HRIDCA
Certification Practice Statement

Edition 2.0

Status: February 21, 2017

Contents

Foreword

The Croatian electronic identity card (hereinafter: eOI) is an identification document of Croatian citizens, issued by the Ministry of the Interior (hereinafter: MUP) pursuant to the Identity Card Act [1].

The eOI is a required document for Croatian citizens over 18 years of age with registered residence in the Republic of Croatia, and every citizen of the Republic of Croatia has the right to apply for an eOI. Depending on their age, persons receive a pair of keys and corresponding certificates stored on eOI chip.

Two types of certificates are issued on the electronic identity card:

a) The identification certificate, which is a means of electronic identification and meets the high level security requirements for pursuant Article 8, paragraph 2 c) of EU Regulation No. 910/2014 [9],

b) Signing certificate, which is a qualified certificate for electronic signature and meets the requirements set out in Annex I to EU Regulation No. 910/2014 [9]

Both certificates are issued by the Agencija za komercijalnu djelatnost d.o.o. (hereinafter: AKD), which is a qualified trust service provider and which had been granted a qualified status by the supervisory body, the Ministry in Croatia in charge of economy.

The electronic identity card is a qualified electronic signature creation device and meets the requirements set out in Annex II to *EU Regulation* No. *910/2014* [9].

1. Introduction

1.1. Overview

This document, HRIDCA Certification Practice Statement (hereinafter: CPS) that specify in detail organizational and technical measures which are applied by the HRIDCA in practice when determining identity, issuing certificates and managing their life-cycle.

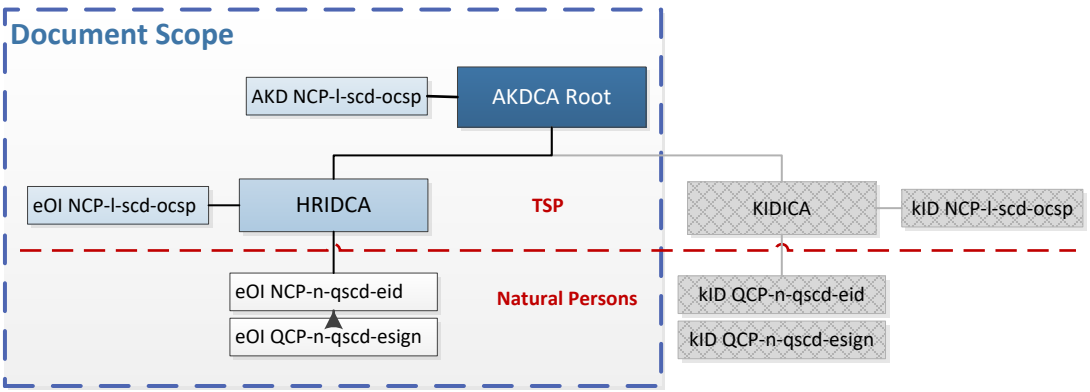
The CPS is harmonized with "AKD Certificate Policy" (hereinafter: CP) that apply to the entire hierarchical structure based on roof certification authority called AKDCA Root that issued the certificate to itself and to the subordinate certification body HRIDCA.

According to *IETF RFC 3647* [33] the Rules correspond to the document called "*Certification Practice Statement CPS*", and the structure and the contents of this document are stringently harmonized with the requirements of this standard.

Security requirements, defined in this document and applied in practice, are harmonized with the strict requirements for qualified trust service providers and qualified trust services that they provide, defined by EU Regulation (No. 910/2014 [9] and Electronic Signature Act [7].

1.1.1. The Scope of the Document

The rules and regulations set forth in this document apply to the subordinate certification body to whom the certification body AKDCA Root issued certificate.



HRIDCA issues personal certificates to physical persons exclusively for the purposes of issuing eOI. Those are the following: sigining certificate (eOI QCP-n-qscd-esign) and identification certificate (eOI NCP-n-qscd-eid).

HRIDCA does not issue certificates to legal persons except OCSP certificate that it issues to itselfs and that serves for a service provision.

1.1.2. The purpose of this document

This document is made for:

- Trust services provider in order to ensure that the security requirements defined in CP are implemented and

- The bodies to evaluate the compliance and to the supervisory bodies to evaluate the capabilities of AKD to provide qualified trust services and to have and maintain the status of qualified service provider

A simplified version of the CPS that does not contain confidential business information is published on the website, and allows persons and relying parties to assess the suitability of the certificate for a particular purpose.

Security requirements, defined in this document and applied in practice, are harmonized with the strict requirements for qualified trust service providers and qualified trust services that they provide, defined by EU Regulation (No. 910/2014 [9] and Electronic Signature Act [7].

1.2. Document name and identification

1.2.1. Document name

Table 1: Document name

Code:	PRO-I-91-02
Name:	HRIDCA Certification Practice Statement Lite
Edition:	2.0
Publication date:	April 1, 2017
Author:	AKD, Agencija za komercijalnu djelatnost d.o.o
OID:	1.3.6.1.4.1.43999.5.1, 1.3.6.1.4.1.43999.5.2
Document type:	Certificate Practice Statement
Availability:	http://eid.hr/cps

Table 2: History of the amendments to the document

Issue	Date	Explanation of the description
1.3.	08.06.2015	First issue of the document
1.4.	28.06.2016	Specified the frequency of media change in 5.5.3 d
2.0	1.4.2017	Harmonization with EU Regulation from 2015 and new ETSI norms

1.2.2. Identification code

The identification code (OID), reserved by the AKD PKI is 1.3.6.1.4.1.43999.

Identification code of the root certification body AKDCA Root is 1.3.6.1.4.1.43999.5.

Identification codes covered by these CPS are:

a) eOI Qualified certificates – OID 1.3.6.1.4.1.43999.5.1

The rules against which eOI QC certificates are issued are equivalent to the rules eOI **QCP-n-qscd**, according to 5.3. ETSI EN 319 411-2 [27] that are implemented for EU qualified certificates for physical persons with private key on qualified device for production of electronic signature (OID: 0.4.0.194112.1.2)

b) eOI Normalized certificates OID 1.3.6.1.4.1.43999.5.2

The rules against which eOI NC certificates are issued are equivalent to the rules **NCP+**, according to 5.3. ETSI EN 319 411-1 [26] that are implemented for EU normalized certificates for physical persons with private key on qualified cryptographic device (oid 0.4.0.194112.1.2)

Table 3: Identification code

HRIDCA Personal Certificates		
Name	Code	OID
eOIsigning certificate	eOI QCP-n-qscd-esign	1.3.6.1.4.1.43999.5.1.2.1.2.10
eOI identification certificate	eOI NCP-n-qscd-eid	1.3.6.1.4.1.43999.5.2.2.1.2.20
OCSP certificate*	eOI NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.2.1.2.2.90

*OCSP certificate serves for service provision and it is not publicly issued.

1.3. PKI participants

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

- Policy Management Authority – PMA,
- Certification Authority – CA,
- Registration Authority – RA,
- Persons,
- Relying parties, and
- Manufacturer.

Obligations and responsibilities of all AKD PKI participants are introduced in Article 9.6.

1.3.1. Policy Management Authority – PMA

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

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

The PMA is responsible for defining, introducing and administering general rules, provision of certificate policy (CP), PKI Disclosure Statement (PDS), and this Certification Practice Statement (CPS) as well as Security Operating Procedures and implementing documents related to the operation of the AKD PKI and provision of the trust services.

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

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

1.3.2. Certification Authority – CA

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

The CA provides the following trust services:

- **Certificate Generation Service**: it creates and signs certificates based on data gathered through registration service,
- **Revocation Management Service**: it performs the certificate revocation and provides information on the certificate's status,
- **Revocation Verification Service**: it informs the relying parties on the status of the certificate and enables the verification through the CRL or OCSP,
- **Dissemination service**: it informs persons and relying parties on certificates, the terms and certification conditions and other information related to certificates and certification services.

The PKI infrastructure established by the AKD PKI is arranged hierarchically as described in Article 1.1.1.

1.3.3. Registration Authority – RA

The Ministry of the Interior (MUP) is the competent government body for issuing of the eOI.

MUP is the registration authority (hereinafter: registration service provider or RA) verifying identities and identification data of natural persons under which HRIDCA issues, renews, revokes and suspends certificates.

MUP manages independently its personnel in police administrations and police stations (PU/PP), operating as the local registration authorities (LRA) and performing the registration activities of persons pursuant the Identity Card Act [1].

The affairs of the PU/PP include:

a) informing persons on procedures for registration and issuance of the eOI,
b) receiving requests for issuance, revocation and suspension of certificates on the eOI,
c) identity validation of persons and applicants,
d) making the conclusion of the Agreement on certification services possible with physical persons,
e) delivery of certificates and eOI.

MUP and AKD conclude an agreement under which the MUP undertakes to provide an implementation of the security rules and procedures described in this document, particularly in chapter 3 and points 5.3 and 5.5.

1.3.4. Persons

Persons are natural persons to whom the OI has been issued, who have received the certificate on the identity card and which have concluded an Agreement on certification services with the AKD in accordance with the Identity Card Act [1].

The person has to act pursuant PKI Disclosure Statement.

The person is considered as the entity, listed on the certificate, and signatory who produces electronic signature and uses the certificate on its own personal behalf.

In CA certificates, the subject of certificate is the name of CA system of trust services provision. Similar applies to OCSP certificate. Whenever the subject of the certificate is not a natural person then the natural persons – certificate custodians are appointed who are responsible for protection of corresponding private key and SCD.

1.3.5. Relying parties

The relying parties are natural or legal persons that provide electronic 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 a verification of the person's identity and validation of the electronic signature to the relying party.

1.3.6. Manufacturer

The AKD is the manufacturer of eOI supplying eOI to the persons together with devices and products.

The manufacturer provides the following services:

In accordance with the CP and CPS, the manufacturer performs the following affairs:

a) preparation and production of eOI,
b) generating pairs of the cryptographic keys of persons and their entry to the eOI,
c) personalization of card body and chip of eOI
d) distribution of eOI to the persons using the services of the RA,

The manufacturer has to ensure that the eOI is a qualified means for the creation of electronic signature (*Qualified Electronic Signature Creation Device – QSCD*).

1.4. Certificate usage

Detailed information on the contents of the certificate are available in Chapter 7 of this document. When determining the use of certificate it is important to take into consideration all terms and conditions of this document, and especially the interoperability criteria stated in Article 3.2.6 and other business rules and regulations stated and defined in Article 9.

1.4.1. Appropriate certificate uses

1.4.1.1. CA Certificates

CA certificates are used by the service provider for signing certificates and CRL.

This group consists of:

- AKD Root CA certificate that issued and signed HRIDCA certificate and
- HRIDCA certificate that was used to sign OCSP Certificate as well as certificates issued to end users (eOI NCP-n-qscd-eid i eOI QCP-n-qscd-esign).

Corresponding private key of CA certificate is kept in a safe cryptographic device. The purpose of CA certificate, according to X.503 v3 extension, "Key Usage" is "Certificate Signing, Off-line CRL Signing". This extension is marked as critical.

1.4.1.2. OCSP Certificates

HRIDCA OCSP certificates are issued by HRIDCA and they are used by the service provider for signing OCSP replies.

Corresponding private key of OCSP certificate is kept in a safe cryptographic device. The purpose of OCSP certificate, according to X.503 v3 extension, "Key Usage" is "Digital signature". This extension is marked as critical.

The purpose of OCSP certificate, according to X.503 v3 extension, "Extended Key Usage" is "OCSP signing".

