for private keys managed by qualified trusted service provider on behalf of the signatory are delivered to natural person or person representing the legal person (authorized representative) following the procedures set out in KIDCA CPS [55].

d) The private keys of the certificates for devices and systems (CA, TSU, OCSP) are generated in the SCD device in a secure environment where they remain during their use. Whenever the certificates for devices or systems (CA, TSU, OCSP) are issued, it is necessary to authorise the natural person which take care of the private key and SCD when applicable.

3.2.2. *Authentication of legal person identity*

Data collection and verification conducted by RA/LRA, in the registration process of organization or legal person, is carried out in accordance with the national law in the Republic of Croatia and rules set out in section 6.2.2 of the ETSI EN 319 411-2 [17].

3.2.3. *Authentication of individual identity*

In the registration process of individuals, RA/LRA validates person's identity and, if applicable, special markings of person which is certification subject, in accordance with the national law in the Republic of Croatia and rules set out in section 6.2.2 of the ETSI EN 319 411-2 [17].

3.2.4. *Non-verified subscriber information*

The RA/LRA does not verify additional contact information, as a person is responsible for their accuracy.

3.2.5. *Validation of authority*

Rules set out in the corresponding CPS are applied, [54] and [55].

3.2.6. *Criteria for interoperation*

No stipulation.

3.2.7. *Miscellaneous provisions on initial identity validation*

Rules set out in the corresponding CPS are applied, [54] and [55].

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*

The following rules apply:

a) Upon issuance of the new pair of keys, information and documents provided during the initial identity validation according to section 3.2.3 may be used.
b) The information verification is carried out the same way as in the initial identity validation in section 3.2.3.
c) Care should be taken that all information and documents, collected upon initial identity validation, are still valid and are restored when necessary.

3.4. Identification and authentication for revocation request

Identification and authentication of the person upon submitting a request for revocation is carried out according to requirements of the ETSI EN 319 411-2 [17], section 6.2.4.

4. Certificate life-cycle operational requirements

4.1. Certificate Application

4.1.1. *Who can submit a certificate application*

Application can be submitted by:

a) natural person who is certification subject,
b) legal representative of the organization affiliated with certification subject,
c) authorised representative on behalf of the legal person – creator of seal, and
d) authorised CA personnel for CA, TSU and OCSP certificate application.

The rules for issuing of the certificates are set out in the corresponding CPS, [54] and [55].

4.1.2. *Enrolment process and responsibilities*

The rules are set out in the corresponding CPS, [54] and [55].

4.2. Certificate application processing

4.2.1. *Performing identification and authentication functions*

Identity of natural persons is validated according to the rules set out in section 3.2.3.

Identity of natural persons affiliated to organization is validated according to the rules set out in section 3.2.3.

Identify of organization or legal person is validated according to the rules set out in section 3.2.2.

4.2.2. *Approval or rejection of certificate applications*

The rules applied are set out in the corresponding CPS, [54] and [55].

4.2.3. *Time to process certificate applications*

The rules applied are set out in the corresponding CPS, [54] and [55].

4.3. Certificate issuance

4.3.1. *CA actions during certificate issuance*

Actions during certificate issuance are in accordance with ETSI EN 319 411-1 [16], section 6.3.3 and rules set out in the corresponding CPS, [54] and [55].

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

The rules applied are set out in the corresponding CPS, [54] and [55].

4.4. Certificate acceptance

4.4.1. *Conduct constituting certificate acceptance*

Certificate acceptance is conducted in accordance with ETSI EN 319 411-2 [17], section 6.3.3 and rules set out in the corresponding CPS, [54] and [55].

4.4.2. *Publication of the certificate by the CA*

The rules applied are set out in the corresponding CPS, [54] and [55].

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

The rules applied are set out in the corresponding CPS, [54] and [55].

4.5. Key pair and certificate usage

4.5.1. *Subscriber private key and certificate usage*

Issued certificates and corresponding private keys are used by the natural person or authorized representative of the legal person. Subject of certification or legal person is named in the *„Subject"* field of certificate.

Subject of certification or representative of legal person on behalf of the legal person having accepted the conditions for providing certification services or concluded Agreement on certification services are obligated to fulfil the responsibilities indicated in section 9.6.4 for the entire life-cycle of certificate (see section 4.9).

Conditions for providing certification services include:

a) Information about certification service provider, scope of provided services and rules for providing the services,
b) Information about certificate types, appropriate and prohibited certificate usage and certificate status related services,
c) Information on authentication means, activation data and private keys used in AKD mPotpis service for remote signature and seal creation,
d) Representations and warranties of natural persons, certification services provider and relying parties,
e) Information regarding liability, prices, etc.,
f) Data protection and confidentiality provisions,
g) Communication, complaint and dispute resolution procedures and
h) Applicable conditions and agreements, CP, CPS, government law regulations and supervision 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 responsibilities indicated in section 9.6.5.

4.6. Certificate renewal

4.6.1. *Circumstances 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 4.7.1).

4.6.2. *Who may request renewal*

The rules from section 4.1 apply.

4.6.3. *Processing certificate renewal requests*

The rules from section 4.2 apply.

4.6.4. *Notification of new certificate issuance to subscriber*

The rules from section 4.3 apply.

4.6.5. *Conduct constituting acceptance of a renewal certificate*

The rules from section 4.4.1 apply.

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

The rules from section 4.4.2 apply.

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

The rules from 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 4.6), or
b) If the certificate must be modified (refer to 4.8), or
c) In the case of issuing of new certificate after revocation (refer to 4.9).

The CA does not reactivates the revoked certificate, but a new pair of keys and a new certificate is issued to the person in case of a)-c) requests. Detailed rules are out in the corresponding CPS, [54] and [55].

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

The rules from section 4.1 apply.

4.7.3. *Processing certificate re-keying requests*

The rules from section 4.2 apply.

4.7.4. *Notification of new certificate issuance to subscriber*

The rules from section 4.3 apply.

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

The rules from section 4.4.1 apply.

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

The rules from section 4.4.2 apply.

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

The rules from 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, or
b) It was found that the information, contained in the certificate, are incorrect.

Any modification of the certificate means issuing of a new pair of keys (refer to section 4.7.1). Additional circumstances and rules are set out in the corresponding CPS, [54] and [55].

