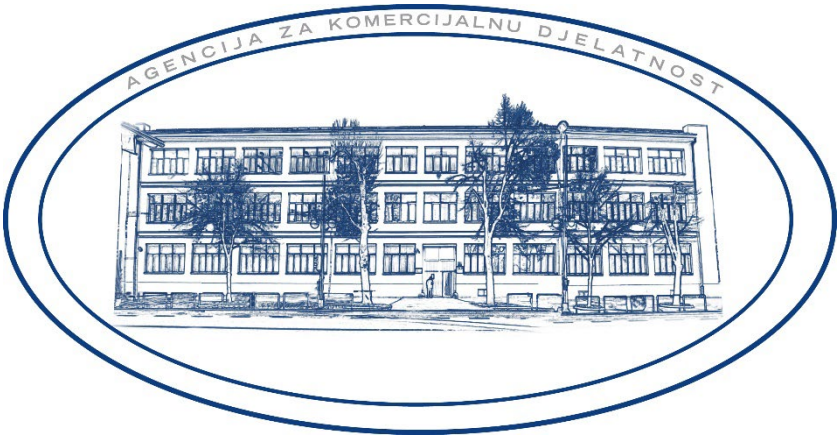


CERTILIA
PRAVILNIK O POSTUPCIMA CERTIFICIRANJA

Izdanje 1.1

Vrijedi od 14.06.2025.

1 Uvod

1.1 Pregled dokumenta

U AKD-u je uspostavljeno krovno certifikacijsko tijelo AKDCA Root koje izdaje certifikat samom sebi te podređenim certifikacijskim tijelima.

CERTILIA je podređeno certifikacijsko tijelo koje izdaje certifikate fizičkim i pravnim osobama te certifikate za potrebe pružanja AKD usluge izdavanja kvalificiranog vremenskog žiga i OCSP usluge.

CERTILIA izdaje i kvalificirane certifikate koji se koriste isključivo u CERTILIA mPotpis servisu za udaljeno elektroničko potpisivanje i udaljeno elektroničko pečatiranje a koji su povezani s privatnim ključevima u udaljenom QSCD uređaju kojima upravlja AKD u ime potpisnika ili autora pečata.

Ovaj dokument, *„CERTILIA Pravilnik o postupcima certificiranja" (dalje u tekstu Pravilnik ili CPS ili CERTILIA CPS),* strukturom i sadržajem odgovara dokumentu *„Certification Practice Statement*", sukladno IETF RFC 3647 [36]. Pravilnik je usklađen sa dokumentom AKD PKI Opća pravila pružanja usluga certificiranja [53] *(dalje u tekstu Opća pravila ili CP)*.

Pravilnik specificira organizacijske i tehničke mjere koje AKD u praksi primjenjuje prilikom utvrđivanja identiteta osoba te izdavanja i upravljanja životnim ciklusom certifikata na QSCD uređaju.

Također, Pravilnik sadrži organizacijske i tehničke mjere koje AKD u praksi primjenjuje prilikom utvrđivanja identiteta osoba i izdavanja i upravljanja životnim ciklusom certifikata i privatnih ključeva i upravljanja sredstvima elektroničke identifikacije (*eID means*) koji se koriste u CERTILIA mPotpis servisu a koji upravlja udaljenim QSCD uređajem i privatnim ključevima za kreiranje kvalificiranog elektroničkog potpisa u ime potpisnika odnosno kvalificiranog elektroničkog pečata u ime autora pečata (*Trustworthy system supporting server signing –TW4S*) te sadrži odredbe dokumenta *„SSASC practice statement", sukladno* ETSI TS 119 431-1 [23] odnosno CEN EN 419 241-1 [32].

Tehnički profili i specifikacije u punom opsegu mogu biti dodatno opisani i u zasebnim internim dokumentima.

Dokument je dostupan tijelima za ocjenjivanje sukladnosti i nadzornim tijelima te služi kao osnova za procjenu sposobnosti AKD-a da pruža kvalificirane usluge povjerenja i da s pravom nosi status kvalificiranog pružatelja usluge.

Pojmovi koji se koriste u ovome dokumentu, a koji su navedeni u Prilogu 1 ovoga dokumenta, preuzeti su iz *Uredbe (EU) br. 910/2014[1], koju je izmijenila Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. i Uredba (EU) 2024/1183 Europskog parlamenta i Vijeća od 11. travnja 2024. koju je ispravio Ispravak Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014* i obvezujućih normi.

Sigurnosni zahtjevi definirani u ovome dokumentu te primijenjeni u praksi, usklađeni su sa zahtjevima za kvalificirane pružatelje usluga povjerenja i kvalificirane usluge povjerenja koje oni pružaju, a koji su propisani *Uredbom (EU) br. 910/2014[1].*

Pružanje usluge izdavanja kvalificiranog vremenskog žiga nije u opsegu certificiranja predviđenog ovim dokumentom te su pravila i postupci pružanja usluge izdavanja vremenskog

žiga detaljno opisani u AKD QTSA Pravila i postupci pružanja usluga vremenskog žiga *(dalje u tekstu: TSP/PS)* [54].

U slučaju proturječnosti, primjenjuju se odredbe sadržane u dokumentima, slijedećim redoslijedom (od značajnijeg):

1) ETSI Politike: QCP-n-qscd, NCP+, QCP-l-qscd
2) CP certifikacijskog tijela,
3) Ovaj CPS.

1.2 Naziv dokumenta i identifikacija

1.2.1 Naziv dokumenta

Oznaka :	PRO-IV-302-00
Naziv:	CERTILIA Pravilnik o postupcima certificiranja, za javnu objavu
Izdanje:	1.1
Datum objave:	01.06.2025.
Datum stupanja na snagu:	14.06.2025.
Autor:	AKD d.o.o
Tip dokumenta:	Certificate Practice Statement
Dostupnost:	https://www.certilia.com

Povijest promjena dokumenta je navedena u prilogu 4 ovog dokumenta.

1.2.2 Identifikacijska oznaka

Identifikacijska oznaka (OID) rezerviran od strane AKD je 1.3.6.1.4.1.43999, te interno dodijeljeno za PKI 5.

U sljedećoj tablici su navedene identifikacijske oznake pravila po kojim se izdaju certifikati.

Tablica 1: Identifikacijska oznaka

CERTILIA Osobni certifikati		
Naziv	Oznaka	OID
Osobni potpisni certifikat CERTILIA1	CERTILIA QCP-n-qscd-ksign	1.3.6.1.4.1.43999.5.14.2.1.2.1
Osobni identifikacijski certifikat CERTILIA2	CERTILIA NCP+ kident	1.3.6.1.4.1.43999.5.15.2.1.2.2
Osobni certifikat za udaljeni potpis CERTILIA3	CERTILIA QCP-n-qscd-krsign	1.3.6.1.4.1.43999.5.14.6.1.2.1
CERTILIA certifikati za elektronički pečat		
Naziv	Oznaka	OID
Certifikat za elektronički pečat	CERTILIA QCP-l-qscd-kseal	1.3.6.1.4.1.43999.5.14.2.2.3.4
Certifikat za udaljeni elektronički pečat	CERTILIA QCP-l-qscd-krseal	1.3.6.1.4.1.43999.5.14.6.2.3.4

CERTILIA certifikati za AKD TSA		
Naziv	Oznaka	OID
CERTILIA TSU certifikat	CERTILIA QCP-l-scd-tsa	1.3.6.1.4.1.43999.5.14.1.2.2.8

Prema poglavlju 5.3 ETSI EN 319 411-2 [16], pravila po kojima se izdaju osobni potpisni certifikati CERTILIA1 i CERTILIA3 ekvivalentna su pravilima **QCP-n-qscd** čija je identifikacijska oznaka:

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

Prema poglavlju 5.3 ETSI EN 319 411-1 [15], pravila po kojima se izdaju osobni identifikacijski certifikati CERTILIA2 ekvivalentna su pravilima **NCP+** čija je identifikacijska oznaka:

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

Prema poglavlju 5.3 ETSI EN 319 411-2 [16] pravila po kojima se izdaju certifikati za elektronički pečat ekvivalentna su pravilima **QCP-l-qscd** čija je identifikacijska oznaka:

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

Prema poglavlju 5.2, Anex A.2, ETSI TS 119 431-1 [23] pravila po kojima AKD implementira i upravlja okružjem CERTILIA mPotpis sa udaljenim QSCD uređajem za kreiranje udaljenog elektroničkog potpisa u ime potpisnika ili udaljenog elektroničkog pečata u ime autora pečata (CERTILIA mPotpis servis) ekvivalentna su pravilima **EUSCP: EU SSASC Policy** čija je identifikacijska oznaka:

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

1.3 PKI Sudionici

U kontekstu ovoga dokumenta, sudionici AKD PKI su:

a) Certifikacijsko tijelo (engl. *Certification Authority – CA*),
b) Pružatelj servisa za serversko potpisivanje *(engl. Server Signing Application Service Provider - SSASP)*
c) Povjerenstvo za upravljanje pravilima certificiranja (engl. *Policy Management Authority – PMA),*
d) Registracijsko tijelo (engl. *Registration Authority –RA*),
e) Osobe,
f) Pouzdajuće strane (engl. *Relying party*) i
g) Ostali

Obveze i odgovornosti svih sudionika AKD PKI su navedene u poglavlju 9.6.

1.3.1 Certifikacijsko tijelo - CA

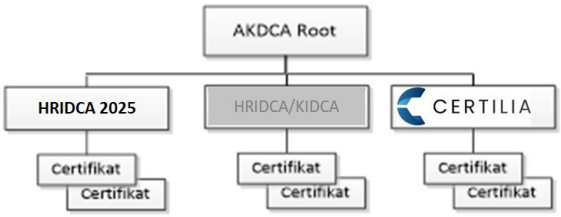
Certifikacijsko tijelo *(u daljnjem tekstu: pružatelj usluga certificiranja ili CA)* je tijelo uspostavljeno u AKD-u, koje je autorizirano od PMA da izdaje certifikate u skladu s Općim pravilima [53] i ovim Pravilnikom.

CA pruža sljedeće usluge povjerenja:

a) **Usluga generiranja certifikata**: kreira i potpisuje certifikate temeljem podataka prikupljenih kroz uslugu registracije.
b) **Usluga upravljanja opozivom certifikata**: provodi opoziv certifikata i osigurava podatke o statusu certifikata.
c) **Usluga provjere statusa certifikata**: informira pouzdajuće strane o statusu certifikata i omogućava im provjeru kroz CRL ili OCSP.
d) **Usluga informiranja**: informira osobe i pouzdajuće strane o pravilima i uvjetima certificiranja te ostalim informacijama vezanim uz certifikate i usluge certificiranja.

PKI infrastruktura uspostavljena od strane AKD PKI uređena je hijerarhijski tako da se sastoji od krovnog CA (AKDCA Root) koji izdaje certifikat samom sebi te podređenim CA koji izdaje certifikate osobama.

Slika 1: Hijerarhijski model



CERTILIA izdaje certifikate fizičkim i pravnim osobama za potrebe izdavanja certifikata na QSCD.

CERTILIA izdaje certifikate fizičkim i pravnim osobama koji se koriste u sklopu servisa CERTILIA mPotpis za udaljeni elektronički potpis i udaljeni elektronički pečat a kojima AKD upravlja u ime osoba.

1.3.2 Pružatelj servisa za serversko potpisivanje - SSASP

AKD upravlja okružjem CERTILIA mPotpis za izradu elektroničkog udaljenog potpisa i udaljenog elektroničkog pečata. Certifikate koji se koriste u okružju servisa za udaljeno potpisivanje i pečatiranje izdaje CERTILIA.

Okružje CERTILIA mPotpis omogućuje:

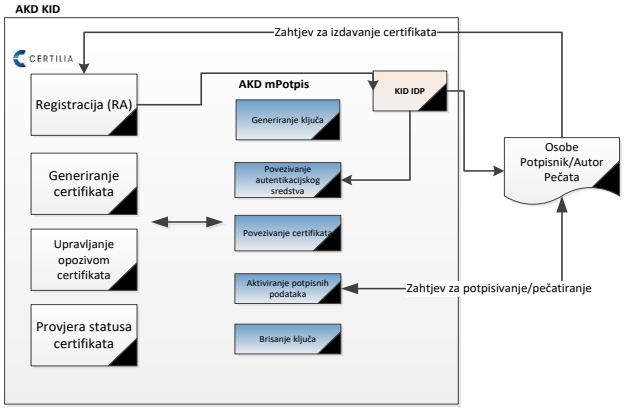
a) **Generiranje privatnog ključa** *(engl. signing key generation service)* – generira privatne ključeve za potpis u udaljenom QSCD uređaju i prosljeđuje u CERTILIA RA dokaz o provedenom uručenju osobi.
b) **Povezivanje certifikata sa privatnim ključem** *(engl. certificate linking service)* – povezuje privatni ključ sa pripadajućim certifikatom izdanim od strane CERTILIA.
c) **Povezivanje autentikacijskog sredstva sa privatnim ključem** *(engl. eID means linking service)*– povezuje autentikacijski mehanizam sa privatnim ključem u svrhu pružanja osobi kontrole nad podacima za kreiranje udaljenog elektroničkog potpisa/pečata.

d) **Aktiviranje podataka za kreiranje potpisa** *(engl. signature activation service)* – verificira podatke za aktivaciju potpisnih podataka i aktivira pripadajući privatni ključ za potpisivanje u svrhu kreiranja udaljenog elektroničkog potpisa.

e) **Brisanje privatnog ključa** (*engl. signing key deletion service*) – trajno osiguravanje nemogućnosti korištenja potpisnog ključa.

f) **Dostupnost autentikacijskih sredstava** *(engl. eID means provision service)* – omogućuje osobama korištenje dozvoljenih autentikacijskih sredstava za pristup CERTILIA mPotpis servisu. AKD omogućuje osobama korištenje dvofaktorskih autentifikacijskih sredstava i mehanizama za pristup CERTILIA mPotpis servisu registriranih u AKD IDP odnosno CERTILIA IDP sustavu.

Slika 1a: CERTILIA mPotpis okružje(SSASC)



1.3.3 Povjerenstvo za upravljanje pravilima certificiranja – PMA

AKD je pružatelj usluga povjerenja kojem vjeruju osobe i pouzdajuće strane te snosi cjelokupnu odgovornost za sve usluge povjerenja, bez obzira pruža li ih samostalno ili u suradnji s trećim stranama.

Povjerenstvo za upravljanje pravilima certificiranja *(u daljnjem tekstu: povjerenstvo ili PMA)* upravlja pružanjem usluga povjerenja i radom AKD PKI u cjelini te propisuje i nadzire provedbu sigurnosnih zahtjeva koji su propisni ovim dokumentom.

PMA je odgovoran za definiranje, uvođenje i administriranje Općih pravila [53], ovog Pravilnika, sigurnosno operativnih procedura i provedbenih dokumenata vezanih uz AKD PKI i pružanje usluga povjerenja.

PMA se sastoji od više članova koji posjeduju specijalistička znanja vezana uz kriptografiju i informacijsku sigurnost kao i uz regulatorne, poslovne, pravne, formalne i tehničke aspekte pružanja usluga certificiranja.

Kako bi se osigurala provedba općih pravila i pravilnika u okolnostima kada se usluga povjerenja realizira u suradnji s trećim stranama, PMA je odgovorno za definiranje odredbi u sporazumima koji će se sklopiti s trećim stranama.

1.3.4 Registracijsko tijelo - RA

Agencija za komercijalnu djelatnost osigurava ulogu Registracijskog tijela.

AKD može realizirati ulogu registracijskog tijela *(u daljnjem tekstu: pružatelj usluga registracije ili RA)* koji provjerava identitete i identifikacijske podatke fizičkih osoba temeljem kojih CERTILIA izdaje, obnavlja, opoziva i suspendira certifikate:

a) samostalno,
b) ugovaranjem sa drugom pravnom ili fizičkom osobom.

Poslovi RA su:

a) informiranje osoba o postupcima registracije i izdavanja certifikata,
b) zaprimanje zahtjeva za izdavanje, opoziv i suspenziju certifikata,
c) utvrđivanje identiteta osoba i podnositelja zahtjeva,
d) omogućavanje prihvaćanja Uvjeta pružanja usluga certificiranja,
e) uručivanje certifikata na QSCD u posjed i
f) poslovi izdavanja i povezivanja autentifikacijskih sredstava za pristup CERTILIA mPotpis servisu za kreiranje udaljenog elektroničkog potpisa i pečata.

AKD pruža poslove RA putem vlastitog RA ureda sa mogućnošću izlaska na lokaciju naručitelja (mobilni RA ured) te putem on-line usluga.

AKD osigurava informacijski sustav za obavljanje registracijskih poslova - AKD RA. Pristup AKD RA sustavu imaju ovlaštene osobe – zaposlenici AKD-a ili podugovorenog RA ureda. Sve osobe koje pristupaju AKD RA sustavu su educirane za obavljanje registracijskih poslova i rad u AKD RA aplikaciji a pristupaju isključivo identifikacijskim certifikatom izdanim sa CERTILIA sustava.

U slučaju ugovaranja sa drugom pravnom ili fizičkom osobom AKD će ugovorom osigurati provedbu sigurnosnih pravila i postupaka koji su opisani u ovome dokumentu, posebno u poglavlju 3 te točkama 5.3 i 5.5.2.

1.3.5 Osobe

Osobe subjekti certificiranja

Osobe subjekti certificiranja (engl. Subject) su fizičke osobe čije je ime i prezime navedeno u subjektu certifikata u poljima Common name, givenName i surname, odnosno osobni identifikacijski broj sadržan u polju serialNumber, te kojima je izdan i uručen certifikat na QSCD uređaju i/ili registracijski kodovi za registraciju certifikata i postavljanje aktivacijskih podataka koji se koriste u sklopu servisa CERTILIA mPotpis za udaljeni elektronički potpis ili udaljeni elektronički pečat i koje su vlastoručnim potpisom prihvatile primjenjive AKD-ove uvjete pružanja usluga certificiranja za fizičke i/ili pravne osobe ili organizacije.

Osobe naručitelji

Osobe naručitelji (engl. Subscriber) su fizičke ili pravne osobe koje su podnijele zahtjev za izdavanje certifikata, te su ujedno i vlasnici certifikata. Ukoliko se osoba koja je subjekt certificiranja i osoba naručitelj razlikuju, a naručitelj je organizacija i ispunjeni su zahtjevi iz 3.2.3.1. f) i g.), tada naziv i osobni identifikacijski broj organizacije mogu biti upisani u organizationName i organizationIdentifier atributima u subjektu certifikata.

Autor pečata

Autor pečata je pravna osoba koja izrađuje elektronički pečat i čiji podaci su navedeni u subjektu certifikatu u poljima organizationName i organizationIdentifier te sa nazivom certifikata pečata kojim se pravna osoba predstavlja upisanim u polje CommonName.

Ovlašteni predstavnik

Osoba ovlaštena za zastupanje autora pečata ili treća osoba sa punomoći osobe ovlaštene za zastupanje. Ovlaštenom predstavniku uručuju se izdani certifikati na QSCD i/ili registracijski kodovi za registraciju certifikata i postavljanje aktivacijskih podataka koji se koriste u sklopu servisa CERTILIA mPotpis za udaljeni elektronički pečat te on/ona u ime autora pečata prihvaća primjenjive AKD-ove uvjete pružanja usluga certificiranja za pravne osobe.

Certifikat je moguće zatražiti za sve osobe za koje je moguće provesti postupak identifikacije jednakovrijedan fizičkom i dokazati identitet. Certifikat je moguće zatražiti putem Registracijskog tijela (RA) koristeći RA urede, RA mobilne urede ili dostupne on-line usluge.

Identitet osoba se dokazuje ispravom koja može služiti kao dokaz identiteta (osobna iskaznica ili putovnica), prema uređujućim zakonima i izdanom od nadležnog tijela u RH ili EU.

Drugi identifikacijski dokumenti na stranim jezicima (osim osobne iskaznice ili putovnice) prihvaćaju se uz službene dokumente i potvrde izdane od strane javnopravnih tijela RH (npr. OIB potvrda) a u čijem je postupku izdavanja obavljena fizička identifikacija osobe. U slučaju da osoba nema prethodno izdane dokumente i potvrde od strane javnopravnih tijela RH, prihvaća se identifikacijski dokument (osim osobne iskaznice ili putovnice) isključivo u prijevodu na hrvatski jezik, ovjeren od strane sudskog tumača u RH.

U sklopu on-line usluge za podnošenje zahtjeva za izdavanje certifikata, identitet osoba dokazuje se autentikacijom na elektroničku uslugu sredstvom elektroničke identifikacije visoke razine sigurnosti notificiranog na EU ili nacionalnoj razini i/li upotrebom kvalificiranog elektroničkog potpisa izdanog od strane kvalificiranog EU izdavatelja. AKD prihvaća identifikaciju sredstvima koje sadrže identifikacijski certifikat izdan sa KIDCA, CERTILIA ili HRIDCA sustava.

Zahtjev predan on-line uslugom ili zaprimljen elektroničkim putem mora biti elektronički potpisan kvalificiranim potpisnim certifikatom.

Certifikati se izdaju po sljedećim pravilima:

a) Fizičkim osobama do 18 godina izdati se može isključivo identifikacijski certifikat.
b) Punoljetnim fizičkim osobama i fizičkim osobama povezanim s organizacijom, starijim od 18 godina, može se izdati identifikacijski i potpisni certifikat.
c) Pravnim osobama izdaju se certifikati za elektronički pečat.

Certifikati se osobama uručuju na QSCD uređaju ili na infrastrukturi pružatelja usluge koji upravlja podacima u ime potpisnika ili autora pečata odnosno na udaljenom QCSD uređaju u sklopu servisa za udaljeni elektronički potpis i udaljeni elektronički pečat - CERTILIA mPotpis.

1.3.6 Pouzdajuće strane

Pouzdajuće strane (engl. *Relying party*) su fizičke ili pravne osobe koje pružaju elektroničke usluge i koje djeluju temeljem razumnog pouzdanja u certifikat i pružatelja usluga povjerenja.

Certifikat omogućuje pouzdajućoj strani povezivanje javnog ključa i elektroničkog potpisa s korisnikom, odnosno provjeru identiteta korisnika i validaciju elektroničkog potpisa.

1.3.7 Ostali

Ostali sudionici su pravne ili fizičke osobe koje ne pružaju ili ne koriste usluge certificiranja, ali sudjeluju u različitim procesima koji utječu ili mogu utjecati na same usluge povjerenja.

AKD prepoznaje uloge i odgovornosti proizvođača i distributera HSM uređaja, pružatelja softverskih rješenja i hardverske opreme, te davatelja različitih usluga povezanih sa PKI.

QSCD uređaj koji kvalificirani pružatelj usluge koristi u okružju za upravljanje podacima za kreiranje udaljenog elektroničkog potpisa/pečata (CERTILIA mPotpis servis) u ime osobe subjekta certificiranja ili autora pečata je HSM uređaj koji isporučuje proizvođač i distributer HSM uređaja.

Udaljeni QSCD uređaj je sukladan zahtjevima ISO/IEC 15408 [43] *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5* i prema pravilima definiranim u Prilogu II *Uredbe (EU) br. 910/2014 [1]*.

Proizvođač koji proizvodi i pruža usluge opskrbe QSCD uređajima namijenjenima za uručenje u posjed osobama je AKD.

QSCD uređaj je sukladan ISO/IEC 15408 [43] *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5, ALC_DVS.2* i prema pravilima definiranim u Prilogu II *Uredbe (EU) br. 910/2014 [1]*.

U skladu s općim pravilima i pravilnikom, proizvođač obavlja sljedeće poslove:

a) pripremu i proizvodnju sigurnih QSCD za osobe,
b) generiranje parova kriptografskih ključeva osoba te njihov unos u QSCD,
c) distribuciju QSCD osobama direktno ili putem RA te
d) osigurava da je QSCD kvalificirano sredstvo za izradu elektroničkog potpisa/pečata (engl. *Qualified Electronic Signature Creation Device – QSCD*) sukladno CC EAL4+.

1.4 Uporaba certifikata

Svi PKI Sudionici u AKD PKI su cijelo vrijeme obvezni koristiti certifikate sukladno AKD PKI Općim pravilima pružanja usluga certificiranja (CP) [53], Pravilnicima o postupcima certificiranja (CPS), uvjetima pružanja usluga te svim nadležnim zakonima i uredbama.

1.4.1 Primjerene uporabe certifikata

1.4.1.1 CERTILIA NCP+ kident Osobni identifikacijski certifikat (1.3.6.1.4.1.43999.5.15.2.1.2.2)

Osobe i pouzdajuće strane trebaju biti svjesne pravila uporabe osobnog identifikacijskog certifikata:

a) Visoka razina sigurnosti koja se može pripisati osobnom identifikacijskom certifikatu utemeljena je kriterijima koji su propisani u Provedbenoj odluci komisije (EU) 2015/1502 [5] što znači:
   - da pruža visoku razinu osiguranja identiteta fizičke osobe,
   - da osigurava zaštitu od kopiranja i neovlaštene izmjene od napadača s visokim napadačkim potencijalom,
   - da ga osoba u čijem je vlasništvu može pouzdano zaštititi od uporabe od strane drugih osoba,
   - da je isporučen samo u posjed osobe koja je subjekt certificiranja,
   - da posjeduje visoko pouzdan mehanizam autentikacije i
   - da ga izdaje pružatelj usluga koji ima uspostavljenu učinkovitu praksu upravljanja informacijskom sigurnošću.

b) Osobni identifikacijski certifikat izdaje se na kvalificiranom sredstvu za izradu elektroničkog potpisa (QSCD) koje ispunjava zahtjeve utvrđene u Prilogu II *Uredbe (EU) br. 910/2014* [1] i kako je propisano Provedbenom odlukom komisije (EU) 2019/650 [6].

c) U osobnom identifikacijskom certifikatu je imenovana fizička osoba, subjekt certificiranja, koja ga treba koristiti u privatne svrhe, ali i za poslovnu uporabu.

d) Identifikacijski certifikat se koristi za autentikaciju osobe na elektroničke usluge.

e) Ukoliko postoji povezanost između fizičke osobe i organizacije, podaci o organizaciji će biti upisani u „Subject“ polju certifikata pod atributima *organizationName* i *organizationIdentifier*

Osobni identifikacijski certifikat prikladan je za autentikaciju na CERTILIA mPotpis servis za udaljeno elektroničko potpisivanje i pečatiranje.

1.4.1.2 CERTILIA QCP-n-qscd-ksign Osobni potpisni certifikat (1.3.6.1.4.1.43999.5.14.2.1.2.1)

Osobe i pouzdajuće strane trebaju biti svjesne pravila uporabe osobnog potpisnog certifikata:

a) Osobni potpisni certifikat je kvalificirani certifikat za elektronički potpis koji ispunjava zahtjeve utvrđene u Prilogu I *Uredbe (EU) br. 910/2014 [1]*.

b) Izdavatelj osobnog potpisnog certifikata je kvalificirani pružatelj usluga povjerenja kojemu je nadzorno tijelo odobrilo kvalificirani status.

c) Ovlašteno tijelo za ocjenjivanje sukladnosti iz čl. 2 stavka 13 Uredbe (EZ) br. 765/2008 [9] obavlja ocjenjivanje sukladnosti pružatelja kvalificiranih usluga povjerenja kako bi potvrdilo da su ispunjeni zahtjevi *Uredbe (EU) br. 910/2014 [1]*.

d) Osobni potpisni certifikat izdaje se na kvalificiranom sredstvu za izradu elektroničkog potpisa (QSCD) koje ispunjava zahtjeve utvrđene u Prilogu II *Uredbe (EU) br. 910/2014 [1]* i kako je propisano Provedbenom odlukom komisije (EU) 2019/650 [6].

e) U osobnom potpisnom certifikatu je imenovana fizička osoba, subjekt certificiranja, koja ga treba koristiti u privatne svrhe, ali i za poslovnu uporabu. Osobni potpisni

certifikat služi kao podrška pri izradi kvalificiranog elektroničkog potpisa kako je specificirano u čl. 3 točka 12 *Uredbe (EU) br. 910/2014 [1]*.

f) Ukoliko postoji povezanost između fizičke osobe i organizacije, podaci o organizaciji će biti upisani u „Subject“ polju certifikata pod atributima *organizationName* i *organizationIdentifier*

g) Ako nije posebnim ugovorom ili na drugi način određeno, ukupna odgovornost AKD-a prema osobama i pouzdajućim stranama koje se razumno pouzdaju u certifikat ograničena je iznosom police osiguranja sukladno poglavlju 9.8.