1.4.1.3. eOI QCP-n-qscd-eid eOI identification certificate

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

a) eOI identification certificate is the means of electronic identification with high level of security, as specified in Article 8, paragraph 2 c) of the EU Regulation No. 910/2014 [9].

b) Minors are allowed to use eOI identification certificate as a support to the electronic signature. However, it is recommended to all adult natural persons to use the signing certificate for such purpose.

c) In the "Subject" field eOI of identification certificate is the named natural person.

d) eOI personal certificates are used for private purposes as well as for business purpose when it is not necessary to confirm the affiliation of a person to a business subject.

e) The purpose of eOI identification certificate, according to X.503 v3 extension, "Key Usage" is "Digital signature". This extension is marked as critical.

1.4.1.4. eOI QCP-n-qscd-esign eOI signing certificate

Persons and relying parties should be aware of the rules of use of an eOI signing certificate:

a) eoi signing certificate serves is suited for qualified electronic signature creation, as defined in Article 3, paragraph 12 of the Regulation (EU) No. 910/2014 [9],

b) eOI personal certificate may be suited in the process of making an advanced electronic signature based on a qualified certificate as defined in Articles 26 and 27 of the Regulation (EU) No. 910/2014 [9]

c) In the "Subject" field eOI of identification certificate is a named natural person.

d) The purpose of eOI identification certificate, according to X.503 v3 extension, "Key Usage" is "Non Repudiation". This extension is marked as critical.

e) eOI signing certificate is used for private purposes, as well as for business purposes when it is not necessary to confirm the affilitation of the person to a business certificate

f) eOI signing certificate is an EU qualified certificate, and qualified electronic signature made by this certificate has the same validity and legal effects as a handwritten signature

1.4.2. Prohibited certificate uses

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

a) Any use of the certificate, except for those specified in point 1.4.1, is prohibited.

b) Certificates are not intended for data encryption

c) Certificates do not contain an extension with an e-mail address
d) If an eOI certificate is used as a support to the electronic signature, such signature is not considered as a qualified electronic signature.

When checking the validity of the certificate that is described in Article 9.6.4 of this document, relying parties have to check OID certificate as in Article 1.2.2 in order to make a valid decision about the acceptance or rejection of the certificate in use.

1.5. Document administration

1.5.1. Organization administering the document

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

1.5.2. Contact information

Mailing address:

Agencija za komercijalnu djelatnost d.o.o
Policy Management Authority
Savska cesta 31
HR-10000 Zagreb
Croatia

e-mail: pma@akd.hr
webpage: http://eid.hr

1.5.3. Person determining CPS suitability for the policy

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

- national and EU regulations related to the electronic identification and trust services,
- technical specifications, standards and procedures related to the electronic identification and trust services, and
- internal security rules and operating procedures relating to the implementation of actions and activities of the certification service provider.

Should a need to amend the document be determined, the PMA start the procedure of harmonization of the documentation and determine the commencement date of the implementation of the new operational procedures or rules for the provision of services.

1.5.4. CPS approval procedures

All members of the PMA must give their consent for the adoption and publication of the document before the issuance of the document and its commencement date of the implementation and following every amendment to the document.

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 [9], ETSI EN 119 411-1 [26] and ETSI EN 119 411-2 [27].

2. Publication and repository responsibilities

2.1. Repositories

CA ensures the repository and makes all the information needed for the certificate's status verification available to the public including:

a) information about the certificate status that are available as a OCSP service

b) the last issued by CRL via HTTP and LDAP protocol for AKDCA Root and HRIDCA and

c) CA certificates.

The repository data are stated in the below table:

Table 4: Repository data

Information	AKDCA Root	HRIDCA
CRL: HTTP protocol	http://crl1.eid.hr/akdcaroot.crl http://crl2.eid.hr/akdcaroot.crl	http://crl1.eid.hr/hridca.crl http://crl2.eid.hr/hridca.crl
CRL: LDAP protocol	ldap://ldap.eid.hr	ldap://ldap.eid.hr
OCSP service	http://ocsp.eid.hr/akdcaroot	http://ocsp-hridca.eid.hr/hridca
CA certificates	http://eid.hr/cert/akdcaroot.crt	http://eid.hr/cert/hridca.crt

Data for the certificate's status verification are contained in the certificate.

Valid and current certificates of persons, issued by the HRIDCA are contained in the structure of the public directory, they may be publicly available under conditions set forth in Article 2.4.

2.2. Publication of certification information

All information, needed by the persons and relying parties in order to use the certification services are published by the HRIDCA on an electronic identity card web portal.

The public section of the web portal, http://eid.hr, is made available to the public, where the following information are published:

- Certification Policy, http://eid.hr/cps,
- HRIDCA CPS, http://eid.hr/cps,
- PKI Disclosure Statement, http://eid.hr/cps,
- notifications related to the provision of certification services, and
- other information that the CA and the manufacturer deem relevant to users and relying parties.

The CA establishes a private section of web portal where registered persons have access to.
The following information is published in the private section of the web portal:

- application and instructions necessary for the installation and use of the eOI,

- electronic service for certificate's status and suspension verification,
- review and modification of the registration data, and
- contact information to help the users.

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 available in Croatian, and a portion of the content, including CP, CPS and PDS may be available in Croatian and in English.

c) The certificates in the repository are published immediately after their issuance.

d) Information on the certificate's status is available under the conditions specified in point 4.10.

e) The availability of the repository is 24 hours a day, 7 days a week in accordance with the best business practices.

f) Following the system failure or other factors that are out of the CA's control, all available measures are undertaken in order to ensure a system recovery within the shortest time possible.

g) Continuous availability (24/7) of repository is maintained, pursuant best business practices.

h) All available resources will be deployed in order to ensure recovery of the system as soon as it is possible, following system malfunction or after the influence of other factors that are not under control of CA

2.4. Access controls on repositories

The following rules apply:

- CA certificates, CP, CPS, PDS and basic information on the web portal are available to the public without restrictions.
- Additional information and services of direct checking of the status and certificate suspension on the web portal may be available only to registered persons.
- The HRIDCA does not set any restrictions in relation to the availability of information that are necessary for checking the status of the certificate.
- The right to view certificates of persons will be available for search purposes to the bodies of the public sector of the Republic of Croatia when necessary
- The CA reserves the right to take appropriate measures to protect the repository and web portal from the misuse.

3. Identification and authentication

3.1. Naming

3.1.1. Types of names

The name of the certificate or unique set of data that undoubtedly represents the owner of the certificate is entered in the "*Subject*" field of each certificate.

Name of the certificate is determined pursuant ITU-T X.520 [46] or IETF RFC 5280 [35] recommendations.

When determining the Subject field the rules and recommendations of ITU-T X.501 [47] for CA certificates and OCSP service certificates, the "Subject" field is be formed from:

commonName:	Name of the CA certificate or OCSP service
organizationIdentifier:	Legal person identifier of trust services provider
organizationName:	Name of the legal person – qualified trust service provider
countryName:	Code of the country

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

CommonName:	Name of the natural person
serialNumber:	Serial number
givenName:	Name of the natural person
Surname:	Surname of the natural person
organizationalUnitName:	Type of the certificate
organizationName:	Name of the organization with whom the person is affiliated with
countryName:	Code of the country

3.1.2. Need for names to be meaningful

The names in the "Subject" field have to meaningful and have to make it possible to identify a natural person in a doubtless and unique way.

3.1.3. Anonymity or pseudonymity of subscribers

Not supported.

3.1.4. Rules for interpreting various name forms

Rules for interpreting various name forms for CA and OCSP certificates are indicated in following table.

Table 5: Rules for interpreting various name of CA and OCSP certificates

CA and OCSP certificates		
Field	Description	Value
CommonName (cn)	Name of CA or OCSP system	AKD CA Root

		AKD CA Root OCSP HRIDCA HRIDCA OCSP
organizationalName (O)	Name of the legal person-trust service provider	AKD d.o.o.
organizationalIdentifier	VATHR-OIB: VAT indicates a legal person OIB is a tax identification number of a legal person HR is the code of the country A minus sign "-" (0x2D (ASCII), U+002D (UTF-8))	VATHR-58843087891
countryName (C)	2 letter ISO country code (HR)	HR

The fules of interpretation of the names for the certificates of physical persons are stated in the below table.

Table 6: The rules of interpreting the names of physical person

Natural persons		
Field	Explanation	Value
CommonName (cn)	Represents the name and the surname of the natural person	Name Surname
serialNumber	PNO is a code indicating a natural person HR is the code of the country A minus sign "-" (0x2D (ASCII), U+002D (UTF-8)) OIB is a personal identification number	PNOHR-OIB
givenName (g)	Represents the name of the person	Name
Surname (sn)	Represents the surname of the person	Surname
organizationalUnitName (OU)	Specifies the type of the certificate	Identification Signature
organizationName (O)	Name of the CA that issues certificates	AKD d.o.o.
countryName (C)	2 letter ISO country code (HR)	HR

3.1.5. Uniqueness of names

In the "Subject" field of each certificate unique information on the natural person are entered to whom the certificate is issued.

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

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 of persons are generated in the HSM device and they are entered, together with accompanying certificates in a secure environment on a chip.
b) eOI with private keys and certificates are delivered to the person direclty after determining his/her identity.
c) Private keys of the CA and OCSP certificate are generated in the SCD device in a secure environment under supervision of CA personnel and they remain there while they are used.

3.2.2. Authentication of organization identity

Not applicable.

The HRIDCA issues no certificates to legal persons.

3.2.3. Authentication of individual identity

3.2.3.1. Collection of information on natural persons

Collection and verification of data on persons are carried out in accordance with the Ordinance on the forms and records of identity cards [2].

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

- Basic information about the person including:
  - full name and surname,
  - gender,
  - citizenship,
  - date of birth,
  - OIB,
  - place and address of residence.
- Color photograph and fingerprint of the left and right index finger are required as well as person's signature are all scanned.
- Appropriate documents for the verification of the name, identity and the basis for the issuance of the eOI and certificate are required.
- Documents that are considered as relevant evidence in the process of determining the identity of the natural persons in accordance with the national law in the Republic of Croatia include:
  - previously issued public documents (identity card or passport),

- certificate of nationality,
- excerpt from the birth register,
- birth certificate, and
- marriage certificate.

3.2.3.2. Information verification on natural persons

The PU/PP offices collect and verify information and documents about a natural person in order to ensure that each information, contained in the certificate, is verified and confirmed.

Processes for identifying and verifying the identity of natural persons are conducted in accordance with the best identification practices for natural persons in the Republic of Croatia that includes, but is not limited to:

a) verification of the existence and identity of the natural person with the direct identification and the physical presence of a person on the basis of the adduced document,
b) verification assessing whether collected information correspond to those stated in the adduced documents,
c) when applicable, the comparison of the collected information with those that have been collected in an earlier issuing process of public documentation, conducted by MUP,
d) authenticity verification for the enclosed/adduced documents,
e) determining whether a person is a citizen of Croatia and whether there is a basis for the issuance of the eOI,
f) determining whether there is a basis for obtaining certificate on eOI against the following criteria:
   - children until the age of 5 obtain an eOI without a certificate
   - persons older than 5 and younger than 18 obtain only an identification certificate
   - Persons of legal age (i.e. older than 18) obtain both certificates: identification and signing certificate
   - And persons older than 65 obtain eOI with both certificates or without certificates
g) verification of completed payment of the fee for the eOI and
h) verification on entering the contractual relationship between the user and the certification service provider in regard to the acceptance of obligations and responsibilities.

3.2.4. Information about persons that are not checked

Contact information are requested by a person: phone number and e-mail address

PU/PP does not check contact information, the person is responsible for the accuracy of those information

3.2.5. Checking the card body

3.2.5.1. Verification by the RA/LRA officers

The following rules apply:

- Before assigning tasks to the PU/PP officers, verification is made, as well as the unambiguous validation of the identity and reliability of the officers pursuant Article 5.3.