4.8.2. *Who may request certificate modification*

The rules from section 4.1 apply.

4.8.3. *Processing certificate modification requests*

The rules from section 4.2 apply.

4.8.4. *Notification of new certificate issuance to subscriber*

The rules from section 4.3 apply.

4.8.5. *Conduct constituting acceptance of modified certificate*

The rules from section 4.4.1 apply.

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

The rules from section 4.4.2 apply.

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

The rules from 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 authorised 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.
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 unauthorised use of the QSCD has been reported, private key or activation data is not in solely possession of the subject of certification or Authorised Representative or whenever the private key compromising is possible. Private key activation PIN for certificate for remote signing used in AKD mPotpis service is permanently lost.
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 authorised or it was retroactively withdrawn.
l) It was found that the certificate was not issued in accordance with the CPS or CP.
m) The CA certificate was revoked.

The CA certificate is revoked under the following circumstances:

n) 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.
o) The CA private key compromising has been established.
p) When the certification service provider, due to technical, contractual or any other reason, ceases to issue certificates or ceases to provide certification services.

Additional circumstances and rules for revocation may be specified in the corresponding CPS, [54] and [55].

4.9.2. *Who can request revocation*

The certificate revocation may be requested by:

a) The natural person named as certification subject or his/her legal representative,
b) Authorized representative or legal representative on the behalf of legal person,
c) Authorized RA/LRA personnel,
d) PMA and
e) Authorized CA personnel.

4.9.3. *Procedure for revocation request*

The rules applied are set out in the corresponding CPS, [54] and [55].

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.

Additional rules may be set out in the corresponding CPS, [54] and [55].

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

CA must process the revocation request within a reasonable time accordingly to the rules specified in the corresponding CPS, [54] and [55].

4.9.6. *Revocation checking requirement for relying parties*

Services concerning the certificate's status are available on-line.

Should the relying party, for any reason at a particular moment, fail to obtain information concerning the certificate's status, 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) CRL contains information about time of issuance and validity period.
b) Subordinate CA obliges to issue a CRL at least 1-time within 24 hours.
c) The period of the validity for HRIDCA/KIDCA CRL is 24 hours from the time of the issuance of the CRL.
d) AKDCA CRL is valid for 90 days after the CRL issuance.
e) In the case of the CA certificate revocation, the CRL list is issued within 24 hours.
f) If the validity period of the certificate that is revoked and present on the CRL list expires, the certificate can be removed from the CRL list.
g) 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 the certificate's status via the OCSP service.

OCSP respond must be according to IETF RFC 6960 [36] and IETF RFC 5019 [41].

Certificate for OCSP service complies with the rules set out in IETF RFC 6960 [36], and it accordingly contains the id-pkix-ocsp-nocheck extension.

4.9.10. *On-line revocation checking requirements*

The on-line certificate's status verification via OCSP service is enabled according to the rules specified in the corresponding CPS, [54] and [55], and:

a) The OCSP service is available via HTTP protocol at the address published in the field „AuthorityInformationAccess“ in each certificate.
b) 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.
c) 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".
d) If the OCSP service receives a request for the certificate's status verification, and CA certificate status is not verified or CA certificate's status is not valid, it does not respond with a status "Good".
e) 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*

Other forms of revocation advertisements may be specified in the corresponding CPS, [54] and [55].

4.9.12. *Special requirements re-key compromise*

The CA, in accordance with the chapter 4.9.1, revokes the certificate if the private key was confirmed compromised.

4.9.13. *Circumstances for suspension*

Circumstances for suspension of certificates include:

a) An authorised request for the certificate suspension was 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 may be subsequently 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 authorised request for the withdrawal of the suspension of the certificate has been submitted.
h) The 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) The natural person named as certification subject or his/her legal representative,
b) Authorized representative or legal representative on the behalf of legal person - creator of seal,
c) Authorized RA/LRA personnel,
d) PMA and
e) Authorized CA personnel.

4.9.15. *Procedure for suspension request*

Procedures for suspension request are specified in the corresponding CPS, [54] and [55].

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 limited time period.

If the withdrawal of the suspension of a certificate is not requested within limited time period from the submission of the request for suspension, the suspended certificate will be revoked.

Limited time period is specified in the corresponding CPS, [54] and [55].

4.10. Certificate status services

4.10.1. *Operational characteristics*

Public addresses for status verification using the OCSP service and retrieving the CRL are contained in the issued certificates.

Services concerning the certificate's status are in accordance to ETSI EN 319 411-2 [17], section 6.3.10.

Procedures applied are set out in the corresponding CPS, [54] and [55].

4.10.2. *Service availability*

Rules specified in the corresponding CPS, [54] and [55] are applied, including:

a) Services for revocation, suspension/withdrawal of the suspension of a certificate in RA/LRA offices are available during work hours.
b) Under normal circumstances requests for suspension/withdrawal of the suspension of a certificate may be submitted on-line, 24 hours a day, 7 days a week.
c) Under normal circumstances availability of services for CRL and OCSP verification of the current certificate's status is 24 hours a day, 7 days a week.
d) In order to shorten the processing time and certificate's status verification it is recommended to use the OCSP protocol.
e) In the case of system failure, the service is available within the shortest time possible and in accordance with the positive business practices.

4.10.3. *Optional features*

Not foreseen.

4.11. End of subscription

End of subscription occurs under following circumstances:

a) The validity period of the person's certificate has expired (field *„Valid to"*) or
b) Person's certificate has been revoked.

4.12. Key escrow and recovery

The CA does not escrow or recover the private keys of persons on QSCD (card).

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 [44] 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 controls the physical access to the entire PKI infrastructure, data and all system components related to the provision of the trust services and conduct the activities of assessment and combating the risk.

Physical security measures are applied in accordance with the ETSI EN 319 401 [14] and chapter 11 of the ISO/IEC 27002 [47].

Implemented physical security measures are set out in the corresponding CPS, [54] and [55].

5.1.1. *Site location and construction*

In order to achieve specified levels of security, facilities and areas where the information system is located and where the activities to provide certification services are taking place, are organised into security zones.

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

The production CA systems are located in a high-security area where the most stringent physical, technical and procedural protection measures are being applied.

5.1.2. *Physical access*

The physical access to facilities and areas in which the CA systems are located and CA related activities are undergoing are controlled and monitored. Moreover, the access rights are limited to the authorised personnel.