1.4.1.3 CERTILIA QCP-n-qscd-krsign Osobni certifikat za udaljeni elektronički potpis (1.3.6.1.4.1.43999.5.14.6.1.2.1)

Osobe i pouzdajuće strane trebaju biti svjesne pravila uporabe osobnog certifikata namijenjenog za udaljeni elektronički potpis:

a) Certifikat za udaljeni potpis je kvalificirani certifikat za elektronički potpis koji ispunjava zahtjeve utvrđene u Prilogu I *Uredbe (EU) br. 910/2014 [1]*.

b) Izdavatelj certifikata za udaljeni potpis je kvalificirani pružatelj usluga povjerenja kojemu je nadzorno tijelo odobrilo kvalificirani status.

c) Ovlašteno tijelo za ocjenjivanje sukladnosti iz čl. 2 stavka 13 Uredbe (EZ) br. 765/2008 [9] obavlja ocjenjivanje sukladnosti pružatelja kvalificiranih usluga povjerenja kako bi potvrdilo da su ispunjeni zahtjevi *Uredbe (EU) br. 910/2014 [1]*.

d) Certifikat za udaljeni potpis izdaje se sa CERTILIA sustava u sklopu CERTILIA mPotpis na udaljeno kvalificirano sredstvo za izradu elektroničkog potpisa koje ispunjava zahtjeve utvrđene u Prilogu II Uredbe (EU) br. 910/2014 [1] i kako je propisano Provedbenom odlukom komisije (EU) 2016/650 [6]. Udaljeni QSCD uređaj je sukladan Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented by AVA_VAN.5.

e) U certifikatu je imenovana fizička osoba, subjekt certificiranja, koja ga treba koristiti u privatne svrhe, ali i za poslovnu uporabu. Certifikat služi kao podrška pri izradi kvalificiranog elektroničkog potpisa kako je specificirano u čl. 3 točka 12 *Uredbe (EU) br. 910/2014 [1]*.

f) Ukoliko postoji povezanost između fizičke osobe i organizacije, podaci o organizaciji će biti upisani u „Subject“ polju certifikata pod atributima organizationName i organizationIdentifier

g) Ako nije posebnim ugovorom ili na drugi način određeno, ukupna odgovornost AKD-a prema osobama i pouzdajućim stranama koje se razumno pouzdaju u certifikat ograničena je iznosom police osiguranja sukladno poglavlju 9.8.

1.4.1.4 CERTILIA QCP-l-qscd-kseal Certifikat za elektronički pečat (1.3.6.1.4.1.43999.5.14.2.2.3.4)

Osobe i pouzdajuće strane trebaju biti svjesne pravila uporabe certifikata za elektronički pečat:

a) Certifikat za elektronički pečat je kvalificirani certifikat za elektronički pečat koji ispunjava zahtjeve utvrđene u Prilogu I *Uredbe (EU) br. 910/2014 [1]*.

b) Izdavatelj certifikata za elektronički pečat je kvalificirani pružatelj usluga povjerenja kojemu je nadzorno tijelo odobrilo kvalificirani status.

c) Ovlašteno tijelo za ocjenjivanje sukladnosti iz čl. 2 stavka 13 Uredbe (EZ) br. 765/2008 [9] obavlja ocjenjivanje sukladnosti pružatelja kvalificiranih usluga povjerenja kako bi potvrdilo da su ispunjeni zahtjevi *Uredbe (EU) br. 910/2014 [1]*.

d) Certifikat za elektronički pečat izdaje se na kvalificiranom sredstvu za izradu elektroničkog potpisa (QSCD) koje ispunjava zahtjeve utvrđene u Prilogu II *Uredbe (EU) br. 910/2014 [1]* i kako je propisano Provedbenom odlukom komisije (EU) 2016/650 [6].

e) U certifikatu za elektronički pečat je imenovana pravna osoba, autor pečata, koja ga treba koristiti za poslovnu uporabu. Certifikat služi kao podrška pri izradi kvalificiranog elektroničkog pečata kako je specificirano u čl. 3 točka 27 *Uredbe (EU) br. 910/2014 [1]*.

f) Ako nije posebnim ugovorom ili na drugi način određeno, ukupna odgovornost AKD-a prema osobama i pouzdajućim stranama koje se razumno pouzdaju u certifikat ograničena je iznosom police osiguranja sukladno poglavlju 9.8.

1.4.1.5 CERTILIA QCP-l-qscd-krseal Certifikat za udaljeni elektronički pečat (1.3.6.1.4.1.43999.5.14.6.2.3.4)

Osobe i pouzdajuće strane trebaju biti svjesne pravila uporabe certifikata za udaljeni elektronički pečat:

a) Certifikat za udaljeni elektronički pečat je kvalificirani certifikat za elektronički pečat koji ispunjava zahtjeve utvrđene u Prilogu I *Uredbe (EU) br. 910/2014 [1]*.

b) Izdavatelj certifikata za udaljeni elektronički pečat je kvalificirani pružatelj usluga povjerenja kojemu je nadzorno tijelo odobrilo kvalificirani status.

c) Ovlašteno tijelo za ocjenjivanje sukladnosti iz čl. 2 stavka 13 Uredbe (EZ) br. 765/2008 [9] obavlja ocjenjivanje sukladnosti pružatelja kvalificiranih usluga povjerenja kako bi potvrdilo da su ispunjeni zahtjevi *Uredbe (EU) br. 910/2014 [1]*.

d) Certifikat za udaljeni elektronički pečat izdaje se sa CERTILIA sustava u sklopu CERTILIA mPotpis servisa na udaljeno kvalificirano sredstvo za izradu elektroničkog pečata koje ispunjava zahtjeve utvrđene u Prilogu II *Uredbe (EU) br. 910/2014 [1]* i kako je propisano Provedbenom odlukom komisije (EU) 2016/650 [6]. QSCD uređaj je sukladan *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented by AVA_VAN.5*.

e) U certifikatu za udaljeni elektronički pečat je imenovana pravna osoba, autor pečata, koja ga treba koristiti za poslovnu uporabu. Certifikat služi kao podrška pri izradi kvalificiranog elektroničkog pečata kako je specificirano u čl. 3 točka 27 *Uredbe (EU) br. 910/2014 [1]*.

f) Ako nije posebnim ugovorom ili na drugi način određeno, ukupna odgovornost AKD-a prema osobama i pouzdajućim stranama koje se razumno pouzdaju u certifikat ograničena je iznosom police osiguranja sukladno poglavlju 9.8

1.4.2 Zabranjene uporabe certifikata

Svaka uporaba certifikata, osim onih koje su navedene u točki 1.4.1, je zabranjena.

Osobe i pouzdajuće strane trebaju biti svjesne ograničenja koja su vezana uz korištenje certifikata:

a) Certifikati nisu namijenjeni za šifriranje podataka.

b) Kada se osobni identifikacijski certifikat koristi za podršku elektroničkom potpisu takav se potpis neće se smatrati kvalificiranim elektroničkim potpisom.
c) Kvalificirani potpisni certifikat se ne može koristiti za bilo koju drugu namjenu osim za podršku elektroničkom potpisu odnosno kvalificiranom elektroničkom potpisu.
d) Kvalificirani certifikat za elektronički pečat se ne može koristiti za bilo koju drugu namjenu osim za podršku elektroničkom pečatu odnosno kvalificiranom elektroničkom pečatu.

1.5 Administracija dokumenta

1.5.1 Organizacija odgovorna za održavanje dokumenta

Za izradu i administraciju dokumenta odgovoran je PMA koji djeluje u sklopu AKD-a.

1.5.2 Kontakt podaci

Poštanska adresa:

AKD d.o.o
Povjerenstvo za upravljanje pravilima certificiranja (PMA)
Savska cesta 31
10000 Zagreb
Hrvatska
e-mail: pma@akd.hr
web: https://www.certilia.com

1.5.3 Ocjenjivanje usklađenosti dokumenta

PMA je odgovoran za ocjenjivanje usklađenosti dokumenta s:

- nacionalnom i EU regulativom vezanom uz elektroničku identifikaciju i usluge povjerenja,
- tehničkim specifikacijama, normama i postupcima vezanim uz elektroničku identifikaciju i usluge povjerenja i
- internim sigurnosnim pravilima i operativnim postupcima vezanim uz provedbu aktivnosti i djelovanje pružatelja usluga certificiranja.

Ukoliko se utvrdi potreba za izmjenom dokumenta, PMA će pokrenuti postupak usklađivanja dokumentacije i odrediti početak primjena novih operativnih postupaka ili pravila pružanja usluga.

1.5.4 Postupak odobravanja dokumenta

Prije izdavanja općih pravila i pravilnika te početka njihove primjene, kao i nakon svake izmjene koja utječe na PKI sudionike, PMA daje suglasnost za prihvaćanje i objavljivanje dokumenta.

Glavni direktor odobrava objavu općih pravila i pravilnika.

1.6 Definicije i kratice

Definicije pojmova i kratice koji se koriste u ovome dokumentu, a koji su navedeni u prilogu 1 i prilogu 2 ovoga dokumenta, usklađeni su s *Uredbom (EU) br. 910/2014 [1]*, ETSI EN 319 411-1 [15], ETSI EN 319 411-2 [16] i ostalim obvezujućim normama i dokumentima.

2 Repozitorij i objavljivanje informacija

2.1 Repozitorij

AKD pruža usluge provjere statusa certifikata te javnosti stavlja na raspolaganje sve informacije koje su potrebne za provjeru statusa certifikata (Tablica 2).

Tablica 2: Podaci o repozitoriju

Informacije	AKDCA Root	CERTILIA
CRL: HTTP protokol	http://crl1.eid.hr/akdcaroot.crl http://crl2.eid.hr/akdcaroot.crl	https://crl.certilia.com/certilia.crl
OCSP usluga	http://ocsp.eid.hr/akdcaroot	https://ocsp.certilia.com
CA certifikati	http://eid.hr/cert/akdcaroot.crt	https://certilia.com/cert/certilia.crt

Podaci za provjeru statusa certifikata sadržani su u certifikatu.

Točna lokacija je uvijek objavljena u samom certifikatu u polju CRL Distribution Points i(li) Authority Info Access.

2.2 Portal za objavljivanje informacije

Sve informacije koje su potrebne osobama i pouzdajućim stranama za korištenje usluga certificiranja objavljuje CERTILIA na web portalu i RA uredima.

Javnosti je dostupan javni dio portala https://www.certilia.com na kojem se objavljuju sljedeće informacije:

a) Opća pravila pružanja usluga certificiranja (CP) [53],
b) Pravilnik o postupcima certificiranja CERTILIA (CPS),
c) Uvjeti pružanja usluga certificiranja (PDS),
d) obavijesti vezane uz pružanje usluga certificiranja,
e) druge informacije koje se smatraju relevantnim za korisnike i pouzdajuće strane i
f) kontakt podaci za pomoć korisnicima.

CA uspostavlja privatni dio portala kojem mogu, na poveznici https://portal.certilia.com, pristupiti osobe koje su se registrirale, nakon provedene aktivacije korisničkog računa i prijave. Ako osobe u roku od 30 dana od uspješnog podnošenja zahtjeva za cerificiranja ne aktiviraju svoj korisnički račun, njihov zahtjev će biti storniran. Korisnički račun bez aktivnih certifikata izdanih od CERTILIA certifikacijskog tijela će biti izbrisan.
Na privatnom dijelu portala objavljene su sljedeće informacije i servisi:

a) aplikacija i upute potrebne za instalaciju i korištenje QSCD,
b) elektronička usluga za suspenziju certifikata,
c) pregled i promjena osobnih podataka za kontakt,
d) upravljanje autentikacijskim sredstvima za pristup CERTILIA mPotpis servisu za udaljeni elektronički potpis i pečat i

e) CERTILIA mPotpis servis za udaljeno potpisivanje i pečatiranje.

2.3 Vrijeme objavljivanja i učestalost objave informacija

Vrijede pravila:

a) Informacije na portalu dostupne su odmah nakon njihovog formalnog odobrenja.
b) Svi sadržaji na portalu su na hrvatskom jeziku, a dio sadržaja može biti dostupan i na engleskom jeziku.
c) Opća pravila [53], pravilnik i uvjeti pružanja usluga certificiranja dostupni su na hrvatskom i na engleskom jeziku.
d) U slučaju nepodudaranja u sadržaju dokumenata na engleskom jeziku sa sadržajem dokumenata na hrvatskom jeziku, važeća je verzija dokumenta na hrvatskom jeziku.
e) Podaci u repozitoriji objavljuju se odmah nakon njihovog izdavanja.
f) Informacije o statusu certifikata dostupne su pod uvjetima navedenim u točki 4.10.
g) CA je osigurava stalnu raspoloživost repozitorija 24 sata na dan, 7 dana u tjednu u skladu s najboljim poslovnim praksama.
h) Nakon kvara sustava ili drugih čimbenika koji nisu pod kontrolom CA, primjenjuju se sva raspoloživa sredstva kako bi se osigurao oporavak sustava u najkraćem mogućem roku.

2.4 Kontrole pristupa repozitoriju

Vrijede pravila:

a) Osnovne informacije na portalu dostupne su javnosti putem javne podatkovne veze i bez ograničenja, a prema standardnoj razini dostupnosti.
b) U slučaju potrebe, AKD može osigurati uslugu sa višom razinom dostupnosti , prema komercijalnim uvjetima.
c) Dodatne informacije i usluge na portalu dostupne su samo registriranim osobama.
d) CA ne postavlja nikakva ograničenja vezano uz korištenje CRL i OCSP usluga.
e) Certifikati osobe neće biti dostupni javnosti za pretraživanje osim ako za to ne postoje opravdani tehnički razlozi prema pouzdajućim stranama i osigurana suglasnost osobe.
f) CA zadržava pravo poduzimanja odgovarajućih mjera zaštite repozitorija i portala od zlouporabe.

3 Identifikacija i autentikacija

3.1 Određivanje imena

3.1.1 Tipovi imena

U polju „Subject“ svakog certifikata upisano je ime certifikata, odnosno jedinstven skup podataka koji nedvojbeno predstavlja najmanje osobu, subjekt certificiranja ili autora pečata ili pravnu osobu.

Ime certifikata određuje se u skladu s preporuci ITU-T X.520 [50] ili IETF RFC 5280 [38].

Pri određivanju polja „Subject“, primjenjuju se pravila navedena u preporuci ITU-T X.501 [51].

Postoje tipovi imena:

a) osobni certifikati koji imenuju fizičku osobu - subjekt certificiranja (potpisnik),
b) certifikati za elektronički pečat koji imenuju pravnu osobu – autora pečata i
c) CA certifikati, TSU certifikati i certifikati OCSP usluge koji imenuju CERTILIA ili CERTILIA OCSP ili AKD QTSA uslugu kao pravnu osobu.

3.1.2 Smislenost imena

Za CA certifikate i certifikate OCSP usluge i TSU certifikate polje „Subject“ formira se od:

commonName:	Ime CA certifikata, odnosno OCSP ili AKD QTSA usluge
organizationIdentifier:	Identifikator pravne osobe tj. VAT broj
organizationName:	Ime pravne osobe - kvalificiranog pružatelja usluge povjerenja
countryName:	Kôd države u kojoj djeluje pravna osoba

Za certifikate osoba polje „Subject“ formira se od:

commonName:	Ime i prezime fizičke osobe
serialNumber:	Serijski broj
givenName:	Ime fizičke osobe
Surname:	Prezime fizičke osobe
organizationalUnitName:	Tip certifikata (RSignature za udaljeni potpisni, Sigature za potpisni ili Identification za identifikacijski)
organizationName (Opcija):	Naziv organizacije s kojom je osoba povezana
organizationIdentifier(Opcija):	VAT identifikator organizacije sa kojom je osoba povezana (prema ETSI EN 319 412-1, čl. 5 [17])
countryName:	Dvoslovni ISO kod države

Za certifikate koji se izdaju pravnim osobama (certifikati za elektronički pečat) polje „Subject“ formira se od:

commonName:	Naziv certifikata
organizationalUnitName:	Tip certifikata
organizationName:	Naziv pravne osobe, autora pečata
organizationIdentifier:	VAT identifikator pravne osobe
countryName:	Kod države u kojoj je pravna osoba registrirana

3.1.3 Anonimnost i pseudonimi osobe

Nije podržano.

3.1.4 Pravila tumačenja imena

Polje „Subject“ svih certifikata koje izdaje pružatelj usluga certificiranja certifikata formira se u skladu s IETF RFC 5280 [38] te preporukom standarda ETSI EN 319 412-2 [18] odnosno ETSI EN 319 412-3 [19].

Pravila tumačenja imena navedena su u tablici 3.

U tablici 3, vrijednosti stupca „Obveza / Sadržaj“ označavaju:

1.) Obveza
   a. M (*engl. Mandatory*) – obveznu prisutnost polja u certifikatu
   b. O (*engl. Optional*) – ne obveznu prisutnost polja u certifikatu
2.) Sadržaj
   a. Fixed – označava unaprijed određenu vrijednost
   b. Variable – označava promjenjivu vrijednost koja ne ovisi o podacima fizičkih i/ili pravnih osoba
   c. Holder Variable – označava promjenjivu vrijednost koja ovisi o podacima fizičkih i/ili pravnih osoba

Tablica 3: Pravila tumačenja imena

Fizičke osobe			
Polje	Vrijednost	Obveza / Sadržaj	Pojašnjenje
commonName (cn)	Ime Prezime	M/Holder Variable	Predstavlja ime i prezime fizičke osobe
serialNumber	Identifikator fizičke osobe	M/Holder Variable	3 znaka za tip reference identiteta osobe, dvoslovni ISO kod države, „-„identifikacijski broj“, npr: PNOHR-OIB, sukladno točki 5.1.3 ETSI EN 319 412-1 [18].

givenName (g)	Ime	M/Holder Variable	Predstavlja ime osobe subjekta certificiranja
Surname (sn)	Prezime	M/Holder Variable	Predstavlja prezime osobe subjekta certificiranja
organizationalUnitName (OU)	Identification Signature Rsignature	M/ Variable	Određuje tip certifikata (RSignature za udaljeni potpisni, Sigature za potpisni ili Identification za identifikacijski)
organizationName (O)	ORGANIZACIJA d.o.o.	O/Holder Variable	Naziv organizacije s kojom je fizička osoba povezana
organizationIdentifier	VATHR-1234567890	O/Holder Variable	Sadrži prefix VAT za porezni broj, HR kao kod države, "-" (0x2D (ASCII), U+002D (UTF-8)) i 1234567890 porezni broj organizacije za fizičke osobe povezane s organizacijom
countryName (C)	Dvoslovni ISO kod države	M/Holder Variable	ISO kod države osobe subjekta certificiranja

Pravne osobe (CA, OCSP, QTSA)			
Polje	Vrijednost	Obveza / Sadržaj	Pojašnjenje
commonName (cn)	AKDCA Root CERTILIA	M/Fixed	Predstavlja naziv CA
	AKDCA Root OCSP CERTILIA OCSP AKD QTSA	M/Fixed	Predstavlja naziv OCSP sustava/Usluge vremenskog žiga
organizationIdentifier	VATHR-58843087891	M/Fixed	VAT označava da se radi o pravnoj osobi HR je kod države Znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) 58843087891 je porezni identifikacijski broj AKD-a (pravne osobe)
organizationName (O)	AKD d.o.o	M/Fixed	AKD d.o.o je naziv pravne osobe
countryName (C)	HR	M/Fixed	HR je kod države pravne osobe

Pravne osobe (elektronički pečat)			
Polje	Vrijednost	Obveza / Sadržaj	Pojašnjenje
commonName (cn)	Naziv pečata	M/Holder Variable	Naziv certifikata za pečat kojim se pravna osoba, autor pečata, predstavlja.
organizationIdentifier	VATHR-1234567890	M/Holder Variable	VAT označava da se radi o pravnoj osobi HR - Dvoslovni ISO kod države Znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) 1234567890 je porezni broj pravne osobe (OIB za HR, porezni broj za strane države)
organizationalUnitName (OU)	Seal Rseal	M/ Variable	Određuje tip certifikata
organizationName (O)	PRAVNA OSOBA d.o.o.	M/Holder Variable	Naziv pravne osobe, autora pečata
countryName (C)	Dvoslovni ISO kod države	M/Holder Variable	Dvoslovni ISO kod države u kojoj je registrirana pravna osoba

3.1.5 Jedinstvenost imena

U polju „Subject“ svakog izdanog certifikata upisani su jedinstveni podaci o fizičkoj osobi kojoj se izdaje certifikat, odnosno o pravnoj osobi u slučaju postojanja povezanosti fizičke osobe sa organizacijom ili za CA certifikate, certifikate OCSP usluge, TSU certifikate i certifikate za elektronički pečat.

Jedinstvenost imena fizičke osobe osigurana je atributom „serialNumber“ u polju „Subject“, dok se jedinstvenost imena pravne osobe izdavatelja osigurava atributom „organizationIdentifier“ u polju „Issuer“. U slučaju postojanja povezanosti fizičke osobe s organizacijom, jedinstvenost imena organizacije je osigurana atributom „organizationIdentifier“ u polju „Subject“.

Jedinstvenost imena pravne osobe – autora pečata za izdavanje certikata za elektronički pečat osigurana je atributom „organizationIdentifier“ u polju „Subject“.

3.1.6 Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka

Nije primjenjivo.

3.2 Inicijalno utvrđivanje identiteta

3.2.1 Metoda dokazivanja posjeda privatnog ključa

Privatni ključevi osobnih certifikata i certifikata za elektronički pečat na kartici (QCP-n-qscd-ksign, QCP-l-qscd-kseal i NCP+ kident) generiraju se u HSM uređaju te se u sigurnom okružju kvalificiranog pružatelja usluga povjerenja unose na kvalificirano sredstva za izradu elektroničkog potpisa (QSCD).

Privatni ključevi osobnih certifikata za udaljeni potpis i udaljenih certifikata za elektronički pečat (QCP-n-qscd-krsign i QCP-l-qscd-krseal) generiraju se i koriste u udaljenom HSM uređaju u sklopu servisa CERTILIA mPotpis koji se nalazi u sigurnom okružju kvalificiranog pružatelja usluga povjerenja. Udaljeni HSM je QSCD uređaj (kvalificirano sredstvo za izradu elektroničkog potpisa) sukladan ISO/IEC 15408 [43] *Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5* i prema pravilima definiranim u Prilogu II *Uredbe (EU) br. 910/2014 [1]*.

Privatni ključevi i pripadajući certifikati za udaljeni potpis i udaljeni pečat, generiraju se u trenutku kada je osoba ili autor pečata pristupio servisu CERTILIA mPotpis dozvoljenim dvofaktorskim autentikacijskim sredstvom registriranim u CERTILIA IDP sustavu, čime je potvrdio svoj identitet, i unosom referentnog i autorizacijskog koda dobivenih nakon uspješno zaprimljenog i obrađenog zahtjeva za izdavanje certifikata na e-mail ili SMS te podešavanja PIN-a za privatni ključ. Nakon što je generiranje privatnog ključa i pripadajućeg certifikata završeno, osoba ili autor pečata u CERTILIA mPotpis servisu unosom prethodno definiranog PIN-a za privatni ključ potvrđuje preuzimanje certifikata i posjed privatnog ključa.

AKD kao kvalificirani pružatelj usluga povjerenja prilikom generiranja ključeva korisnika, osigurava tehničke procese i metode provjere kojima se jamči povezanost osoba, odnosno potpisnika i autora pečata s privatnim ključem, koji odgovara javnom ključu za koji se izdaje certifikat, kao i kontrola potpisnika, odnosno autora pečata nad privatnim ključem.

Privatni ključevi OCSP certifikata (NCP-l-scd-ocsp) i TSU certifikata generiraju se u HSM uređaju u sigurnom okružju CA koje je autoriziralo fizičku osobu – skrbnika certifikata da se brine o HSM uređaju i korespondirajućem privatnom ključu.

3.2.2 Potvrda identiteta pravnih osoba

Prikupljanje informacija o pravnim osobama provodi se kod izdavanja certifikata:

a) pravnim osobama za certifikate za elektronički pečat i
b) fizičkim osobama koje su povezane s organizacijom u slučaju kada organizacija ima status pravne osobe te kod kojih su ime i identifikator pravne osobe sadržani u polju „Subject“ certifikata.

3.2.2.1 Prikupljanje informacija o pravnim osobama

U svrhu utvrđivanja identiteta pravnih osoba prikupljaju se sljedeće informacije i dokumenti:

a) Osnovne informacije o pravnoj osobi koje moraju uključiti, ali se ne ograničavaju na:

- sadašnji naziv pravne osobe,
- OIB ili porezni broj ili drugi jedinstveni identifikator pravne osobe,
- država sjedišta pravne osobe.

b) Kada je to potrebno, od pravne osobe će se zahtijevati:
- adresa sadašnjeg sjedišta pravne osobe,
- dodatne informacije za kontakt: e-mail adresa, broj telefona ili drugi podaci.

c) Dokumenti koji se smatraju prihvatljivim dokazima o nazivu, statusu i postojanju pravne osobe s kojom je fizička osoba subjekt certificiranja povezana su:
   a. Izvadak iz službene evidencije u RH
      i. Trgovačka društva - izvadak ili elektronički zapis iz Sudskog registra ili,
      ii. Obrti - izvadak ili elektronički zapis iz Obrtnog registra ili,
   b. izvadak ili ispis elektroničkog zapisa iz matičnog registra u zemlji EU, preveden na hrvatski jezik i ovjeren od strane ovlaštenog sudskog tumača u RH.

d) Dokumenti koji se smatraju prihvatljivim dokazima povezanosti fizičke osobe subjekta certificiranja i pravne osobe su:
   a. Potpisana i ovjerena potvrda izdana od strane organizacije kojom se dokazuje povezanost organizacije s fizičkom osobom subjektom certificiranja.

e) Tijekom trajanja perioda na kojeg su izdani certifikati od strane s pružatelja usluga povjerenja, pravna osoba dužna je prijaviti svaku promjenu informacija o pravnoj osobi i dostaviti pripadajuće dokumente.

Prikupljanje informacija i podataka o pravnim osobama može se vršiti dohvatom podataka iz dostupnih nadležnih elektroničkih registara ili automatski kroz AKD RA sustav.

U slučaju nepodudaranja podataka sa dostavljenih dokumenata i zahtjeva za izdavanje certifikata sa podacima dohvaćenim iz nadležnih registara RA će uvažiti podatke iz registara o čemu odmah obavještava ovlaštenog predstavnika pravne osobe.

3.2.2.2 Provjera informacija o pravnim osobama

Postupak provjere pravne osobe uključuje, ali se ne ograničava na:

a) provjeru postojanja pravne osobe tako da se izvrši upit u nadležni registar i/ili se provjere prikupljeni dokumenti o nazivu, statusu i postojanju pravne osobe,

b) provjeru imena pravne osobe tako da se utvrdi odgovara li ime pravne osobe u zahtjevu imenu kojim se pravna osoba služi u pravnom prometu

c) provjeru identifikacijskog broja pravne osobe tako da se provede upit na nacionalni OIB sustav i provjeri odgovara li OIB ili porezni broj ili drugi jedinstveni identifikator pravne osobe onom koji je pridružen nazivu pravne osobe.

Provjera informacija i podataka o pravnim osobama može se vršiti dohvatom podataka iz dostupnih nadležnih elektroničkih registara ili automatski kroz AKD RA sustav.

U slučaju nepodudaranja podataka sa dostavljenih dokumenata i zahtjeva za izdavanje certifikata sa podacima dohvaćenim iz nadležnih registara RA će uvažiti podatke iz registara o čemu odmah obavještava ovlaštenog predstavnika pravne osobe.

3.2.3 Potvrda identiteta fizičkih osoba

3.2.3.1 Prikupljanje informacija o fizičkim osobama

Prikupljanje i provjera podataka o osobama provodi se u skladu s AKD uputama za rad registracijskog tijela (RA) [55].

U svrhu utvrđivanja identiteta fizičkih osoba prikupljaju se sljedeće informacije i dokumenti:

a) Osnovne informacije o osobi subjektu certificiranja i(li) ovlaštenom predstavniku, koje uključuju:
   - puno ime i prezime,
   - Vrsta i broj dokumenta kojim se dokazuje identitet
   - OIB ili drugi nacionalni identifikacijski broj iz identifikacijskog dokumenta,
   - adresa prebivališta
   - datum rođenja.

b) Zahtijevaju se odgovarajući dokumenti ili informacije za provjeru imena, identiteta i osnove za izdavanje certifikata.

c) Dokumenti koji se smatraju prihvatljivim dokazima identiteta za izdavanje certifikata fizičkim osobama su:
   - osobna iskaznica,
   - putovnica.

d) Ukoliko je fizička osoba subjekt certificiranja povezana sa organizacijom, prikupljaju se dodatne informacije i dokumenti:
   - puno ime i pravni status organizacije,
   - dokaz o postojanju i statusu organizacije,
   - dokaz da je osoba povezana sa organizacijom.
   - dokaz da je osoba ovlaštena za zastupanje

e) Dokumenti koji se smatraju prihvatljivim dokazima povezanosti fizičke osobe subjekta certificiranja i organizacije su:
   a. Potpisana i ovjerena potvrda izdana od strane organizacije kojom se dokazuje povezanost organizacije sa fizičkom osobom subjektom certificiranja.

f) Dokumenti koji se smatraju prihvatljivim dokazima da je fizička osoba ovlašteni predstavnik pravne osobe:
   a. Izvadak iz službene evidencije u RH
      i. Trgovačka društva - izvadak ili elektronički zapis iz Sudskog registra ili,
      ii. Obrti - izvadak ili elektronički zapis iz Obrtnog registra ili,
      iii. Komore – statut i matični zakon ili,
      iv. Slobodne djelatnosti - izvadak ili elektronički zapis iz matične Komore i rješenje Porezne uprave/ispostave,
   b. izvadak ili ispis elektroničkog zapisa iz matičnog registra u zemlji EU, preveden na hrvatski jezik i ovjeren od strane ovlaštenog sudskog tumača u RH.

c. Uz Izvadak iz a.) ili b) ovog stavka, dodatno punomoć osobe koja je u Izvatku navedena kao ovlaštena za zastupanje

Prikupljanje informacija i podataka o osobama može se vršiti dohvatom podataka iz dostupnih nadležnih elektroničkih registara ili automatski kroz AKD RA sustav, te iz kvalificiranog elektroničkog potpisa zahtjeva zaprimljenog putem elektroničke on-line usluge.