- A reliable authentication method is used in the authentication process of the officers in the information system of the PU/PP.
- In order to prevent conflict of interest, the subject of the certificate and the officer of PU/PP must not be the same person. The PU/PP officer who require the certificate, do not identify himself/herself nor enter the request for the issuance of his/her own certificate in the information system of the PU/PP.

3.2.5.2. Verification of CA personnel

The following rules apply:

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

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

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

d) During operation, software module that performs an automated collection, verification and sending of the requests to be processed, authenticates itself to the information system of the CA using SSL client authentication.

3.2.6. Criteria for interoperation

The eOI is an identification document of Croatian citizens whose issuance is regulated by the Identity Card Act [1].

The criteria relevant for the determining of interoperability of the eOI and the certificate on the eOI include:

a) High level of security of electronic identification implemented in the process of use of eOI certificate is based on the criteria set by Commission Implementing Decision (EU) No. 2015/1502 [11] and this applies to the following:
   - It offers a high level of ensuring the identity of a person
   - It is an anti-counterfeiting means that prevents unauthorized changes of the attackers with high attacking potential
   - It can be safely used by the person who owns it and it prevents others to use it
   - It is delivered to only one person
   - It contains a very reliable mechanism of authentication
   - It is issued by a service provider who has a highly efficient information service management practice

b) Signing certificate is a qualified certificate for electronic signature, as specified in point 15 of Article 3 of the Regulation (EU) No. 910/2014 [9], and meets the requirements set out in Annex I to the Regulation (EU) No. 910/2014 [9][9].

c) Identification certificate is issued according to the same rules that applies for the signing certificate and serves as a means of high level of security, according to Article 8, paragraph 2 c) of the Regulation (EU) No. 910/2014 [9].

d) Croatian Ministry in charge of Administration is a supervisory body in charge of electronic identification, it carries out an expert examination of electronic identification pursuant Commission Implementing Decision (EU) No. 2015/296.

e) The certificates are issued by the qualified trust service provider, as specified in point 20 of Article 3 of the Regulation (EU) No. 910/2014 [9], and which had been granted a qualified status by the supervisory body, the Ministry in charge of economy and commerce.

f) The eOI, where the certificates are issued on, is a qualified electronic signature creation device, as specified in point 23 of Article 3 of the Regulation (EU) No. 910/2014 [9], and which meets the requirements set out in Annex II to the Regulation (EU) No. 910/2014 [9].

g) The eOI has all necessary functionalities of the European citizen card according to the CEN/TS 15480 [49]] and it is interoperable and suitable for use in e-commerce at national and European level.

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 Article 3.3.2, are applied.

3.3.2. Identification and authentication for re-key after revocation

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

a) When issuing a new pair of keys information and documents may be used that are ensured during the whole process of initial identity validation according to Article 3.2.3.

b) Checking information is carried out in the same way as they are checked the first time the identity is validated.

c) Persons submitting requests due to the expiration of previously issued identity card or for some other reason it no longer serves its purpose submit a color photograph and the old identity card which are voided and returned to the person.

d) Persons submitting requests due the name or surname modification additionally submit an excerpt from the birth register which specifies the note on the new name or new surname, which person is obliged to use in legal transactions, or it submits a marriage certificate.

3.4. Identification and authentication for revocation request

Identity verification of the person upon submitting a request for revocation is carried out with the direct identification and the physical presence of a person on the basis of the adduced document.

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

The acceptable remote method of authentication includes authentication to user web protection of authenticity using data which is confirmed via e-mail.

Data for authentication to web portal are contained in a security envelope which is delivered to the person upon collection of the certificate.

4. Certificate life-cycle operational requirements

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Submitting an application for the issuing of the OI and the certificate on the OI is carried out in accordance with the Identity Card Act [1]:

a) Application for the issuing of the certificate is submitted by natural person, who is named as the subject of the certificate.
b) The legal representative submits an application for the issuing of the certificate for a child or a person deprived of legal capacity,
c) An authorized PU/PP official enters the certificate application in the information system of the PU/PP.

The application for related CA and OCSP certificate is submitted by authorized personnel of CA.

4.1.2. Enrollment process and responsibilities

The process of submitting an application for the issuing of an identity card or the certificate on the identity card is defined by the Identity Card Act [1]. The Ministry publishes instructions on eOI issuing procedure on its official website.

The following rules are prescribed:

a) The application for the issuing of an identity card is submitted on the locations of the PU/PP of the Ministry within official working hours.
b) The application for the issuing of an identity card is submitted on the prescribed form whose layout and content are prescribed by the Ordinance on the forms and records of identity cards [2].
c) The persons are required to confirm that the personal identification data at the time of submission of an application are complete and accurate by signing the application for the issuing of an identity card.
d) Upon submission of the application, the person enters into an Agreement on certification services with the AKD and it confirms the acceptance of his/her obligations and responsibilities by signing it.
e) The application for the issuing of an identity card is accompanied by the confirmation of payment according to the Ordinance on prices of identity cards [3].

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

a) Identity of physical persons is confirmed within a procedure, defined in chapter 3.2.3.
b) Procedures defined in Article 3.2.5 apply on authorized officers of RA/LRA and CA personnel

4.2.2. Approval or rejection of certificate applications

The following rules apply:

a) The PU/PP officers decide on the approval or rejection of the certificate application to the persons.

b) The certificate application is rejected if:
   - there is a suspicion that the information gathered about natural persons are not accurate, complete or reliable,
   - information verification process concerning natural persons is not be successfully carried out according to Article 3.2.3.2.,
   - there is no basis for issuing eOI or eOI certificates
   - the payment of the issuing fee is not made
   - the certificate application has been withdrawn after submission of application, or
   - it has been determined subsequently in the course of submission of the application that certificate application has not been authorized.

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

d) All submitted applications are entered into the information system which meets the security requirements set out in Article 6.5 and 6.6.

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

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

4.2.3. Time to process certificate applications

Certificate application processing is carried out in accordance with the time limit for identity card issuance, prescribed by the Identity Card Act [1]:

a) within 30 days from the submission of the application, if the application is submitted within the regular procedure,

a) within 10 days from the submission of the application, if the application is submitted within the accelerated procedure,

b) within 3 days from the submission of the application, if the application is submitted within the expedited procedure.

4.3. Certificate issuance

4.3.1. Actions during certificate issuance

a) Certificates can be issued to natural person only if the authorized person entered the application into PU/PP information system for eOI

b) Immediately after entering the certificate application in the information system of the PU/PP, data necessary to complete the application is sent to the manufacturer through a secure communication channel.

c) The CA does not verify the completeness, accuracy and uniqueness of the received data for the issuance of the eOI and the certificate, but it relies on the verification carried out in the PU/PP.
d) The manufacturer produces an eOI with a chip and a printed design, and built-in security elements which provide a physical protection against counterfeiting or modifications in accordance with the requirements of the MUP as the issuer of the eOI.
e) The process of issuing of a certificate, generating pairs of keys and PINs and their entry into the eOI is carried out in a secure environment which meets the requirements set out in Article 6.5 and 6.6.
f) The profile of the issued certificates must be in accordance with the requirements set out in Article 7.1.
g) The CA keys, that are used to sign the certificates and keys of the persons are protected by using measures and procedures, prescribed in Article 6.2.
h) Following the process of producing and individualization, the eOI is properly packaged and delivered to the PU/PPin which the person has applied for its issuance.
i) In case of an expedited eOI procedure, eOIs are delivered to the addresses of the PU of corresponding PP in which the person applied for the identity card issuance.

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

Upon submission of the application, the authorized PU/PP officers inform the person when his/her eOI is produced and when it can be collected.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

The following rules apply:

a) The eOI with the certificates are delivered to the person in the PU/PP following the identity validation by the direct identification in the physical presence of a person.
b) The identity verification is carried out on the basis of the adduced identification data or a valid document, or by inspecting the existing data in the records of identity cards.
c) It is deemed that the signatory has accepted the private key and the certificate at the time of delivery of the eOI.
d) At the time the eOI is being collected, the person is informed of the conditions applicable for the use of the certificate and has already signed an agreement (according to the chapter 4.1.2).
e) If the person fails to collect the eOI within 90 days, it is deemed that the certificate was not accepted.
f) Certificates that have not been accepted are revoked in line with the procedure described in Article 4.9.3.

4.4.2. Publication of the certificate by the CA

The certificates are published in the public directory immediately following the certificate issuance.

Certificates of the person are not available for the public search unless the consent of the person is provided.

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

The information that the certificate has been issued and that the eOI has been produced the CA sends to the information system of the PU/PP through a secure communication channel.

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

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

4.5. Key pair and certificate usage

4.5.1. Subscribers

An undamaged security envelope containing registration data for the web portal and the eOI activation is delivered to the persons.

Every person to whom a certificate is issued has to sign an agreement on certification services provision as defined in Article 9. 3 of the Act on Croatian Identity Card and they have to act pursuant to the terms and conditions of eOI certification services provision, i.e. they have to meet all their obligations defined in Article 9.6.4.

eOI terms of certification services contain the following:

a) information about the certification services provider, about the scope of those services and about the rules of service provision
b) types, purpose and limitations of certificate as well as methods of checking the certificate,
c) all the responsibilities and liabilities of natural persons, service provider and relying parties.
d) Business information related to warranties, prices, conclusion of the agreement and terms and conditions of termination of the agreement
e) Laws and regulations related to security of information and privacy
f) Communication with users, claims, settlement of disputes and applicable law and
g) Applicable laws and regulations and supervision of the certification service provider.

4.5.2. Relying party public key and certificate usage

The relying parties who rely on eOI certificates and certification services provided by HRIDCA have to act pursuant eOI terms and conditions of certification services provision, and they have to meet all the responsibilities set out in Article 9.6.5.

4.6. Certificate renewal

4.6.1. Circumstance for certificate renewal

The certificate must be renewed if the period of validity has expired.

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

4.6.2. Who may request renewal

The rules from point 4.1 apply.

4.6.3. Processing certificate renewal requests

The rules from point 4.2 apply.

4.6.4. Notification of new certificate issuance to subscriber

The rules from point 4.3 apply.

4.6.5. Conduct constituting acceptance of a renewal certificate

The rules from point 4.4.1 apply.

4.6.6. Publication of the renewal of certificate by the CA

The rules from point 4.4.2 apply.

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

The rules from point 4.4.3 apply.

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

A new pair of keys and new certificate will be 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 certification revocation (refer to 4.9).

The HRIDCA does not keep private keys of persons, nor it reactivates the revoked certificate, but a new eOI with a new pair of keys and a new certificate is issued to the person.

4.7.2. Who may request certification of a new public key

The rules from point 4.1 apply.

4.7.3. Processing certificate re-keying requests

The rules from point 4.2 apply.

4.7.4. Notification of new certificate issuance to subscriber

The rules from point 4.3 apply.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

The rules from point 4.4.1 apply.

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

The rules from point 4.4.2 apply.

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

The rules from point 4.4.3 apply.

4.8. Certificate modification

4.8.1. Circumstance for certificate modification

Circumstance for certificate modification includes:

a) there was a modification of a personal name or a personal identification number, 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 4.7.1).

4.8.2. Who may request certificate modification

The rules from point 4.1 apply.

4.8.3. Processing certificate modification requests

The rules from point 4.2 apply.

4.8.4. Notification of new certificate issuance to subscriber

The rules from point 4.3 apply.

4.8.5. Conduct constituting acceptance of modified certificate

The rules from point 4.4.1 apply.