Physical access to high-security zones is carried out with the presence of at least two authorized persons.

5.1.3. *Power and air conditioning*

The areas where the information infrastructure is located are properly air-conditioned, and all equipment is connected to the source of uninterrupted power supply.

5.1.4. *Water exposures*

The AKD takes appropriate protection measures against flooding.

5.1.5. *Fire prevention and protection*

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

5.1.6. *Media storage*

Media containing relevant data in scope of this document, logs, archives or backups are stored in security containers located in secure zones protected by physical and logical controls.

In order to prevent an unauthorised 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 [47].

5.1.7. *Waste disposal*

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

5.1.8. *Off-site backup*

The backups are kept in security containers at two separate locations in secure zone which meets the same or higher level of physical and logical protection requirements as set out in this document.

5.2. Procedural controls

Procedural controls are specified in detail in the corresponding CPS, [54] and [55].

5.2.1. *Trusted roles*

The authorised employees who are involved in the implementation of the certification activities are granted the appropriate trusted roles with clearly defined responsibilities and authorisations in accordance with the ETSI EN 319 401 [14], CEN TS 419 261 [32], ETSI TS 119 431-1 [24] and CEN EN 419 241-1 [33].

The trusted roles include, but are not limited to the security administrators, RA officers, officers for the revocation, information system administrators, operators and controllers.

5.2.2. *Number of persons required per task*

The principle of split knowledge and dual control is included in all the activities of the management of cryptographic keys and administration of the critical information systems.

5.2.3. *Identification and authentication for each role*

All information equipment is configured in such manner which enforces a strict compliance with the defined security rules and prevents the implementation of the activities without prior authentication of authorised 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 enforced.

Identification and authentication of the RA officers and CA personnel are carried out according to the rules set out in the corresponding CPS, [54] and [55].

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.

5.3. Personnel controls

Personnel controls are implemented in accordance with the ETSI EN 319 401 [14] and chapter 7 of the ISO/IEC 27002 [47].

5.3.1. *Qualifications, experience, and clearance requirements*

When employing, the AKD conducts a strict selection procedure in accordance with the documented internal rules.

When changing duties or termination of employment, the user's access rights for CA area and user rights for CA information system will be revoked from by the authorized CA staff.

RA authorized personnel will revoke user rights for the RA information system from the RA officers in case of changing duties or termination of employment.

5.3.2. *Background check procedures*

A formal process to assess the suitability of the employee for a specific role is performed according to the predefined criteria when assigning roles and selecting employees that are involved in the implementation of the certification activity

In order to assigning duties to the CA personnel and RA/LRA officers it is necessary to reliably establish the suitability of personnel, their reliability and conscientiousness, and verify their identity.

When selecting CA personnel, it is strictly considered that the employee has the permanent work contract with AKD.

In the event that all or some RA affairs are contracted to the third party, the third party must undertake to fulfil the RA personnel requirements set forth in this point. RA officers must be employees of third party.

5.3.3. *Training requirements*

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

The AKD provides internal procedures and training instructions for education of RA/LA and CA personnel, in order to ensure that employees understand and are aware of their obligations and responsibilities.

Professional training is provided for AKD's employees in order to obtain an adequate knowledge needed to perform the business functions of the employees.

In the event that all or some RA affairs are contracted to the third party, the third party must undertake to fulfil the RA personnel training requirements set forth in this point.

5.3.4. *Retraining frequency and requirements*

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

Informing the employees about the rules of conduct, their obligations and responsibilities, is carried out during the introduction of the new internal rules and in the event of significant changes, at least once every two years.

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 unauthorised actions*

A strict disciplinary action shall be 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.

In the event that all or some of RA affairs are delegated to the third party and third party is using services of independent contractors, the third party must undertake to abide by the CP and CPS in order to provide registration services.

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 the certification authority.

5.4. Audit logging procedures

5.4.1. *Types of events recorded*

The following rules apply:

a) Audit logs must be available in electronic form, where this is not possible, evidence must be provided in the printed form.

b) Audit logs include, but are not limited to, the following records:
   - natural and legal persons registration, certificate's life-cycle management: issuing, revoke, suspension and withdrawal of suspension,
   - management of cryptographic keys and QSCD,
   - service operation, and
   - administration and maintenance of the information system.

c) Audit logs are sufficient, as evidence of meeting the security requirements, in order to perform the monitoring or in order to adequately investigate the unauthorised use of the information system, should the need arise.

d) Audit logs are kept in form which allows their representation as evidence of compliance with security requirements.

e) Information systems generating audit logs are provided with reliable time service source, in order to log valid date and time of recorded event.

Detailed rules are set out in the corresponding CPS, [54] and [55].

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 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*

Configuration procedures are established in order to ensure that audit logs on critical information systems cannot be erased or automatically overwritten.

Audit logs are adequately protected and credible and may be presented as material evidence in possible subsequent court proceedings.

Protection of audit logs includes protection against unauthorised reading, modification, destruction and disruption of integrity.

5.4.5. *Audit log backup procedures*

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

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 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.

Audit logs of all critical information systems are managed by log management system.

The log management system provides searching of audit logs, by the type, date and time of the event.

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 assessment is performed by analysing audit logs in the log management systems and using approved software tools.

5.5. Records archival

5.5.1. *Types of records archived*

All types of records in scope of providing the certification service are archived including, but are not limited to:

a) audit logs and events as set forth in section 5.4.1,
b) evidence of identity of natural and legal persons provided in registration process as set forth in section 3 of CP and corresponding CPS, [54] and [55].
c) all types of records, including documents and videos, resulting from the ceremony of generating the CA key as set forth in section 6.1.1,
d) certificates data and records, certificate's life-cycle management records,
e) cryptographic keys and QSCD management records,
f) CP, CPS and PDS, and
g) other data and documentation in accordance with the legal regulations.

Detailed rules are set out in the corresponding CPS, [54] and [55].

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*

Archived data are adequately protected and credible and may be presented as material evidence in possible subsequent court proceedings.

Protection of the archive includes protection against unauthorised reading, modification, destruction and disruption of integrity.

5.5.4. *Archive backup procedures*

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

Storage media with archive data is periodically reviewed and copied to other media in order to ensure protection against aging or technological obsolescence.