U slučaju nepodudaranja podataka sa dostavljenih dokumenata i zahtjeva za izdavanje certifikata sa podacima dohvaćenim iz nadležnih registara RA će uvažiti podatke iz registara o čemu odmah obavještava osobu.

3.2.3.2 Provjera informacija o fizičkim osobama

Vrijede pravila:

a) RA prikuplja i provjerava informacije i dokumente kako bi se osiguralo da je svaka informacija sadržana u certifikatu provjerena i potvrđena.

b) Postupci utvrđivanja i provjere identiteta fizičkih osoba subjekta certificiranja, pripadnosti organizaciji, te ovlaštenja za zastupanje provode se u skladu s nacionalnom, EU identifikacijskom praksom kao i relevantnim EU aktima kojima se uređuje razmjena podataka u svrhu postizanja interoperabilnosti.

Postupak provjere uključuje, ali se ne ograničava na:

a) provjeru postojanja i identiteta fizičke osobe subjekta certificiranja neposrednom identifikacijom uz fizičku prisutnost osobe temeljem predočenog dokumenta,

b) provjeru postojanja i identiteta fizičke osobe subjekta certificiranja identifikacijom uz fizičku prisutnost osobe obavljenu u Javnobilježničkom uredu, temeljem prikupljenog Zahtjeva za certificiranje osobe ovjerenog kod javnog bilježnika, sukladno članku 60. Utvrđivanje istovjetnosti i članku 77. Ovjera potpisa Zakona o javnom bilježništvu [10], a što ispunjava zahtjeve članka 24. stavka 1 točke (a) *Uredbe (EU) br. 910/2014 [1]*

c) posredne identifikacije na način koji pruža jednaku razinu sigurnosti utvrđivanja identiteta fizičke osobe kao i postupak neposredne identifikacije,

d) AKD provodi postupak posredne identifikacije fizičke osobe pomoću certifikata kvalificiranog elektroničkog potpisa izdanog temeljem neposredne identifikacije fizičke osobe,

e) Posredna identifikacija je moguća i pomoću sredstava elektroničke identifikacije, za koja je prije izdavanja kvalificiranog certifikata osigurana fizička prisutnost fizičke osobe i koja ispunjavaju zahtjeve u pogledu sigurnosnih razina „značajna“ ili visoka“, sve sukladno odredbama članka 8. *Uredbe (EU) br. 910/2014 [1],*

f) provjeru naziva, statusa i postojanja organizacije, u slučaju pripadnosti fizičke osobe organizaciji temeljem predočenih dokumenata ili izvadaka,

g) provjeru povezanosti fizičke osobe subjekta certificiranja sa organizacijom temeljem predočenog dokumenta,

h) provjeru ovlaštenja fizičke osobe za zastupanje pravne osobe temeljem uvida u matični registar i po potrebi temeljem predočenog dokumenta,

i) provjera odgovaraju li prikupljene informacije onima koje su navedene u predočenim dokumentima,

j) provjera vjerodostojnosti priloženih/predočenih dokumenata i izvadaka,

k) utvrđivanje postoji li osnova za izdavanje identifikacijskog odnosno potpisnog certifikata,
l) provjera o prihvaćanju primjenjivih „Uvjeta pružanja usluga certificiranja“ davatelja usluga certificiranja od strane osobe.

Provjera informacija i podataka o osobama može se vršiti dohvatom podataka iz dostupnih nadležnih elektroničkih registara ili automatski kroz AKD RA sustav.

U slučaju nepodudaranja podataka sa dostavljenih dokumenata i zahtjeva za izdavanje certifikata sa podacima dohvaćenim iz nadležnih registara RA će uvažiti podatke iz registara o čemu odmah obavještava osobu.

3.2.4 Informacije o osobama koje se ne provjeravaju

Od osoba se može tražiti naziv certifikata kao dodatna informacija.

RA ne provjerava broj mobitela, e-mail adresu i dodatne informacije već je za njihovu točnost odgovorna osoba. Podatak e-mail adresa ili broj mobitela mogu se dodatno verificirati prilikom pristupa privatnom portalu u slučaju kada potpisnik ili autor pečata koristi servis CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje.

3.2.5 Provjera ovlasti

Ukoliko je u zahtjevu za izdavanje certifikata fizičkim osobama naznačena povezanost osobe subjekta certificiranja sa organizacijom, službenik RA će prije prihvaćanja zahtjeva, u matičnom registru nadležnom za organizaciju koja izdaje potvrdu, dodatno provjeriti je li potpisnik sa potvrde izdane od strane organizacije iz 3.2.3.1 pod g.) ujedno i osoba ovlaštena za zastupanje organizacije.

Kod Zahtjeva za izdavanje certifikata za elektroničke pečate, prije prihvaćanja zahtjeva, provesti će se provjera i potvrda identiteta ovlaštenog predstavnika sukladno točkama 3.2.3.1. i 3.2.3.2.

Dodatno će se u matičnom registru nadležnom za pravnu osobu, provjeriti postojanje ovlaštenja za zastupanje ovlaštenog predstavnika. U slučaju kada identitet ovlaštenog predstavnika iz Zahtjeva ne odgovara identitetu osobe ovlaštene za zastupanje koja je navedena u matičnom registru, dodatno se zahtjeva punomoć osobe navedene u matičnom registru

Utvrđivanje identiteta opunomoćenika provodi se na jednak način kao i provjera identiteta osobe ovlaštene za zastupanje.

Provjera ovlasti i identiteta ovlaštenog zastupnika može se vršiti dohvatom podataka iz dostupnih nadležnih elektroničkih registara ili automatski kroz AKD RA sustav.

U slučaju nepodudaranja podataka sa dostavljenih dokumenata i zahtjeva za izdavanje certifikata sa podacima dohvaćenim iz nadležnih registara RA će uvažiti podatke iz registara o čemu odmah obavještava ovlaštenog predstavnika pravne osobe.

3.2.6 Kriteriji za interoperabilnost

Nije određeno.

3.3 Identifikacija i autentikacija kod obnove certifikata

3.3.1 Identifikacija i autentikacija kod redovite obnove certifikata

Primjenjuju se pravila identifikacije i potvrđivanje identiteta kod izdavanja novog para ključeva u poglavlju 3.3.2

3.3.2 Identifikacija i autentikacija kod izdavanja novog para ključeva

Kod izdavanja novog para ključa primjenjuju se sljedeće sigurnosne mjere i postupci:

a) Pravila utvrđivanja identiteta ista su kao i pravila kod inicijalnog utvrđivanja identiteta (točka 3.2.3)
b) Kod izdavanja novog para ključeva mogu se koristiti informacije i dokumenti koji su osigurani tijekom inicijalnog utvrđivanja identiteta
c) Osobe koje podnose zahtjev zbog promjene osobnog imena ili promjene prezimena ili naziva organizacije obvezno dodatno prilažu identifikacijsku ispravu ili dokaz, u kojoj je navedeno novo osobno ime ili prezime ili naziv organizacije kojim se osoba dužna služiti u pravnom prometu. Promjene se također mogu provjeravati i elektronički iz nadležnih registara prilikom obrade zahtjeva u AKD RA sustavu.

3.4 Identifikacija i autentikacija kod opoziva certifikata

Provjera identiteta osobe kod podnošenja zahtjeva za opoziv provodi se temeljem podnesenog zahtjeva. Potvrdom identiteta podnositelja zahtjeva utvrđuje se i ovlaštenje podnositelja za podnošenje zahtjeva.

Prilikom podnošenja zahtjeva u RA uredu identitet se provjerava neposrednom identifikacijom uz fizičku prisutnost osobe, temeljem predočenog dokumenta.

Za opoziv certifikata za elektronički pečat i certifikata osoba povezanih sa organizacijom kada je osoba podnositelj zahtjeva za opoziv različita od osobe subjekta certificiranja provodi se provjera identiteta ovlaštenog predstavnika ili zastupnika.

Identifikacija i potvrda identiteta podnositelja može se provesti i validacijom i verifikacijom kvalificiranog elektroničkog potpisa osobe ili ovlaštenog predstavnika elektronički dostavljenog zahtjeva za opoziv certifikata.

Kod podnošenja zahtjeva za suspenziju certifikata provjera identiteta osobe se može provesti i na daljinu, elektroničkim putem, uz korištenje adekvatne metode autentikacije.

Prihvatljiva metoda autentikacije na daljinu uključuje autentikaciju na korisnički portal uz verifikaciju akcija putem e-mail-a pri čemu se za svaku uspješno provedenu autentikaciju i verfikaciju smatra da je osoba podnijela zahtjev za suspenzijom certifikata.

Podaci za autentikaciju na portal uručuju se korisniku kod preuzimanja certifikata kako je opisano u poglavlju 6.4.

4 Provedbeni zahtjevi vezani uz životni ciklus certifikata

4.1 Podnošenje zahtjeva za izdavanje certifikata

4.1.1 Tko može podnijeti zahtjev za izdavanje certifikata

Osoba naručitelj podnosi zahtjev za izdavanje certifikata fizičkim osobama u formi Zahtjeva za izdavanje certifikata što uključuje, ali nije ograničeno na sve informacije i dokaze predviđene ovim Pravilnikom, Općim uvjetima kao i prihvaćanje primjenjivih Uvjeta pružanja usluga certificiranja i drugih dokumenata na temelju čega certifikati mogu biti izdani.

Osoba ovlašteni predstavnik podnosi zahtjev za izdavanje certifikata za pečat u formi Zahtjeva za izdavanje certifikata za pečat što uključuje, ali nije ograničeno na sve informacije i dokaze predviđene ovim Pravilnikom, Općim uvjetima kao i prihvaćanje primjenjivih Uvjeta pružanja usluga certificiranja i drugih dokumenata na temelju čega certifikati mogu biti izdani.

4.1.2 Postupak podnošenja zahtjeva za izdavanje certifikata

Postupak podnošenja zahtjeva za izdavanje certifikata dostupan je na portalu https://www.certilia.com/, te u prostorima RA Registracijskog tijela.

Propisana su sljedeća pravila:

a) Zahtjev za izdavanje certifikata podnosi se putem Registracijskog tijela (RA) ili elektroničke on-line usluge.
b) Zahtjev za izdavanje certifikata podnosi se na propisanom obrascu koji je dostupan u RA uredima, na portalu https://www.certilia.com/ ili je sadržan u elektroničkoj on-line usluzi.
c) Osobe su dužne potpisom na zahtjevu za izdavanje certifikata potvrditi da su osobni identifikacijski podaci u trenutku podnošenja zahtjeva cjeloviti i točni.
d) Prilikom podnošenja zahtjeva za izdavanjem certifikata osobe naručitelji, osobe subjekti certificiranja, osobe ovlašteni predstavnici svojim potpisom, odnosno ovjerom i potpisom potvrđuju da su pročitali, razumjeli, te da prihvaćaju svoje obveze i odgovornosti iz AKD-ovih primjenjivih „Uvjeta pružanja usluga certificiranja“.
e) Dokaz o plaćanju osigurava RA, osim u slučaju zahtjeva za certifikate za udaljeno potpisivanje koji se na izdaju punoljetnim korisnicima eOI u skladu s izmjenama i dopunama Zakona o osobnoj iskaznici (NN 144/2020).

4.2 Obrada zahtjeva za izdavanje certifikata

4.2.1 Provedba identifikacije i autentikacije

a) Identitet fizičkih osoba potvrđuje se u postupcima koji su navedeni u točki 3.2.3.
b) Identifikacija i autentikacija službenika RA i osoblja CA potvrđuje se u postupku koji je definiran u poglavlju 3.2.5.
c) Postupci vezani uz provjeru službenika RA i osoblja CA definirani su u poglavlju 5.3.
d) RA može podatke o osobama navedene u zahtjevu provjeravati u nadležnim nacionalnim registrima, ili putem AKD RA informacijskog sustava, o čemu RA službenik obavještava

osobu o postupku. U slučaju da podaci sa zahtjeva ne odgovaraju podacima iz nacionalnih registara, RA će uvažiti podatke iz nacionalnih registara kao relevantne.

e) U slučajevima opisanim pod stavkom c), RA može izmijeniti osobne podatke iz zahtjeva, navedene u poglavlju 3.2.3. i 3.2.2., podacima koji su provjerom dohvaćeni u nacionalnim registrima.

4.2.2 Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

RA odnosno on-line usluga odlučuje o prihvaćanju ili odbijanju zahtjeva za izdavanje certifikata.

Zahtjev za izdavanje certifikata će biti odbijen:

a) ako postoji sumnja da prikupljene informacije o fizičkim ili pravnim osobama nisu točne, cjelovite ili vjerodostojne,
b) ako postupak provjere informacija o fizičkim osobama nije uspješno proveden prema poglavljima 3.2.3.2,
c) ako postupak provjere informacija o pravnim osobama nije uspješno proveden prema poglavljima 3.2.2.2,
d) ako je u zahtjevu naznačena povezanost fizičke osobe i organizacije koja je pravna osoba, a postupak provjere informacija o pravnim osobama nije uspješno proveden prema 3.2.2.2,
e) ako osoba ne prihvaća podatke dohvaćene iz nadležnog registra kao važeće,
f) ako je zahtjev za izdavanje certifikata naknadno nakon podnošenja zahtjeva povučen ili
g) ako je naknadno nakon podnošenja zahtjeva utvrđeno da zahtjev za izdavanje certifikata nije bio autoriziran.

Ako je zahtjev za izdavanje certifikata odbijen, osoba naručitelj se informira usmenim putem o razlozima odbijanja zahtjeva.

Zahtjev za izdavanje certifikata će biti prihvaćen ako je potvrđen identitet fizičke osobe subjekta certificiranja prema poglavljima 3.2.3. ili pravne osobe prema poglavljima 3.2.2.

Svi podneseni zahtjevi unose se u informacijski sustav RA koji ispunjava sigurnosne zahtjeve navedene u poglavljima 6.5 i 6.6.

Obrasci, ugovori i sva tiskana dokumentacija koja se prikuplja u postupku podnošenja zahtjeva pohranjuje se i čuva u skladu s pravilima navedenim u poglavlju 5.5.2.

Elektronički potpisani zahtjevi za izdavanje certifikata zaprimljeni putem on-line usluge čuvaju se u AKD RA sustavu u skladu s pravilima navedenim u poglavlju 5.5.2.

Zaštita osobnih podataka prikupljenih u postupku registracije fizičkih osoba provodi se u skladu s pravilima koja su navedena u poglavlju 9.4

4.2.3 Vrijeme obrade zahtjeva za izdavanje certifikata

Obrada zahtjeva za izdavanje certifikata provodi se u roku od 7 radnih dana od dana podnošenja zahtjeva.

4.3 Postupak izdavanja certifikata

4.3.1 Postupci tijekom izdavanja certifikata

a) Fizičkim i pravnim osobama se mogu izdati certifikati samo ako je proveden proces provjere podataka i odobren zahtjev u informacijskom sustavu AKD RA.
b) Nakon unošenja zahtjeva za izdavanje certifikata u informacijski sustav, podaci potrebni za realizaciju zahtjeva šalju se u CA kroz siguran komunikacijski kanal.
c) CA ne provjerava cjelovitost, točnost i jedinstvenost zaprimljenih podataka za izdavanje certifikata, već se oslanja na provjeru izvršenu u RA.
d) Certifikati se osobama mogu izdati isključivo temeljem zahtjeva zaprimljenog od RA.
e) U slučaju izdavanja certifikata na QSCD koji se uručuje osobi subjektu certificiranja ili ovlaštenom predstavniku, proizvođač izrađuje QSCD s čipom s otisnutim dizajnom ili ugrađuje certifikat i primarni ključ na certificirani QSCD u vlasništvu subjekta certificiranja.
f) Postupak izrade i izdavanja certifikata te generiranja parova ključeva i njihovog unošenja u udaljeni QSCD uređaj, kao i njihove pohrane i upotrebe u slučajevima kada kvalificirani pružatelj usluga povjerenja upravlja podacima za izradu elektroničkih potpisa u ime potpisnika ili autora pečata, vrši se u sigurnom okružju servisa CERTILIA mPotpis i na način koje ispunjava sigurnosne zahtjeve navedene u poglavljima 6.5 i 6.6.
g) Profil izdanog certifikata mora biti u skladu sa zahtjevima koji su navedeni u poglavlju 7.1.
h) CA ključevi koji se koriste za potpisivanje certifikata kao i ključevi osobe štite mjerama i postupcima koji su propisani u poglavlju 6.2.

4.3.2 Obavješćivanje o izdavanju certifikata

Osoba subjekt certificiranja ili osoba ovlašteni predstavnik može biti informiran o datumu izdavanja certifikata i preuzimanja QSCD uređaja ili preuzimanja certifikata za udaljeno potpisivanje i pečatiranje u sklopu servisa CERTILIA mPotpis:

a) u postupku podnošenja zahtjeva putem ovlaštenih RA službenika
b) po obradi zahtjeva na adresu elektroničke pošte ili broj mobitela naveden u postupku podnošenja zahtjeva.

4.4 Prihvaćanje certifikata

4.4.1 Provedba postupka prihvaćanja certifikata

a) Certifikat preuzima osoba subjekt certificiranja ili osoba ovlašteni predstavnik.
b) Odmah po preuzimanju osoba subjekt certificiranja ili osoba ovlašteni predstavnik obavlja provjeru sadržaja certifikata, te u slučaju da ne prihvaća bilo koji dio certifikata o istome odmah informira AKD.

c) U slučajevima kada se QSCD uručuje, smatra se da je osoba subjekt certificiranja ili osoba ovlašteni predstavnik prihvatila privatni ključ i certifikat u trenutku uručenja QSCD.

d) U trenutku preuzimanja QSCD, osoba je informirana o uvjetima korištenja certifikata i već je prihvatila Uvjete pružanja usluga certificiranja (prema poglavlju 4.1.2).

e) Ako osoba ne preuzme QSCD u roku od 120 dana, smatra se da nije prihvatila certifikat.

f) U slučajevima kada kvalificirani pružatelj usluga povjerenja upravlja podacima za izradu elektroničkih potpisa u ime osobe subjekta certificiranja ili autora pečata, u sklopu servisa CERTILIA mPotpis, smatra se da je certifikat prihvaćen u trenutku prvog korištenja odnosno nakon uspješno provedenog postupka koji se sastoji od:

   a. Uspješno zaprimljeni referentni i autorizacijski kodovi za preuzimanje certifikata za udaljeno potpisivanje ili pečatiranje, generirani u servisu CERTILIA mPotpis temeljem zahtjeva u AKD RA.

   b. Uspješna prijava na servis CERTILIA mPotpis dvofaktorskim sredstvom autentikacije registriranim u CERTILIA IDP sustavu.

   c. Uspješna registracija certifikata u servisu CERTILIA mPotpis unosom referentnog i autorizacijskog koda te postavljanjem PIN-a za aktivaciju privatnog ključa za potpisivanje ili pečatiranje i

   d. Prva aktivacija ključa postavljenim PINom u servisu CERTILIA mPotpis.

   e. Ako osoba ne provede postupke c. do d. u roku od 120 dana, smatra se da nije prihvatila certifikat.

g) Certifikati koji nisu prihvaćeni opozivaju se po proceduri koja je opisana u poglavlju 4.9.3.

4.4.2 Objava certifikata od strane CA

Certifikati osoba neće biti dostupni javnosti za pretraživanje. AKD zadržava pravo naknadne objave certifikata dostupnih javnosti za pretraživanje, u slučaju potrebe i prema komercijalnim uvjetima.

4.4.3 Obavješćivanje drugih strana o izdavanju certifikata

Informaciju da je certifikat izdan i da je QSCD izrađen odnosno da je korisnik preuzeo certifikat za udaljeni potpis ili pečat u sklopu servisa CERTILIA mPotpis prosljeđuju se informacijskom sustavu AKD RA.

CA ne obavještava druge strane o izdavanju certifikata.

Osobe mogu dostaviti svoj certifikat drugim stranama, kada je to potrebno.

4.5 Korištenje ključeva i certifikata

4.5.1 Osobe

U slučajevima kada je osoba u posjedu para ključeva na QSCD uređaju u posjedu te njima samostalno upravlja, vrijede pravila:

a) Osobi subjektu certificiranja ili osobi ovlaštenom predstavniku podaci za registraciju na portal i/ili aktivaciju QSCD uređaja s certifikatima mogu biti dostavljeni na e-mail

ili SMS podatke navedene u zahtjevu za izdavanje certifikata, ako je tako naznačeno u zahtjevu.

Na QSCD se može nalaziti:

a) potpisni certifikat koji je kvalificirani certifikat i koji je namijenjen za izradu elektroničkog potpisa,
b) certifikat za elektronički pečat, koji je kvalificirani certifikat i koji je namijenjen za izradu elektroničkog pečata i(li)
c) identifikacijski certifikat koji je sredstvo elektroničke identifikacije visoke razine sigurnosti i koji je namijenjen za autentikaciju na elektroničke usluge.

U slučajevima kada je osoba u kontroli para ključeva na udaljenom QSCD uređaju u sklopu servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje vrijede pravila:

a) Osobi subjektu certificiranja ili osobi ovlaštenom predstavniku dostavljaju se na e-mail ili SMS podaci za registraciju na portal i registracijski kodovi koji se koriste u trenutku preuzimanja i registraciju certifikata te postavljanja PINa pripadajućeg privatnog ključa certifikata u CERTILIA mPotpis servisu.

Na udaljenom QSCD uređaju se može nalaziti:

a) potpisni certifikat koji je kvalificirani certifikat i koji je namijenjen za izradu udaljenog elektroničkog potpisa i(ili)
b) certifikat za elektronički pečat, koji je kvalificirani certifikat i koji je namijenjen za izradu udaljenog elektroničkog pečata.

Certifikati izdani fizičkim osobama su vlasništvo osobe naručitelja, te ih osoba subjekt certificiranja koristi u privatne svrhe, ali i za poslovnu uporabu.

Certifikati izdani pravnim osobama su vlasništvo autora pečata, te ih osoba ovlašteni predstavnik koristi za poslovnu uporabu.

Osobe su prihvatile uvjete korištenja usluga certificiranja kojim su se obvezale da će ispuniti svoje obveze navedene u točki 9.6.4.

Uvjeti pružanja usluga certificiranja sadrže:

a) informacije o pružatelju usluga certificiranja i o opsegu usluga koje on pruža i o pravilima pružanja usluga,
b) tipove i namjenu certifikata te način provjere perioda važenja i valjanost certifikata,
c) postupanje s autentikacijskim i PIN podacima za pristup servisu CERTILIA mPotpis i korištenje privatnih ključeva i pripadajućih certifikata za udaljeni potpis ili pečat,
d) obveze i odgovornosti fizičkih i pravnih osoba, pružatelja usluga i pouzdajućih strana,
e) poslovne informacije vezane uz jamstva, cijene, sklapanje i raskid ugovora,
f) odredbe vezane uz zaštitu podataka i privatnosti,
g) komunikacija s korisnicima, pritužbe, rješavanje sporova i mjerodavno pravo i
h) primjenjivi zakoni i nadzor nad pružateljem usluga certificiranja.

4.5.2 Pouzdajuće strane

U skladu s uvjetima korištenja usluga certificiranja, pouzdajuće strane, koje se oslanjaju na certifikate i usluge certificiranja obvezuju se:

a) da će se prije korištenja usluga certificiranja informirati na portalu o uvjetima korištenja usluga certificiranja i prihvatljivom načinu korištenja usluga certificiranja,
b) da će samostalno procijeniti i utvrditi prikladnost korištenja certifikata za odgovarajuću namjenu,
c) da će prije ostvarivanja povjerenja u certifikat utvrditi da certifikat nije istekao i da nije opozvan, a prema podacima koji su navedeni u certifikatu,
d) da će provjeru valjanosti certifikata vršiti koristeći autorizirani izvor i pouzdanu opremu i

   da će provjeru statusa certifikata osoba i svih certifikata na certifikacijskoj stazi provoditi prema postupcima koji su definirani u IETF RFC 5280 [38] i IETF RFC 3739 [37].

4.6 Obnova certifikata

4.6.1 Razlozi za obnovu certifikata

Certifikat treba obnoviti ako ističe rok valjanosti certifikata.

Svaka obnova certifikata podrazumijeva izdavanje novog para ključeva (vidi 4.7.1).

4.6.2 Tko može zatražiti obnovu certifikata

Vrijede pravila iz točke 4.1.

4.6.3 Obrada zahtjeva za obnovu certifikata

Vrijede pravila iz točke 4.2.

4.6.4 Obavještavanje korisnika o obnovi certifikata

Vrijede pravila iz točke 4.3.

4.6.5 Provedba prihvaćanja obnovljenog certifikata

Vrijede pravila iz točke 4.4.1.

4.6.6 Objavljivanje certifikata po obnovi certifikata

Vrijede pravila iz točke 4.4.2.

4.6.7 Obavještavanje drugih strana o obnovi certifikata

Vrijede pravila iz točke 4.4.3.

4.7 Izdavanje novog para ključeva

4.7.1 Razlozi za izdavanje novog para ključeva

Novi par ključeva će biti izdan:

a) ako certifikat treba obnoviti (vidi 4.6) ili
b) ako certifikat treba promijeniti (vidi 4.8) ili
c) ako je došlo do opoziva certifikata (vidi 4.9).

CA ne reaktivira opozvani certifikat već će se osobi izdati novi par ključeva i novi certifikat.

4.7.2 Tko može zatražiti izdavanje novog para ključeva

Vrijede pravila iz točke 4.1.

4.7.3 Obrada zahtjeva za izdavanje novog para ključeva

Vrijede pravila iz točke 4.2.

4.7.4 Obavještavanje korisnika o izdavanju novog para ključeva

Vrijede pravila iz točke 4.3.

4.7.5 Provedba prihvaćanja novog para ključeva

Vrijede pravila iz točke 4.4.1.

4.7.6 Objavljivanje certifikata po izdavanju novog para ključeva

Vrijede pravila iz točke 4.4.2.

4.7.7 Obavještavanje drugih strana o izdavanju novog para ključeva

Vrijede pravila iz točke 4.4.3.

4.8 Promjena certifikata

4.8.1 Razlozi za promjenu certifikata

Razlozi za promjenu certifikata su

a) došlo je do promjene u podacima koji su sadržani u certifikatu,
b) utvrđeno je da informacije sadržane u certifikatu nisu ispravne Ili
c) trajni gubitak PIN za certifikate za udaljeno potpisivanje ili pečatiranje izdane u sklopu servisa CERTILIA mPotpis.

Svaka promjena certifikata podrazumijeva izdavanje novog para ključeva (vidi 4.7.1).

4.8.2 Tko može zatražiti promjenu certifikata

Vrijede pravila iz točke 4.1.

4.8.3 Obrada zahtjeva za promjenu certifikata

Vrijede pravila iz točke 4.2.

4.8.4 Obavještavanje korisnika o promjeni certifikata

Vrijede pravila iz točke 4.3.

4.8.5 Provedba prihvaćanja promijenjenog certifikata

Vrijede pravila iz točke 4.4.1.

4.8.6 Objavljivanje certifikata po promjeni certifikata

Vrijede pravila iz točke 4.4.2.

4.8.7 Obavještavanje drugih strana o promjeni certifikata

Vrijede pravila iz točke 4.4.3.