4.8.6. Publication of the modified certificate by the CA

The rules from point 4.4.2 apply.

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

The rules from point 4.4.3 apply.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

The reasons for revocation of certificate of natural persons are the following:

a) An authorized request for the certificate revocation has been submitted
b) A modification in certificate data or there were changes and modifications of the personal name or personal identification number has been reported of the natural person that are contained in the "Subject" field of the certificate.
c) A loss, theft or malfunction of eOI has been reported
d) A misuse or unauthorized use of the identity card has been reported or whenever the private key compromising is possible
e) A cessation of validity of the certificate before the expiration of the period for which the certificate has been issued due to reasons that are specified by Article 15 of Identity Card Act [1].
f) 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
g) The court, public prosecution or institution that conduct judicial or criminal investigation request a certificate revocation in order to prevent a crime
h) Certificate has been revoked or changed due to operational reasons. This includes the following situations:
   - It was found out that the private key does not fit to public key in the certificate or it was determined later on that the data in the certificate are not accurate.
   - It was found that the certificate application was not authorized or it was withdrawn later on
   - It was found that the certificate was not issued in accordance with the HRIDCA CPS or CP
i) HRIDCA certificate is revoked.

HRIDCA certificate is revoked in the following situations:

j) 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 point 1.3
k) HRIDCA private key compromising has been established
l) AKDCA Root certificate was revoked.
m) Should HRIDCA, due to technical, contractual or any other reason, cease to issue certificates or cease to provide certification services.

4.9.2. Who can request revocation

The certificate revocation may be requested by:

a) Natural person named as the subject of the certificate or his/her legal representative for reasons indicated in points 4.9.1. a) to d),
b) Authorized PU/PP officers for reasons indicated in points 4.9.1 a) or g),
c) Authorized CA personnel for reasons indicated in point 4.9.1 from h) to m).

4.9.3. Procedure for revocation request

Clear instructions concerning procedures to be taken in case of occurrence of the reason for the certificate revocation are available on the web portal as defined in 4.1.9.,

The following procedures for the certificate revocation request are applied:

a) Persons submit the certificate revocation request:
   - in the offices of the PU/PP during working hours, or
   - by using a web portal, following the procedure for suspension of certificate that is defined in Article 4.9.15., at all times: 24/7

b) The certificate revocation request by the person is accepted only if the identity of the applicant is determined in accordance with the rules for identity validation in line with the Article 3.4.,

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

d) CA and OCSP revocation procedure is initiated and approved by the PMA.

4.9.4. Revocation request grace period

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

If there was a modification of the data concerning personal name or personal identification number, the person is required to request a revocation within 2 days from the date the modification occurred.

4.9.5. Time within which CA must process the revocation request

The following rules are applied:

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

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

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

d) The maximum amount of time that can elapse between receiving the certificate revocation request and the publication of the status is 24 hours.

e) The certificate that is permanently revoked (i.e. that is not suspended) cannot be re-activated, and its status cannot be changed.

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

g) The CA provides a secure environment in which the certificate revocation procedure is performed pursuant Articles 6.5., 6.6. and 6.7.

4.9.6. Revocation checking requirement for relying parties

Information verification 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, and then it is obligated to either reject the use of the certificate or assume risk and responsibilities, and bear consequences for the use of a certificate whose status has not been confirmed.

4.9.7. CRL issuance frequency

The CRL is issued according to the following rules:

a) Every CRL contains information about the time of issuing and validity period of CRL
b) HRIDCA oblige to issue a CRL at least 1-time within 24 hours.
c) The new CRL is issued at least 10 minutes before the expiration of the validity of the previous CRL.
d) Under regular work conditions, the KRIDCA generates and issue the CRL every 12 hours.
e) The period of the validity of CRL that is issued by HRIDCA is 24 hours from the time of the issuance of the CRL.
f) AKDCA Root validity period CRL is 90 days after the CRL issuance.
g) In the case of the HRIDCA and AKDCA Root certificate revocation, the AKDCA Root will issue CRL within 24 hours.
h) If the validity period of the certificate that is revoked expires, , information about certificate revocation can be removed from the CRL.
i) 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 continuously monitored.

4.9.8. Maximum latency for CRL

The maximum latency from the moment of CRL issuance to the moment of CRL publication on-line is 10 minutes in normal operating conditions.

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 reply has to meet the requirements of IETF RFC 6960 [36] and IETF RFC 5019 [40].

OCSP certificates contain id-pkix-ocsp-nocheck extension as required by CA/Browser Forum BRG [16] and as defined in IETF RFC 6960 [36].

4.9.10. On-line revocation checking requirements

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

a) The OCSP service is available via HTTP protocol at the address published in the authorityInformationAccess field in each certificate.
a) The HRIDCA refreshes the information that is published via OCSP at least every 24 hours.

b) Under regular work conditions, the HRIDCA refreshes the information that is published via OCSP immediately following receipt of the certificate revocation request.

c) The validity of the response by the HRIDCA OCSP service is a maximum of 24 hours.

d) The AKDCA refreshes the information that is published via OCSP at least every 90 days.

e) In the event of the certificate revocation of HRIDCA, the AKDCA Root refreshes the information that is published via OCSP within 24 hours.

f) Every response of the OCSP service is signed electronically by the certificate which is issued by the same CA that issued the certificate for which the certificate's status verification is requested.

g) If the OCSP service receives a request for the certificate's status verification, which has not yet been issued, it does not respond with a status "good".

h) The reply of OCSP certificate status service will not be "good" if the status of CA certificate is not checked of if CA certificate is not valid.

i) In order to ensure the availability of the service in accordance with the rules set forth in this chapter, the operation of the OCSP service is continuously monitored.

4.9.11. Other forms of revocation advertisements available

The HRIDCA provides certificate's status verification directly to registered persons in the private section of the web portal (refer to 2.2.)

4.9.12. Special requirements related to key compromise

HRIDCA, in accordance with the Article 4.9.1, revokes the certificate if the private key has been confirmed as compromised.

4.9.13. Circumstances for suspension

Circumstances for suspension of the person's certificates include:

a) An authorized request for the certificate suspension has been submitted,

b) A disappearance of the eOI has been reported,

c) There is a possibility that the certificate revocation request is subsequently withdrawn,

d) There is no possibility for the certificate revocation request to be submitted in a timely manner for any reason, indicated in point 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 not insignificant,

Circumstances for the withdrawal of the suspension of the person's certificate include:

f) An authorized request for the withdrawal of the suspension of the certificate has been submitted,

g) eOI has been found,

h) 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 person named as the subject of the certificate or his/her legal representative,
b) authorized PU/PP officer,
c) authorized CA personnel.

4.9.15. Procedure for suspension request

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

The following rules apply:

a) The persons submit suspension request for their certificate:
   - in the offices of the PU/PP during working hours, or
   - remotely using electronic services for the certificate suspension.
b) The certificate suspension request is accepted only if the identity of the applicant is determined in accordance with the rules for identity validation in line with the Article 3.4.
c) If the request for suspension or withdrawal of suspension is granted, it is forwarded for further processing by the CA.
d) The maximum amount of time that can elapse between receiving the request for suspension or withdrawal of the suspension of a certificate and the publication of the status is 24 hours.
e) The system for the suspension or withdrawal of the suspension of a certificate has a reliable source of time and it provides a valid record of the date and time that are synchronized with UTC at least once a day.
f) The CA provides a secure environment in which the procedure for the suspension or withdrawal of the suspension of a certificate is performed.

4.9.16. Limits on suspension period

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

By withdrawal of the suspension request, certificate is re-activated, removed from CRL and it becomes valid again.

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

4.10. Certificate status services

4.10.1. Operational characteristics

The following rules are applied:

a) The CA provides on-line CRL verification services via HTTP and LDAP protocol and OCSP service for the certificate's status verification.

b) The information concerning revoked certificates with the expired validity, basic certificate field:" Valid to" is deleted from the publicly available CRL and OCSP services, but remain archived at the CA.

c) Public address for status verification of HRIDCA certificate by using the OCSP service is: http://ocsp-hridca.eid.hr/hridca.

d) Public addresses to retrieve the HRIDCA CRL on the web server: http://crl1.eid.hr/hridca.crl and http://crl2.eid.hr/hridca.crl.

e) Public address to retrieve the CRL through a public directory: ldap://ldap.eid.hr/cn=HRIDCA,o=AKD d.o.o.,c=HR?certificateRevocationList;binary.

f) The order according to which the relying party retrieves the information concerning the certificate's status:

   1) OCSP service: http://ocsp-hridca.eid.hr/hridca
   2) HTTP CRL: http://crl1.eid.hr/hridca.crl
   3) HTTP CRL: http://crl2.eid.hr/hridca.crl
   4) LDAP CRL:
      ldap://ldap.eid.hr/cn=HRIDCA,o=AKD d.o.o.,c=HR?certificateRevocationList;binary

g) Integrity and authenticity of information on the certificate status is ensured by electronic signature: CRL is signed by HRIDCA certificate, and OCSP rely by HRIDCA OSCP certificate.

4.10.2. Service availability

The following rules apply:

a) The service of receipt of request for revocation or suspension of certificate is available during working hours in PU/PP offices.

b) In normal operating conditions, a request for suspension of the certificate can be submitted electronically at all time, i.e. 24/7.

c) In normal operating conditions, availibilty of CRL and OCSP certificate status checking is 24/7.

d) The response time for CRL and OCSP verification of the certificate's status in a maximum of 10 seconds.

e) In order to shorten the processing time and certificate's status verification it is recommended to use the OCSP protocol.

f) In the case of system failure, the service is available within the shortest time possible and in accordance with the best business practices.

4.10.3. Optional features

Not foreseen.

4.11. End of subscription

eOI certificates are issued wit the period of the certificate validity of 5 years.

During the validity period the person will act pursuant the eOI terms and conditions of certification service provision.

The certificate ceases to be valid if:

a) the validity period expired, basic field of the certificate "Valid to"
b) if it was revoked at an earlier time.

4.12. Key escrow and recovery

Not applicable.

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

5. Facility, management, and operational controls

5.1. Physical controls

The AKD controls the physical access to all PKI infrastructure data and all components related to the provision of the trust services and conducts activities of assessment and risk management.

The physical security measures are implemented in accordance with ETSI EN 319 401 [24]and the chapter 11 of the ISO/IEC 27002[45].

Detailed information on physical security measures implemented by service provider are available in the by-laws.

5.1.1. Site location and construction

The information system of the CA and the manufacturing facilities where the eOI are produced and individualized are located within a business complex of the AKD.

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

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

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

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

5.1.2. Physical access

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

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

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

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

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

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

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

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

5.1.3. Power and air conditioning

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

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

5.1.4. Water exposures

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

5.1.5. Fire prevention and protection

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

The fire protection system consists of:

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

5.1.6. Media storage

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

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

In order to prevent an unauthorized disclosure, modification, relocation or destruction of the information stored on the media, security measures are established in accordance with the chapter 8 of the ISO/IEC 27002 [42].

5.1.7. Waste disposal

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

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

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

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

5.1.8. Off-site backup

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

5.2. Procedural controls

5.2.1. Trusted roles

The authorized employees who are involved in the implementation of the certification activities are granted the appropriate trusted roles with clearly defined responsibilities and authorizations pursuant ETSI EN 319 401 [24] Norm and CEN TS 419 261 [23].

The trusted roles include, but are not limited to:

a) **Security administrators** are responsible for the implementation and enforcement of the security rules in practice.

b) **RA officers** are responsible for verification of data and data preparation that must be carried out when issuing certificates and granting approval for certificate applications.

c) **Revocation officers** are responsible for the implementation of the change of status of certificates

d) **Information system administrator** is responsible for the installation, configuration and maintenance of information systems.

e) **Operators** are responsible for the performance of the daily activities on information systems and to save and restore data when needed.

f) **System Auditors** are responsible for the daily review of the reports concerning the operation of the system, audit logs and archives when needed.