5.5.5. *Requirements for time-stamping of records*

All archival records contain reliable date and time information using reliable time service source. Cryptographic time-stamping of archive records is not required.

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 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 and authorized employee in charge of the archives.

Verification of the data from the archives is carried out depending on the method applied for the data authenticity 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 shorter than the validity period of the CA certificate that issued the latter, and
- that the cryptographic algorithms and parameters are always suitable for use and in accordance with the recommendations referred to in the ETSI TS 119 312 [22].

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.

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 associated with the certification service provider.

5.7. Compromise and disaster recovery

5.7.1. *Incident and compromise handling procedures*

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, in accordance with chapter 16 of the ISO/IEC 27002 [47].

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

All corruptions of computing resources, software and/or data are recorded and processed in accordance with the internal security rules and procedures.

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 service of the compromised CA system is ceased,
b) the CA certificate revocation procedure is initiated,
c) person's certificate revocation procedure, issued by the compromised CA, is initiated,
d) persons and relying parties are informed via the web portal,
e) third party delegated all or some of RA affairs is informed,
f) competent national and supervisory bodies and other interested parties are informed,
g) in the case of the suspicion of elements of a crime, the latter is reported to the police in order to initiate an investigation process, and
h) the process of generating a new CA key is initiated.

5.7.4. *Business continuity capabilities after a disaster*

The AKD has 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.

The AKD ensures a high availability and uninterrupted continuation of the activities for the following services:

- revocation management services,
- revocation status services, and
- dissemination services.

Business continuity management is in accordance with chapter 17 of the ISO/IEC 27002 [47].

5.8. CA or RA termination

In the event of the termination of the KIDCA certification services, AKD will act according to Act Implementing the 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) inform all participants regarding possible planned cessation of certification services,
b) revoke the authorisations and cancel agreements with the suppliers, external personnel and delegated third parties that have been entrusted with the implementation of the affairs related to the provision of services,
c) inform the competent national authorities and consult on further actions to be taken regarding the cessation of providing certification services,
d) conduct a system transition to a new certification service provider, when necessary, if possible,
e) continue to maintain or submit the collected documentation and archival materials,
f) cease to issue certificates or cease to provide specific service, and
g) properly destroy cryptographic keys and all copies thereof.

6. Technical security controls

Technical security controls are specified in detail in the corresponding CPS, [54] and [55].

6.1. Key pair generation and installation

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 organised 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 assessors, public notary and other invited witnesses.

d) The record of the implementation of the ceremony of generating the CA key, video of the ceremony and all accompanying documentation, including technical script and a printout of the CA private key is stored in the archives.

e) The process of generating the keys and their entry in the QSCD is performed by the manufacturer in the physically secure environment in a high-security area.

f) The CA keys and keys of persons are generated, used and stored in the HSM module that implements standards and control functions as specified in the section 6.2.1. taking into account that cryptographic algorithms and parameters are always suitable for use and in accordance with the recommendations of ETSI TS 119 312 [22]

g) Keys for certificates for the remote electronic signature and remote electronic seal are generated in HSM module in AKD mPotpis service that implement standards and control functions as specified in the section 6.2.1 and kept in a secure environment for electronic signature creation.

6.1.2. *Private key delivery to subscriber*

Private key delivery to subscriber procedures are set out in the corresponding CPS, [54] and [55].

6.1.3. *Public key delivery to certificate issuer*

Public keys are delivered to CA in accordance with section 6.5.1 of the ETSI EN 319 411-2 [17] and corresponding CPS, [54] and [55].

6.1.4. *CA public key delivery to relying parties*

The root and subordinate CA's public keys are available in the certificates on the web portals (see section 2.2).

The authenticity 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 CA’s 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.

Size of keys used in AKD mPotpis service for remote signature and seal creation are set out in KIDCA CPS [55].

6.1.6. *Public key parameters generation and quality checking*

The CA keys, TSU keys and OSCP keys as well as keys of natural/legal persons are generated on the HSM device in accordance with the FIPS 186-4 [43] or other equivalent standard approved by the PMA.

In general, in order to generate the CA keys, TSU keys, OCSP keys and keys of natural/legal persons, cryptographic algorithms and parameters are used in accordance with the ETSI TS 119 312 [22].

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

The X.509 v3 certificates are issued to CA, OCSP, TSU and subscribers in accordance with the IETF RFC 5280 [39], and their purpose is defined by the value of the „*Key Usage*“ field as set forth in certificate profile (see section 7).

„K*ey Usage“ extension* is set out as critical for all issued certificates.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. *Cryptographic module standards and controls*

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 [42].

The AKD combines physical, logical, and procedural controls in order to ensure adequate protection of the HSM and private keys.

When the private keys are delivered in possession of subject of certification or Authorised 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 [44] and demonstrates the compliance with the forms of protection of the series EN 419 211 [26], [27], [28], [29], [30] and [31].

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 and used in HSM module i.e. remote QSCD in AKD mPotpis service that meets the requirements EAL4+ augmented with AVA_VAN.5 ISO/IEC 15408 [44] and rules set out in Anex II of Regulation (EU) No. 910/2014 [1]

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

Management procedures of the cryptographic keys is carried out in strict compliance with the principle of split knowledge n out of m, which ensures that the private keys are always under the control of more persons and one person may not come into possession of cryptographic materials that may be used for the regeneration of the cryptographic keys.

6.2.3. *Private key escrow*

Subscriber private keys are not escrowed.

The following rules apply:

a) After they are generated, the private keys of the CA and OCSP service remain stored in the HSM device. Minimum dual control access is enforced on the HSM device.
b) A system that manages the AKD Root CA private key and the associated OCSP system are connected to a computer network and remains inactive (offline) the entire time, and they are activated only when necessary.
c) A system that manages the CA's private key is constantly available and is used solely for the signing of the certificates of persons and CRL. The same applies to the associated OCSP system that is signing 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.
e) The AKD does not provide a permanent storage of the keys of natural/legal persons when certificates are issued on QSCD device delivered in person's possession. Detailed rules for key escrow for private keys used in AKD mPotpis service for remote signature or seal creation are set out in KIDCA CPS [55].

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 are provided.

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

The private keys of persons are not copied.