4.9 Opoziv i suspenzija certifikata

4.9.1 Koji su razlozi za opoziv certifikata

Certifikat se opoziva u sljedećim situacijama:

a) Podnesen je autorizirani zahtjev za opoziv certifikata.
b) Prijavljena je promjena podataka u certifikatu odnosno došlo je do promjene podataka u atributima polja „Subject“ certifikata (npr. u imenu ili nazivu ili identifikacijskom broju fizičke ili pravne osobe ili nazivu certifikata).
c) Utvrđene su greške u podacima u certifikatu ili na tijelu QSCD uređaja tijekom obrade zahtjeva, izdavanja certifikata, personalizacije QSCD uređaja, personalizacije aktivacijskog podatka ili drugih aktivnosti pružatelja usluga certificiranja, prije uručenja ili prihvaćanja certifikata.
d) Prijavljen je gubitak ili kvar QSCD.
e) Prijavljena je zlouporaba ili neautorizirano korištenje QSCD, privatni ključ ili aktivacijski podaci su prestali biti u isključivom posjedu osobe subjekta certificiranja ili autora pečata ili uvijek kad je moguća kompromitacija privatnog ključa. Trajno je izgubljen PIN za aktivaciju privatnog ključa za udaljeno potpisivanje ili pečatiranje izdane u sklopu servisa CERTILIA mPotpis.
f) Prijavljen je prestanak prethodno utvrđene povezanosti između osobe subjekta certificiranja i organizacije kao osobe naručitelja.
g) Utvrđen je prestanak valjanosti certifikata prije isteka perioda na koji je certifikat izdan zbog smrti osobe ili ako više ne postoji osnova po kojoj je izdan certifikat.

h) Nastupile su izvanredne okolnosti i slučaj više sile, uključujući elementarne vremenske i prirodne nepogode, odron zemlje, poplave, požar, rat, vojne operacije, terorizam, upade u fizički prostor, upade u informacijski sustav ili građanske nemire.

i) Sud, javno tužiteljstvo ili institucija koja provodi sudsku ili kriminalističku obradu zahtjeva opoziv certifikata kako bi se spriječilo kazneno djelo.

j) Utvrđeno je da privatni ključ ne odgovara javnom ključu u certifikatu ili je naknadno utvrđeno da podaci u certifikatu nisu ispravni.

k) Utvrđeno je da zahtjev za izdavanje certifikata nije bio autoriziran ili je naknadno povučen.

l) Utvrđeno je da su korisniku eOI kojem je u skladu s izmjenama i dopunama Zakona o osobnoj iskaznici (NN 144/2020) bio izdan udaljeni certifikat za potpis opozvani certifikati prije više od 45 dana ili je izdana nova eOI s novim certifikatima zbog promjene osobnog imena ili OIB-a.

m) Utvrđeno je da certifikat nije izdan u skladu s pravilnikom ili općim pravilima.

n) CA certifikat je opozvan.

CA certifikat će biti opozvan u sljedećim situacijama:

a) Obvezujućim regulatornim zahtjevom ili normom propisano je da tehnička i sigurnosna svojstva certifikata kao što su kriptografski algoritam ili duljina ključa, predstavljaju neprihvatljivi rizik za sve sudionike navedene u točki 1.3.

b) Utvrđena je kompromitacija CA privatnog ključa.

c) Ako pružatelj usluga certificiranja zbog tehničkog, ugovornog ili bilo kojeg drugog razloga prestane izdavati certifikate ili prestane pružati usluge certificiranja.

4.9.2 Tko može zahtijevati opoziv certifikata

Opoziv certifikata izdanih fizičkim osobama, može zahtijevati:

a) fizička osoba koja je imenovana kao subjekt certifikata ili njen zakonski zastupnik, zbog razloga koji su navedeni u točkama 4.9.1, a) do b), d) do g),

b) osoba naručitelj putem zakonskog zastupnika, zbog razloga koji su navedeni u točci 4.9.1, a) do b), d) do g)

c) autorizirani službenik RA/LRA, zbog razloga koji su navedeni u točkama 4.9.1, a) do g) i l)

d) autorizirano osoblje CA uz suglasnost PMA, zbog razloga koji su navedeni u točki 4.9.1, od i) do o),

e) PMA, zbog razloga koji su navedeni u točki 4.9.1 i

f) Zahtjev za opoziv CA , OCSP i TSU certifikata podnosi PMA.

Opoziv certifikata izdanih pravnim osobama, može zahtijevati:

a) autor pečata putem ovlaštenog predstavnika, zbog razloga koji su navedeni u točkama 4.9.1, a) do b), d) do g)

b) autorizirani službenik RA/LRA, zbog razloga koji su navedeni u točkama 4.9.1, a) do g),

c) autorizirano osoblje CA uz suglasnost PMA, zbog razloga koji su navedeni u točki 4.9.1 od i) do o),

d) PMA, zbog razloga koji su navedeni u točki 4.9.1,

e) zahtjev za opoziv CA , OCSP i TSU certifikata podnosi PMA.

4.9.3 Postupci kod podnošenja zahtjeva za opoziv certifikata

Primjenjuju se sljedeći postupci kod podnošenja zahtjeva za opoziv certifikata:

a) Putem portala dostupne jasne upute o postupcima koje trebaju poduzeti u slučaju nastanka razloga za opoziv certifikata navedene u 4.1.9.

b) Zahtjev za opoziv certifikata se podnosi:
   a. u uredima RA u radno vrijeme ili
   b. putem privatnog web portala po proceduri za suspenziju certifikata koja je navedena u točki 4.9.15 kontinuirano 24/7
   c. putem drugih kanala elektroničke komunikacije kojima je moguće provesti identifikaciju i potvrdu identiteta podnositelja kako je utvrđeno u točki 3.4

c) Zahtjev za opoziv certifikata će se prihvatiti samo ako je identitet podnositelja zahtjeva utvrđen sukladno pravilima za utvrđivanje identiteta prema poglavlju 3.4.

d) Odobrene zahtjeve za opoziv certifikata RA službenici unose u AKD RA sustav.

e) Zahtjevi za opoziv certifikata iz AKD RA sustava se prosljeđuju na daljnju obradu CA.

f) Opoziv CA certifikata inicira i odobrava PMA.

4.9.4 Vremenski period za podnošenje zahtjeva za opoziv

Zahtjev za opoziv certifikata treba biti podnesen u najkraćem mogućem roku od nastanka razloga za opoziv.

Ako su se promijenili podaci sadržani u certifikatu (ime, naziv, identifikacijski broj fizičke ili pravne osobe, naziv certifikata) osoba, autor pečata ili ovlašteni predstavnik su dužni zatražiti opoziv u najkraćem mogućem roku od dana nastanka promjene.

4.9.5 Vremenski period obrade zahtjeva za opoziv od strane CA

Primjenjuju se sljedeća pravila:

a) Odmah nakon što je zaprimljena informacija o pojavi razloga za opoziv certifikata, započinje istraživanje problema i u roku od 24 sata donosi se odluka o opozivu certifikata ili drugoj aktivnosti koja će se provesti.

b) Pri donošenje odluke o opozivu certifikata razmatraju se:
   - autentičnost i pouzdanost zaprimljene informacije o nastanku razloga za opoziv,
   - brojnost zahtjeva za opoziv certifikata,
   - relevantnost i autoriziranost izvora zahtjeva za opoziv,
   - zakonske obveze i
   - posljedice koje mogu nastati uslijed (ne)opoziva certifikata.

c) Ako je donesena odluka o prihvaćanju zahtjeva za opoziv, u roku od 60 minuta CA će obraditi zahtjev i objaviti informaciju o opozivu certifikata.

d) Maksimalno vrijeme koje može proteći između zaprimanja zahtjeva za opoziv certifikata i objave statusa certifikata je 24 sata.

e) Sustav za opoziv certifikata raspolaže s pouzdanim izvorom vremena i osigurava važeću zabilješku datuma i vremena koja se sinkronizira s UTC barem jedan puta dnevno.
f) CA osigurava sigurno okružje u kojem se provodi postupak opoziva certifikata u skladu s točkama 6.5, 6.6 i 6.7.
g) Certifikat koji je trajno opozvan (tj. koji nije suspendiran), ne može se reaktivirati i njegov status se više ne može promijeniti.

4.9.6 Zahtjev za provjeru statusa certifikata za pouzdajuće strane

Pouzdajuća strana treba provjeriti status certifikata prije pouzdavanja u certifikat.

Usluge za provjeru informacije o statusu certifikata dostupne su putem Interneta (sukladno točkama 4.9.9. i 4.9.10. ovog dokumenta).

Ako pouzdajuća strana zbog bilo kojih razloga u određenom trenutku ne može dobiti informacije o statusu certifikata, tada je dužna ili odbiti uporabu certifikata ili na sebe prihvatiti rizik te preuzeti odgovornosti i snositi posljedice korištenja certifikata čiji status nije potvrđen.

4.9.7 Učestalost izdavanja CRL

CRL se izdaje po sljedećim pravilima:

a) CERTILIA se obvezuje da će CRL izdati barem jednom u roku od 24 sata.
b) Nova CERTILIA CRL lista će se izdati barem 10 minuta prije isteka valjanosti prethodne CRL.
c) U redovnim uvjetima rada, CERTILIA generira i izdaje CRL svakih 12 sati.
d) Period valjanosti CERTILIA CRL je 24 sata od trenutka izdavanja CRL.
e) Za AKDCA CRL je valjanost 90 dana od trenutka izdavanja CRL.
f) U slučaju opoziva CA certifikata, CRL lista će se izdati u roku od 24 sata.
g) Ako je istekao period valjanosti certifikata koji je opozvan i koji je na CRL listi, on može biti maknut s CRL liste.
h) Kako bi se osigurala dostupnost CRL u skladu s pravilima koja su navedena u ovom poglavlju, pravovremenost izdavanja CRL se nadzire.

4.9.8 Maksimalno kašnjenje objave CRL

Maksimalno dozvoljeno kašnjenje od trenutka izdavanja CRL do trenutka objave CRL u javnom imeniku ili putem interneta je 10 minuta.

4.9.9 Dostupnost on-line provjere statusa certifikata

AKD PKI omogućava on-line provjeru statusa certifikata putem OCSP usluge.

AKD OCSP usluga dostupna je preko protokola HTTP na adresi objavljenoj u polju „Authority Information Access“ svakog certifikata.

OCSP odgovor sukladan je s IETF RFC 6960 [35] i IETF RFC 5019 [40].

4.9.10 Zahtjevi za on-line provjeru statusa certifikata

Omogućena je on-line provjera statusa certifikata putem OCSP usluge po sljedećim pravilima:

a) CERTILIA će osvježiti informacije koje se objavljuju preko OCSP barem svaka 24 sata.
b) U redovnim uvjetima rada CERTILIA će osvježiti informacije koje se objavljuju preko OCSP odmah po dobivanju zahtjeva za opoziv certifikata.
c) Valjanost odgovora usluge CERTILIA OCSP je maksimalno 24.
d) AKDCA će osvježiti informacije koje se objavljuju preko OCSP barem svakih 90 dana.
e) U slučaju opoziva certifikata podređenog CA, AKDCA će osvježiti informacije koje se objavljuju preko OCSP u roku od 24 sata.
f) Svaki odgovor OCSP usluge je elektronički potpisan certifikatom koji je izdan od istog CA koji je izdao certifikat za kojeg se traži provjera statusa certifikata.
g) Ako OCSP usluga primi zahtjev za provjeru statusa certifikata koji još nije izdan, tada neće odgovoriti sa statusom „good“.
h) Kako bi se osigurala dostupnost usluge u skladu s pravilima koja su navedena u ovom poglavlju, rad OCSP usluge se kontinuirano nadzire.

4.9.11 Ostali načini provjere

AKD osigurava provjeru statusa certifikata registriranim osobama na privatnom dijelu portala koji je dostupan putem interneta na adresi https://www.certilia.com.

AKD može ponuditi OCSP uslugu sa višom razinom dostupnosti uz ugovor i cjenik.

4.9.12 Specifični zahtjevi vezani uz kompromitaciju ključeva

CA će, sukladno poglavlju 4.9.1, opozvati certifikat ukoliko je potvrđena kompromitacija privatnog ključa.

4.9.13 Razlozi za suspenziju certifikata

Razlozi za suspenziju certifikata su:

a) Podnesen je autorizirani zahtjev za suspenziju certifikata.
b) Prijavljen je nestanak QSCD ili sumnja na prestanak isključivog posjeda privatnog ključa i/ili aktivacijskih podataka.
c) Postoji mogućnost da podneseni zahtjev za opoziv certifikata bude naknadno nakon podnošenja zahtjeva povučen.
d) Nije moguće pravovremeno podnijeti zahtjev za opoziv certifikata zbog bilo kojeg razloga navedenog u točki 4.9.1.
e) Nije moguće pravovremeno donijeti odluku o opozivu certifikata kada su posljedice koje mogu nastati uslijed neopoziva certifikata značajne.
f) U slučaju neizvršavanja ugovornih obaveza od strane primatelja usluga certificiranja.

Razlozi za povlačenje suspenzije certifikata su:

g) Podnesen je autorizirani zahtjev za povlačenje suspenzije certifikata.
h) Pronalazak QSCD ili prestanak postojanja razloga navedenih pod b).

i) Prestanak razloga zbog kojeg je tražena suspenzija certifikata.

4.9.14 Tko može tražiti suspenziju certifikata

Zahtjev za suspenziju mogu podnijeti:

a) Osobe subjekti certificiranja, odnosno njezin zakonski zastupnik ili osoba ovlašteni predstavnik ili zastupnik pravne osobe ili organizacije.
b) Ostali - bilo koja fizička ili pravna osoba putem RA.

4.9.15 Postupci kod podnošenja zahtjeva za suspenziju certifikata

Osobama su putem portala dostupne jasne upute o postupcima koje trebaju poduzeti u slučaju nastanka razloga za suspenziju certifikata koji su navedeni u 4.9.13.

Primjenjuju se sljedeća pravila:

a) Osobe subjekti certificiranja podnose zahtjev za suspenziju svoga certifikata:
   - u uredima RA u radno vrijeme ili
   - na daljinu korištenjem elektroničke on-line usluge za suspenziju certifikata.
b) Ostali podnose zahtjev za suspenziju certifikata:
   - u uredima RA u radno vrijeme.
c) Elektronička on-line usluga za suspenziju certifikata dostupna je kontinuirano 24/7. Usluzi se pristupa dvofaktorskim autentikacijskim sredstvom registriranim u CERTILIA IDP sustavu.
d) Zahtjev za suspenziju certifikata zaprimljen od subjekta certificiranja ili ovlaštenog predstavnika ili osobe ovlaštene za zastupanje će se prihvatiti samo ako je identitet podnositelja zahtjeva utvrđen sukladno pravilima za utvrđivanje identiteta prema poglavlju 3.4.
e) Zahtjev za suspenziju certifikata zaprimljen u RA uredu od bilo koje druge pravne ili fizičke osobe će se prihvatiti samo ako je podnositelj u posjedu pripadajućeg QSCD.
f) Ako zahtjev za suspenziju ne može biti potvrđen u roku od 24 sata, tada se status certifikata neće mijenjati.
g) Ako je zahtjev za opoziv odobren proslijedit će se na daljnju obradu CA.
h) Maksimalno vrijeme koje može proteći između zaprimanja zahtjeva za suspenziju ili povlačenje suspenzije certifikata i objave statusa certifikata je 24 sata.
i) Sustav za suspenziju i povlačenje suspenzije certifikata raspolaže s pouzdanim izvorom vremena i osigurava važeću zabilješku datuma i vremena koja se sinkronizira s UTC barem jednom dnevno.
j) CA osigurava sigurno okružje u kojem se provodi postupak suspenzije i povlačenja suspenzije certifikata.

4.9.16 Ograničenje na trajanje suspenzije

U slučaju prestanka razloga za suspenziju certifikata navedenih u točki 4.9.13., moguće je zahtijevati povlačenje zahtjeva za suspenziju certifikata u roku od 8 dana.

Ako u roku od 8 dana od podnošenja zahtjeva za suspenziju nije zahtijevano povlačenje suspenzije certifikata, suspendirani certifikat će biti opozvan.

4.10 Usluge provjere statusa certifikata

4.10.1 Operativna svojstva

Primjenjuju se pravila:

a) CA putem Interneta osigurava usluge provjere CRL putem HTTP te OCSP uslugu provjere statusa certifikata.
b) Informacije o opozvanim certifikatima kojima je istekao rok valjanosti (Expiry Date) brišu se s javno dostupnih CRL, ali ostaju arhivirani kod CA i dostupni putem OCSP usluge
c) Javna adresa za provjeru statusa korištenjem OCSP usluge je: https://ocsp.certilia.com.
d) Javna adresa za dohvat CRL na web poslužitelju je: https://crl.certilia.com/certilia.crl.
e) Za slučaj razlike u statusima OCSP usluge i CRL (vidi točku 4.9.7), ažurniji i točan je odgovor OCSP usluge i njega treba implementirati.

4.10.2 Dostupnost usluga

CERTILIA osigurava:

a) AKD osigurava neprekinuti rad i dostupnost svojih kritičnih usluga 24 sata na dan, 7 dana u tjednu. To obuhvaća:
   - usluga on-line zaprimanja zahtjeva za izdavanje certifikata,
   - usluge upravljanja opozivom, suspenzijom i povlačenjem suspenzije certifikata,
   - usluge provjere statusa certifikata,
   - usluge servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje,
   - usluge informiranja.
b) Odzivno vrijeme za CRL i OCSP provjeru trenutnog statusa certifikata je maksimalno 10 sekundi.
c) Kako bi se skratilo vrijeme obrade i provjere statusa certifikata preporuka je koristiti OCSP protokol.
d) U slučaju ispada sustava usluga će biti dostupna u najkraćem mogućem roku i u skladu s pozitivnim poslovnim praksama.

Ostale usluge CERTILIA dostupne su unutar radnog vremena RA ureda.

4.10.3 Opcionalna svojstva

Nije predviđeno.

4.11 Kraj korištenja certifikata

Rok valjanosti certifikata je prema poglavlju 6.3.2.
Certifikat će prestati biti valjan i prije isteka roka valjanosti ako se ranije opozove.

Ako Korisnik otkaže ugovor o certificiranju prije isteka valjanosti certifikata, AKD će opozvati sve certifikate na koje se odnosi taj ugovor.

4.12 Pohrana kod treće osobe (engl. escrow) i oporavak privatnog ključa

CA ne obavlja pohranu kod treće osobe i oporavak privatnih ključeva osoba.

4.12.1 Pohrana i oporavak privatnog ključa u servisu CERTILIA mPotpis

Privatni ključevi koji se koriste u sklopu servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje pohranjuju se u sigurnom okruženju udaljenog QSCD uređaju koji je sukladan zahtjevima *EAL4+ augmented with AVA_VAN.5* prema ISO/IEC 15408 [43] i prema pravilima definiranim u Prilogu II *Uredbe (EU) br. 910/2014 [1]*.

AKD ne omogućuje osobama oporavak privatnih ključeva koji se koriste u sklopu servisa CERTILIA mPotpis.

5 Fizičke, organizacijsko-upravljačke i provedbene mjere zaštite

5.1 Mjere fizičke zaštite

AKD ima dokumentiranu i implementiranu politiku fizičke sigurnosti i kontrolira fizički pristup svim podacima i komponentama sustava vezanim uz pružanje usluga povjerenja.

Provode se aktivnosti procjene i suzbijanja rizika, a kako bi se prevenirala oštećenja i smetnje u pružanju usluga te spriječio neovlašteni fizički pristup objektu, prostorima i informacijama, uspostavljene su sigurnosne mjere u skladu s poglavljem 11 ISO/IEC 27002 [46].

5.1.1 Lokacija objekta i konstrukcija

Informacijski sustav CA te proizvodni pogoni u kojima se izrađuje i individualizira QSCD te upravlja okružjem CERTILIA mPotpis i udaljenim QSCD uređajem za kreiranje elektroničkog potpisa i pečata smješteni su u poslovnom kompleksu AKD-a.

Objekti AKD-a su masivne konstrukcije, a vrata, glavni ulaz i ranjive točke (prozori, krovovi, ograde, prilazi za vozila i isporuku) konstruirani su tako da osiguravaju adekvatnu zaštitu od neautoriziranog pristupa.

Prema vrsti, namjeni i značaju aktivnosti koja se u njima provodi, svi prostori AKD-a su ustrojeni u sigurnosne zone: pristupna, administrativna, ograničena, djelatna i sigurna zona.

Sigurnosne zone odijeljene su fizičkim barijerama, a mjere zaštite koje se primjenjuju u sigurnosnim zonama proporcionalne su čimbenicima rizika.

CA sustavi i proizvodni pogoni su smješteni u djelatnoj i sigurnoj zoni (zone visoke sigurnosti) gdje se primjenjuju najstrože fizičke, tehničke i proceduralne mjere zaštite.

5.1.2 Fizički pristup

Implementirane su sofisticirane mjere tehničke zaštite koje osiguravaju zaštitu perimetra i unutarnjih prostora. Mjere zaštite uključuju fizičke barijere, video nadzor, kontrolu pristupa, sustav protupožarne zaštite i protuprepadna zaštita.

Zaštitari su stalno prisutni na objektu 7/24, a cijeli poslovni kompleks AKD-a, neprekidno je nadziran iz centralnog nadzornog sustava 7/24.

Svi informacijski sustavi koji su funkciji pružanja usluga smješteni su u računalnoj sobi u zoni visoke sigurnosti, a pristup prostorima je ograničen na ovlašteno osoblje koje obavlja administratorske aktivnosti i nadzor.

Kontrola pristupa objektima i prostorima AKD-a ostvaruje se korištenjem ID kartice.

Fizički pristup zonama visoke sigurnosti ostvaruje se primjenom biometrijskih metoda za identifikaciju osoba.

Fizički pristup informacijskoj opremi CA sustava ostvaruje se isključivo uz dvojnu kontrolu.

Informacijski sustav tehničke zaštite bilježi sve aktivnosti korištenja prava pristupa kao i sve promjene na sustavu kontrole pristupa.

Postupci dodjeljivanja prava pristupa prostorima provode se sukladno dokumentiranim internim pravilima.

5.1.3 Sustavi za klimatizaciju i napajanje

Prostor računalne sobe u kojoj je smještena informacijska infrastruktura propisno je klimatiziran. Sva oprema spojena je na izvor neprekinutog napajanja, a za slučaj prestanka napajanja gradske energetske mreže na duži period od 48 sati osiguran je i agregat rezervnog napajanja.

Sustav za klimatizaciju i napajanje se nadzire i redovito održava, a kapaciteti sustava su dostatni za provedbu operativnih poslova.

5.1.4 Opasnost od poplave

Objekti i prostori u kojima se smješta informacijska infrastruktura i u kojima se odvijaju aktivnosti pružanja usluga certificiranja smješteni su na mjestu koje je osigurano od poplave.

5.1.5 Protupožarna zaštita

U prostoru sigurne zone implementirane su odgovarajuće mjere zaštite od požara sukladno važećoj zakonskoj regulativi.

Sustav protupožarne zaštite čine:

a) automatizirani sustavi za dojavu i gašenje požara
b) vatrogasni aparati za gašenje početnih požara
c) hidrantska mreža i
d) pomoćna oprema i pomagala za evakuaciju i spašavanje.

5.1.6 Pohrana medija

Svi mediji su propisno označeni i pohranjeni u sigurnosne spremnike, a postupanje s medijima je definirano internim sigurnosnim pravilima.

Fizički pristup sigurnosnim spremnicima i svoj fizičkoj opremi povezanoj s kriptografskim aktivnostima kao što su mediji, kriptografski uređaji, fizički ključevi, pametne kartice, tokeni, zaporke i sl. ostvaruje se isključivo uz dvojnu kontrolu.

Kako bi se spriječilo neautorizirano otkrivanje, modifikacija, premještanje ili uništavanje informacija koje su pohranjeni na medijima, uspostavljene su sigurnosne mjere u skladu s poglavljem 8 ISO/IEC 27002 [46].

5.1.7 Uništavanje uređaja i medija

Svi tiskani i elektronički mediji za koje ne postoji potreba arhiviranja na siguran način se uništavaju metodama koje osiguravaju razumnu pouzdanost da se uništeni podaci ne mogu povratiti.

Uništavanje kriptografskih medija vrši se komisijski uz prisutnost najmanje 2 osobe.

Uništavanje fizičke opreme koja je povezana s kriptografskim aktivnostima provodi se korištenjem rezačica.

Sigurnosna razina rezačica koje se koriste za uništavanje određuje se prema stupnju tajnosti podataka za koje se koristi, a koja se određuje prema internim procedurama.

5.1.8 Sigurnosne kopije na drugoj lokaciji

Sigurnosne kopije se čuvaju na dvije odvojene lokacije te na izdvojenoj lokaciji u prostorima i sigurnosnim spremnicima koji udovoljavaju jednakim ili višim sigurnosnim zahtjevima.

5.2 Organizacijsko-upravljačke mjere zaštite

5.2.1 Povjerljive uloge

Ovlaštenim radnicima koji sudjeluju u provedbi aktivnosti certificiranja dodijeljene su odgovarajuće povjerljive uloge s jasno definiranim odgovornostima i ovlaštenjima u skladu s normama ETSI EN 319 401 [13], CEN TS 419 261 [31] i ETSI TS 119 431-1 [23] odnosno CEN EN 419 241-1 [32].

Povjerljive uloge uključuju ali se ne ograničavaju na:

a) **Administratori sigurnosti:** Odgovorni za implementaciju i provedbu sigurnosnih pravila u praksi.
b) **RA službenici**: Osobe odgovorna za provjeru informacija i pripremu podataka koja se nužno provodi pri izdavanju certifikata i odobrenje zahtjeva za izdavanje certifikata.
c) **Službenici za opoziv**: Odgovorni za provedbu zahtjeva za promjenu statusa certifikata.
d) **Administrator informacijskog sustava**: Odgovorni za instalaciju, konfiguraciju i održavanje informacijskih sustava
e) **Operateri**: Odgovorni za provedbu dnevnih aktivnosti na informacijskim sustavima te za spas i povrat podataka kada je to potrebno.
f) **Kontrolori**: Odgovorni za dnevni pregled izvještaja o radu sustava, revizijskih zapisa i arhive kada je to potrebno.

Povjerljive uloge vezane uz upravljanje kriptografskim ključevima su:

g) **Koordinatori kriptografskih ključeva**: Odgovorni za sve aktivnosti vezane uz upravljanje kriptografskim ključevima.
h) **Skrbnici kriptografskih ključeva**: Odgovorni za čuvanje komponenti kriptografskih ključeva i drugih sigurnosnih materijala i medija koji su im povjereni.

5.2.2 Broj osoba potrebnih za obavljanje aktivnosti

Kako bi se zaštitile sigurnosno osjetljive funkcije i informacije strogo se poštuju načela:

a) Dijeljenog znanja: Svaka od dvije ili više različitih osoba raspolaže samo s jednom komponentom podatka (npr. kriptografskog ključa) tako da niti jedna osoba samostalno se može pristupiti ili koristiti podatak.
b) Dvojna kontrola: Dvije ili više različitih osoba moraju provoditi neku aktivnost zajedno tako da niti jedna osoba ne može samostalno provoditi sigurnosno osjetljivu funkciju.

Princip dvojne kontrole primjenjuje se na logičkoj i fizičkoj razini.

5.2.3 Identifikacija i potvrđivanje identiteta za svaku ulogu

Sva informacijska oprema konfigurirana je tako da forsira strogo poštivanje dokumentiranih internih sigurnosnih pravila te onemogućava provedbu aktivnosti bez prethodne autentikacije ovlaštenih osoba.

Autentikacija se ostvaruje najmanje korisničkim računom i zaporkom, a uvijek kada je to potrebno ili kada je tehnički podržano forsira se primjena više faktorske autentikacije.

Identifikacija i autentikacija RA službenika i CA osoblja odvija se prema pravilima:

Provjera RA:

a) Prije dodjeljivanja zaduženja službenicima RA provodi se provjera te nedvojbeno utvrđivanje identiteta i pouzdanosti službenika.
b) U postupku autentikacije službenika na informacijskom sustavu AKD RA koristi se dvofaktorska autentikacija identifikacijskim certifikatom na pametnoj kartici izdanim sa CERTILIA sustava.
c) Kako bi se spriječio sukob interesa, osoba naručitelj ili osoba subjekt certificiranja i službenik RA ne smije biti ista osoba. Službenik RA koji zahtjeva certifikat ne smije identificirati sam sebe niti unositi zahtjev za izdavanje vlastitog certifikata u informacijski sustav RA.

Provjera CA:

a) Pri dodjeljivanju povjerljivih uloga osoblju CA, provjerava se jesu li kandidati pouzdani i prikladni i jesu li u stalnom radnom odnosu kod CA.
b) Tijekom ceremonije generiranja CA ključa javni bilježnik provodi službeni postupak identifikacije svih sudionika ceremonije uz fizičku prisutnost osobe temeljem predočenog dokumenta.
c) Kada se izdaju certifikati za CA, TSU ili OCSP uslugu, u suradnji s ljudskim resursima provjerava se je li skrbnik kriptografskog ključa u stalnom radnom odnosu kod CA.
d) Pristup informacijskom sustavu CA omogućen je isključivo uz dvojnu kontrolu.
e) Softverski modul koji automatizirano prikuplja, provjerava i šalje zahtjeve na obradu, autenticira se informacijskom sustavu CA korištenjem SSL/TLS klijent autentikacije.

5.2.4 Uloge koje zahtijevaju odvajanje zaduženja

Pri dodjeli povjerljivih uloga strogo se poštuju principi segregacije zaduženja kako bi se spriječio potencijalni sukob interesa i zlouporaba ovlasti.

Primjenjuju se pravila:

a) Osoba koja se autenticira kao administrator sigurnosti ili službenik za opoziv ili RA službenik ne smije imati ovlasti kontrolora.
b) Osoba koja se autenticira kao administrator informacijskog sustava ili operater ne smije imati ovlasti kontrolora ili administratora sigurnosti.
c) Osoba koja se autenticira kao RA službenik ili kontrolor ne smije imati ovlasti administratora sigurnosti, administratora informacijskog sustava ili operatera.

d) Administrator sigurnosti, administrator informacijskog sustava ili operater smije imati prava čitanja revizijskih zapisa koja su dodijeljena kontroloru ako je to potrebno.