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

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

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

5.2.2. Number of persons required per task

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

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

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

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

5.2.3. Identification and authentication for each role

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

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

Identification and authentication of the RA officers and CA personnel are carried out according to the rules specified in point 3.2.5.

5.2.4. Roles requiring separation of duties

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

The following rules are applied:

a) The person who authenticates himself/herself as a security administrator or an official for the revocation or an RA officer may not have the authorizations of a System Auditor.

b) The person who authenticates himself/herself as an information system administrator or System Operator may not have the authorizations of a System Auditor or a security administrator.

c) The person who authenticates himself/herself as an RA officer or a System Auditor may not have the authorizations of a security administrator, an information system administrator or an operator.

d) The security administrator, information system administrator or System Operator may have the rights for the reading of audit logs that are assigned to the System Auditor if necessary.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

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

a) professional qualifications,

b) previous employments,

c) criminal records,

d) medical fitness, and

e) credit/financial capacity in accordance with legal regulations.

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

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

All access rights of the employees of CA will be terminated, as well as their user rights for CA IS whenever they change jobs within the company or upon termination of their employment.

Registration body will terminate user rights to PU/PP IS whenever the officers of PU/PP change jobs or upon termination of their employment.

5.3.2. Background check procedures

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

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

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

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

Potential CA personnel and officers of PU/PP are thoroughly vetted prior to employment: their identity, capabilities and reliability is checked.

All personnel who participate in CA activities have to be permanently employed by the certification service provider.

All officers of PU/PP are government employees and they are permanently employed by the registration body (MUP).

5.3.3. Training requirements

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

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

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

CA employees are adequately informed about the security requirements and rules of conduct in the process of implementing certification procedures.

MUP ensures that the officers of PU/PP get all necessary instructions and that they undergo professional training in order to be aware of their responsibilities and obligations.

5.3.4. Retraining frequency and requirements

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

Informing the employees about the rules of conduct is carried out during the introduction of the new internal rules and in the event of significant changes, at least once in 2 years

The aim of the informing includes the following:

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

5.3.5. Job rotation frequency and sequence

The CA 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 Article 5.3.2.

5.3.6. Sanctions for unauthorized actions

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

5.3.7. Independent contractor requirements

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

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

5.3.8. Documentation supplied to personnel

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

5.4. Audit logging procedures

5.4.1. Types of events recorded

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

Types of audit logs include:

a) logs on the management of the certificate's life-cycle, which include, but are not limited to:
   - user registration,
   - certification,
   - data preparation and SSCD creation,
   - revocation, suspension, withdrawal of the suspension of a certificate, and
   - issuance and publication of the CRL.

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

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

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

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

5.4.2. Frequency of processing log

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

Periodic control is carried out for less critical activities.

5.4.3. Retention period for audit log

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

All audit logs are archived in accordance with the archiving rules, described in Article 5.5.

5.4.4. Protection of audit log

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

a) All system clocks and times are mutually harmonized so that audit logs contain a valid record of the date and time.
b) Confidential data are exempt or are masked so that they do not be included in the audit logs.
c) A cryptographic protection of integrity of all critical audit logs is implemented to be protected from any kind of modification or deletion.
d) Unauthorized access to the audit logs is prevented.
e) System configuration that deactivates the audit log entries is disabled.
f) Audit logs cannot be deleted, nor can they automatically overwrite existing data.

5.4.5. Audit log backup procedures

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

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

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

5.4.6. Audit collection system (internal vs. external)

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

Audit logs of all critical systems are included in the log management system.

Audit log events can be searched according to type 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.

5.4.8. Vulnerability assessments

A system vulnerability analysis is performed based on examination of all audit logs in the audit log management system.

Examination and analysis of system vulnerability is carried out periodically, by using approved software tools, pursuant internal security rules and activities are undertaken immediately after the discovery of the vulnerability to address them.

5.5. Records archival

5.5.1. Types of records archived

All data related to service provision are archived, which include, but are not limited to:

a) Audit logs as defined in Artice 5.4.1.,
b) Documentation and information gathered in the registration process of all natural and legal persons as defined in 3.2.2.1 and 3.2.3.1.
c) Documentation produced in the ceremony of generation of CA keys as in Article 6.1.1.,
d) Certificates and data on certificates life's cyle
e) data related to the management of cryptographic keys, and OSCD,
f) documentation on the rules of service provision (CP, CPS and PDS)
g) other data and documentation in accordance with legal regulations.

5.5.2. Retention period for archive

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

5.5.3. Protection of archive

The following measures of protection are applied:

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

The AKD, as the creator and owner of the public archival and registry material, acts in accordance with the provisions of the Archival Materials and Archives Act (Official Gazette 105/97, 64/00, 65/09, 125/11).

5.5.4. Archive backup procedures

Archive backup procedures are performed in the high-security area, and backup archives are stored in another location.

5.5.5. Requirements for time-stamping of records

Not applicable.

5.5.6. Archive collection system (internal or external)

Archive collection is made internally depending on the type of records.

The collection and archiving of data and documentation that is generated in the registration process of persons in the PU/PP is regulated by the agreement.

5.5.7. Procedures to obtain and verify archive information

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

Only authorized persons have access to archive information.

Verification of the data from the archives include checking the data integrity protection.

5.6. CA Key changeover

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

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

- that the validity period for each certificate issued is always be shorter than the validity period of the CA certificate that issued the latter, and
- that the cryptographic algorithms and parameters is always be suitable for use and in accordance with the recommendations referred to in the ETSI TS 119 312 [32],
- 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 point 6.1.1.

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

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

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

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

In case of malfunctions or corruptions of computing resources, software and/or data, provisions of Chapter 16 of ISO/IEC 27002 [42] will be implemented.

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

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

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

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

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

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

5.7.3. Entity private key compromise procedures

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

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

a) certification of the compromised CA system shall be ceased,
b) the CA certificate revocation procedure shall be initiated,
c) person's certificate revocation procedure, issued by the compromised CA, shall be initiated,
d) persons and relying parties shall be informed via the web portal,
e) competent national and supervisory bodies and other interested parties shall be informed,
f) in the case of the suspicion of elements of a crime, the latter shall be reported to the police in order to initiate an investigation process, and
g) the process of generating a new CA key shall be initiated.

5.7.4. Business continuity capabilities after a disaster

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

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

The business continuity plan includes a procedure for acting in emergency situations and system recovery plan.

Business continuity management is carried out pursuant the rules and regulations set forth in Chapter 17 ISO/IEC 27002. The AKD ensures a high availability and uninterrupted continuation of the activities for the following services:

- management services by the certificate revocation,
- certificate's status verification services and
- Dissemination service.

Services of certificate generation, registration and supply of devices are carried out during working hours.

5.8. CA or RA termination

In the event of the termination services, the AKD consults MUP and Croatian ministry in charge of commerce and economy and administration in order to confirm further steps related to termination of services.

6. Technical security controls

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 organized and supervised by the PMA.
b) The ceremony is carried out in a physically secure environment in the high-security area according to defined procedures and pre-prepared technical script.
c) The ceremony is attended by employees entrusted with the roles (Article 5.2), internal and external assessors, public notary and other invited witnesses.
d) Before the start of the ceremony in the presence of a public notary, a formal identification of persons and the assignment of devices, security envelopes and forms of storage are carried out.
e) The process of generating the CA key is carried out according to a pre-prepared technical script that includes the inspection of the equipment, cables, security settings and equipment parameters and every command that is entered into the information system during the implementation process.
f) The ceremony includes the creation of backup of the CA keys and other data and storage of the cryptographic materials and other contents to the defined locations.
g) During the ceremony, the records of the contents in the safe cabinets with stored cryptographic materials on primary and backup locations are certified.
h) During the ceremony, the internal and external assessors certify the technical script and the printout of the certificate by CA (certification authority) (with the public key) confirming that the process of generating the key has been carried out correctly and that the integrity of the generated keys has been ensured.

i) After the ceremony, the public notary certifies the record of implementation of the ceremony with the confirmed identity and statements of participants.
j) The certified technical script signed by all participants of the ceremony, a printout of the CA certificate, a record of the implementation of the ceremony and a video of the ceremony of generating the CA key are stored in the archives.
k) The process of generating the keys of persons and their entry in the eOI is performed by the manufacturer in the physically secure environment in a high-security area.
l) The CA keys and keys of persons are generated, used and stored in the HSM module that implement standards and control functions as specified in the chapter 6.2.1.

6.1.2. Private Key delivery to subscriber

The eOI with private keys are dispatched to persons to the PU/PP after the completion of the production process where they are delivered to the person after identity validation by the direct identification in the physical presence of a person.

6.1.3. Public Key delivery to certificate issuer

Immediately after generating the keys of persons, the manufacturer obtains a certificate from the HRIDCA using electronic service.

The manufacturer sends the public key of the person using the PKCS#10 format of the application, and the HRIDCA returns it within the issued certificate.

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

6.1.4. CA Public Key delivery to relying parties

The AKDCA Root and HRIDCA public keys are available in the certificates on the web portal (refer to the Article 2.2), and are also contained in the eOI.

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

6.1.5. Key sizes

The AKDCA Root and HRIDCA keys are 4096 bits long with the RSA 256 algorithm.

The OCSP keys are 2048 bits long with the RSA 256 algorithm.

The keys of persons are 2048 bits long with the RSA 256 algorithm.

6.1.6. Public key parameters generation and quality checking

The CA and OSCP keys as well as keys of persons are generated by a random number generation device in HSM device. The parameters of a public key for RSA algorithm are in accordance with the FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf) or other equivalent norm approved by the PMA.

In general, in order to generate the CAand OCSP keys and keys of persons, cryptographic algorithms and parameters are used in accordance with the ETSI TS 119 312 [32].

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

The X.509 v3 certificates are issued to persons in accordance with IETF RFC 5280 [35], and their purpose are defined by the value of the “keyUsage” extension.

Extension "Key usage" of all certificates is marked as critical extension.

Extension "Key usage" has the following values:

a) For the CA certificates: Certificate Signing, Off-line CRL Signing, CRL Signing.

b) For the OCSP certificates: Digital Signature.

c) For eOI signing certificate is "Non Repudiation"

d) For eOI identification certificate: Digital Signature.

OCSP certificates have additional extension *"Extended Key Usage"* with the value *"OCSP Signing".*

6.2. Private Key Protection

6.2.1. Cryptographic module standards and controls

The following rules apply:

a) The CA and OCSP keys as well as keys of persons are generated in HSM device that demonstrates compliance with the FIPS PUB 140-2 level 3 [38] standard.

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

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

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

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

f) Following generation, the private keys of persons are entered in the eOI, which are, as a qualified electronic signature creation device (QSCD) that meet the requirements of the EAL 4+ according to the ISO/IEC 15408 [39] and demonstrate the compliance with the forms of protection of the series EN 419 211 [17], [18], [19], [20], [21] and [22].

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

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

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

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

6.2.3. Private Key escrow

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

a) After they are generated, the private keys of the CA and OCSP service remain stored in the HSM device under supervision of at least 2 persons.
b) A system that manages the AKDRoot CA private key is activated only when necessary.
c) A system that shall manage the HRIDCA private key shall be constantly available and shall be used solely for the signing of the certificates of persons and CRL. The same shall apply to appropriate OCSP system which signs the replies to enquiries regarding the certificate's status.
d) The cryptographic keys outside the HSM device may only be in the encrypted form and in accordance with the rules specified in point 6.2.6.