6.2.5. *Private key archival*

The CA, TSU and OCSP 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*

Whenever the CA, TSU and OCSP private keys are found outside the HSM device, for the purpose of key backup or transfer to another HSM device, the same or greater level of security of the private key is guaranteed.

Private key transfer from QSCD device delivered in person's possession into another QSCD device is not supported.

Rules for key transfer for private keys used in AKD mPotpis service for remote signature or seal creation are set out in KIDCA CPS [55].

6.2.7. *Private key storage on cryptographic module*

The 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 of QSCD delivered in person's possession, the 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 is carried out in accordance with the section 6.2.8.

6.2.8. *Method of activating private key*

The activation of the CA private key in the HSM device is carried out solely under the dual control of authorised personnel.

Once activated, the private key of the CA, TSU or OCSP service remains activated during the time that the HSM device is turned on. After power cycling, the HSM device, activation of the private keys is carried out again.

The activation of the private key of a person is performed one time by the mechanism, provided by the QSCD.

The activation of the private keys on the QSCD may be possible only following the activation of the QSCD device.

The activation of the private key managed by qualified trusted service provider on behalf of the certification subject or creator of seal is carried out by using two-factor authentication and private key activation PIN in AKD mPotpis service, when creating electronic signature or electronic seal and according to rules set out in KIDCA CPS [55].

6.2.9. *Method of deactivating private key*

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.

The private key of a person is deactivated by removing the QSCD from the reader or using a mechanism, provided by the device itself.

The deactivation of the private key managed by qualified trusted service provider on behalf of the certification subject or creator of seal in AKD mPotpis service is carried out automatically after creating electronic signature or electronic seal and according to rules set out in KIDCA CPS [55].

6.2.10. *Method of destroying cryptographic key*

Method used for destroying cryptographic key is provided by the HSM manufacturer.

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, TSA service or OCSP termination.

The destruction of files with encrypted private keys of persons in the information system is carried out automatically, immediately following the individualisation and putting the private key of persons on the QSCD.

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 is carried out using a secure method that is provided by the manufacturer of the HSM device. When the certificate of the private key used for remote signature or seal creation is revoked the aforementioned method used for destroying the private key is executed automatically.

The destruction of the private key is carried out using verified method which guarantees that the destroyed private key is able to be recovered or reused in any way.

6.2.11. *Cryptographic Module Rating*

See 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 is archived to enable the subsequent verification of electronic signatures and provides 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 5.

Table 5: Validity period of the certificate

Certificate	Validity period
Certificate of the root certification authority - AKDCA Root	2038-01-19 03:14:07+00:00
Certificate of the subordinate certification authority	15 years
Certificate for signing of OCSP replies	3 years
TSU certificate for signing AKD QTSA replies	5 years

Certificate's validity period is contained in issued certificate. Issued certificate is valid from the date of issuing, *"Valid from"* field, to the expiry date, *"Valid to"* field.

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.

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.

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 validity period of the certificates issued to persons (natural or legal) are set out in corresponding CPS, [54] and [55].

6.4. Activation data

6.4.1. *Activation data generation and installation*

Activation data generation and installation of CA's private keys are according to manuals provided by the manufacturer of HSM.

The activation data is used to protect the access to private keys on the QSCD.

Generating the activation data, their entry into the QSCD and printing in the security envelopes is carried out under the dual control in the manufacturer's secure environment of the QSCD.

The activation of the QSCD and setting of PINs to protect private keys on the QSCD of the person is conducted independently under instruction to activate QSCD which is available on the web portal.

When the qualified trusted service provider manages the signature creation data on behalf of the subject of certification or creator of seal registration codes are generated in the HSM device and managed in a secure environment of the CA system. Registration codes for certificate registration and setting the activation data PIN for the private key in AKD mPotpis service is delivered to subject of certification or authorized representative.

Rules applied are set out in corresponding CPS, [54] and [55].

6.4.2. *Activation data protection*

Activation data protection is as set out in corresponding CPS, [54] and [55].

6.4.3. *Other aspects of activation data*

Other measures to protect the activation data and registration codes against loss, modification, disclosure and unauthorised use are carried out in accordance with documented internal procedures.

Persons are responsible for the protection of the activation data and registration codes following their delivery.

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 [46] and ISO/IEC 27002 [47] standards.

In addition, technical requirements related to the computer security are implemented according to the requirements of the ETSI EN 319 401 [14] standards as well as according to the requirements set forth in CEN TS 419 261 [32], ETSI TS 119 431-1 [24] and CEN EN 419 241-1 [33].

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

6.6.1. *System development controls*

The management of the development process and the entire life-cycle of the software are in accordance with chapter 14 of the ISO/IEC 27002 [47].

6.6.2. *Security management controls*

The management of the computing resources is in accordance with chapter 12 of the ISO/IEC 27002 [47] including following controls, but are not limited to:

a) managing system security and protecting from viruses, malware and unauthorized software,
b) data recovery and protection of storage media from destruction, data loss and unauthorized access,
c) archive and records keeping, and prevention from technological obsolescence,
d) authorization management,
e) managing maintenance and patching in accordance with manufacturer recommendation, and
f) system vulnerability testing.

6.6.3. *Life-cycle security controls*

Periodical controls and supervision of information systems is being conducted for the entire life-cycle.

The management of business relations and suppliers is in accordance with chapter 15 of the ISO/IEC 27002 [47].

6.7. Network security controls

Network controls are established as defined in chapter 13 of the ISO/IEC 27002 [47], Annex B of the CEN TS 419 261 [32] and in accordance to document CA/Browser Forum NetSec **Error! eference source not found.**, ETSI TS 119 431-1 [24] and CEN EN 419 241-1 [33].

6.8. Time-stamping

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

7. Certificate, CRL and OCSP profiles

7.1. Certificate profiles

Profiles of all certificates are made pursuant IETF RFC 5280 [39] and Recommendation ITU-T X.509 [50].

Profile certificates are pursuant to the requirements of:

- ETSI EN 319 412-1 [18] for all certificates,
- ETSI EN 319 412-2 [19] for natural persons certificates,
- ETSI EN 319 412-3 [20] for CA,OCSP and legal persons (seal) certificates, and
- ETSI EN 319 412-5 [21] for EU qualified certificates.

Profiles for TSU certificates are made pursuant ETSI EN 319 422 [23] and IETF RFC 3161 [40].