5.3 Osoblje

5.3.1 Kvalifikacije, radno iskustvo i sigurnosne provjere

Pri zapošljavanju radnika AKD provodi strogi selekcijski postupak, a standardna procedura zapošljavanja uključuje provjeru:

a) stručne spreme i profesionalnih kvalifikacija,
b) prethodnih zaposlenja,
c) evidencija o kažnjavanju,
d) zdravstvene sposobnosti i
e) kreditne/financijske sposobnosti sukladno zakonskim propisima.

Svi radnici su potpisali ugovor o radu te su se obvezali da će poštivati utvrđena sigurnosna pravila.

Članovi PMA i svi ovlaštenici kojima je dodijeljena povjerljiva uloga i koji sudjeluju u provedbi aktivnosti CA su u stalnom su radnom odnosu s AKD-om i nisu u poslovnom odnosu s drugim pružateljima usluga certificiranja.

5.3.2 Postupak provjere prikladnosti radnika za korisničku ulogu

Pri dodjeljivanju uloga i odabiru radnika koje će sudjelovati provedbi aktivnosti certificiranja provodi se službeni postupak procjene prikladnosti radnika za određenu ulogu prema unaprijed definiranim kriterijima.

Radniku neće biti povjerena provedba aktivnosti certificiranja ako je utvrđena neka od sljedećih činjenica:

a) lažno predstavljanje ili falsifikacija podataka,
b) nepovoljni ili nepouzdani podaci o stručnoj spremi i profesionalnim kvalifikacijama,
c) utvrđena kriminalna aktivnost ili pravomoćna osuda,
d) nedostatak financijske odgovornosti,
e) postupanje protivno internim sigurnosnim pravilima.

Pri odabiru radnika za uloge vezane uz upravljanje kriptografskim ključevima strogo se vodi računa da su radnici zaposleni u različitim organizacijskim jedinicama AKD-a.

5.3.3 Zahtjevi za obukom

Svi radnici kojima je dodijeljena povjerljiva uloga i koji sudjeluju u provedbi aktivnosti CA imaju odgovarajuću stručnu spremu, znanja i iskustvo potrebno za izvršavanje povjerene im uloge.

AKD osigurava potrebna ekspertna znanja, iskustvo i kvalifikacije vezane uz poznavanje koncepata PKI infrastrukture, kriptografskih algoritama i uređaja te uz informacijsku sigurnost.

AKD osigurava stručno usavršavanje svojih radnika kako bi se stekla odgovarajuća znanja potrebna za obavljanje poslovne funkcije radnika.

Pored navedenog, radnici koji sudjeluju u provedbi aktivnosti certificiranja su primjereno informirani o pravilima rada prije nego preuzmu svoje obveze.

Cilj informiranja je:

a) osigurati razumijevanje sigurnosnih zahtjeva i internih sigurnosnih pravila,
b) osigurati svjesnost radnika o svojoj ulozi i odgovornostima u poslovnom procesu,
c) omogućiti prepoznavanje sigurnosnih problema i incidenata te reagiranje u skladu s potrebama poslovne funkcije te
d) osigurati provedbu plana neprekinutosti poslovanja.

5.3.4 Periodična obnova znanja i obuka

Program stručnog usavršavanja radnika provodi se kontinuirano, a posebno kod značajnih promjena.

Informiranje radnika o pravilima rada provodi se prilikom uvođenja novih internih pravila i kod značajnijih promjena, a najmanje jednom godišnje.

5.3.5 Periodična rotacija i provjera radnika

Radnici kojima su dodijeljene povjerljive uloge vezane uz upravljanje kriptografskim ključevima su svake tri godine podvrgnuti ponovnoj procjeni prikladnosti prema poglavlju 5.3.2.

5.3.6 Sankcije

Prema radnicima koji ne postupaju sukladno utvrđenim i dokumentiranim procedurama primjenjuje se strogi disciplinski postupak.

5.3.7 Zahtjevi za vanjske suradnike

Vanjski suradnici ne sudjeluju u provedbi aktivnosti CA i nisu im dodijeljene povjerljive uloge.

Zahtjevi za posjetitelje, konzultante i vanjske suradnike koji sudjeluju u provedbi održavanja sustava opisani su internim procedurama.

5.3.8 Dokumentacija dostupna radnicima

Svim radnicima koji sudjeluju u provedbi aktivnosti CA dostupna je dokumentacija potrebna za obavljanje svakodnevnih radnih zadataka, koja uključuje interna sigurnosna pravila, procedure i radne upute kao i specifične upute proizvođača za administriranje i održavanje sustava.

5.4 Upravljanje revizijskim zapisima

5.4.1 Tipovi događaja koji se zapisuju

Revizijski zapisi su u pravilu dostupni u elektroničkom obliku, a informacijski sustavi ih kreiraju automatski. Tamo gdje nije moguće osigurati revizijske zapise u elektroničkom obliku, osigurani su pisani dokazi o ispunjenju sigurnosnih zahtjeva koji su navedeni u ovome dokumentu.

Tipovi revizijskih zapisa su:

a) zapisi o upravljanju životnim ciklusom certifikata što uključuje, ali se ne ograničava na
   - registracija korisnika,
   - autentikacija korisnika na elektroničku on-line uslugu za zaprimanje zahtjeva za izdavanje certifikata,
   - izdavanje certifikata na QSCD uređaju u posjedu,
   - priprema podataka i izrada QSCD,
   - dostavu registracijskih kodova i podataka i aktivacijskih podataka e-mailom ili SMS,
   - autentikaciju korisnika na servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje,
   - izdavanje certifikata na udaljenom QSCD uređaju u sklopu servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje,
   - opoziv, suspenzija, povlačenje suspenzije certifikata i
   - izdavanje i objava OCSP.
b) zapisi o postupcima upravljanja kriptografskim ključevima u CERTILIA sustavima i servisu CERTILIA mPotpis što uključuje, ali se ne ograničava na
   - generiranje,
   - aktivaciju,
   - korištenje,
   - učitavanje,
   - pohranu,
   - oporavak i
   - uništavanje.
c) zapisi o administriranju i održavanju sustava što uključuje, ali se ne ograničava na
   - pokretanje i zaustavljanje aplikacija,
   - praćenje rada sustava (upozorenja, alarmi, zastoji, greške, korištenje resursa i sl.),
   - promjene konfiguracija kritičnih sustava,
   - spas i povrat podataka,
   - prava pristupa podacima i sl.

Revizijski zapisi su dostatni kako bi se mogao provoditi nadzor odnosno kako bi se neovlaštena uporaba informacijskog sustava mogla adekvatno istražiti ako za to nastane potreba.

Revizijski zapisi sadržavaju najmanje sljedeće podatke:

- identifikacija korisnika,

- tip događaja,
- datum i vrijeme događaja,
- uspješne i neuspješne događaje,
- ishodište događaja i
- podatke, komponente sustava ili resurse kojima se pristupilo.

5.4.2 Učestalost obrade revizijskih zapisa

Pohrana, zaštita i obrada revizijskih zapisa provodi se u realnom vremenu uz automatsko alarmiranje pojave sigurnosnih događaja za sve kritične aktivnosti.

Za manje kritične aktivnosti provodi se periodična kontrola.

5.4.3 Period čuvanja revizijskih zapisa

Revizijski zapisi za sve kritične sustave su kopirani, zaštićeni i sačuvani najmanje tri mjeseca on-line.

Revizijski zapisi vezani uz aktivnosti administriranja i održavanja sustava čuvaju se najmanje jednu godinu.

Revizijski zapisi vezani uz upravljanje životnim ciklusom certifikata i upravljanje kriptografskim ključevima arhiviraju se u skladu s pravilima arhiviranja koja su opisana u poglavlju 5.5.

5.4.4 Zaštita revizijskih zapisa

Revizijski zapisi su adekvatno zaštićeni i vjerodostojni te se mogu prezentirati kao materijalni dokazi u kasnijim eventualnim sudskim postupcima. To uključuje barem sljedeće zaštitne mehanizme:

a) Svi sistemski satovi i vremena su međusobno usklađeni, kako bi revizijski zapisi sadržavali važeću zabilješku datuma i vremena.
b) Povjerljivi podaci su izuzeti ili su maskirani tako da nisu sadržani u revizijskom zapisima.
c) Implementirana je kriptografska zaštita izvornosti svih kritičnih revizijskih zapisa od bilo kakve vrste modifikacije ili brisanja.
d) Spriječen je neautorizirani pristup revizijskim zapisima.
e) Omogućena je konfiguracija sustava koja će deaktivirati centralizirani sustav upravljanja revizijskim zapisima.
f) Administratori sustava ne smiju mijenjati ili brisati manje kritične revizijske zapise koji nisu uključeni u sustav upravljanja revizijskim zapisima.

5.4.5 Sigurnosne kopije revizijskih zapisa

Utvrđene su redovite i automatizirane aktivnosti vezane uz izradu sigurnosnih kopija revizijskih zapisa.

Primjenjuju se različite metode izrade sigurnosnih kopija na dnevnoj, tjednoj, kvartalnoj odnosno godišnjoj osnovi.

Postupak povrata podataka iz sigurnosnih kopija je poznat, testiran i pouzdan te osigurava povrat podataka u razumnom vremenu.

5.4.6 Prikupljanje revizijskih zapisa

Uspostavljen je sustav upravljanja revizijskim zapisima (engl. *Log Management System*) koji provodi automatsku pohranu, zaštitu i obradu revizijskih zapisa u realnom vremenu.

Revizijski zapisi svih kritičnih sustava uključeni su u sustav upravljanja revizijskim zapisima dok se manje kritični zapisi prikupljaju ručnim ili djelomično ručnim postupcima.

5.4.7 Obavješćivanje i alarmiranje

Sustav upravljanja revizijskim zapisima provodi automatsku obradu revizijskih zapisa u realnom vremenu i automatski alarmira u slučaju pojave sigurnosnih događaja za sve kritične aktivnosti.

AKD će, samo ako postoji potreba, obavijestiti subjekte koji su uzrokovali bilježenje revizijskog zapisa informacijskom sustavu.

5.4.8 Procjena ranjivosti sustava

Analiza ranjivosti sustava provodi se korištenjem odobrenih softverskih alata i to za sve informacijske sustave u zonama visoke sigurnosti.

Vanjska analiza ranjivosti provodi se periodički, a interna analiza se provodi prilikom značajnih promjena konfiguracije.

Odmah po otkrivanju ranjivosti poduzimaju se aktivnosti za njihovo rješavanje.

5.5 Arhiviranje zapisa

5.5.1 Tipovi zapisa koji se arhiviranju

Arhiviraju se sve aktivnosti upravljanja životnim ciklusom certifikata što uključuje, ali se ne ograničava na:

a) podatke o osobama prikupljena u postupku registracije i pripadna dokumentacija,
b) certifikate i podatke o postupcima obrade zahtjeva za izdavanje certifikata,
c) podatke o postupcima izrade, distribucije i uručenja QSCD,
d) podatke o postupcima izrade i distribucije registracijskih i aktivacijskih podataka,
e) podatke o postupcima autentikacije na elektroničku on-line uslugu za zaprimanje zahtjeva za izdavanje certifikata,
f) podatke o postupcima autentikacije na elektroničku on-line uslugu za upravljanje certifikatima,
g) podatke o postupcima registracije i upotrebe certifikata i aktivacije privatnih ključeva servisa CERTILIA mPotpis,
h) evidenciju opozvanih certifikata i podatke o postupcima obrade zahtjeva za opoziv, suspenzije i povlačenje suspenzije certifikata,
i) podatke o izdavanju i objavi OCSP,
j) revizijske zapise vezane uz upravljanje životnim ciklusom certifikata,
k) revizijske zapise vezane uz upravljanje kriptografskim ključevima.

5.5.2 Period čuvanja arhiviranih zapisa

Svi arhivirani podaci i dokumentacija navedena u poglavlju 5.5.1 čuva se najmanje 7 godina nakon isteka valjanosti certifikata.

5.5.3 Zaštita arhive

Primjenjuju se sljedeće mjere zaštite:

a) Arhivski mediji su pohranjeni na adekvatno osigurano mjesto, a pravo pristupa arhivskim podacima ograničeno je na samo ovlaštene osobe.
b) Implementirana je zaštita izvornosti zapisa od bilo kakve vrste modifikacije kao što su kriptografska zaštita i pohrana na medije s jednokratnim pisanjem.
c) Implementirane su mjere zaštite medija od brisanja, a također se izrađuju najmanje 2 kopije medija koje se pohranjuju na različitim lokacijama.
d) Mediji s arhivskim podacima se povremeno provjeravaju te prepisuju na drugi medij kako bi se osigurala zaštite od starenja ili tehnološkog zastarijevanja.

AKD kao stvaratelj i imatelj javnoga arhivskog i registraturnoga gradiva postupa u skladu s odredbama Zakona o arhivskom gradivu i arhivima (NN 61/2018).

5.5.4 Postupci izrade sigurnosnih kopija arhive

Postupci izrade sigurnosnih kopija arhive provode se u štićenom prostoru, a sigurnosne kopije arhive se čuvaju na drugoj lokaciji.

5.5.5 Zahtjevi za zaštitu zapisa vremenskim žigom

Nije primjenjivo.

5.5.6 Prikupljanje arhivske građe

Prikupljanje arhivske građe vrši se interno.

Prikupljanje i arhiviranje podataka i dokumentacije koja nastaje u postupku registriranja osoba u vanjskim RA regulirano je ugovorom.

5.5.7 Postupci dobivanja i provjere arhiviranih podataka

Postupcima dobivanja podataka iz arhive upravlja stručno osposobljen radnik zadužen za pismohranu.

Provjera podataka iz arhive vrši se u ovisnosti o primijenjenoj metodi zaštite izvornosti podataka.

5.6 Promjena ključa

Prije isteka perioda valjanosti CA certifikata certifikacijsko tijelo će prestati izdavati certifikate, promijeniti CA ključ i početi izdavati certifikate koristeći novi promijenjeni CA ključ.

Promjena CA ključa će se planirati i provesti pravovremeno vodeći računa:

- da period valjanosti svakog izdanog certifikata uvijek bude kraći od perioda valjanosti CA certifikata koji ga je izdao i
- da su kriptografski algoritmi i parametri uvijek prikladni za korištenje i u skladu s preporukama ETSI TS 119 312 [21].

Postupak promjene CA ključa provodi se po proceduri generiranja ključa koja je navedena u točki 6.1.1.

Novi CA ključ će biti dostupan svim sudionicima postupka certificiranja na način koji je opisan u točki 6.1.4.

Svi sudionici postupka certificiranja će biti informirani o generiranju novog para ključa CA, a novi CA certifikat će im biti dostavljen na način na koji se dostavlja postojeći CA certifikat, a koji je opisan u točki 6.1.4.

Pružatelj usluga povjerenja će voditi računa da postupak generiranja novog para CA ključeva ne uzrokuje neugodnosti ili zastoje osobama, pouzdajućim stranama i ostalim sudionicima koji su povezani s pružanjem usluga certificiranja.

5.7 Kompromitacija i oporavak

5.7.1 Incidenti i postupci u slučaju kompromitacije

AKD ima definiran i dobro dokumentiran poslovni proces i propisane formalne odgovornosti kako bi se osigurala brza i učinkovita reakcija u slučaju pojave incidenta.

Incidenti koji se bilježe i obrađuju obuhvaćaju kvarove računalnih resursa, softvera i/ili podataka, a u slučajevima kada je došlo do kompromitacije računalnih resursa, softvera i/ili podataka incidenti se klasificiraju i tretiraju kao sigurnosni događaji po definiranoj internoj proceduri.

5.7.2 Kvarovi računalnih resursa, softvera i/ili podataka

Kvarovi računalnih resursa, softvera i/ili podataka koji se bilježe i obrađuju obuhvaćaju, ali se ne ograničavanju na:

- zatajenje hardverske opreme i softvera,
- nepravilnosti u radu,
- preopterećenja kapaciteta ili degradacija usluge,
- ranjivosti i detektirane slabosti sustava,
- nedostupnost servisa, mreže ili aplikacije i sl.

AKD ima uspostavljen informacijski sustav koji upravlja incidentima tako da su osigurani dokazi da se incidenti bilježe i da se na njih pravovremeno i na adekvatan način reagira.

Postupak upravljanja incidentima provodi se kroz sljedeće faze: prijava, klasifikacija, eskalacija, istraživanje, rješavanje i zatvaranje incidenta.

Postupci rješavanja incidenta uključuju oporavak sustava, povrat podataka iz sigurnosnih kopija te zamjenu opreme kada je to potrebno.

5.7.3 Postupanje u slučaju kompromitacije

U slučajevima kada je došlo do kompromitacije računalnih resursa, softvera i/ili podataka provode se postupci obrade sigurnosnih događaja u skladu s internim sigurnosnim pravilima.

U slučaju da je došlo do kompromitiranja ključa CA postupa se na sljedeći način:

a) prestaje s izdavanjem certifikata na kompromitiranom CA sustavu,
b) pokreće se postupak opoziva CA certifikata,
c) pokreće se postupak opoziva certifikata osoba koje je izdao kompromitirani CA,
d) informiraju se osobe i pouzdajuće strane putem portala,
e) informiraju se nadležna državna i nadzorna tijela i ostale zainteresirane strane,
f) u slučaju sumnje da postoje elementi kaznenog djela izvješćuje se policija radi pokretanje istražnog postupka i
g) pokreće se postupak generiranja novog CA ključa.

5.7.4 Upravljanje kontinuitetom poslovanja

AKD ima uspostavljene, dokumentirane, implementirane i održavane planove i procedure kako bi se osigurao kontinuitet poslovanja u slučaju zastoja u radu IT sustava, kao i u slučaju prirodnih katastrofa, nesreća, velikih kvarova opreme i namjernih akcija.

Svi radnici koji imaju definiranu ulogu i odgovornost za kontinuitet poslovanja upoznati su sa svojim funkcijama i zaduženjima vezanim uz provođenje plana oporavka.

Plan neprekinutosti poslovanja uključuje procedure za postupanje u hitnim situacijama i plan oporavka sustava.

Sigurnosne mjere koje se poduzimaju su u skladu s implementiranim i prihvaćenim normama sustava upravljanja.

AKD osigurava visoku dostupnost i neprekinuto odvijanje aktivnosti za slijedeće usluge:

- usluge upravljanja opozivom certifikata,
- usluge provjere statusa certifikata,
- usluge informiranja i
- usluge servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje.

5.8 Prestanak rada

U slučaju prestanka rada odnosno pružanja usluga povjerenja AKD će postupiti sukladno odredbama Zakona o provedbi *Uredbe (EU) br. 910/2014* [2] i konzultirati nadležna tijela o daljnjim postupcima koji će se poduzeti najmanje tri mjeseca prije planiranog prestanka pružanja usluga povjerenja.

Postupci prestanka rada, ovisno o prestanku pružanja usluga povjerenja ili pojedine usluge ili servisa u sklopu pružanja usluga povjerenja će uključivati najmanje:

a) informiranje korisnika i pouzdajućih strana o mogućem planiranom prestanku pružanja usluga certificiranja ili pojedine usluge ili servisa ili servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje,
b) osigurati nastavak obavljanja usluga povjerenja kod drugog pružatelja usluga povjerenja uz razuman napor, ako je moguće,
c) ukidanje autorizacija i otkazivanje ugovora,
d) predaju prikupljene dokumentacije i arhivske građe,

e) prestanak izdavanja certifikata ili pružanja pojedine usluga ili rada servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje.

f) propisno uništenje kriptografskih ključeva i podataka.

6 Tehničke mjere zaštite

6.1 Generiranje i dostava para ključeva

6.1.1 Generiranje ključeva

Vrijede pravila:

a) Postupak inicijalnog generiranja para CA ključeva provodi se službenom ceremonijom generiranja CA ključeva koju organizira i nadzire PMA.
b) Ceremonija se provodi u fizički sigurnom okružju u zoni visoke sigurnosti prema definiranoj proceduri i unaprijed pripremljenoj tehničkoj skripti.
c) Ceremoniji prisustvuju radnici kojima su povjerene uloge (poglavlje 5.2), interni i vanjski revizori, javni bilježnik te ostali pozvani svjedoci.
d) Prije početka ceremonije u nazočnosti javnog bilježnika provodi se službena identifikacija osoba te dodjela uređaja, sigurnosnih omotnica i obrazaca za pohranu.
e) Postupak generiranja CA ključa provodi se prema unaprijed pripremljenoj tehničkoj skripti koja uključuje kontrolu opreme, kablova, sigurnosnih postavki i parametara opreme te svaku komandu koja se tijekom provedbe postupka unosi u informacijski sustav.
f) Ceremonija uključuje izradu sigurnosnih kopija CA ključeva i drugih podataka te pohranu kriptografskih materijala i drugih sadržaja na definirane lokacije.
g) Tijekom ceremonije ovjeravaju se evidencije sadržaja sefova u kojima su pohranjeni kriptografski materijali na primarnim i backup lokacijama.
h) Tijekom ceremonije interni i vanjski revizori ovjeravaju tehničku skriptu te ispis certifikata CA (s javnim ključem) kojom potvrđuju da je postupak generiranja ključa korektno obavljen i da je osigurana izvornost generiranih ključeva.
i) Po završetku ceremonije javni bilježnik ovjerava zapisnik o provedbi ceremonije s potvrđenim identitetom i izjavama sudionika.
j) Ovjerena tehnička skripta s potpisima svih sudionika ceremonije, ispis CA certifikata, zapisnik o provedbi ceremonije te video zapis ceremonije generiranja CA ključa pohranjuju se u arhivi.
k) Postupak generiranja ključeva osoba i certifikata za elektronički pečat i njihov unos u QSCD vrši proizvođač u fizički sigurnom okružju u zoni visoke sigurnosti.
l) CA ključevi kao i ključevi osoba se generiraju, koriste i čuvaju u HSM modulu koji implementira norme i upravljačke funkcije kako je navedeno u poglavlju 6.2.1.
m) Ključevi certifikata za udaljeni potpis i udaljeni pečat se generiraju, čuvaju i koriste u HSM modulu koji implementira norme i upravljačke funkcije kako je navedeno u poglavlju 6.2.1., u sigurnom okruženju CERTILIA mPotpis servisa za kreiranje udaljenog elektroničkog potpisa i pečata u ime potpisnika i autora pečata.
n) Pri generiranju ključeva vodi se računa da su kriptografski algoritmi i parametri uvijek prikladni za korištenje i u skladu s preporukama ETSI TS 119 312 [21].

6.1.2 Dostava privatnog ključa osobama

QSCD s privatnim ključevima osoba otpremaju se u RA po završetku proizvodnog procesa, gdje se uručuje osobi subjektu certificiranja ili ovlaštenom predstavniku autora pečata nakon utvrđivanja identiteta neposrednom identifikacijom u fizičkoj prisutnosti osobe. QSCD s privatnim ključevima može se uručiti osobi subjektu certificiranja ili ovlaštenom predstavniku autora pečata dostavnom službom uz osiguranje dokaza o provedenom utvrđivanju identiteta neposrednom identifikacijom u fizičkoj prisutnosti osobe.

U slučaju kada se generiraju privatni ključevi za potrebe udaljenog elektroničkog potpisa ili udaljenog elektroničkog pečata, u sklopu servisa CERTILIA mPotpis, privatni ključevi se ne dostavljaju osobama već se čuvaju na siguran način u sigurnom okružju u zoni visoke sigurnosti. Fizička osoba ili autor pečata (njegov ovlašteni predstavnik) pristupaju servisu CERTILIA mPotpis koji uspostavljenim mehanizmima osigurava isključivu kontrolu osobe nad privatnim ključem.

Isključiva kontrola nad privatnim ključem i njegova aktivacija provodi se postupkom:

a) Uspješno zaprimljeni referentni i autorizacijski kodovi za preuzimanje certifikata za udaljeno potpisivanje ili pečatiranje i generirani u CA temeljem zahtjeva u AKD RA,
b) Uspješna prijava na servis CERTILIA mPotpis dvofaktorskim sredstvom autentikacije registriranim u CERTILIA IDP sustavu,
c) Uspješna registracija certifikata u servisu CERTILIA mPotpis unosom referentnog i autorizacijskog koda te postavljanjem PIN-a za aktivaciju privatnog ključa za potpisivanje ili pečatiranje
d) Aktivacija i potvrda kontrole nad ključem postavljenim PINom u servisu CERTILIA mPotpis.
e) Primjenjuju se postupci, mehanizmi i kontrole opisane u poglavlju 6.2.8.1 ovog dokumenta.

6.1.3 Dostava javnog ključa CA-u

Odmah po generaciji ključeva osoba, proizvođač ili CERTILIA mPotpis servis pribavlja certifikat od CERTILIA korištenjem elektroničke usluge.

Proizvođač ili CERTILIA mPotpis servis šalje javni ključ osobe korištenjem PKCS#10 formata zahtjeva, a CERTILIA ga vraća u sklopu izdanog certifikata.

Autentikacija proizvođača i CERTILIA mPotpis servisa obavlja se korištenjem klijentskog certifikata, a kako bi se osigurala zaštita cjelovitosti i izvornosti javnog ključa koristi se siguran komunikacijski kanal (SSL/TLS).

6.1.4 Dostava javnog ključa CA pouzdajućim stranama

Javni ključevi AKDCA Root i CERTILIA su dostupni u certifikatima na portalu (vidi poglavlje 2.2).

Provjera izvornosti CA certifikata provodi se korištenjem sažetka certifikata koji je dostupan na portalu, a koji se na zahtjev pouzdajuće strane može i dostaviti sigurnim kanalom.

6.1.5 Duljine ključeva

AKDCA Root ključevi su duljine 4096 bita, RSA algoritam.

Ključevi OCSP usluge su duljine 3072 bita, RSA algoritam.

Ključevi certifikata koji se izdaju sa CERTILIA sustava su duljine 384 bita, ECDSA P-384 algoritam. Iznimno, ključevi certifikata koji se, najdulje do 31.12.2026.g., izdaju fizičkim osobama na AKD eID Card 1.0 su duljine 2048 bita, RSA algoritam.

6.1.5.1 Duljine ključeva u servisu mPotpis

Ključevi certifikata koji se izdaju sa CERTILIA sustava i koriste u sklopu servisa mPotpis za udaljeno potpisivanje i pečatiranje su duljine 348 bita, ECDSA P-384 algoritam.

Jednokratni transportni ključevi za prijenos SAD podataka za aktiviranje privatnog ključa su duljine 256 bita, ECDH protokol.

Duljine ostalih ključeva koji se koriste u CERTILIA mPotpis servisu opisani su u poglavlju 6.2.8.1.

6.1.6 Generiranje i provjera kvalitete parametara javnog ključa

CA ključevi, ključevi OSCP kao i ključevi osoba generirani su korištenjem generatora slučajnih brojeva na HSM uređaju. Parametri javnog ključa za RSA i ECDSA algoritme su u skladu s normom FIPS 186-4 [42] ili drugom ekvivalentnom normom koju odobri PMA.

Općenito, za generaciju CA ključeva i ključeva osoba koriste se kriptografski algoritmi i parametri u skladu s preporukama ETSI TS 119 312 [21].

6.1.7 Namjena ključeva (po X.509 v3 polju uporabe ključa)

Izdaju se X.509 v3 certifikati u skladu s IETF RFC 5280 [38], a njihova namjena definirana je kroz vrijednost polja „keyUsage“.

Za CA certifikate „keyUsage“ je: Certificate Signing, Off-line CRL Signing, CRL Signing.

Za OCSP certifikate „keyUsage“ je: Digital Signature.

Za TSU certifikate „keyUsage“ je: Digital Signature i „Extended Key Usage“ je: Time Stamping.

Za identifikacijski certifikat osobe „keyUsage“ je: Digital Signature i Key Agreement.

Za potpisni certifikat osobe „keyUsage“ je: Non-Repudiation.

Za certifikate za elektronički pečat „keyUsage“ je: Non-Repudiation.

6.2 Zaštita privatnog ključa

6.2.1 Norme i upravljačke funkcije kriptografskog modula

Vrijede pravila:

a) CA ključevi, TSU ključevi i ključevi OCSP kao i ključevi osoba generiraju se u modulu koji demonstrira sukladnost s FIPS PUB 140-2 level 3 [41] standardom.
b) Inicijalizacija HSM uređaja i generiranje ključeva CA provodi se tijekom ceremonije generiranja CA ključa kako je opisano u poglavlju 6.1.1.
c) Pristup HSM uređaju i svi postupci upravljanja kriptografskim ključevima uključujući generiranje, korištenje, učitavanje, pohranu, oporavak i uništavanje kriptografskih ključeva, provode se isključivo u sigurnoj zoni pod dvojnom kontrolom.

d) Kako bi se aktivnosti vezane uz HSM uređaje i kriptografske ključeve provodile u skladu s definiranim sigurnosnim pravilima, pojedinim osobama je dodijeljena povjerljiva uloga koordinatora upravljanja kriptografskim ključevima.

e) Procedure upravljanja kriptografskim ključevima su dokumentirane i vode se uredne evidencije koje osiguravaju dokaze o provedbi aktivnosti sukladno sigurnosnim zahtjevima.

f) U slučajevima kada se privatni ključevi osoba uručuju u posjed osobe subjekta certificiranja ili osobe ovlaštenog predstavnika, isti se nakon generiranja unose u QSCD koji kao kvalificirano sredstvo za izradu elektroničkog potpisa, zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 [43] te demonstrira sukladnost s obrascima zaštite iz serije EN 419 211 [25], [26], [27], [28], [29] i [30].

g) U slučajevima kada kvalificirani pružatelj usluga povjerenja upravlja podacima za izradu elektroničkih potpisa u ime osobe subjekta certificiranja ili autora pečata, isti se generiraju i koriste isključivo unutar HSM uređaja (udaljeni QSCD) u sklopu servisa CERTILIA mPotpis koji zadovoljava zahtjeve *EAL4+ augmented with AVA_VAN.5* prema ISO/IEC 15408 [43] i prema pravilima definiranim u Prilogu II *Uredbe (EU) br. 910/2014 [1]*.