The rules for storage of the private keys of persons:

e) The individual private keys of persons are encrypted immediately following generation using the cryptographic keys whose strength is equal or greater than the key that is protected,
a) In addition, private keys are encrypted within the shared file which is transferred to the manufacturer in its center for individualization,
b) The decrypting of the private key of a person is carried out in the manufacturer's safe area and only within the minimum time necessary for their entry into the eOI chip,
c) The keys that are used to encrypt/decrypt the private keys of persons in the production, are also be stored in the HSM device that demonstrates the compliance with the FIPS PUB 140-2 level 3 [38] [38] standard,
d) The AKD does not provide permanent storage of the keys of persons; they are deleted immediately following the individualization of the eOI.

6.2.4. Private Key backup

The CA and OCSP private key backup is carried out in the protected area of the high security arein accordance with the rules set out in points 6.2.1 and 6.2.2.

Backups of the CA private keys are stored in a secure safe high security area as well as in a secondary location where the same or higher level of protection of the private key is provided.

The private keys of persons are not copied.

6.2.5. Private Key archival

The CA private keys are not archived.

The 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

The CA private key is transferred to another HSM device only if the new device is in accordance with the FIPS PUB 140-2 level 3 [38] standards.

When the CA private key is outside of the HSM module for the purposes of backup, the hardware protection mechanisms of the private key is used, which is provided by the manufacturer of the HSM device, and which are in accordance with the FIPS PUB 140-2 level 3 [38] standard.

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

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

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

The private keys of persons that are forwarded to the manufacturer are encrypted in accordance with the rules specified in point 6.2.3.

6.2.7. Private key storage on cryptographic module

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

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

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

The activation of private keys on the HSM device or on the eOI is carried out in accordance with the chapter 6.2.8.

6.2.8. Method of activating private key

The activation of the private key in the HSM device:

a) The activation of the CA and OCSP private key in the HSM device is carried out solely under the dual control of authorized persons.
b) The activation is carried out using the hardware resource for activation and associated secret PIN.
c) Once activated, the private key in the HSM device remains activated during the time that the HSM device is turned on.
d) After turning off and later on turning on the HSM device, activation of the private keys is carried out again.

The activation of the private key of a person on the eOI:

e) The activation of the private key of a person is performed one time by entering a PIN.
f) Activation of the private keys in the eOI is possible only following the activation of the eOI, which is carried out in accordance with the rules specified in point 6.4.1.

6.2.9. Method of deactivating private key

The deactivation of the private key in the HSM device:

a) The private key of the CA is deactivated if the HSM device or system that controls the private key is not active or is not in operation. The same applies to as the OCSP private key.

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

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

6.2.10. Method of destroying cryptographic key

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

a) The destruction of the CA 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 or OCSP termination.
b) When the need arises, the destruction of the private key on the HSM device is carried out using a secure method that is provided by the manufacturer of the HSM device, which guarantees that the destroyed private key is able to be recovered or reused in any way.
c) The destruction of cryptographic keys is carried out by the commission in the presence of at least 2 persons to whom trusted roles have been assigned and record of destruction is provided.
d) The method of destruction of cryptographic keys is carried out in a safe manner, in the areas of the secure zone as described in detail in the documented internal procedures.
e) Destruction of backups and archive of the private key is carried out using the method described in point 5.1.7.

The method of destroying the private keys of persons:

f) The destruction of files with encrypted private keys of persons on the information system is carried out with an automated method, following the process of individualization and putting the private key of persons on the eOI.
g) The destruction of the encrypted private keys on the information system is carried out using the proven safe method and provided audit log of destruction.

6.2.11. Cryptographic Module Rating

It refers to the point 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 and OCSP services, are an integral part of the certificate which are archived to enable the subsequent verification of electronic signatures and provide the evidence for judicial, administrative and other procedures.

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

6.3.2. Certificate operational periods and key pair usage periods

The validity period of the certificate is given below, in Table 7.

Table 7: Validity period of the certificate

Certificate	Validity period
Certificate of the root certification authority called AKDCA Root	to 2038-01-19 03:14:07+00:00
Certificate of the subordinate certification authority called HRIDCA	up to 15 years
Certificate for signing of OCSP replies	up to 3 years
Certificates of persons	up to 5 years

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

Validity period of every certificate is contained in every certificate. The certificate is valid from the date of the issuance (basic certificate field: "Valid from") until the expiration date (basic certificate field: "Valid to") and should not be used after the expiration of the validity.

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

6.4. Activation data

6.4.1. Activation data generation and installation

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

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

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

e) The activation of the eOI is carried out by the person individually after collecting the eOI using the data for the activation in the security envelope and according to the instruction for the eOI activation that is available on the web portal of the eOI.
f) During the activation of the eOI, PINs are set to protect private keys, and PUK value is set to unlock the eOI.
g) Persons are informed of their obligations related to the protection of the activation data or PINs.

6.4.2. Activation data protection

The manufacturer undertakes the following measures for the activation of the data protection:

a) Generating the activation data, their entry into the eOI and printing in the security envelopes are carried out under the dual control in the manufacturer's secure environment of the eOI.
b) The security envelopes with the activation data are packed in separate packages and sent to the PU/PP, regardless of the sending of the eOI.
c) The security envelopes with the activation data are delivered to the persons in the PU/PP.

Persons are informed of implemented protection measures of the eOI and PINs to protect private keys on the eOI:

d) After 6 consecutive attempts of entering the wrong PIN, the eOI locks,
e) The locked eOI the person may unlock independently using the PUK value set during the activation of the eOI,
f) After 6 consecutive attempts of entering the wrong PUK, the eOI blocks,
g) The blocked eOI may be unblocked only by the PU/PP official in a secure environment using the electronic service to unblock the eOI,
h) The unblocking of the eOI is carried out in the physical presence of the person after identity validation of said person.

6.4.3. Other aspects of activation data

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

In accordance with the documented internal procedures, the AKD performs the protection of the activation data against generation, installation, printing in the security envelopes and the destruction of the activation data until the transport and delivery of the security envelopes to the persons.

After the delivery of the security envelopes, the persons are responsible for the protection of the activation data.

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 [41] and ISO/IEC 27002 [42] standards.

In addition, technical requirements related to the computer security are implemented according to the requirements of the ETSI EN 319 401 [24] norm as well as according to the requirements set forth in the document called CA/Browser Forum NetSec [15], i.e. CEN TS 419 261 [23].

This means the following:

a) Internal security standards are documented and there is a number of procedures and instructions which are regularly updated in order to be in compliance with the security requirements.
b) The organizational and management structure with clearly defined trusted roles and responsibilities are established.
c) The rules related to employees, security guards, visitors and external service personnel are defined prior and during the contractual relationship and after the expiry of the contract.

d) Measures to protect the property and data that include defining the owner, classification and operation are applied.
e) Appropriate systems for physical protection of facilities, areas and information equipment are established.
f) Management of authorizations and access rights is restrictive and dual control for the implementation of all critical operations involving the issuing, deletion or modification of the certificate or its status are established.
g) Strict rules related to the management of cryptographic keys and equipment are prescribed and implemented.
h) Regular measures to maintain the security of the network and computer equipment including protection against malicious code, management of audit logs and security testing are carried out.
i) The system is continuously monitored and alarmed in order to allow the detection, registration and timely response to unauthorized actions or irregular occurrences.
j) Backups are created and stored, and business continuity management procedures are established.
k) Management rules for incidents, modifications, problems and requirements are established.

6.5.2. Computer security rating

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

6.6. Life-cycle technical controls

6.6.1. Management of system/software development

In accordance with chapter 14 of the ISO/IEC 27002 [42], controls over the development and life-cycle of the software are established, which includes:

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

6.6.2. Audit/controls of security management

In accordance with chapter 12 of the ISO/IEC 27002 [42], controls over computing resources are established, which includes:

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

c) The resources are regularly monitored, adjusted and planned in order to ensure sufficient capacities and the required system performances,
d) Risk assessment is carried out pursuant Norm ISO/IEC 27005 [44] during which business and technical aspects related to provision of services are taken into consideration,
e) The development, testing and production environment are strictly separated in order to reduce risks of unauthorized access and modification to the production environment,
f) The computer systems are protected from viruses, malware and unauthorized software,
g) Backups are regularly created and are protected from damage, loss and unauthorized access in order to prevent data loss,
h) Audit logs are provided and all measures for their protection are taken.

6.6.3. Audit/controls of life cycle security

During a life cycle periodic audits and supervision of security of information system are carried out.

In accordance with the chapter 15 of the ISO/IEC 27002 [42], controls related to business relations and suppliers are established, which includes:

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

6.7. Network security controls

The network controls are established as defined in Chapter 13 ISO/IEC 27002 [42], Appendix B CEN TS 419 261 [23] and CA/Browser Forum NetSec [15].

This includes the following network controls:

a) All computing resources are segmented into logically separate, specific functional units called network zones,
b) The following network zones are established:
   - PKI CA zone, where computing resources for the implementation of the services of generating and management of certificate revocation is be located,
   - PKI service zone, where computing resources for the implementation of the services of informing and certificate's status verification is located,
   - Perso service zone, where computing resources for uploading cryptographic keys on eOI and printing activation data on security envelopes,
   - DMZ where computing resources that are exposed directly to the public is located.
c) Clear rules are defined and established so that specific network zone applies the same physical, technical and procedural protection measures,
d) The equipment and hardware between the network zones are physically separated and placed into separate computer cabinets,
e) Computer cabinets are placed in areas within the adequate zone of physical security, and protected by the appropriate measures of physical security in accordance with the Article 5.1,
f) Wiring and all physical points of connections and active and passive network equipment is controlled and monitored,

g) The physical access to computing resources and network equipment is limited to persons with trusted roles that are authorized to administer the software,

h) The network zones are separated by firewalls, and between network zones the network traffic according to the formally approved lists of allowed services are strictly regulated,

i) The communication between the network zones is carried out through the secure channels separated intentionally and logically and which protect the data against modification and disclosure,

j) Only the communication, necessary for the implementation of service is enabled between the network zones, and any communication other than the one explicitly granted is prohibited,

k) The limited access to the network zone may be carried out in the following way:

- the secure zone may be accessed only from the service and operational zone,
- the service and operational zone may be accessed only from the control and access zone.

l) Reports on every change to the firewall configuration are automatically generated,

m) Intrusion detection system, that monitors the network traffic in the active and service zone and alarm all suspicious activities in real time, is implemented,

n) Vulnerability testing is carried out periodically and for every major configuration change, and all critical vulnerabilities are resolved within the shortest time possible,

o) A system penetration test is carried out in the event of significant changes and at least once a year.

6.8. Time-stamping

All information equipment has a harmonized system clocks and reliable source of time so that all audit logs contain a valid record of the date and time. The maximum permissible deviation in time is 1 second.

7. Certificate, CRL, and OCSP profiles

7.1. Certificate profiles

Forms (profiles) of all certificates are made pursuant IETF RFC 5280 [35] and Recommendation ITU-T X.509 [45].

When determining the profile of certificates the requirements of the following norms apply:

- ETSI EN 319 412-1 [28] generally for all certificates
- ETSI EN 319 412-2 [29] for natural persons
- ETSI EN 319 412-3 [30] for CA and OCSP certificates and
- ETSI EN 319 412-5 [31] for EU qualified certificates

Basic/general fields of all certificates are stated in below table.