The following table contains basic certificate fields.

Table 6: Basic fields

Field	Value/Limitation of the value
Version	X.509 V3, see section 7.1.1
Serial Number	Unique positive number 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's Public Key
SignatureValue	Issuer's signature of the certificate, generated and coded according to IETF RFC 5280 [39].

7.1.1. *Version number*

X.509 version V3 is used.

7.1.2. *Certificate extensions*

7.1.2.1. *Extensions of CA certificate*

The following table contains extensions of CA certificate.

Table 7: Extensions of CA certificate

Field	Certificate type	Value
Key Usage*	All CA	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints*	All CA	Subject Type=CA Path Length Constraint=None
Subject Key Identifier	All CA	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	All CA	Derived using the SHA-1 hash of the public key.
Authority Info Access	AKDCA Root	N/A
	HRIDCA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eid.hr/cert/akdcaroot.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.eid.hr/akdcaroot
	KIDCA	[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/akdcaroot.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.id.hr/akdcaroot
Certificate Policies	AKDCA Root	N/A
	HRIDCA	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
	KIDCA	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info:

		Policy Qualifier Id=CPS Qualifier: http://id.hr/cps
CRL Distribution Points	AKDCA Root	N/A
	HRIDCA	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.eid.hr/akdcaroot.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.eid.hr/akdcaroot.crl [3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.eid.hr/cn=AKDCA Root,o=AKD d.o.o.,c=HR?certificateRevocationList;binary (ldap://ldap.eid.hr/cn=AKDCA%20Root,o=AKD%20d.o.o.,c=HR?certificateRevocationList%3Bbinary)
	KIDCA	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.id.hr/akdcaroot.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.id.hr/akdcaroot.crl [3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.id.hr/cn=AKDCA Root,o=AKD d.o.o.,c=HR?certificateRevocationList;binary (ldap://ldap.id.hr/cn=AKDCA%20Root,o=AKD%20d.o.o.,c=HR?certificateRevocationList%3Bbinary)

**Critical field*

7.1.2.2. *Extensions of OCSP certificate*

The following table contains extensions of OCSP certificate.

Table 8: Extensions of OCSP certificate

Field	Type of certificate	Value
Key Usage*	All OCSP	Digital Signature (80)
Enhanced Key Usage	All OCSP	OCSP Signing (1.3.6.1.5.5.7.3.9)
Basic Constraints*	All OCSP	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	All OCSP	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	All OCSP	Derived using the SHA-1 hash of the public key.

Authority Info Access	AKDCA Root OCSP	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://eid.hr/cert/akdcaroot.crt
	HRIDCA OCSP	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://eid.hr/cert/hridca.crt
	KIDCA OCSP	[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
Certificate Policies	AKDCA Root OCSP	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.0.1.2.1.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
	HRIDCA OCSP	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.2.1.2.1.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
	KIDCA OCSP	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.5.1.2.1.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://id.hr/cps
OCSP No Revocation Checking	All OCSP	id-pkix-ocsp-nocheck 05 00 (1.3.6.1.5.5.7.48.1.5)

**Critical field*

7.1.2.3. *Extensions of certificates*

Extensions for certificates issued to natural and legal persons are set out in the corresponding CPS, [54] and [55].

Profile certificates are pursuant to the requirements of:

- ETSI EN 319 412-1 [18] for all certificates,
- ETSI EN 319 412-2 [19] for natural persons certificates,
- ETSI EN 319 412-3 [20] for legal persons (electronic seal) certificates, and
- ETSI EN 319 412-5 [21] for EU qualified certificates.

7.1.2.4. *Extensions of TSU certificate*

Extensions for TSU certificates are set out in the KIDCA CPS [55].

7.1.3. *Object identifier (OID)*

Algorithms with accompanying OID identifiers that are issued in AKD PKI system based on AKD Root CA are set out in the corresponding CPS, [54] and [55].

7.1.4. *Types of names*

X.509 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 the corresponding CPS, [54] and [55].

7.1.5. *Limitations of names*

Not applicable.

7.1.6. *Object identifier (OID) of Certificate Policy*

For each certificate containing extension *„Certificate Policies"*, OID is specified in accordance to section 1.2.2.

7.1.7. *Use of extension Policy Constraints*

Not applicable.

7.1.8. *Syntax and semantics of CP qualifiers*

Each certificate containing extension *„Certificate Policies"*, address of CP and CPS, [54] and [55], is specified in qualifier, in accordance to section 2.2.

7.1.9. *Process semantics for critical extension Certificate Policies*

Not applicable.

7.2. CRL profiles

CRL profiles of the AKDCA Root, HRIDCA and KIDCA issuer support X.509 version 2 pursuant the requirements defined IETF RFC 5280 [39]. Basic fields of CRL profiles for AKDCA Root, HRIDCA and KIDCA certificate issuers are specified in Table 9.

Table 9: Basic fields of CRL profiles

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.509 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 version V2 is used.

7.2.2. *CRL extensions*

The following table contains CRL extensions.

Table 10: CRL Extensions

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

7.3. OCSP profile

7.3.1. *Version number*

OCSP version V1 is used.

7.3.2. *Extension of OCSP certificate*

OCSP service respond is in accordance with the RFC 6960 [36].

8. Compliance audit and other assessments

8.1. Frequency or circumstances of assessment

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

The supervision of the management system in order to verify the compliance with the ISO/IEC 9001 [48], ISO/IEC 27001 [46] and ISO/IEC 14298 [45] standards is 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 programme.

8.2. Identity/qualifications of assessor

The assessment of the compliance with the Regulation (EU) No. 910/2014 [1] is carried out by the competent 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 [15] .

Supervision of the management system is carried out by the authorised audit companies, according to the ISO/IEC 9001 [48], ISO/IEC 2700 [46] and ISO/IEC 14298 [45] standards.

Internal assessments are carried out by persons who have the necessary knowledge and skills to implement the assessments in accordance with the rules set forth in the CP and CPS, [54] and [55].

8.3. Assessor's relationship to assessed entity

The external assessors are independent and delegated by the competent national body or authorised external audit company.

The internal assessment is carried out by the person, appointed by the PMA.

8.4. Topics covered by assessment

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

Internal assessments include the implementation of the certification services or specific service, prescribed procedures and protection measures in accordance with the CP and CPS, [54] and [55].