6.2.2 Upravljanje privatnim ključem od strane više osoba (n od m)

Postupci upravljanja kriptografskim ključevima provode se uz strogo poštivanje principa dijeljenog znanja što znači da je za regeneriranje kriptografskog ključa potrebno n od ukupno m kriptografskih komponenata (n od m).

Imenovani su pojedinci kojima je dodijeljena povjerljiva uloga skrbnika i svaki je skrbnik dobio u posjed samo jednu kriptografsku komponentu.

Za pristup i provedbu bilo kakve aktivnosti na HSM uređaju potrebna je dvojna kontrola koja se ostvaruje između koordinatora upravljanja i skrbnika kriptografskog ključa, a da bi se kriptografski ključ mogao regenerirati potrebna je prisutnost dva ili više skrbnika kriptografskog ključa.

6.2.3 Pohrana privatnog ključa kod treće osobe

Pohrana privatnih ključeva osoba kod treće osobe (engl. *key escrow*) se ne primjenjuje.

Pravila pohrane privatnih ključeva CA, TSU i OCSP usluge:

a) Nakon njihove generacije privatni ključevi CA, TSU i OCSP usluge ostaju pohranjeni u HSM uređaju koji demonstrira sukladnost s FIPS PUB 140-2 level 3 [41].

b) Sustav koji upravlja s privatnim ključem AKDRoot CA sustav nije spojen na računalnu mrežu i cijelo je vrijeme isključen (offline), a pokreće se samo kada je to potrebno.

c) Sustav koji upravlja s privatnim ključem CERTILIA je stalno dostupan i koristi se isključivo za potpisivanje certifikata osoba i CRL. Isto vrijedi i za OCSP sustave koji potpisuju odgovore na upit o statusu certifikata.

d) Kriptografski ključevi izvan HSM uređaja mogu biti isključivo u šifriranom obliku u skladu s pravilima navedenim u točki 6.2.6.

Pravila pohrane privatnih ključeva koji se uručuju na QSCD u posjed osobi:

a) AKD ne provodi trajnu pohranu privatnih ključeva osoba.

b) Pojedinačni privatni ključevi osoba se odmah nakon generacije šifriraju kriptografskim ključevima čija je snaga jednaka ili veća od ključa koji se štiti.
c) Dodatno, privatni ključevi se šifriraju u sklopu skupne datoteke koja se prenosi proizvođaču u njegov centar za individualizaciju.
d) Dešifriranje privatnog ključa osobe provodi se u sigurnom prostoru proizvođača i to samo kroz minimalno vrijeme potrebno za njihov unos u čip QSCD.
e) Ključevi koji se koriste za šifriranje/dešifriranje privatnih ključeva osoba u proizvodnji, također su pohranjeni u HSM uređaju koji demonstrira sukladnost s FIPS PUB 140-2 level 3 [41] standardom.
f) Odmah nakon individualizacije QSCD, privatni ključevi osoba se brišu.

6.2.3.1 Pohrana privatnog ključa u servisu CERTILIA mPotpis

Pravila pohrane privatnih ključeva kojima upravlja kvalificirani pružatelj usluga povjerenja u ime subjekta certificiranja ili autora pečata u sklopu servisa CERTILIA mPotpis :

a) Pojedinačni privatni ključevi se generiraju i čuvaju u sigurnom okruženju servisa CERTILIA mPotpis odnosno udaljenog QSCD uređaja koji je sukladan zahtjevima *EAL4+ augmented with AVA_VAN.5* prema ISO/IEC 15408 [43] i prema pravilima definiranim u Prilogu II *Uredbe (EU) br. 910/2014 [1]*.
b) Pojedinačni privatni ključevi se odmah nakon generacije šifriraju kriptografskim ključevima generiranim kriptografskim mehanizmima koje omogućuje implementirani udaljeni QSCD uređaj i kako je opisano u poglavlju 6.2.8.1.

6.2.4 Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje privatnog ključa CA provodi se u štićenom prostoru sigurne zone u skladu s pravilima koja su navedena u točkama 6.2.1 i 6.2.2.

Sigurnosne kopije CA privatnih ključeva pohranjene su i na sekundarnoj lokaciji gdje je osiguran ista ili viša razina zaštite privatnog ključa.

Pravila vezana uz sigurnosno kopiranje CA privatnog ključa primjenjuju se i za OCSP privatne ključeve.

Privatni ključevi osoba se ne kopiraju.

Privatni ključevi koji se koriste u sklopu servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje pohranjuju se u sigurnom okruženju udaljenog QSCD uređaju koji je sukladan zahtjevima *EAL4+ augmented with AVA_VAN.5* prema ISO/IEC 15408 [43] i prema pravilima definiranim u Prilogu II *Uredbe (EU) br. 910/2014 [1]*.

AKD ne omogućuje osobama oporavak privatnih ključeva koji se koriste u sklopu servisa CERTILIA mPotpis.

6.2.5 Arhiviranje privatnog ključa

CA privatni ključevi se ne arhiviranju.

OCSP i TSU privatni ključevi se ne arhiviraju.

Privatni ključevi osoba se ne arhiviraju.

Privatni ključevi u udaljenom QSCD uređaju servisa CERTILIA mPotpis se ne arhiviraju.

6.2.6 Prijenos privatnog ključa u kriptografski uređaj ili iz njega

Privatni ključ CA se može prenijeti na drugi HSM uređaj samo ako je novi uređaj u skladu s FIPS PUB 140-2 level 3 [41] standardom.

Kada je CA privatni ključ izvan HSM modula, za potrebe sigurnosne pohrane koriste se hardverski mehanizmi zaštite privatnog ključa koje osigurava proizvođač HSM uređaja, koji su u skladu s FIPS PUB 140-2 level 3 [41] standardom.

Uvijek kada je privatni ključ CA izvan HSM uređaja zbog prijenosa na drugi uređaj ili zbog potrebe sigurnosne pohrane, jamči se ista ili viša razina sigurnosti privatnog ključa.

Pravila vezana uz prijenos CA ključa u HSM uređaj ili iz njega primjenjuju se i za OCSP i TSU ključeve.

Kriptografski ključevi izvan HSM uređaja mogu biti isključivo u šifriranom obliku.

Privatni ključevi osoba koji se šalju proizvođaču QSCD uređaja koji se uručuje u posjed šifrirani su se u skladu s pravilima navedenim u točki 6.2.3. i ne mogu se prenositi između kriptografskih uređaja.

Privatni ključevi osoba u udaljenom QSCD uređaju u sklopu servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje koriste se u sigurnom okružju koje implementira HSM uređaj i koji je sukladan ISO/IEC 15408 [43] Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented by AVA_VAN.5, opisano u HSM Securty Target.

6.2.7 Čuvanje ključa u kriptografskom modulu

Privatni ključ CA, OCSP i TSU usluge u izvornom čitljivom obliku nalazi se samo unutar HSM uređaja, a može se koristiti tek nakon što se provede postupak njihove aktivacije.

Nakon proizvodnje, privatni ključ osoba u izvornom čitljivom obliku nalazi se samo unutar QSCD.

Svoje privatne ključevi osobe mogu koristiti tek nakon što se provede postupak aktivacije QSCD.

Aktivacija privatnih ključeva na QSCD uređaju i na udaljenom QSCD uređaju u servisu CERTILIA mPotpis provodi se u skladu s poglavljem 6.2.8.

6.2.8 Metoda aktivacije privatnog ključa

Aktivacija privatnog ključa u HSM uređaju:

a) Aktivacija privatnog ključa CA, OCSP i TSU koji su u HSM uređaju provodi se isključivo pod dvojnom kontrolom ovlaštenih osoba.
b) Jednom aktiviran, privatni ključ u HSM uređaju ostaje aktiviran sve dok je HSM uređaj uključen.
c) Nakon isključivanja i ponovnog uključivanja HSM uređaja ponovo se provodi aktivacija privatnih ključeva.

Aktivacija privatnog ključa osobe u QSCD u posjedu:

a) Aktivacija privatnog ključa osobe provodi se jednokratno unosom PIN-a.
b) Postavljenje PIN vrijednosti i aktivacija privatnih ključeva na QSCD moguća je tek nakon aktivacije QSCD koja se provodi u skladu s pravilima navedenim u točki 6.4.1.

6.2.8.1 Aktivacija privatnog ključa za izradu udaljenog elektroničkog potpisa ili pečata u servisu CERTILIA mPotpis

Aktivacija privatnog ključa kada kvalificirani pružatelj usluga povjerenje upravlja podacima za izradu elektroničkog potpisa u ime subjekta certificiranja ili autora pečata na udaljenom QSCD uređaju u sklopu CERTILIA mPotpis servisa:

a) Aktivacija privatnog ključa moguća je isključivo nakon autentikacije osobe subjekta certificiranja ili autora pečata na servis CERTILIA mPotpis dvofaktorskim sredstvom autentikacije registriranim u CERTILIA IDP sustavu.
b) Privatni ključ korišten za potpis se automatski deaktivira nakon potpisivanja i HSM sjednica se prekida.
c) Generirani aktivacijski podaci se ne pohranjuju u CERTILIA mPotpis sustavu.

Kontrole za štićenje od prijetnji usmjerenih na aktivacijske podatke (SAD) i sam aktivacijski podatak te privatne ključeve u udaljenom QSCD uređaju u okružju CERTILIA mPotpis za udaljeno elektroničko potpisivanje i pečatiranje uključuju: *on-line guessing, offline guessing, credential duplication, replay, man-in-the middle, credential theft, phishing, eavesdropping, spoofing i masquerading* napade.

6.2.9 Deaktivacija privatnog ključa

Deaktivacija privatnog ključa u HSM uređaju:

a) Privatni ključ CA, TSU, ili OCSP usluge je deaktiviran ukoliko HSM uređaj ili sustav koji upravlja privatnim ključem nije aktivan ili nije u funkciji.
b) Privatni ključ OCSP i TSA se deaktivira na isti način kao i privatni CA ključ.

Deaktivacija privatnog ključa osobe na QSCD:

a) Privatni ključ osobe se deaktivira vađenjem QSCD iz čitača.
b) Privatni ključ osobe ne može se koristiti ako je QSCD zaključana ili blokirana kako je navedeno u točki 6.4.2.

Kada kvalificirani pružatelj usluga povjerenje upravlja podacima za izradu elektroničkog potpisa u ime subjekta certificiranja ili autora pečata na udaljenom QSCD uređaju u sklopu CERTILIA mPotpis servisa, deaktivacija privatnog ključa se provodi automatski nakon izrade elektroničkog potpisa ili pečata.

6.2.10 Postupci uništavanja kriptografskih ključeva

Postupak uništavanja privatnog ključa CA, TSU odnosno OCSP, usluge:

a) Uništavanje privatnog ključa CA, TSU ili OCSP usluge provodi se:
   - ako se HSM uređaj iznosi iz sigurne zone radi popravka ili zamjene opreme ili
   - nakon isteka perioda valjanosti certifikata ili
   - nakon prestanka rada CA, AKD QTSA ili OCSP.

b) Kada za to nastane potreba, uništavanje privatnog ključa na HSM uređaju provodi se korištenjem sigurne metode koju osigurava proizvođač HSM uređaja, a koja jamči da se uništeni privatni ključ ni na koji način neće moći oporaviti ili ponovo koristiti.
c) Uništavanja kriptografskih ključeva provodi se komisijski od strane najmanje 2 autorizirane osobe kojima su dodijeljene povjerljive uloge te uz osiguran zapisnik o uništenju.
d) Postupak uništavanja kriptografskih ključeva provodi na siguran način, u prostorima sigurne zone kako je detaljno opisano u dokumentiranim internim procedurama.
e) Uništavanje sigurnosnih kopija i arhiva privatnog ključa provodi se postupkom koji je opisan u točki 5.1.7.

Postupak uništavanja privatnih ključeva osoba na QSCD uređaju u posjedu:

a) Uništavanje datoteka s šifriranim privatnim ključevima osoba na informacijskom sustavu provodi se automatiziranim postupkom, nakon postupka individualizacije i stavljanja privatnih ključeva osoba na QSCD.
b) Uništavanje šifriranih privatnih ključeva na informacijskom sustavu provodi se korištenjem provjerene sigurne metode te uz osiguran revizijski zapis o uništenju.

Postupak uništavanja privatnih ključeva kada kvalificirani pružatelj usluga povjerenje upravlja podacima za izradu elektroničkog potpisa u ime subjekta certificiranja ili autora pečata u sklopu CERTILIA mPotpis servisa u udaljenom QSCD uređaju:

a) Kada za to nastane potreba, uništavanje privatnog ključa na HSM uređaju provodi se korištenjem sigurne metode koju osigurava proizvođač HSM uređaja, a koja jamči da se uništeni privatni ključ ni na koji način neće moći oporaviti ili ponovo koristiti.
b) Postupak uništavanja kriptografskih ključeva provodi na siguran način, u prostorima sigurne zone kako je detaljno opisano u dokumentiranim internim procedurama.
c) Uništavanje privatnog ključa u slučaju kada je opozvan korespondirajući certifikat za udaljeno potpisivanje ili pečatiranje provodi se automatski u sklopu servisa CERTILIA mPotpis korištenjem sigurne metode koju osigurava proizvođač HSM uređaja, a koja jamči da se uništeni privatni ključ ni na koji način neće moći oporaviti ili ponovo koristiti.
d) Uništavanje sigurnosnih kopija i arhiva privatnog ključa provodi se prema pravilima opisanim u točki 5.1.7.

6.2.11 Ocjena kriptografskog modula

Vidjeti točku 6.2.1.

6.3 Ostali vidovi upravljanja kriptografskim ključevima

6.3.1 Arhiviranje javnog ključa

Javni ključevi svih osoba kojima su izdani certifikati uključujući javne ključevi CA, TSU i OCSP usluga sastavni su dio certifikata koji se arhiviraju da bi se omogućila naknadna provjera elektroničkog potpisa te osigurali dokazi u sudskim, upravnim i drugim postupcima.

Primjenjuju se pravila arhiviranja koja su navedena u poglavlju 5.5.

6.3.2 Period valjanosti certifikata i kriptografskih ključeva

Period važenja certifikata naveden je u tablici 4.

Tablica 4: Period valjanosti *certifikata*

Certifikat	Period valjanosti
Certifikat krovnog certifikacijskog tijela AKDCA Root	do 2038-01-19 03:14:07+00:00
Certifikat podređenog certifikacijskog tijela CERTILIA	do 15 godina
Certifikat za potpis OCSP odgovora	do 3 godine
TSU certifikat (za potpis AKD QTSA odgovora)	do 5 godina
Certifikati fizičkih osoba (QSCD u posjedu)	do 3 godine
Certifikati za udaljeni elektronički potpis	do 2 godine
Certifikati za elektronički pečat (QSCD u posjedu)	do 2 godine
Certifikati za udaljeni elektronički pečat	do 2 godine

Period važenja privatnog ključa jednak je periodu važenja korespondirajućeg certifikata.

Period važenja privatnog ključa za TSU certifikat je 2 godine (ekstenzija „privateKeyUsagePeriod“).

Privatni ključ se ne smije koristiti nakon isteka važenja korespondirajućeg certifikata, njegovog opoziva ili suspenzije.

Certifikacijsko tijelo će prestati izdavati certifikate, promijeniti CA ključ i početi izdavati certifikate na novom CA prije isteka perioda valjanosti prema pravilima koja su navedena u točki 5.6.

Certifikat je valjan od datuma izdavanja do isteka roka valjanosti i ne smije se koristiti nakon isteka tog roka.

Tijekom perioda valjanosti certifikata, certifikat može biti suspendiran ili trajno opozvan nakon čega prestaje biti valjan i ne smije se više koristiti.

6.4 Aktivacijski podaci

6.4.1 Generiranje i instalacija aktivacijskih podataka

Proizvođač provodi generiranje i instalaciju aktivacijskih podataka u skladu sa sljedećim pravilima:

a) Aktivacijski podaci su generirani u HSM uređaju i cijelo vrijeme ostaju šifrirani kriptografskim ključem koji je pohranjen u HSM-u.
b) Dešifriranje aktivacijskih podataka u informacijskom sustavu provodi se samo kroz minimalno vrijeme potrebno za njihov unos u QSCD odnosno za slanje na e-mail ili SMS .
c) Odmah nakon stavljanja aktivacijskih podataka osoba na QSCD odnosno nakon slanja na e-mail ili SMS, provodi se uništavanje datoteka s šifriranim aktivacijskim podacima

d) Uništavanje podataka na informacijskom sustavu provodi se automatiziranim postupkom, korištenjem sigurne metode te uz osiguran revizijski zapis o uništenju.

U slučaju kada kvalificirani pružatelj usluga certificiranja upravlja podacima za kreiranje elektroničkog potpisa u ime subjekta certificiranja ili autora pečata u sklopu servisa CERTILIA mPotpis:

a) Registracijski kodovi odnosno referentni i autorizacijski kod za registraciju certifikata u CERTILIA mPotpis servisu generiraju i čuvaju se u sigurnom okruženju CERTILIA mPotpis sustava i dostavljaju se osobama elektroničkom poštom ili SMS porukom.
b) Referentni i autorizacijski kodovi koriste se u procesu registracije certifikata u servisu CERTILIA mPotpis prilikom čega osoba subjekt certificiranja ili autor pečata postavlja PIN za aktivaciju privatnog ključa prilikom potpisivanja ili pečatiranja.
c) Nakon uspješne registracije registracijski kodovi se više ne mogu koristiti u CERTILIA mPotpis servisu.

Osobe provode aktivaciju QSCD-a u skladu sa sljedećim pravilima:

a) Aktivaciju QSCD osoba subjekt certificiranja ili autor pečata provodi samostalno nakon preuzimanja QSCD korištenjem dobivenih podataka za aktivaciju, a prema uputi za aktivaciju QSCD koja je dostavljena korisniku i dostupna na portalu QSCD .
b) Tijekom aktivacije QSCD postavljaju se PIN-ovi za zaštitu privatnih ključeva kao i PUK vrijednost za otključavanje QSCD.

U slučaju kada kvalificirani pružatelj usluga certificiranja upravlja podacima za kreiranje elektroničkog potpisa u ime subjekta certificiranja ili autora pečata u sklopu servisa CERTILIA mPotpis osobe provode aktivaciju privatnog ključa u udaljenom QSCD uređaju prilikom preuzimanja certifikata u servisu CERTILIA mPotpis, koristeći registracijske kodove zaprimljene e-mailom ili SMS porukom i postavljanjem PIN-a za aktivaciju privatnog ključa.

Osobe su informirane o svojim obvezama vezanim uz zaštitu registracijskih kodova i aktivacijskih podataka odnosno PIN-ova.

6.4.2 Zaštita aktivacijskih podataka

Kada se certifikati isporučuju na QSCD uređaju proizvođač poduzima sljedeće mjere zaštite aktivacijskih podataka:

a) Generiranje aktivacijskih podataka te njihov unos u QSCD i ispis u sigurnosne omotnice provodi se pod dvojnom kontrolom u sigurnom okružju proizvođača QSCD.
b) Aktivacijski podaci mogu se dostavljati osobama na e-mail ili SMS navedene u zahtjevu za izdavanje certifikata za koje osoba jamči da im samo ona može pristupiti, ako je tako navedeno u zahtjevu nakon prethodne provjere točnosti u postupku aktivacije CERTILIA korisničkog računa.

Osobe su informirane o implementiranim mjerama zaštite QSCD i PIN-ova za zaštitu privatnih ključeva na QSCD:

a) Nakon 6 uzastopnih pokušaja unosa pogrešnog PIN-a QSCD se zaključava.

b) Zaključanu QSCD osoba subjekt certificiranja može otključati samostalno, korištenjem PUK vrijednosti koja je postavljena tijekom aktivacije QSCD.
c) Nakon 6 uzastopnih pokušaja unosa pogrešnog PUK-a QSCD se blokira.
d) Blokiranu QSCD može deblokirati samo službenik RA u sigurnom okružju korištenjem elektroničke usluge za deblokadu QSCD.
e) Deblokada QSCD provodi se u fizičkoj prisutnosti osobe subjekta certificiranja, a nakon utvrđivanje identiteta osobe.

6.4.2.1 Zaštita aktivacijskih podataka u servisu CERTILIA mPotpis

U slučaju kada kvalificirani pružatelj usluga certificiranja upravlja podacima za kreiranje elektroničkog potpisa u ime subjekta certificiranja ili autora pečata na udaljenom QSCD uređaju odnosno u sklopu servisa CERTILIA mPotpis poduzimaju se sljedeće mjere zaštite registracijskih kodova:

a) Registracijski kodovi (referentni i registracijski kodovi) za preuzimanje certifikata generiraju se i čuvaju u sigurnom okruženju CERTILIA mPotpis servisa i udaljenog QSCD uređaja i šalju se na e-mail ili SMS subjekta certificiranja ili autora pečata navedene na zahtjevu za izdavanje certifikata.
b) Registracijski kodovi koriste se za preuzimanje jednog certifikata i postavljanje PIN-a za aktivaciju privatnog ključa u CERTILIA mPotpis servisu i ne mogu se više koristiti za bilo koju drugu namjenu.
c) Preuzimanje certifikata je moguće isključivo nakon prijave subjekta certificiranja ili autora pečata na CERTILIA mPotpis servis dvofaktorskim sredstvom autentikacije registriranim u CERTILIA IDP sustavu.
d) Registracijski kodovi važeći su 120 dana od trenutka njihovog generiranja.

Aktivacijski podaci za aktivaciju privatnog ključa i privatni ključevi u udaljenom QSCD uređaju u okružju CERTILIA mPotpis za udaljeno elektroničko potpisivanje i pečatiranje štite se prema opisanom u poglavlju 6.2.8.1.

6.4.3 Ostale odredbe o aktivacijskim podacima

AKD primjenjuje adekvatne mjere zaštite aktivacijskih podataka i registracijskih kodova od gubitka, modifikacije, otkrivanja i neautoriziranog korištenja.

U skladu s dokumentiranim internim procedurama AKD provodi:

a) zaštitu aktivacijskih podataka za QSCD uređaj od generiranja, instalacije, slanja na SMS ili e-mail i uništavanja aktivacijskih podataka do transporta i uručivanja aktivacijskih podataka osobama i
b) zaštitu registracijskih kodova za registraciju certifikata u CERTILIA mPotpis servisu i postavljanje PIN-a privatnog ključa od generiranja, instalacije i uništavanja registracijskih kodova do slanja osobama.

Aktivacijski podaci za QSCD uređaj mogu se, uz načine opisane u pojedinim točkama ovog dokumenta, dostaviti poštujući sigurnosne zahtjeve na sljedeće načine:

a) elektroničkom poštom (e-mail),
b) SMS porukom,
c) ispisani na siguran način u RA uredima osobno subjektu certificiranja ili ovlaštenom predstavniku autora pečata i
d) kombinacijom metoda a) do c).

Registracijski kodovi za registraciju certifikata u CERTILIA mPotpis servisu i postavljanje PINa privatnog ključa dostavljaju se na e-mail ili SMS podatke osobe subjekta certificiranja ili ovlaštenog predstavnika dobivene prilikom registracije.

Nakon što su im dostavljeni aktivacijski podaci i/ili registracijski kodovi, osobe su odgovorne za njihovu zaštitu. Osobe mogu mijenjati aktivacijske podatke za korištenje privatnih ključeva samostalno koristeći aplikaciju za korištenje QSCD uređaju te u servisu CERTILIA mPotpis za privatne ključeve koji se koriste za udaljeno potpisivanje i pečatiranje.

6.5 Mjere zaštite računalnih resursa

6.5.1 Posebni tehnički zahtjevi za računalnu sigurnost

Računalni resursi se štite mjerama sigurnosti prema ISO/IEC 27001 [45] i ISO/IEC 27002 [46] normama.

Pored toga, implementirani su tehnički zahtjevi vezani uz računalnu sigurnost u skladu s zahtjevima normi ETSI EN 319 411-1 [15] i ETSI EN 319 411-2 [16] kao i sa zahtjevima koji su navedeni u dokumentu CEN TS 419 261 [31] te ETSI TS 119 431-1 [23] odnosno CEN EN 419 241-1 [32].

To znači:

a) Dokumentirani su interni standardi sigurnosti te postoji niz procedura i uputa koje se redovito ažuriraju kako bi bile u skladu s sigurnosnim zahtjevima.
b) Uspostavljena je organizacijska i upravljačka struktura s jasno definiranim povjerljivim ulogama i odgovornostima.
c) Definirana su pravila vezana uz radnike, zaštitare, posjetitelje i vanjske servisere prije i tijekom ugovornog odnosa te nakon isteka ugovora.
d) Primjenjuju se mjere zaštite imovine i podataka koje obuhvaćaju definiranje vlasnika, klasificiranje i rukovanje.
e) Uspostavljeni su adekvatni sustavi fizičke zaštite objekata, prostora i informacijske opreme.
f) Upravljanje autorizacijama i pravima pristupa je restriktivno i uspostavljena je dvojna kontrola za provedbu svih kritičnih operacija koje uključuju izdavanje, brisanje ili promjenu certifikata ili njihovog statusa.
g) Propisana su i implementirana stroga pravila vezana uz upravljanje kriptografskim ključevima i opremom.
h) Provode se redovite mjere održavanja sigurnosti mrežne i računalne opreme koje uključuju zaštitu od malicioznog koda, upravljanje revizijskim zapisima i sigurnosna testiranja.
i) Sustav se kontinuirano nadzire i alarmira kako bi se omogućilo detektiranje, registriranje i pravovremena reakcija na neautorizirane radnje ili neregularne pojave.

j) Izrađuju se i pohranjuju sigurnosne kopije, te su uspostavljene procedure upravljanja neprekinutošću poslovanja.
k) Uspostavljena su pravila upravljanja incidentima, promjenama, problemima i zahtjevima.

6.5.2 Ocjena računalne sigurnosti

Periodično se provodi ispitivanje, testiranje, provjeravanje, vrednovanje i ocjenjivanje sigurnosti računalnih resursa i njihove sukladnosti s normama navedenim u točki 6.5.1.

6.6 Životni ciklus i tehničke kontrole

U skladu s poglavljem 12 ISO/IEC 27002 [46] uspostavljene su kontrole nad računalnim resursima što uključuje:

a) Procedure su dokumentirane, povjerljive uloge su dodijeljene i uspostavljena je odgovornost kako bi se osigurala korektna i sigurna provedba aktivnosti.
b) Organizacijske, poslovne kao i tehničke promjene na računalnim sustavima su kontrolirane.
c) Resursi se redovito nadziru, podešavaju i planiraju kako bi se osigurali dostatni kapaciteti i zahtijevane performanse sustava.
d) Provodi se procjena rizika u skladu s normom ISO/IEC 27005 [48] pri čemu se uzimaju u obzir poslovni i tehnički aspekti povezani s pružanjem usluga.
e) Razvojna, testna i produkcijska okružja su strogo odijeljena kako bi se smanjili rizici od neautoriziranog pristupa i promjene produkcijskog okružja.
f) Računalni sustavi su zaštićeni od virusa, zloćudnog koda i neautoriziranog softvera.
g) Sigurnosne kopije se redovito izrađuju i štite od oštećenja, gubitka i neautoriziranog pristupa kako bi se spriječio gubitak podataka.
h) Osigurani su revizijski zapisi i poduzete su sve potrebne mjere njihove zaštite.

U skladu s poglavljem 14 ISO/IEC 27002 [46] uspostavljene su kontrole nad razvojem i životnim ciklusom softvera što uključuje:

a) Uspostavljena je metodologija razvoja softvera, a proces razvoja se redovito nadzire i vrednuje.
b) Osigurana je adekvatna zaštita izvornog i izvršnog koda.
c) Softveri se ispituju i podvrgavaju opsežnim testiranjima i ocjenjivanju prije njihove implementacije u produkcijsku okolinu.
d) U skladu s procjenom rizika implementiraju se sigurnosne korekcije softvera, a cjelokupan postupak upravljanja verzijama, korekcijama i promjenama softvera je definiran i kontroliran.

U skladu s poglavljem 15 ISO/IEC 27002 [46] uspostavljene su kontrole vezane uz poslovne odnose i dobavljače što uključuje:

a) Postupak nabave i ocjenjivanje dobavljača provodi se prema dokumentiranim procedurama.
b) Sigurnosni zahtjevi su definirani ugovorima, a postupci vezani uz provedbu ugovora se nadziru kako bi se osigurala sigurna isporuka opreme ili provedba usluga.