Table 8: Basic/General fields

Field	Value/Limits of the value
Version	X.509 V3, see 7.1.1

Serial Number	Unique positive No. with 32 bit entropy
Signature Algorithm	SHA256RSA, see 7.1.3.
Issuer DN	See 7.1.4.
Valid from	utcTime
Valid to	utcTime(Valid from +period of certificate validity pursuant 6.3.2).
Subject DN	See 7.1.4.
Subject Public Key	Subject Public Key
Signature Value	Issuer's signature of the certificate, generated and coded according to IETF RFC 5280 [35]

7.1.1. Version Number

X.509 version V3 is used.

7.1.2. Certificate extensions

7.1.2.1. Certificate CA extensions

Extensions of HRIDCA certificates are stated in the following table.

Table 9: HRIDCAcertificate extensions

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

*Critical fields

7.1.2.2. Extensions of private individuals' certificates

Table 10: Extensions of private individuals' certificates

Field	Certificate type	Value
Key Usage*	eOI NCP-n-qscd-eid	Digital Signature
	eOI QCP-n-qscd-esign	Non-Repudiation
Basic Constraints*	All End Entity	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.
Authority Info Access	All End Entity	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eid.hr/cert/hridca.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-hridca.eid.hr/hridca
Certificate Policies	eOI NCP-n-qscd-eid	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.2.2.1.2.20 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
	eOI QCP-n-qscd-esign	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.1.2.1.2.10 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
CRL Distribution Points	All End Entity	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.eid.hr/hridca.crl [2]CRL Distribution Point

		Distribution Point Name: Full Name: URL=http://crl2.eid.hr/hridca.crl [3]CRL Distribution Point Distribution Point Name: Full Name: URL= ldap://ldap.eid.hr/cn=HRIDCA,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)
qcStatements	eOI NCP-n-qscd-eid	N/P
	eOI QCP-n-qscd-esign	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://eid.hr/cps/HRIDCA-pds2-0-en.pdf language=en PdsLocation: url= https://eid.hr/cps/HRIDCA-pds2-0-hr.pdf language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-esign(1) (0.4.0.1862.1.6.1)

*Critical fields

7.1.3. Object identifier (OID)

Algorithms with accompanying OID identifiers for all certificates that are issued by HRIDCA are shown in Table 11.

Table 11: Algorithms and accompanying object identifiers

Algorithm	OID
Sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

7.1.4. Types of names

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

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

7.1.5. Limitations of names

N/A.

7.1.6. Object identifier (OID) of CP

In all certificates that contain extension "Certificate Policies" and accompanying OID as specified in Article 1.2 of this document.

7.1.7. Use of extension Policy Constraints

N/A.

7.1.8. Syntax and semantics of CP qualifiers

There is an address where CP and CPS can be accessed on every certificate that contains extension "Certificate Policies" as stated in Article 2.2 of this document.

7.1.9. Process semantics for critical extension Certificate Policies

N/A.

7.2. CRL profiles

CRL profiles that are issued by HRIDCA support X.509 version 2 pursuant the requirements defined in IETF RFC 5280 [35]. In the below table the Basic CRL fields are listed.

Table 12: Basic CRL fields

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

7.2.1. Number of version

X.509 verzija V2 is used.

7.2.2. CRL extensions

Table 13: Extension CRL issued by HRIDCA are listed in the below table:

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

7.3. OCPS profile

Certificate of OCSP service is created pursuant IETF RFC 6960 [36].
HRIDCA OCSP basic fieldsare defined below.
Table 14: Basic fields of HRIDCA *OCSP*

Field	Value/Limitation of value
Version	X.509 V3, see 7.3.1
Serial Number	Unique positive No. with 32 bit entropy
Signature Algorithm	SHA256RSA, see 7.1.3.
Issuer DN	see 7.1.4.
Valid from	utcTime
Valid to	utcTime(Valid from +5 years)
Subject DN	see 7.1.4.
Subject Public Key	Subject Public Key
SignatureValue	Issuer's signature of the certificate, generated and coded according to IETF RFC 5280 [35]

7.3.1. Version number

X.509 version V3 is used.

7.3.2. Extension of OCSP certificate

Table 15: Extension of HRIDCA OCSP certificate

Field	Value
Key Usage*	Digital Signature

Enhanced Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)
Basic Constraints*	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	Derived using the SHA-1 hash of the public key
Authority Key Identifier	Derived using the SHA-1 hash of the public key
Authority Info Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://eid.hr/cert/hridca.crt
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.2.1.2.1.90 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
OCSP No Revocation Checking	id-pkix-ocsp-nocheck 05 00 (1.3.6.1.5.5.7.48.1.5)

**Critical Field*

8. Compliance audit and other assessments

8.1. Frequency or circumstances of assessment

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

The regular supervision by the trust service providers and conformity assessment with the Regulation (EU) No. 910/2014 [9] is carried out every 24 months.

The regular supervision of the management system in order to verify the compliance with the ISO/IEC 9001 [43], ISO/IEC 27001 [41] and ISO/IEC 14298[40] [40][39] standards are carried out at least every 12 months.

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

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

8.2. Identity/qualifications of auditor

The assessment of the compliance with the Regulation (EU) No. 910/2014 [9] will be carried out by the auditor that is, in accordance with the Regulation (EC) No. 765/2008 [13][13], authorized as competent for the implementation of the conformity assessment of a qualified trust service provider and qualified trust service the latter provides.

Qualifications and requirements that refer to auditors are defined in the Norm ETSI EN 319 403 [25].

Supervision of the management system is carried out by the authorized audit companies, according to the ISO/IEC 9001 [43], ISO/IEC 27001 [41] and ISO/IEC 14298 [40] standards.

The internal auditors must:

- have the knowledge in the field of the PKI and information security,
- have the knowledge and understanding of the ETSI EN 319 401 [24], ETSI EN 319 411 [26] and [27] norms and other technical specifications that are referenced in this document,
- know the provisions of the CP and CPS of Procedure on Certification Procedures,
- know the legislation in the field of e-commerce, information security and data confidentiality protection, and
- have the skills necessary for the implementation of internal audits.

Internal audit is made pursuant ISO/IEC 9001 [43], ISO/IEC 27001 [41].

8.3. Assessor's/Auditor's relationship to the subject of audit

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

The internal assessment/audit within the AKD is carried out by the person appointed by the PMA.

8.4. Topics covered by assessment

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

The internal audit includes, but is not limited to:

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

8.5. Actions taken as a result of deficiency

In the event of non-compliance, the following activities are conducted:

a) The examination of the circumstances related to the non-compliance is conducted, the cause of the non-compliance is determined and corrective actions are proposed.
b) The PMA analyses the proposals and produce an operational plan to eliminate non-compliances, which include a description of activities and planned time limits.
c) Tasks related to the implementation and monitoring of the implementation of the operational plan are assigned.
d) Should a non-compliance, which significantly affects the security of the provision of trust services or prevents the fulfillment of the statutory requirements, be established, the PMA requests cessation of the provision of service.
e) The AKD undertakes all necessary actions in order to prevent the adverse impact of the cessation of the provision of service.

f) The AKD continues to provide services when the PMA establishes that the reason as to why the cessation of service occurred no longer exists.

8.6. Communication of results

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

The AKD, in accordance with legal provisions, submits a report on conformity assessment to the ministry in charge of commerce and economy, as a supervisory body.

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 point 9.1.4.

9.1.2. Certificate access fees

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

9.1.3. Revocation or status information access fees

The service for the certificate revocation is not charged.

The persons and relying parties may use the certificate's status verification services free of charge.

9.1.4. Fees for other services

Registration service of natural persons and services of producing and individualization of the card are charged through the price of the eOI.

The price of the eOI is determined by the implementing acts arising from the Identity Card Act [1].

The information and services, available through the web portal of eOI, are not charged.

9.1.5. Refund policy

There are no provisions.

9.2. Financial responsibility

9.2.1. Insurance coverage

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

The AKD has an insured liability risk for damages arising from the provision of certification services in the amount specified in point 9.2.3.

The AKD is liable for damages that are inflicted on any natural or legal person for failure to fulfill its obligations in accordance with this document and the Regulation (EU) No. 910/2014 [9].

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 fulfill obligations of the user.

The rules for the participants in the provision of certification services are regulated in accordance with the Civil Obligations Act [8].

9.2.2. Other assets

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

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

9.2.3. Insurance or warranty coverage for end-entities

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

The total value of the insurance policy amounts to HRK 2,000,000.00.

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 [5], law-based regulations or internal rules, the disclosure of which to the unauthorized person may cause harmful consequences for the participants of the certification process.

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

a) personal data and documentation collected in the registration process in accordance with the chapter 9.4,
b) databases, audit logs and archives of the service providers,
c) reports on the implementation of activities and procedures of the provision of services,
d) business communication between the participants of the certification process, and

e) other data of various types, important for the operations or interests of the participants.

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

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

9.3.2. Information not within the scope of confidential information

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

a) certificates, certificate revocation lists and information on the certificate's status,
b) information and documents, published on the web portal,
c) data whose disclosure would not undermine the Constitution and statutory rights and freedoms of natural and legal persons,
d) data that are published by the AKD on its official website or which they are required to publish in order to meet their obligations under the Freedom of Information Act [6],
e) other data whose unrestricted distribution is permitted or required for the realization of business goals.

9.3.3. Responsibility to protect confidential information

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

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

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

9.4. Privacy of personal information

9.4.1. Privacy plan

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

Persons are informed that the AKD 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 MUP take appropriate technical and organizational protection measures against unauthorized or unlawful processing and against accidental loss, destruction or damage to personal data.

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

9.4.2. Information treated as private

The MUP collects and processes personal data for the purpose of issuing identity cards.

In accordance with the Identity Card Act [1], the MUP keeps records whose content is prescribed by the Ordinance on the forms and records of identity cards [2] .

In order to meet the statutory requirements related to the implementation of the services, the personal data set forth in point 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 points 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 point 4.4.2.

The personal data that contained in the certificate are not confidential.

9.4.4. Responsibility to protect private information

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

A lawful processing of the personal data is ensured in accordance with the provisions of the Personal Data Protection Act [4] and related subordinate acts or the Directive 95/46/EC [14].

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 Agreement on certification services the persons give consent to the certification service provider for the 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 in writing for the implementation of the procedure or investigation of the irregular or illegal conduct.

9.4.7. Other information disclosure circumstances

There are no provisions.

9.5. Intellectual property rights

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

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

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

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

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

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

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

9.6. Representations and warranties

9.6.1. PMA representations and warranties

PMA is responsible for:

a) Defining, introducing and administering CP, CPS, PDS, 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 documentation with the Regulation (EU) No. 910/2014 [9] and binding national, European or international standards.
c) Monitoring of the implementation of the security requirements, which are prescribed by this document.

9.6.2. CA representations and warranties

Certification body is responsible for:

a) the implementation of the Regulation (EU) No. 910/2014 [9] and the application of the administrative and management procedures in accordance with the binding national, European or international standards.
b) the implementation of the certificate generating services, certificate revocation management, certificate's status verification as well as dissemination services in accordance with this document.
c) Timely processing of applications on the basis of complete, accurate and verified data provided by the RA.

d) Provision of personnel with the necessary expertise, reliability, experience and qualifications sufficient for the implementation of the business activities and meeting the requirements set forth in this document.
e) Provision of sufficient financial resources necessary for the provision of certification services in accordance with the requirements set forth in this document.
f) Application of organizational, operational and physical security measures to protect the CA system and data in accordance with this document.
g) Recording and long-term archiving of all relevant information in relation to the data issued and received by the CA, 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 Personal Data Protection Act [4] and Directive 95/46/EC [14].
i) Provision of the ISO/IEC 9001 [43] and ISO/IEC 27001 [41] certificates as proof of quality and security for the provision of certification services.