8.5. Actions taken as a result of deficiency

In the case that non-compliance is established, the operational plan is determined, time limits are set and tasks related to the implementation of the operational plan is assigned.

Should the non-compliance significantly affect the security of the provision of trust services or specific service or prevents the fulfilment of the statutory requirements, the AKD ceases to provide services until the established non-compliance are eliminated.

The AKD undertakes all necessary actions in order to prevent the adverse impact of the cessation of the provision of service to persons or relying parties.

Once the assessor determines that the prescribed compliance is achieved, PMA will approve the continuation of certification services or specific service.

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 organisational structure of the AKD.

The AKD shall, in accordance with legal provisions, submit 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

9.1.1. *Certificate issuance or renewal fees*

Certificate issuance or renewal fees are included in the price of the eOI in accordance with section 9.1.4.

Certificate issuance or renewal fees for certificates issued by KIDCA are determined in price list or specified in separate contract concluded with client for providing certification services.

9.1.2. *Certificate access fees*

Search for certificates in the HRIIDCA public directory is enabled to the bodies of public sector of the Republic of Croatia free of charge.

For certificates issued by KIDCA and enabled search services in KIDCA public directory, AKD may set the certificate access fees within a separate contract concluded with client.

9.1.3. *Revocation or status information access fees*

Revocation or status information access services for the HRIDCA certificates are free of charge.

For certificates issued by KIDCA, AKD may set the fees for revocation or status information access services.

9.1.4. *Fees for other services*

For HRIDCA certificates, registration service of natural persons and services of producing and individualisation of the card is charged through the price of the eOI.

The price of the eOI is determined by the implementing acts arising from the Identity Card Act [13].

For KIDCA certificates and KIDCA related services AKD may independently or in collaboration with third parties determine the price and charge a fee for other services.

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.

Additional terms can be set out in CPS, [54] and [55].

9.2. Financial responsibility

9.2.1. *Insurance coverage*

The AKD establishes a system of accountability; determines the limits of reliance in certificates and clearly defines 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.

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 is the amount of HRK 2,000,000.00.

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 data marked as business secrets or are defined as business secrets by the Data Confidentiality Act [10], law-based regulations or internal rules, the disclosure of which to the unauthorised person may cause harmful consequences for the participants of the certification process.

The confidential business data include data of various types, important for the operations, provision of services or interests of the participants.

More detailed information on the scope of confidential information is available in the corresponding CPS, [54] and [55].

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

The data that are not considered as confidential business data mean all business data whose disclosure does not adversely affect the business, provision of services or the interests of participants of the certification procedure.

This includes certificates, certificate revocation list, information on the certificate's status and all information and documents that are published on the web portal.

The confidential business data are not be considered 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].

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.

The duty to keep secrets pertains to all participants of the certification procedure that have become aware of the confidential business data referred to in section 9.3.1 in any way.

9.4. Privacy of personal information

9.4.1. *Privacy plan*

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

Persons are informed that the AKD and legal persons providing RA services 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 unauthorised or unlawful processing and against accidental loss, destruction or damage to personal data.

9.4.2. *Information treated as private*

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 publishes certificates in a public directory under the conditions, defined in section 4.4.2.

The personal data contained in the certificates are not confidential.

9.4.4. *Responsibility to protect private information*

The AKD and the contracted RA are responsible for the protection of personal data.

The AKD ensures a lawful processing of the personal data in accordance with the provisions of the Implementation of the General Data Protection Act [4], and related subordinate acts or 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 are enabled if required by legislation, or when requested by the competent court, administrative or other relevant national authority/body 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

The AKD has, as the author and owner of all contents on the web portal, including CP, CPS, certificates, CRL and applications for the QSCD, the unlimited rights of usage, and particular right of reproduction, distribution, publishing and processing.

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 licensing conditions for end users (*End User License Agreement – EULA*) or other provisions concerning the right of usage.

All participants are required to uphold the copyrights and related rights as well as intellectual property rights.

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 the CP, 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 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.

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 generation services, revocation management services, revocation status services 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 organisational, 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, 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 Regulation (EU) No. 2016/679 [3].

i) Provision of the ISO/IEC 9001 [48] and ISO/IEC 27001 [46] 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 providers include:

a) Collection and verification of information on the identities of individuals and legal entities in accordance with this document.

b) Receiving applications by persons, including applications for issuing the certificates, requests for revocation and suspension of the certificates and requests for unblocking and the delivery of the QSCD.

c) 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.

d) Registration of complete, accurate and verified personal identification data on natural persons and their requirements in the information system and forwarding data to manufacturer and CA.

e) Ensuring that registration activities are conducted solely by the reliable and conscientious officers of the RA/LRA whose identity is undoubtedly established and who is adequately trained before they are granted.

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

g) 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.

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

i) No restrictions of accessibility to its services for persons with disabilities, where feasible.

j) Other representations and warranties set out in CPS, [54] and [55].

9.6.4. *Subscriber representations and warranties*

The person is responsible for the following:

a) to present credible evidence of his/her identity in the identification process,

b) to submit accurate and true data in the registration process,

c) to verify that certificate's data are valid,

d) that only the person which is indicated in the certificate or authorized representative of the creator of seal shall use the private key which matches the public key in the certificate,

e) that the certificate at the time of its use has not expired and has not been revoked,

f) that uses certificate only for legal and authorised purposes and in accordance with their appropriate purpose,

g) that he/she responsibly uses and protects the QSCD delivered in possession or two-factor eID means used for AKD mPotpis authentication, private keys , activation data

and registration codes and takes appropriate protection measures against unauthorized access and use,

h) that he/she immediately requests the revocation or suspension of the certificate if there is a 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 they suspect the loss, theft, misuse or unauthorised use of the private key and

i) to request the revocation of a certificate if there is no basis on which the certificate was issued or if it is determined any circumstance for which the certificate should no longer be used.

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 authorised 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 [39] and IETF RFC 3739 [38].

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 Regulation (EU) No. 2016/679 [3].

f) Provision of the ISO/IEC 9001 [48], ISO/IEC 27001 [46] and ISO/IEC 14298 [45] 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 [44] and demonstrates the compliance with the forms of protection of the series EN 419 211 [26], [27], [28], [29], [30] and [31].