6.7 Kontrola mreže

Mrežni resursi se štite mjerama sigurnosti prema poglavlju 13 SO/IEC 27002 [46], CEN TS 419 261 [31] te ETSI TS 119 431-1 [23] odnosno CEN EN 419 241-1 [32].

Uspostavljene su sljedeće kontrole mreže:

a) Svi računalni resursi su odijeljeni u logički razdvojene, posebne funkcionalne cjeline koje se nazivaju mrežne zone.
b) Uspostavljene su sljedeće mrežne zone:
    a. PKI CA zona gdje su smješteni računalni resursi za provedbu usluge generiranje i upravljanja opozivom certifikata,
    b. PKI uslužna zona gdje su smješteni računalni resursi za provedbu usluge informiranja i provjeru statusa certifikata,
    c. Perso uslužna zona gdje su smješteni računalni resursi unos kriptografskih ključeva na QSCD u posjedu,
    d. DMZ gdje su smješteni računalni resursi koji su direktno izloženi javnosti.
c) Definirana su i uspostavljena jasna pravila tako da se unutar određene mrežne zone primjenjuju iste fizičke, tehničke i proceduralne mjere zaštite.
d) Oprema i hardver između mrežnih zona fizički su odijeljeni i smješteni u zasebne računalne ormare.
e) Računalni ormari su smješteni u prostore u adekvatnoj zoni fizičke sigurnosti te se štite odgovarajućim mjerama fizičke sigurnosti u skladu s poglavljem 5.1.
f) Ožičenje i sve fizičke točke priključaka i aktivne i pasivne mrežne opreme su kontrolirane i nadzirane.
g) Fizički pristup računalnim resursima i mrežnoj opremi ograničen je na osobe s povjerljivim ulogama koje su autorizirane za administriranje opreme.
h) Mrežne zone su odijeljene vatrozidovima, a između mrežnih zona se strogo regulira mrežni promet prema formalno odobrenim listama dozvoljenih usluga.
i) Komunikacija između mrežnih zona odvija se kroz sigurne kanale koji su namjenski, logički odijeljeni i koji štite podatke od modifikacije i otkrivanja.
j) Između mrežnih zona je omogućena samo ona komunikacija koja je nužna za provedbu usluge i zabranjena svaka komunikacija osim one koja je eksplicitno odobrena.
k) Ograničeni pristup mrežnoj zoni može se ostvariti na sljedeći način:
    a. sigurnoj zoni se može pristupiti samo iz uslužne i djelatne zone,
    b. uslužnoj i djelatnoj zoni se može pristupiti samo iz nadzorne i pristupne zone.
l) Automatizirano se generiraju izvještaji o svakoj promjeni konfiguracije vatrozida.
m) Implementiran je sustav za otkrivanje napada (engl. Intrusion Detection System - IDS), koji nadzire mrežni promet u djelatnoj i uslužnoj zoni te alarmira sve sumnjive aktivnosti u realnom vremenu.
n) Ispitivanje ranjivosti se provodi periodično i kod svake značajnije promjene konfiguracije, a sve kritične ranjivosti se rješavaju u najkraćem mogućem roku.
o) Kod značajnih promjena, a barem jedan puta godišnje, provodi se ispitivanje mogućnosti upada u sustav (engl. Penetration test).

6.8 Upotreba vremenskog žiga

Vrijeme u sustavu certificiranja AKD-a usklađeno je s UTC točnim vremenom.

Revizijski zapisi u AKD PKI sustavima sadržavaju točan podatak o datumu i vremenu njihovog nastanka, uz odstupanje manje od +/- 1 s.

7 Sadržaj certifikata i CRL

7.1 Profili certifikata

Obrasci (profili) svih certifikata usklađeni su sa IETF RFC 5280 [38] i Recommendation ITU-T X.509 [49].

Profili certifikata koji se izdaju fizičkim osobama su u skladu sa zahtjevima normi ETSI EN 319 412-1 [17] , ETSI EN 319 412-2 [18] kao i sa zahtjevima za izdavanje EU kvalificiranih certifikata prema normi ETSI EN 319 412-5 [20].

Profili certifikata koji se izdaju pravnim osobama su u skladu sa zahtjevima normi ETSI EN 319 412-1 [17] , ETSI EN 319 412-3 [19] kao i sa zahtjevima za izdavanje EU kvalificiranih certifikata prema normi ETSI EN 319 412-5 [20].

CA i OCSP certifikati su sukladni ETSI EN 319 412-3 [19].

Profil TSU certifikata je usklađen s zahtjevima normi ETSI EN 319 422 [22] i IETF RFC 3161 [39].

Tablica 5: Osnovna polja svih certifikata

Polje	Vrijednost/Ograničenja vrijednosti
Version	X.509 V3, vidi točku 7.1.1
Serial Number	Jedinstven pozitivan broj s entropijom od 64 bit-a
Signature Algorithm	ecdsa-with-SHA384, vidi točku 7.1.3.
Issuer DN	Vidi točku 7.1.4.
Valid from	utcTime
Valid to	utcTime(Valid from +period važenja certifikata u skladu s točkom 6.3.2).
Subject DN	Vidi točku 7.1.4.
Subject Public Key	Javni ključ subjekta
SignatureValue	Potpis izdavatelja certifikata, generiran i kodiran prema IETF RFC 5280 [38]

7.1.1 Broj verzije

Koristi se X.509 verzija V3.

7.1.2 Ekstenzije certifikata

7.1.2.1 Ekstenzije CA certifikata

Definirano Općim pravilima pružanja usluga certificiranja. [33]

7.1.2.2 Ekstenzije OCSP certifikata

Definirano Općim pravilima pružanja usluga certificiranja. [33]

7.1.2.3 Ekstenzije TSU certifikata

Tablica 7a: Ekstenzije TSU certifikata

Polje	Vrijednost
Key Usage*	Digital Signature
Extended Key Usage*	Time Stamping (1.3.6.1.5.5.7.3.8)
policyConstraints	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	Derived using the SHA-1 hash of the public key.
Private Key Usage Period	utcTime (Valid from +2 godine)
Authority Info Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://certilia.com/cert/certilia.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://www.ocsp.certilia.com
Certificate Policies	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.14.1.2.2.8 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certilia.com/cps
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=https://crl.certilia.com/certilia.crl
qcStatements	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://www.certilia.com/cps language=en PdsLocation: url= https:// www.certilia.com /cps language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-eseal (2) (0.4.0.1862.1.6.2)

**Kritično polje*

7.1.2.4 Ekstenzije certifikata

Tablica 7b: Ekstenzije certifikata

Polje	Tip certifikata	Vrijednost	Sadržaj
Key Usage*	CERTILIA NCP+ kident	Digital Signature, Key Agreement (88)	Fixed
	CERTILIA QCP-n-qscd-ksign	Non-Repudiation	Fixed
	CERTILIA QCP-n-qscd-krsign	Non-Repudiation	Fixed
	CERTILIA QCP-l-qscd-kseal	Non-Repudiation	Fixed
	CERTILIA QCP-l-qscd-krseal	Non-Repudiation	Fixed
Basic Constraints*	All End Entity	Subject Type=End Entity Path Length Constraint=None	Fixed
Subject Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.	Variable
Authority Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.	Variable
Authority Info Access	All End Entity	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=https://certilia.com/cert/certilia.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=https://ocsp.certilia.com	Fixed
Certificate Policies	CERTILIA NCP+ kident	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.15.2.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certilia.com/cps	Fixed
	CERTILIA QCP-n-qscd-ksign	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.14.2.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier:	Fixed

		https://certilia.com/cps	
	CERTILIA QCP-n-qscd-krsign	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.15.6.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certilia.com/cps	Fixed
	CERTILIA QCP-l-qscd-kseal	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.14.2.2.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certilia.com/cps	Fixed
	CERTILIA QCP-l-qscd-krseal	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.14.6.2.3.4 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://certilia.com/cps	Fixed
Subject Alternative Name	CERTILIA NCP+ kident	Microsoft UPN(1.3.6.1.4.1.311.20.2.3)	O / Holder variable
		RFC822Name=email@domain.tld	O / Holder variable
Extended Key Usage	CERTILIA NCP+ kident	Client Authentication (1.3.6.1.5.5.7.3.2)	M
		Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	M
CRL Distribution Points	All End Entity	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=https://crl.certilia.com/certilia.crl	Fixed
qcStatements			
	CERTILIA QCP-n-qscd-ksign	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://certilia.com/cps language=en PdsLocation: url= https://certilia.com/cps language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6)	Fixed

		Type= id-etsi-qct-esign(1) (0.4.0.1862.1.6.1)	
	CERTILIA QCP-n-qscd-krsign	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://certilia.com/cps language=en PdsLocation: url= https://certilia.com/cps language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-esign(1) (0.4.0.1862.1.6.1)	Fixed
	CERTILIA QCP-l-qscd-kseal	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://certilia.com/cps language=en PdsLocation: url= https://certilia.com/cps language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-eseal (2) (0.4.0.1862.1.6.2)	Fixed
	CERTILIA QCP-l-qscd-krseal	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url=https://certilia.com/cps language=en PdsLocation: url= https://certilia.com/cps language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-eseal (2) (0.4.0.1862.1.6.2)	Fixed

**Kritično polje*

7.1.3 Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koji se izdaju u AKD PKI sustavu zasnovanom na AKD Root CA prikazani su u tablici 8.

Tablica 8: Algoritmi i pripadni identifikatori objekta

Algoritam	OID
Sha256WithRSAEncryption	1.2.840.113549.1.1.11

rsaEncryption	1.2.840.113549.1.1.1
ecdsa-with-SHA384	1.2.840.10045.4.3.3

7.1.4 Oblici naziva

U sve izdane certifikate od strane AKD PKI sustava upisuje se X.500 Distinguished Name u polja „Subject“ i „Issuer“, a prema opisanom u poglavlju 3.1.1. ovog dokumenta.

Oblici naziva za certifikate koji su izdani u AKD PKI sustavu detaljnije su opisani su u poglavlju 3.1.1. te poglavlju 3.1.4. ovog dokumenta.

7.1.5 Ograničenja u nazivima

Ne koristi se.

7.1.6 Identifikator objekata (OID) općih pravila certificiranja

U sve certifikate izdane u AKD PKI okružju sa vršnim AKD Root CA a koji sadrže ekstenziju Certificate Policies sadrže odgovarajući OID identifikator kako je navedeno u poglavlju 1.2. ovog dokumenta.

7.1.7 Upotreba ekstenzije Policy Constraints

Ne koristi se.

7.1.8 Sintaksa i semantika kvalifikatora općih pravila

AKD u svim izdanim certifikatima gdje se koristi ekstenzija Certificate Policies popunjava identifikator CPS koji pokazuje na odgovarajuće dokumente. Osobni certifikati mogu sadržavati dodatno i User Notice identifikator koji može pokazivati na odgovarajući Pravilnik ili Ugovor.

7.1.9 Procesne semantike za kritičnu ekstenziju Certificate Policies

Ne koristi se.

7.2 CRL profili

CRL profili AKCA Root i CERTILIA izdavatelja podržavaju X.509 verziju 2 sukladno zahtjevima definiranim u IETF RFC 5280 [38]. U nastavku su dani CRL profili za AKDCA Root i CERTILIA.

Tablica 9: Osnovna polja CRL

Polje	Vrijednost/Ograničenja vrijednosti
Version	X.509 V2, vidi točku 7.2.1

Signature Algorithm	SHA256RSA (AKDCA Root) i ecdsa-with-SHA384 (CERTILIA), vidi točku 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	Lista opozvanih certifikata koja uključuje serijski broj certifikata koji je opozvan, datum opoziva i razlog opoziva (keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold).

7.2.1 Broj verzije

Koristi se X.509 verzija V2.

7.2.2 CRL ekstenzije

Tablica 10: Ekstenzije AKDCA Root CRL

Polje	Vrijednost/Ograničenja vrijednosti
authorityKeyIdentifier	Derived using the SHA-1 hash of the public key.
CRL Number	Monotonically increasing sequential number.

7.3 OCSP profil

AKD PKI omogućava online provjeru statusa certifikata putem OCSP usluge. Certifikat OCSP usluge (OCSP responder) izdaje CERTILIA odnosno AKDCA Root. Certifikat OCSP usluge je sukladan IETF RFC 5019 [40] i IETF RFC 6960 [35].

U Općim pravilima pružanja usluga certificiranja [33] su dani OCSP profili za AKDCA Root.

7.3.1 Broj verzije

Koristi se X.509 verzija V3.

7.3.2 Ekstenzije OCSP certifikata

Definirano Općim pravilima pružanja usluga certificiranja [33].

8 Provjera usklađenosti

8.1 Učestalost i okolnosti provjere usklađenosti

Ovaj dokument omogućava reviziju s ciljem provjere usklađenosti sa zakonskom regulativom i obvezujućim normama.

Redovni nadzor pružatelja usluga povjerenja i ocjenjivanje sukladnosti s *Uredbom (EU) br. 910/2014 [1]* provodi se svaka 24 mjeseca.

Redovni nadzor sustava upravljanja s ciljem provjere usklađenosti s ISO/IEC 9001 [47], ISO/IEC 27001 [45] i ISO/IEC 14298 [44] normama vrši se najmanje svakih 12 mjeseci.

Interne revizije s ciljem provjere postupanja prema ovome dokumentu i internim procedurama provode se periodično, prema utvrđenom planu i programu.

Nadzorno nacionalno tijelo može u bilo kojem trenutku obaviti reviziju ili zahtijevati obavljanje revizije kako bi utvrdilo jesu li ispunjeni zahtjevi vezanu uz provedbu zakonskih propisa.

8.2 Identitet/kvalifikacije revizora

Ocjenjivanje sukladnosti s *Uredbom (EU) br. 910/2014 [1]* provodi tijelo ovlašteno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje je osigurano akreditacijom prema ETSI EN 319 403 [14].

Nadzor sustava upravljanja sukladno normama ISO/IEC 9001 [47], ISO/IEC 27001 [45] i ISO/IEC 14298 [44] vrše ovlaštene revizijske kuće.

Interni revizori moraju:

- raspolagati znanjima iz područja PKI i informacijske sigurnosti,
- raspolagati znanjima i razumijevanjem norma ETSI EN 319 401 [13], ETSI EN 319 403 [14], ETSI EN 319 411 [15] i [16],
- poznavati odredbe iz općih pravila i pravilnika o postupcima certificiranja,
- poznavati zakonsku regulativu iz područja elektroničkog poslovanja, informacijske sigurnosti i zaštite tajnosti podataka te
- raspolagati vještinama potrebnim za provedbu internih revizija.

8.3 Odnos revizora s predmetom revizije

Vanjski revizori su neovisni i delegirani od nadležnog državnog tijela odnosno ovlaštene vanjske revizijske tvrtke.

Internu reviziju u AKD-u provodi Savjetnik za informacijsku sigurnost ili druga neovisna osoba koju imenuje PMA.

8.4 Područja obuhvaćena revizijom

Vanjske revizije sustava upravljanja obuhvaćaju cjelokupno poslovanje AKD-a.

Interne revizije obuhvaćaju ali se ne ograničavaju na:

- postupke generiranja certifikata,
- postupke generiranja i zaštite svih privatnih ključeva,
- upravljanja opozivom certifikata,

- provedbu usluge provjere statusa certifikata,
- provedbu usluge servisa CERTILIA mPotpis,
- dostupnost i sadržaj usluga informiranja,
- dokumentaciju i sporazume vezane uz uslugu registracije i
- provedbu propisanih postupaka i mjera zaštite u skladu s odredbama općih pravila i pravilnika.

8.5 Postupanje u slučaju nesukladnosti

U slučaju da se utvrdi nesukladnost, izrađuje se operativni plan aktivnosti, utvrđuju se rokovi i dodjeljuju zaduženja vezana uz provedbu operativnog plana.

Ako nesukladnost značajno utječe na sigurnost pružanja usluga certificiranja ili onemogućuje ispunjenje zakonom propisanih zahtjeva, AKD će prekinuti pružanje CERTILIA usluga sve dok se ne otkloni utvrđena nesukladnost.

AKD će poduzeti sve potrebne radnje kako bi spriječio nepovoljan utjecaj prekida pružanja usluga na osobe i pouzdajuće strane.

Nakon što ocjenitelj utvrdi da je postignuta propisana usklađenost, PMA će odobriti nastavak pružanja CERTILIA usluga.

8.6 Priopćavanje rezultata

Izvještaj o provedenoj reviziji odnosno utvrđenoj nesukladnosti dostavlja se PMA, predstavnicima revidiranog područja i odgovornim osobama u skladu s organizacijskom strukturom AKD.

AKD, u skladu s važećom regulativom i zakonskim odredbama, nadzornom tijelu podnosi izvješće o ocjenjivanju sukladnosti u roku od 3 radna dana od primitka izvještaja.

9 Ostale poslovne i pravne stavke

9.1 Naknade za usluge

AKD kao pružatelj usluge certificiranja naplaćuje usluge izdavanja certifikata. Cijena usluga i naknade određuju se internim poslovnim procesima od strane Sektora razvoja poslovanja.

Važeći cjenici usluga i naknada te načini naplate dostupni su osobama i pouzdajućim stranama na način da:

a) AKD objavljuje važeće cjenike usluga na web portalu https://www.certilia.com,
b) AKD po izmjeni cjenika informira djelatnike RA ureda o cijenama i načinima naplate,
c) Službenici RA ureda informiraju osobe i pouzdajuće strane u registracijskim uredima.

AKD može, pored važećih objavljenih cjenika, odrediti cijenu i naplatiti uslugu i naknade posebnim ugovorom. AKD zadržava pravo izmjene cjenika.

9.1.1 Naknade za izdavanje ili obnovu certifikata

Naplata usluga i naknada za izdavanje certifikata vrši se sukladno važećim objavljenim cjenicima.

AKD može odrediti cijenu te naplatiti uslugu i naknade posebnim ugovorom.

U AKD CERTILIA PKI sustavu ne pruža se usluga obnove certifikata te cjenici ne sadrže cijenu za obnovu certifikata.

9.1.2 Naknade za pristup certifikatu

AKD može odrediti cijenu te naplatiti uslugu pretraživanje certifikata u javnom imeniku CERTILIA posebnim ugovorom.

9.1.3 Naknade za opoziv i pristup informacijama o statusu certifikata

AKD može naplaćivati naknade za uslugu suspenzije, opoziva suspenzije i opoziva certifikata izdanih od strane CERTILIA sustava. Naknade se naplaćuju sukladno važećim objavljenim cjenicima.

AKD može naplaćivati naknadu za uslugu davanja informacija o statusu certifikata izdanih od strane CERTILIA sustava. Naknade se naplaćuju sukladno važećim objavljenim cjenicima.

Osim temeljem važećih objavljenih cjenika, AKD može naplaćivati naknade temeljem posebnog ugovora.

9.1.4 Naknade za ostale usluge

AKD može naplaćivati naknade za ostale usluge i proizvode u sklopu uspostavljene usluge certificiranja i izdavanja kvalificiranih certifikata, samostalno ili s ugovornom stranom:

a) Naknadu za uslugu registracije fizičkih osoba u RA uredima,
b) Naknadu za čitač pametnih kartica,
c) Naknadu za grafički dizajn i grafičku pripremu QSCD uređaja,
d) Naknadu za proizvodnju QSCD uređaja,
e) Naknadu za personalizaciju QSCD uređaja,
f) Naknadu za korištenje servisa CERTILIA mPotpis za udaljeno potpisivanje i pečatiranje.
g) Naknadu za isporuku certifikata na QSCD uređaju na lokaciji različitoj od lokacije podnošenja zahtjeva (RA ured na adresi specificiranoj kod podnošenja zahtjeva ili druga lokacija specificirana od strane podnositelja zahtjeva)
h) Naknade vezane za korištenje, nadogradnju, najam ili održavanje programske opreme, hardvera, edukaciju korisnika i sl.

AKD objavljuje iznose naknada i načine naplate za ostale usluge sukladno opisanom u točci 9.1 ovog dokumenta.

Osim temeljem važećih objavljenih cjenika, AKD može određivati iznose naknada i naplaćivati naknade za ostale usluge temeljem posebnog ugovora.

9.1.5 Povrat naknade

AKD osobi podnositelju zahtjeva može izvršiti povrat naknada ukoliko se utvrdi propust ili nedostatak u usluzi ili proizvodu vezanom za pružanje usluge ili ukoliko je prilikom uplate naknade ustanovljena nenamjerna pogreška korisnika usluga i proizvoda.

Uvjeti povrata naknade za usluge i proizvode vezane za izdavanje certifikata objavljeni su na web portalu, a službenici RA ureda informiraju korisnike u uredima. Dodatno, uvjeti mogu detaljno biti navedeni u uvjetima pružanja usluga certificiranja.

9.2 Financijska odgovornost

9.2.1 Pokrivenost osiguranjem

AKD je uspostavio sustav odgovornosti, odredio granice pouzdanja u certifikate i jasno definirao obveze svih korisnika usluga certificiranja. Korisnici usluga su putem portala unaprijed informirani o uvjetima pružanja usluga certificiranja.

AKD ima osiguran rizik od odgovornosti za štete koje nastaju pružanjem usluga certificiranja u iznosu koji je naveden u točki 9.2.3. i koje se odnose na izdavanje sredstava elektroničke identifikacije i pružanje kvalificiranih ili nekvalificiranih usluga izrade, verifikacije i validacije elektroničkih potpisa, elektroničkih pečata ili elektroničkih vremenskih žigova i certifikata koji se odnose na te usluge.

AKD je odgovoran za štete koje nanese svakoj fizičkoj ili pravnoj osobi zbog neispunjavanja obveza u skladu s ovim dokumentom i *Uredbom (EU) br. 910/2014 [1]*.

AKD ne odgovara za štete koje namjerno ili nepažnjom nastanu zbog prekoračivanja granica pouzdanja u certifikat ili zbog neispunjenja obveza korisnika.

AKD može od vanjskog ugovorenog RA zahtijevati da se osigura od šteta koje mogu nastati obavljanjem usluga ugovorenih s vanjskim RA.

Pravila sudionika pružanja usluga certificiranja uređena su u skladu s Zakonom o obveznim odnosima [12].

9.2.2 Ostala sredstva

AKD raspolaže dostatnim financijskim sredstvima za ispunjenje svojih obveza i nesmetano pružanje usluga.

Informacije o radu i financijskom poslovanju AKD-a su javno objavljene na službenim stranicama AKD-a: http://www.akd.hr.

9.2.3 Osiguranje ili garancije za krajnje korisnike

AKD ima osiguran rizik od odgovornosti za štete koje nastaju pružanjem usluga certificiranja.

Polica osiguranja glasi na ukupan iznos od 265.445,62 eura.

Maksimalan iznos financijske odgovornosti koju AKD kao pružatelj usluga certificiranja prihvaća po pojedinačnoj transakciji, iskazan je identifikatorom koji se nalazi u svakom certifikatu.

Identifikator se nalazi u polju *Certificate Policies*, iskazan predzadnjom znamenkom OID broja (npr: Policy Identifier=1.3.6.1.4.1.43999.5.14.2.1.2.1).

Pravila tumačenja identifikatora su dana u poglavlju 9.8.

AKD dodatno osigurava imovinu policom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija i slično, te osiguranja od loma stroja (industrijski lom) i loma stakla, kojima se pokrivaju moguće nastale štete od ispada ili oštećenja instalacija i/ili strojne opreme.

9.3 Povjerljivost poslovnih podataka

9.3.1 Opseg povjerljivih poslovnih podataka

Povjerljivim poslovnim podacima smatraju se svi podaci, u bilo kojem obliku, koje sudionici postupka certificiranja označe povjerljivim ili koji su po prirodi povjerljivi, a zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za sudionike postupka certificiranja.

Povjerljivi poslovni podaci obuhvaćaju, ali se ne ograničavaju na:

a) osobne podatke i dokumentaciju prikupljenu u postupku registracije u skladu s poglavljem 9.4,
b) zbirke podataka, revizijski zapisi i arhiva pružatelja usluga,
c) izvještaje o provedbi aktivnosti i postupaka pružanja usluga,
d) poslovnu komunikaciju između sudionika postupka certificiranja i
e) ostale podatke različitog tipa značajne za poslovanje ili interese sudionika.

Posebna kategorija povjerljivih poslovnih podataka obuhvaća, ali se ne ograničava na:

f) sve privatne ključeve, aktivacijske podatke i podatke za registraciju na portal,
g) sve simetrične ključeve, PIN-ove, zaporke, kodove i svu šifriranu komunikaciju između sudionika, mreže ili komponenata PKI infrastrukture,

h) specifične podatke vezane uz sigurnost i provedbu mjera zaštite podataka, informacijskih sustava, poslovne suradnje, radnika i lokacije obavljanja djelatnosti i
i) planove zaštite i nacrta objekata i prostora te planove vezani uz kontinuitet poslovanja.

9.3.2 Podaci koji se ne smatraju povjerljivim poslovnim podacima

Podaci koji se ne smatraju povjerljivim poslovnim podacima su svi poslovni podaci čije priopćavanje neće štetno utjecati na poslovanje, pružanje usluga ili interese sudionika postupka certificiranja, a posebno:

certifikati, lista opozvanih certifikata i informacije o statusu certifikata,

informacije i dokumenti koji su objavljeni na portalu,

podaci čije priopćavanje neće narušiti Ustavom i zakonima propisana prava i slobode fizičkih i pravnih osoba,

podaci koje AKD objavljuje na svojim službenim stranicama ili koje je dužan objaviti radi ispunjenja obveza iz Zakona o pravu na pristup informacijama [11],

ostali podaci čija je neograničena distribucija dozvoljena ili potrebna za realizaciju poslovnih ciljeva.

9.3.3 Odgovornost za zaštitu povjerljivih poslovnih podataka

Zaštita povjerljivih poslovnih podataka provodi se u skladu s nacionalnim i europskim zakonskim propisima koji uređuju područje zaštite podataka.

Radnici i službenici koji sudjeluju u provedbi postupaka certificiranja, koji ostvaruju pristup i koji postupaju s povjerljivim poslovnim podacima iz točke 9.3.1 dužni su postupati u skladu s internim pravilima i procedurama.

Dužnost čuvanja tajne odnosi se na sve osobe i pouzdajuće strane koje su na bilo koji način saznale povjerljive poslovne podatke.

9.4 Zaštita osobnih podataka

9.4.1 Plan zaštite osobnih podataka

Zaštita osobnih podataka zajamčena je svakoj fizičkoj osobi.

Osobe su informirane da AKD i ugovorene RA pravne osobe obrađuje osobne podatke kako bi ispunio zakonom propisane zahtjeve vezane uz provedbu usluge, te da jamči zakonito postupanje i obradu svih osobnih podatka s kojima raspolaže.

AKD i ugovorene RA pravne osobe poduzima odgovarajuće tehničke i organizacijske mjere zaštite od neautorizirane ili nezakonite obrade kao i od slučajnog gubitka, uništenja ili oštećenja osobnih podataka.

Prijenos osobnih podataka između ugovorenih RA pravnih osoba i AKD-a te između autenticiranih PKI komponenata vrši se kroz šifrirane komunikacijske kanale koji osiguravaju zaštitu integriteta i tajnosti podataka.

9.4.2 Povjerljivi osobni podaci

AKD i ugovorene RA pravne osobe obrađuje osobne podatke za potrebe izdavanja certifikata.

Kako bi se ispunili zakonom propisani zahtjevi vezani uz provedbu usluge, u postupku registracije osoba prikupljaju se osobni podaci koji su navedeni u točki 3.2.3.

Osobni podaci se zadržavaju u sklopu arhive i u dijelu revizijskih zapisa kako je navedeno u točkama 5.4.1 i 5.5.1.

9.4.3 Osobni podaci koji nisu povjerljivi

AKD vodi registar certifikata te može objavljivati certifikate u javnom imeniku pod uvjetima koji su definirani u točki 4.4.2.

Osobni podaci osobe subjekta certificiranja sadržani u certifikatu su ime, prezime i OIB. U slučaju da je osiguran dokaz pripadnosti iz točke 3.2.3.1, u certifikatu mogu biti naziv i OIB organizacije za koju je dokazana pripadnost.

9.4.4 Odgovornost za zaštitu osobnih podataka

AKD i ugovorene RA pravne osobe su odgovorni za zaštitu osobnih podataka.

Osigurana je zakonita obrada osobnih podataka u skladu s odredbama Zakona o provedbi Opće uredbe o zaštiti podataka [4] i vezanih pod-zakonskih akata odnosno *Uredbe (EU) br. 2016/679* [3].

9.4.5 Ovlaštenje za korištenje osobnih podataka

Osim za potrebe ispunjenja zakonskih, odnosno ugovornih obveza po ugovorima kojima se uređuju usluge certificiranja, osobni podaci će se koristiti samo temeljem pisane privole osobe.

Prihvaćanjem Uvjeta pružanja usluga certificiranja osobe su upoznate s korištenjem danih osobnih podataka za potrebe vođenja evidencija te za objavu certifikata u javnom imeniku.