9.6.3. RA representations and warranties

Registration body is responsible for:

a) Collection and verification of data on natural person identities in accordance with the Identity Card Act [1].
b) Receiving applications by persons, including applications for issuing the eOI and certificates, requests for revocation and suspension of the certificates and requests to unblock the eOI and the delivery of the eOI.
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 eOI.
d) Registration of complete, accurate and verified personal identification data on natural persons and their requirements in IS, as well as forwarding for further processing to the manufacturer, i.e. CA.
e) Ensuring that registration activities are conducted solely by the reliable and conscientious PU/PP officers whose identity can be undoubtedly established and who are adequately trained before they are granted authorization.
f) Application of appropriate physical, organizational, operational and implementation security measures to protect the information systems, RA and all data.
g) Recording and long-term archiving of data and documentation 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.
h) Execution of lawful processing of personal data in accordance with the Personal Data Protection Act [4] and Directive 95/46/EC [14].

9.6.4. Subscriber representations and warranties

The person is responsible:

a) to present credible and accurate evidence in the process of identification and submission of the application,

b) to present and submit accurate and correct data in in the registration process are
c) to check that the data in the certificate are accurate and correct. that only the person which is indicated in the certificate uses the private key which matches the public key in the certificate,
d) that the certificate at the time of its use has not expired and has not been revoked,
e) that the certificate is used only for legal and authorized purposes and in accordance with their intended purpose,
f) to use and keep eOI, private keys and activation data in a responsible manner and to take appropriate security measures to prevent unauthorized access and use. that the person requests the revocation or suspension of the certificate if there is modification of personal identification data in the certificate, or if the loss, theft, misuse or unauthorized use of the private key are suspected,

9.6.5. Relying party representations and warranties

The relying parties are responsible:

a) Before using services, to enquire about the CP, CPS, PDS and conditions for providing certification services, and especially concerning their responsibilities and obligations, and the appropriate manner to use the certification services,
b) to independently assess and determine the appropriateness of the certificate use for the appropriate purpose,
c) to establish, before exercising trust in the certificate, that the certificate has not expired and that it is not revoked, all according to the data contained in the certificate,
d) that the verification of the certificate validity is carried out using an authorized source and reliable equipment,
e) to verify the certificate's status of the person and of all certificates in the certification path according to the procedures indicated in IETF RFC 5280 [35] and IETF RFC 3739 [34].

9.6.6. Representations and warranties of the manufacturer

Manufacturer is responsible for:

a) Production of the eOI whose content, form and manner of protection is prescribed by the Identity Card Act [1] and related CPS [2].
b) Data preparation and production of the eOI on the basis of the application and unmodified data provided by the RA.
c) Generating a pair of keys and activation data, obtaining the certificates from the HRIDCA and their entry in the eOI.
d) Generating data for the activation of the eOI and registration on the web portal and production of the security envelopes.
e) Application of adequate physical, organizational, operational and information security measures to protect the information system of the manufacturer and data in accordance with this document.
f) The lawful processing and protection of personal data in accordance with the Personal Data Protection Act [4] and Directive 95/46/EC [14].
g) Provision of the ISO/IEC 9001 [43], ISO/IEC 27001 [41] and ISO/IEC 14298 [40] certificates as proof of quality for the management of business and production of the security printing and security of information systems.

h) Ensuring that the eOI that meets the requirements of the EAL 4+ according to the ISO/IEC 15408 [39] and demonstrates the compliance with the forms of protection of the series EN 419 211 [17], [18], [19], [20], [21] and [22].

9.7. Disclaimers of warranties

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

The AKD is not liable for:

a) damages caused by improper use of the certificate.,
b) damages caused by the false or negligent use of the eOI, private keys, certificates 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

all damages caused intentionally or by negligence by the person or relying party that do not fulfill their obligations or fail to act in accordance with their obligations. The AKD is not responsible for the damages resulting from the provision of false information in the registration process or misrepresentation of the person during the process of identification and identity validation.

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

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

The AKD is not responsible for loss or damages that occur as a result of Force Majeure or other circumstances that AKD has no control or command of as described in Article 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, amounts up to HRK 2,000,000..

The amount of the financial responsibility for the transactions towards persons and relying parties, that uses certificates in an appropriate manner, is limited in accordance with the recommended financial limit specified in chapter 1.4 that amounts to 80'000 HRK per transaction.

9.9. Indemnities

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

The 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 eOI, 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:

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

The AKD is liable should this liability be clearly established by the agreement, CO, CPS 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 commences on the date of the publication of the document on the web portal as set forth in point 2.2.

The PMA decide upon the necessary amendments to the document as well on the publication of the document on the web portal.

9.10.2. Termination

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

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

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

9.10.3. Effect of termination and survival

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

The certificates, issued according to the rules, outlined in the earlier edition of the document continue to be in force until the expiry of the validity period of the certificate or the certificate revocation.

9.11. Individual notices and communications with participants

Informing of persons and relying parties is carried out through the web portal.

The communication with the AKD is carried out in writing or by e-mail using the contact information indicated below, in the Table 16.

Table 16: Contact information of the AKD

Contact information of the AKD:
Agencija za komercijalnu djelatnost d.o.o, Address: Savska cesta 31, 10000 Zagreb, Hrvatska web: http://akd.hr, e-mail: akd@akd.hr Portal: http://eid.hr Helpdesk: Helodesk-eOI@akd.hr Policy management authority: pma@akd.hr.

9.12. Amendments

9.12.1. Procedure for amendment

All significant changes that affect the participants are published in the new editions of the document according to the procedure set forth in point 9.12.2.

Typing errors, minor corrections or modifications that do not affect the participants are published in the versions of the documents. It is not necessary to send prior notice and/or modify the edition of the document.

The edition of the document is marked with the first number in the edition designation of the document, while versions are marked with the second number after the full stop.

Every participant may initiate the amendment to the document using the contact information indicated in point 9.11, and the PMA considers the proposal and decide whether to accept it or reject it.

Should the PMA determine that the proposed amendment is not in accordance with the legal regulations and standards or may impair the quality of the provision of service; the proposal by the participant is rejected.

9.12.2. Notification mechanism and period

The participants are informed on the new edition of the document through the web portal immediately following the publication of the document.

The participants are not informed on the new version of the document.

The accepted proposals by the participants are included in the new edition of the document.

9.12.3. Circumstances under which OID has to be changed

Minor corrections or modifications of content of CP or CPS that do not affect significantly all participants will be published without change of OID.

In case PMA defines that a change or modification of CP or CPS is a significant one, and that it may affect the participants, then a new OID that identifies an appropriate certificate or a group of certificates will be determined.

9.13. Dispute resolution provisions

All disputes and disagreements among the participants shall endeavor to resolve amicably. Should the amicable resolution of the dispute not be achieved, the disputes shall be resolved before the competent court in Zagreb with the application of the legislation of the Republic of Croatia.

9.14. Governing law

For the interpretation of the provisions of this document, provisions of the Regulation (EU) No. 910/2014 [9], 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 point 9.14.

In accordance with the Regulation (EU) No. 910/2014 [9] , the AKD is a qualified trust service provider, which had been granted a qualified status by the supervisory body, i.e a Croatian Ministry in charge of Economy.

9.16. Miscellaneous provisions

9.16.1. Agreement

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

9.16.2. Transfer of liability

N/A

9.16.3. Severability

In case a certain clause, term or condition is held to be unenforceable, the remainder of the agreement should still apply and remain in force.

In case of controversies, disputes or litigation in relation to interpretation, applicability or execution of certification services, terms and conditions stated in CP are applicable, i.e. those set forth in applicable legislature and norms.

9.16.4. Foreclosure

N/A

9.16.5. Force Majeure

AKD is not liable for any losses or damages that are the result of Force Majeure, including, but not limited to: natural disasters, extreme/harsh weather conditions, landslides, floods, fires, war, military operations, terrorism, disruptions in communication infrastructure, disruptions of power supply, restrictions, acts of coercion, or any other form of unfavorable effect of laws, civil unrest or any other circumstances that AKD has no control of.

9.17. Other provisions

N/A

ANNEX 1: Definitions

For the purposes of this document, the following terms and definitions apply:

Source Regulation (EU) br. 910/2014 [9]:

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 online 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. '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;
10. 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;
11. '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;
12. 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;
13. '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;
14. '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;
15. '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;

16. 'qualified trust service' means a trust service that meets the applicable requirements laid down in this Regulation;
17. 'conformity assessment body' means a body defined in point 13 of Article 2 of Regulation (EC) No 765/2008 [13], 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;
18. '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;
19. '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;
20. 'product' means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of trust services;
21. 'electronic signature creation device' means configured software or hardware used to create an electronic signature;
22. 'qualified electronic signature creation device' means an electronic signature creation device that meets the requirements laid down in Annex II;

Source ETSI EN 319 411-1 [26]:

23. 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
24. 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
25. Certificate Revocation List (CRL): signed list indicating a set of certificates that are no longer considered valid by the certificate issuer
26. 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.
27. Certification Practice Statement (CPS): statement of the practices which a Certification Authority employs in issuing managing, revoking, and renewing or re-keying certificates
28. Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [48]

29. 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
30. high security area: specific physical location of the security area where the Root CA key is held
31. 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.
32. registration officer: person responsible for verifying information that is necessary for certificate issuance and approval of certification requests
33. revocation officer: person responsible for operating certificate status changes [i.8]
34. root CA: certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s)
35. 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
36. 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
37. subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate
38. subordinate CA: certification authority whose Certificate is signed by the Root CA NOTE: A subordinate CA issues end user certificates.

ANNEX 2: Acronyms

The acronyms that are used in the document include:

eOI	Electronic Identity Card
MUP	Ministry of Interior
AKD	Agencija za komercijalnu djelatnost
AKDCA	Certification Authority
HRIDCA	Certification Authority for issuing certificates to natural persons for the purposes of the eOI issuance.
PKI	Public Key Infrastructure
CP	Certificate Policy
CPS	Certificate Practice Statement
QCP	Qualified Certificate Policy
PMA	Policy Management Authority
CA	Certificate Authority
RA	Registration Authority
OID	Object Identifier
PU/PP	Police Administration /Police Station
LRA	Local Registration Authority
SCD	Signature Creation Device
SSCD	Secure Signature Creation Device
QSCD	Qualified Electronic Signature Creation Device
NIAS	National Identification and Authentication System
CRL	Certificate Revocation List
CARL	Certification Authority Revocation List
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
HTTP	Hypertext Transfer Protocol
UTC	Coordinated Universal Time
RSA	Rivest, Shamir and Adleman Algorithm
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
DMZ	Demilitarized Zone

ANNEX 3: References

Acts:

[1] Identity Card Act (Official Gazette 62/2015).

[2] Ordinance on the forms and records of identity cards and the organisational, technical and security measures in the process of issuing identity cards (Official Gazette 63/2015).

[3] Ordinance on prices of identity cards (Official Gazette 62/2015).

[4] Personal Data Protection Act (Official Gazette 103/03, 118/06, 41/08, 130/11, 106/12).

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

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

[7] Electronic Signature Act (Official Gazette 10/02, 80/08, 30/14) or eIDAS Implementing Act.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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

[13] 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.

[14] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[15] CA/ Browser Forum NetSec: „Network and certificate system security requirements".

[16] CA/Browser Forum BRG (V1.3.0): "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

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

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

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

[20] 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“.

[21] 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“.

[22] 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“.

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

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

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

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

[27] 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“.

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

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

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

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

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

[33] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[34] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

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

[36] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[37] IETF RFC 5019: "The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments“.

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

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

[40] ISO 14298: "Graphic technology - Management of security printing processes".

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

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

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

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

[45] ITU-T X.509 Recommendation: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

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

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

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

[49] CEN/TS 15480: „Identification Card Systems – European Citizen card"