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 is 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 person's possession, private keys, activation data, certificate or CRL,
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, relying party and other participants that do not fulfil their obligations or fail to act in accordance with their obligations set out in sections 9.6.3, 9.6.4 and 9.6.5.

The AKD shall not be 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 was 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.

The AKD is not responsible for any loss that may arise as a result of force majeure or other circumstances beyond the control of AKD, as defined in section 9.16.5.

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 HRK 2,000,000.

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 HRK 8 000,00
2	Up to HRK 80 000,00
3	Up to HRK 400 000,00

9.9. Indemnities

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

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

a) he/she obtains a certificate based on fraudulent information given in the application for the issuance of the certificate, 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 trust service provider is liable should this liability be clearly established by the agreement, CP, CPS, contract, conditions for providing certification services or the legislation of the Republic of Croatia.

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 validity of certificates which were issued according to the rules outlined in the previous edition of the document, during the validity of the document.

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 section 1.5.2.

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 will be published in the versions of the documents without prior notice and without changing 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 shall be 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 will be resolved amicably. Should the amicable resolution of the dispute is not 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], acts referenced in this document, subordinate acts adopted on the basis of the indicated regulation or the law, and binding national, European or international standards referenced in this document is determinative.

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 that was granted a qualified status by the supervisory body, the ministry responsible for Economy of the Republic of Croatia.

9.16. Miscellaneous provisions

9.16.1. *Entire agreement*

If not in contravention of the legal regulations, provisions of the CP or the CPS, the AKD may, as the trust service provider, enter into separate agreement with other participants in order to protect its own business interests.

9.16.2. *Assignment*

Not applicable.

9.16.3. *Severability*

Should the court or arbitrary body establish that particular provisions of the CP are not enforceable; other provisions of the CP shall remain valid.

Should there be disputes and disagreements as a result of interpretation of provisions set out in this CP, provisions of binding regulation or the law and national, European or international standards referenced in this document shall be applied.

9.16.4. *Enforcement*

Not applicable.

9.16.5. *Force Majeure*

AKD shall not be liable towards affected participant if any instance of force majeure occurred, including weather-related and natural disasters, landslides, floods, fire, war, acts of war, terrorism, disorders in public infrastructure (information and communication, energy, etc.), embargo, lawful restriction or coercion, civil disorders and any other circumstances beyond AKD control.

9.17. Other provisions

Not applicable.

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 [53].
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-stamping 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

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
TSP/PS	Time-stamp 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
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	Policy 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 Implementing the REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Official Gazette 62/17, 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 42/18).

[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] Data Confidentiality Act (Official Gazette 79/07, 86/12).

[11] Freedom of Information Act (Official Gazette 25/13, 85/15).

[12] Civil Obligations Act (Official Gazette 35/05, 41/08, 125/11, 78/15, 29/18).

[13] Identity Card Act (NN 62/15)

Normative references

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

[15] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers".

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

[17] 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".

[18] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[19] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons",

[20] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[21] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

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

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

[24] 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".

[25] 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".

[26] CEN EN 419 211-1: "Protection profiles for secure signature creation device - Part 1: Overview".

[27] CEN EN 419 211-2: "Protection profiles for secure signature creation device - Part 2: Device with key generation".

[28] CEN EN 419 211-3: "Protection profiles for secure signature creation device - Part 3: Device with key import".

[29] 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".

[30] 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".

[31] 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".

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

[33] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements".

[34] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing".

[35] CEN 419 221-5: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".

[36] IETF RFC 6960: „X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol – OCSP (2013)“.

[37] IETF RFC 3647: “Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework”.

[38] IETF RFC 3739: “Internet X.509 Public Key Infrastructure: Qualified Certificates Profile”.

[39] IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“.

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

[41] IETF RFC 5019 (2007): „The Lightweight On-line Certificate Status Protocol (OCSP) Profile for High-Volume Environments“.

[42] FIPS PUB 140-2 (2001): “Security Requirements for Cryptographic Modules”.

[43] FIPS PUB 186-4: „Digital Signature Standard (DSS)“.

[44] ISO/IEC 15408 (parts 1 to 3): “Information technology – Security techniques – Evaluation criteria for IT security”.

[45] ISO/IEC 14298: “Graphic technology – Management of security printing processes”.

[46] ISO/IEC 27001:2013: “Information technology — Security techniques — Information security management systems — Requirements”.

[47] ISO/IEC 27002:2013: „Information Technology – Security Techniques – Code of practice for information security controls“.

[48] ISO/IEC 9001:2015: “Quality management systems – Requirements”.

[49] ISO/IEC 27005:2011: “Information technology – Security techniques – Information security risk management”.

[50] ITU-T X.509 Recommendation: “Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks”.

[51] ITU-T X.520 Recommendation: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".

[52] ITU-T X.501 Recommendation: „Information technology – Open Systems Interconnection – The Directory: Models“.

[53] ITU-R TF.460-6 Recommendation: “Standard-frequency and time-signal emissions”.

AKD documentation

[54] HRIDCA CPS.

[55] KIDCA CPS.

[56] AKD QTSA TSP/PS.

ANNEX 4: History of document amendments

Edition	Reasons for amendment	Date
1.0	Draft 1st Edition of the AKD PKI Certificate Policy Lite	19 May 2015
1.1	More precise formulation of the rule	27 May 2015
1.2	Error correction and standardization of the terminology	28 May 2015
1.3	Published 1st Edition: AKD PKI Certificate Policy Lite	8 June 2015
2.0	2nd Edition: Harmonization with the Commission Implementing Decision (EU) from 2015 and new ETSI standards	15 May 2017
2.1	Error corrections. Harmonization with Act Implementing the Regulation (EU) No 910/ [2]. Corrections and additions regarding the implementation of TSA service.	12 December 2017
2.2.	Error corrections. Harmonization with The Law on the Implementation of the General Data Protection Act. Corrections and additions regarding the implementation of issuing qualified certificates for electronic seal and issuing of certificates for remote signing and remote sealing. Approved Edition.	04 July 2018
2.3	Error corrections. Update and corrections of references. Additions regarding AKD mPotpis service for remote digital signature creation on behalf of the signatory. Approved Edition. Effective from July 15th 2019.	01 July 2019
2.4.	Error corrections. Private key escrow clarification. Legal framework update.	01.05.2020.