9.4.6 Dostupnost podataka mjerodavnim tijelima

Pravo pristupa osobnim podacima će se omogućiti ako to nalažu zakonski propisi ili kada to pisano zahtjeva mjerodavni sud, upravno ili neko drugo mjerodavno državno tijelo radi provedbe postupka ili istraživanja protupropisnog ili nezakonitog postupanja.

9.4.7 Ostale okolnosti objave osobnih podataka

Nema odredbi.

9.5 Prava intelektualnog vlasništva

Svi sudionici su dužni poštovati autorska prava kao i prava intelektualnog vlasništva u skladu s važećim zakonskim propisima.

AKD posjeduje i rezervira sva autorska prava i prava intelektualnog vlasništva povezana s prilagodbama vlastite infrastrukture i zbirkama podataka, izrađenim internet stranicama i objavljenim publikacijama.

AKD je autor i vlasnik svih dokumenata koji su objavljeni na portalu, uključujući opća pravila [53], pravilnik, certifikate i CRL te u skladu s važećim zakonima u Republici Hrvatskoj, AKD zadržava sva autorska i srodna prava nad njima.

AKD je razvio vlastiti izvorni kod te posjeduje i rezervira neograničena autorska prava i prava intelektualnog vlasništva na aplikaciju za QSCD uređaj (AKD eID 2.0 i AKD eID Card 1.0) kao i aplikaciju (middleware) za korištenje QSCD uređaja s kvalificiranim certifikatima isporučenog u sklopu pružanja usluga certificiranja.

AKD kao autor i vlasnik navedenih sadržaja i aplikacija na portalu raspolaže s neograničenim pravima korištenja, a osobito pravom umnožavanja, distribucije, objavljivanja i prerade.

Osobe imaju pravo korištenja QSCD uređaja i aplikacije za korištenje istog prema uvjetima korištenja licenci za krajnje korisnike (*End User Licence Agreement EULA*).

Softver i sva ostala dobra koja se koriste u pružanju usluga povjerenja, a koja su u vlasništvu AKD-a, sudionika postupka certificiranja ili bilo koje treće strane, koriste se u skladu s EULA ili dugim odredbama o pravu korištenja.

9.6 Obveze i odgovornosti

9.6.1 Obveze i odgovornosti PMA

Obveze i odgovornosti PMA su:

a) definiranje, uvođenje i administriranje CP [53], CPD, PDS, sigurnosno-operativnih procedura i provedbenih dokumenata vezanih uz djelovanje AKD PKI i pružanje usluga povjerenja,
b) Održavanje kontinuirane prikladnosti i usklađenosti općih pravila i pravilnika s *Uredbom (EU) br. 910/2014 [1]* te obvezujućim nacionalnim, europskim ili međunarodnim normama.
c) Nadzor provedbe sigurnosnih zahtjeva koja su propisani u CP [53] i CPS.

9.6.2 Obveze i odgovornosti CA

Obveze i odgovornosti CA su:

a) Osiguranje provedbe *Uredbe (EU) br. 910/2014 [1]* te primjene upravnih i upravljačkih postupaka u skladu s obvezujućim nacionalnim, europskim ili međunarodnim normama.
b) Osiguranje provedbe usluga generiranja certifikata, upravljanja opozivom certifikata, provjere statusa certifikata, usluge servisa CERTILIA mPotpis kao i usluga informiranja u skladu s ovim dokumentom.
c) Pravovremena obrada zahtjeva temeljem cjelovitih, točnih i provjerenih podataka dobivenih od RA.
d) Osiguranje osoblja koje posjeduje potrebno stručno znanje, pouzdanost, iskustvo i kvalifikacije dostatne za provedbu poslovnih aktivnosti i ispunjenje zahtjeva koji su utvrđeni ovim dokumentom.
e) Osiguranje dostatnih financijskih sredstva potrebnih za pružanje usluga certificiranja u skladu sa zahtjevima koji su utvrđeni ovim dokumentom.
f) Primjena organizacijskih, provedbenih i fizičkih mjera zaštite CA sustava i podataka u skladu s ovim dokumentom.
g) Bilježenje i dugoročno arhiviranje svih bitnih informacija u vezi s podacima koje izdaje i prima CERTILIA CA i CERTILIA mPotpis servis a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge.

h) Zakonita obrada osobnih podataka u skladu s Zakona o provedbi Opće uredbe o zaštiti podataka [4] i vezanih pod-zakonskih akata odnosno *Uredbe (EU) br. 2016/679* [3].
i) Osiguranje ISO/IEC 9001 [47] i ISO/IEC 27001 [45] certifikata kao dokaza kvalitete i sigurnosti pružanje usluga certificiranja.

9.6.3 Obveze i odgovornosti RA

Obveze i odgovornosti pružatelja usluga registracije (AKD i ugovoreni RA) su:

a) Prikupljanje i provjera podataka o identitetima osoba u skladu s ovim dokumentom.
b) Prikupljanje i provjera dokaza o postojanju organizacija i pripadnosti osoba subjekata certificiranja organizaciji
c) Zaprimanje zahtjeva osoba uključujući zahtjeve za izdavanje certifikata, zahtjeva za opoziv i suspenziju certifikata te zahtjeva za deblokadu QSCD uređaja s certifikatima te uručivanje QSCD uređaja s certifikatima.
d) Izravna provjera i nedvojbeno utvrđivanje identiteta fizičkih osoba neposrednom identifikacijom u fizičkoj prisutnosti osobe prilikom zaprimanja zahtjeva osoba, kao i prilikom uručivanja QSCD uređaja s certifikatima.
e) Upis cjelovitih, točnih i provjerenih osobnih identifikacijskih podataka o osobama i njihovim zahtjevima u evidenciju.
f) Provjera i odobravanje zahtjeva osoba te prosljeđivanje cjelovitih, točnih i provjerenih podataka.
g) Osiguranje da poslove registracije provode isključivo pouzdani i savjesni službenici RA čiji je identitet nedvojbeno utvrđen i koji su adekvatno educirani prije nego što su im dodijeljena ovlaštenja.
h) Primjena organizacijskih, provedbenih i fizičkih mjera zaštite RA sustava te svih podataka i dokumenata prikupljenih u postupku registracije.
i) Bilježenje i dugoročno arhiviranje podataka prikupljenih u postupku registracije i svih bitnih informacija u vezi s podacima koje izdaje i prima RA sustav, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge, i to najkraće na period od 7 godina od dana isteka certifikata na kojeg se odnose.
j) Zakonita obrada osobnih podataka u skladu s Zakona o provedbi Opće uredbe o zaštiti podataka [4] i vezanih pod-zakonskih akata odnosno *Uredbe (EU) br. 2016/679* [3].
k) Provedba tehničkih i organizacijskih mjera za omogućavanje pristupa uslugama registracijskog tijela osobama sa invaliditetom, gdje je to moguće.
l) Provedba poslova opisanih od a) do k) vezano uz izdavanje dvofaktorskih elektroničkih sredstava za pristup servisu CERTILIA mPotpis.

Ugovorene RA pravne osobe sklapaju ugovor o pružanju RA usluge s AKD-om te su dužne, osim navedenih, primjenjivati i poštovati i ostale obveze i odgovornosti navedene u ugovoru.

9.6.4 Obveze i odgovornosti osoba

Osoba je odgovorna:

a) da u postupku identifikacije i podnošenja zahtjeva dostavi točne, istinite i cjelovite podatke,
b) da su svi osobni podaci u certifikatu istiniti,

c) da isključivo osoba koja je navedena u certifikatu kao subjekt certificiranja ili ovlašteni predstavnik autora pečata, koristi privatni ključ koji odgovara javnom ključu u certifikatu,
d) da certifikat u trenutku njegovog korištenja nije istekao i da nije opozvan,
e) da certifikat koristi samo za legalne i autorizirane svrhe te u skladu s njihovom namjenom,
f) da odgovorno koristi i čuva QSCD koji mu je u posjedu ili dvofaktorsko sredstvo elektroničke identifikacije za pristup CERTILIA mPotpis servisu, privatne ključeve i aktivacijske podatke i registracijske kodove te da poduzima odgovarajuće mjere zaštite od neovlaštenog pristupa i uporabe,
g) da odmah zatraži opoziv ili suspenziju certifikata ako je došlo do promjene podataka upisanih u „Subject“ polje certifikata, statusa povezanosti sa organizacijom ili ako sumnja u gubitak, krađu, zlouporabu ili neautorizirano korištenje privatnog ključa i
h) da će se informirati o općim pravilima, pravilnikom i uvjetima pružanja usluga certificiranja u slučaju bilo kakvih nejasnoća i pitanja o svojim odgovornostima i obvezama te prihvatljivom načinu korištenja usluga certificiranja.

9.6.5 Obveze i odgovornosti pouzdajućih strana

Pouzdajuće strane su odgovorne:

a) da se informiraju o općim pravilima, pravilnikom i uvjetima pružanja usluga certificiranja, a posebno o svojim odgovornostima i obvezama te prihvatljivom načinu korištenja usluga certificiranja,
b) da samostalno procijene i utvrde prikladnost korištenja certifikata za odgovarajuću namjenu,
c) da prije ostvarivanja povjerenja u certifikat utvrde da certifikat nije istekao i da nije opozvan, a prema podacima koji su navedeni u certifikatu,
d) da provjeru valjanosti certifikata vrše koristeći autorizirani izvor i pouzdanu opremu,
e) da provjere status certifikata osobe i svih certifikata na certifikacijskoj stazi prema postupcima koji su navedeni u IETF RFC 5280 [38] i IETF RFC 3739 [37] i
f) da prije ostvarivanja povjerenja u elektronički potpis odnosno pečat provjere njegovu ispravnost.

9.6.6 Obveze i odgovornosti ostalih sudionika

Obveze i odgovornosti proizvođača su:

a) Priprema podataka i proizvodnja QSCD s kvalificiranim certifikatima temeljem zahtjeva i nepromijenjenih podataka dobivenih od RA.
b) Generiranje parova ključeva i aktivacijskih podataka, pribavljanje certifikata od CERTILIA te njihovo unošenje u QSCD.
c) Generiranje podataka za aktivaciju QSCD i registraciju na web portal.
d) Primjena organizacijskih, provedbenih i fizičkih mjera zaštite informacijskog sustava proizvođača i podataka u skladu s ovim dokumentom.
e) Zakonita obrada osobnih podataka u skladu s Zakona o provedbi Opće uredbe o zaštiti podataka [4] i vezanih pod-zakonskih akata odnosno *Uredbe (EU) br. 2016/679* [3].

f) Osiguranje ISO/IEC 9001 [47], ISO/IEC 27001 [45] i ISO/IEC 14298 [44] certifikata kao dokaza kvalitete upravljanja poslovanjem i proizvodnjom zaštićenog tiska te sigurnošću informacijskih sustava.

g) Osiguranje da je uređaj na koji se izdaju certifikati kvalificirano sredstvo za izradu elektroničkog potpisa (QSCD), da zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 [43] te da demonstrira sukladnost s obrascima zaštite iz serije EN 419 211 [25], [26], [27], [28], [29] i [30].

Obveze i odgovornosti dobavljača HSM uređaja i ostalih proizvoda, usluga i rješenja povezanih sa pružanjem usluga certificiranja definiraju se u ugovorima sa dobavljačima.

9.7 Odricanje od odgovornosti

AKD daje jamstvo samo za ono za što je kao pružatelj usluga odgovoran, a što je izričito navedeno da je odgovornost AKD-a u točki 9.6.

AKD ne daje jamstvo za:

a) štete koje su prouzročene neprimjerenom uporabom certifikata prema poglavlju 1.4.2,

b) štete prouzročene lažnom ili nemarnom uporabom QSCD uređaja koji je u posjedu osobe, aktivacijskih podataka, certifikata ili CRL-a odnosno odgovora OCSP servisa,

c) štete koje su pretrpljene u vremenu od opoziva certifikata do izdavanja sljedeće CRL,

d) štete prouzročene neispravnošću i pogreškama u softveru i hardveru osobe ili pouzdajuće strane i

e) sve štete koje je namjerno ili nepažnjom prouzročila osoba ili pouzdajuća strana koja ne ispunjava svoje obveze ili ne djeluje u skladu sa svojim obvezama navedenim u 9.6.4 i 9.6.5,

AKD nije odgovoran za štete koje su rezultat davanja pogrešnih informacija u postupku registracije ili lažnog predstavljanja osobe tijekom procesa identifikacije i potvrde identiteta.

AKD ne daje jamstvo ako je došlo do povrede odgovornosti ostalih sudionika, a posebno za upotrebu certifikata izdanih od drugih pružatelja usluga certificiranja.

AKD nije odgovoran za indirektne štete koje mogu proizaći iz korištenja certifikata.

9.8 Ograničenja odgovornosti

Ukupna financijska odgovornost za transakcije obavljene na temelju pouzdavanja u certifikate izdane prema ovom dokumentu iznosi najviše 265.445,62 eura.

Prema osobama i pouzdajućim stranama koje primjereno koriste certifikate visina financijske odgovornosti za transakcije se ograničava, sukladno preporučenom financijskom limitu.

Maksimalan iznos financijske odgovornosti koju AKD kao izdavatelj certifikata prihvaća po pojedinačnoj transakciji, iskazan je predzadnjom znamenkom OID broja u certifikatu, kao identifikatorom.

Primjenjuju se slijedeća pravila:

Identifikator	Financijski limit
1	do 1.061,78 eura
2	do 10.617,82 eura
3	do 53.089,12 eura

9.9 Naknada štete

Svaki sudionik koji je prouzročio štetu zbog nepoštivanja odredbi primjenjivih zakona, normi, općih pravila i pravilnika odgovarati će oštećenom sudioniku.

Fizička i pravna osoba odgovara oštećenoj strani ako:

a) stekne certifikat izdan od CERTILIA temeljem prijevarno danih podataka u zahtjevu za izdavanje certifikata ili
b) djeluje ili se predstavlja u ime druge osobe.

Pouzdajuća strana odgovara oštećenoj strani ako:

a) se pouzda u certifikat bez provjere njegove valjanosti ili
b) neprimjereno koristi certifikat u svrhe za koje nije namijenjen ili unatoč zadanim ograničenjima.

AKD je odgovoran ako je ta odgovornost jasno uspostavljena uvjetima pružanja usluga, korištenja, općim pravilima, pravilnikom ili zakonskom regulativom.

9.10 Trajanje i prestanak valjanosti

9.10.1 Trajanje

Primjena pravila koja su navedena u ovome dokumentu počinju datumom objavljivanja dokumenta na web portalu kako je navedeno u točki 2.2.

PMA odlučuje o potrebi izmjene ili dopune dokumenta kao i o objavi dokumenta na portalu.

9.10.2 Prestanak valjanosti

Dokument prestaje biti valjan kad ga zamijeni novije izdanje dokumenta ili kad se objavi prestanak valjanosti dokumenta.

Informacija o prestanku valjanosti ili objavi nove verzije dokumenta će biti objavljena putem portala.

Prestanak valjanosti dokumenta neće utjecati na valjanost certifikata koji su izdani po pravilima koja su navedena u ranijem izdanju dokumentu, a dok je on bio valjan.

9.10.3 Posljedice prestanka valjanosti i nastavak djelovanja

Pojavom novijeg izdanja dokumenta počinju se primjenjivati i nova pravila koja su u njemu navedena.

Certifikati koji su izdani po pravilima koja su navedena u ranijem izdanju dokumentu će biti valjani sve do isteka perioda valjanosti certifikata ili do opoziva certifikata.

9.11 Pojedinačne obavijesti i komunikacija sa sudionicima

Informiranje osoba i pouzdajućih strana se provodi putem portala.

Komunikacija s AKD se provodi se pisanim putem ili elektroničkom poštom korištenjem kontaktnih podataka koji su navedeni u tablici 13.

Tablica 13: Kontakt podaci AKD-a

Kontakt podaci AKD-a:	
Poštanska adresa:	AKD d.o.o Savska cesta 31 10000 Zagreb Hrvatska
e-mail:	pma@akd.hr

9.12 Izmjene i dopune

9.12.1 Postupak izmjena i dopuna

Sve značajne promjene koje utječu na sudionike objavljuju se kroz nova izdanja dokumenta po proceduri koja je navedena u točki 9.12.2.

Zatipci, manje ispravke ili promjene koje ne utječu na sudionike objavljivati će se kroz inačice dokumenta bez prethodne obavijesti i bez promjene izdanja dokumenta.

Izdanje dokumenta se označava prvim brojem u oznaci izdanja dokumenta, dok su inačice naznačene drugim brojem iza točke.

Svaki sudionik može inicirati promjenu dokumenta korištenjem kontaktnih podataka navedenih u točki 9.11, a PMA će razmotriti prijedlog i odlučiti hoće li prijedlog prihvatiti ili odbiti.

Ako PMA procijeni da predložena promjena nije u skladu sa zakonskim propisima i normama ili može umanjivati kvalitetu pružanja usluga, prijedlog sudionika će biti odbijen.

9.12.2 Način obavještavanja i period

O pojavi novog izdanja dokumenta sudionici će biti obaviješteni putem portala odmah po objavljivanju dokumenta.

O pojavi novije inačice dokumenta sudionici se neće obavještavati.

Prihvaćeni prijedlozi sudionika će se uvrstiti u novo izdanje dokumenta.

9.12.3 Okolnosti pod kojima se mora mijenjati OID

Manje ispravke ili promjene sadržaja CP ili CPS koje ne utječu bitno na sudionike objavljivati će se bez promjene OID-a.

Ako PMA odredi da je promjena CP ili CPS značajna i da može utjecati na sudionike, tada će odrediti novi OID koji će identificirati odgovarajući certifikat ili grupu certifikata.

9.13 Postupak rješavanja sporova

Svi sporovi i neslaganja među sudionicima će se nastojati razriješiti sporazumno. Ako sporazumno razrješenje spora nije postignuto, sporovi će se razriješiti pred mjerodavnim sudom u Zagrebu uz primjenu prava Republike Hrvatske.

9.14 Važeći propisi

Za tumačenje odredbi ovoga dokumenta mjerodavne su odredbe *Uredbe (EU) br. 910/2014 [1]*, zakoni koji su referencirani u ovom dokumentu, podzakonski akti doneseni temeljem navedene uredbe ili zakona, te obvezujuće nacionalne, europske ili međunarodne norme koje su referencirane u ovom dokumentu.

9.15 Usklađenost s važećim propisima

Ovaj dokument je usklađen s važećim propisima kako je navedeno u točki 9.14.

U skladu s *Uredbom (EU) br. 910/2014 [1]*, AKD je kvalificirani pružatelj usluga povjerenja kojem je ministarstvo Republike Hrvatske nadležno za poslove gospodarstva kao nadzorno tijelo odobrilo kvalificirani status.

9.16 Ostale odredbe

Ako to nije protivno zakonskim propisima, odredbama općih pravila ili pravilnika, AKD kao pružatelj usluga povjerenja može s ostalim sudionicima sklopiti ugovor u kojem će se ugovorne strane obvezati na poštivanje obvezujućih zakonskih propisa i normi koji su navedeni u poglavlju 9.14, kao i pravilnika i općih pravila.

PRILOG 1: Definicije

1. „elektronička identifikacija" znači postupak korištenja osobnim identifikacijskim podacima u elektroničkom obliku koji na nedvojben način predstavljaju bilo fizičku ili pravnu osobu ili fizičku osobu koja predstavlja pravnu osobu;
2. „sredstvo elektroničke identifikacije" znači materijalna i/ili nematerijalna jedinica koja sadrži osobne identifikacijske podatke i koja se koristi za autentikaciju na *on-line* uslugu;
3. „osobni identifikacijski podaci" znači skup podataka koji omogućavaju da se utvrdi identitet fizičke ili pravne osobe ili fizičke osobe koja predstavlja pravnu osobu;
4. „sustav elektroničke identifikacije" znači sustav za elektroničku identifikaciju u okviru kojega se izdaju sredstva elektroničke identifikacije fizičkim ili pravnim osobama ili fizičkim osobama koje predstavljaju pravne osobe;
5. „autentikacija" znači elektronički postupak koji omogućava da elektronička identifikacija fizičke ili pravne osobe ili izvornost i cjelovitost podataka u elektroničkom obliku budu potvrđeni;
6. „pouzdajuća strana" znači fizička ili pravna osoba koja se oslanja na elektroničku identifikaciju ili uslugu povjerenja;
7. „tijelo javnog sektora" znači državno, regionalno ili lokalno tijelo, javnopravno tijelo ili udruženje koje se sastoji od jednog ili nekoliko takvih tijela ili jednog ili nekoliko takvih javnopravnih tijela ili privatni subjekt koji je ovlastilo barem jedno od tih vlasti, tijela ili udruženja za pružanje javnih usluga kada djeluju u okviru takve ovlasti;
8. „potpisnik" znači fizička osoba koja izrađuje potpis;
9. „autor pečata" znači pravna osoba koja izrađuje elektronički pečat;
10. „elektronički potpis" znači podaci u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje;
11. „napredan elektronički potpis" znači elektronički potpis koji ispunjava zahtjeve navedene u članku 26. *Uredbe (EU) br. 910/2014 [1]*;
12. „kvalificirani elektronički potpis" znači napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise;
13. „podaci za izradu elektroničkog potpisa" znači jedinstveni podaci koje osoba subjekt certificiranja koristi za izradu elektroničkog potpisa;
14. „certifikat za elektronički potpis" znači elektronička potvrda koja povezuje podatke za validaciju elektroničkog potpisa s fizičkom osobom i potvrđuje barem ime ili pseudonim te osobe;
15. „kvalificirani certifikat za elektronički potpis" znači certifikat za elektroničke potpise koji izdaje kvalificirani pružatelj usluga povjerenja i koji ispunjava zahtjeve utvrđene u Prilogu I. *Uredbe (EU) br. 910/2014 [1]*;
16. „elektronički pečat" znači podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka;

17. „napredan elektronički pečat" znači elektronički pečat koji ispunjava zahtjeve navedene u članku 36. *Uredbe (EU) br. 910/2014 [1]*;
18. „kvalificirani elektronički pečat" znači napredan elektronički pečat koji je izrađen pomoću kvalificiranog sredstva za izradu elektroničkog pečata i koji se temelji na kvalificiranom certifikatu za elektronički pečat;
19. „podaci za izradu elektroničkog pečata" znači jedinstveni podaci koje autor elektroničkog pečata koristi za izradu elektroničkog pečata;
20. „certifikat za elektronički pečat" znači elektronička potvrda koja povezuje podatke za validaciju elektroničkog pečata s pravnom osobom i potvrđuje naziv te osobe;
21. „kvalificirani certifikat za elektronički pečat" znači certifikat za elektronički pečat koji izdaje kvalificirani pružatelj usluge povjerenja i koji ispunjava zahtjeve određene u Prilogu III. *Uredbe (EU) br. 910/2014 [1];*
22. „sredstvo za izradu elektroničkog pečata" znači konfigurirani softver ili hardver koji se koristi za izradu elektroničkog pečata;
23. „sredstvo za izradu kvalificiranog elektroničkog pečata" znači sredstvo za izradu elektroničkog pečata koje mutatis mutandis ispunjava zahtjeve određene u Prilogu II *Uredbe (EU) br. 910/2014 [1];*
24. „usluga povjerenja" znači elektronička usluga koja se u pravilu pruža uz naknadu i koja se sastoji od:
    a) izrade, verifikacije i validacije elektroničkih potpisa, elektroničkih pečata ili elektroničkih vremenskih žigova, usluge elektroničke preporučene dostave i certifikata koji se odnose na te usluge; ili
    b) izrade, verifikacije i validacije certifikata za autentikaciju mrežnih stranica; ili
    c) čuvanja elektroničkih potpisa, pečata ili certifikata koji se odnose na te usluge;
25. „kvalificirana usluga povjerenja" znači usluga povjerenja koja ispunjava odgovarajuće zahtjeve utvrđene u ovoj Uredbi;
26. „tijelo za ocjenjivanje sukladnosti" znači tijelo u smislu članka 2. točke 13. Uredbe (EZ) br. 765/2008 [9] koje je u skladu s tom Uredbom ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža;
27. „pružatelj usluga povjerenja" znači fizička ili pravna osoba koja pruža jednu ili više usluga povjerenja bilo kao kvalificirani ili nekvalificirani pružatelj usluga povjerenja;
28. „kvalificirani pružatelj usluga povjerenja" znači pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status;
29. „proizvod" znači hardver ili softver ili odgovarajuće komponente hardvera ili softvera koji su namijenjeni za korištenje u svrhu pružanja usluga povjerenja;
30. „sredstvo za izradu elektroničkog potpisa" znači konfigurirani softver ili hardver koji se koristi za izradu elektroničkog potpisa;
31. „sredstvo za izradu kvalificiranog elektroničkog potpisa" znači sredstvo za izradu elektroničkog potpisa koje mutatis mutandis ispunjava zahtjeve određene u Prilogu II *Uredbe (EU) br. 910/2014 [1];*
32. "certifikat": javni ključ korisnika koji je zajedno s ostalim informacijama šifriran privatnim ključem CA koji ga je izdao, tako da se ne može krivotvoriti;

33. "Opća pravila pružanja usluga certificiranja (CP)": imenovani skup pravila koja ukazuju na prikladnost certifikata za određenu zajednicu i/ili skupinu sa zajedničkim sigurnosnim zahtjevima;
34. "Lista opozvanih certifikata CRL": potpisana lista s nizom certifikata koje izdavatelj više ne smatra valjanim;
35. "Certifikacijsko tijelo (CA)": tijelo kojem vjeruje jedan ili više korisnika, a koje kreira i dodjeljuje certifikate;

    Napomena 1: CA može biti:

    1) pružatelj usluga povjerenja koji kreira i dodjeljuje javni ključ certifikata; ili
    2) usluga tehničkog generiranja certifikata koju koristi pružatelj usluga certificiranja da kreira i dodjeljuje javni ključ certifikata.
36. "Pravilnik o postupcima certificiranja (CPS)": izjava o praksi koju primjenjuju radnici certifikacijskog tijela u upravljanju postupkom izdavanja, opoziva, obnove ili izdavanja certifikata s novim parom ključeva;
37. "koordinirano svjetsko vrijeme (UTC)": vremenska skala koja je definirana u preporuci ITU-R TF.460-6 [52];
38. „digitalni potpis": podaci koji se dodaju podatkovnom skupu ili kriptografska transformacija podatkovnog skupa koja omogućuje njegovom primatelju dokazivanje izvornosti i cjelovitosti podatkovnog skupa te koja podatkovni skup štiti od krivotvorenja, npr. od strane primatelja;
39. "zona visoke sigurnost": specifična fizička lokacija gdje se čuva privatni ključ krovnog CA;
40. "Registracijsko tijelo (RA)": tijelo koje je prvenstveno odgovorno za identifikaciju i autentikaciju subjekta certifikata;

    Napomena 1: RA pomaže u postupku podnošenja zahtjeva za izdavanje i opoziv certifikata;
41. "službenik RA": radnik odgovoran za provjeru informacija i pripremu podataka koja se nužno provodi pri izdavanju certifikata i odobrenje zahtjeva za izdavanje certifikata;
42. "službenik za opoziv": radnik odgovoran za provedbu zahtjeva za promjenu statusa certifikata;
43. "krovno certifikacijsko tijelo (krovni CA)": certifikacijsko tijelo koje na najvišem nivou djeluju u sklopu hijerarhijske strukture i koje potpisuje certifikat podređenim CA;
44. "siguran kriptografski uređaj": uređaj koji čuva privatni ključ korisnika, štiti taj ključ od kompromitacije i provodi operacije potpisivanja ili dešifriranja u ime korisnika;
45. „sigurna zona": zona (fizička ili logička) zaštićena fizičkim i logičkim kontrolama tako da na odgovarajući način štiti povjerljivost, izvornost i dostupnost sustava pružatelja usluga povjerenja;
46. "subjekt": osoba identificirana u certifikatu kao vlasnik privatnog ključa koji odgovara javnom ključu u certifikatu;
47. Osobe naručitelji (engl. Applicant ili Subscriber) su fizičke ili pravne osoba koje su podnijeli zahtjev za izdavanje certifikata, te su ujedno i vlasnici certifikata;
48. Osobe subjekti certificiranja (engl. Subject); fizičke osobe čije je ime, prezime navedeno u subjektu certifikata u poljima Common name i(li) givenName i surname, odnosno osobni identifikacijski broj sadržan u polju serialNumber;
49. "podređeno certifikacijsko tijelo (podređeni CA): certifikacijsko tijelo čiji je certifikat potpisan korovnim CA;

    Napomena: Podređeni CA izdaje certifikat krajnjim korisnicima.

50. udaljeni uređaj za kreiranje elektroničkog potpis: uređaj za kreiranje elektroničkog potpisa kojem potpisnik ili autor pečata pristupa udaljeno i koji pruža potpunu kontrolu nad procesom elektroničkog potpisivanja u ime potpisnika ili autora pečata;
51. komponenta za serversko potpisivanje server (engl. signing application service component ili SSASC: servis pouzdanog pružatelja usluge koji koristi serversku aplikaciju (okružje) za izradu elektroničkog potpisa u ime potpisnika ili autora pečata;
52. pružatelj servisa za serversko potpisivanje (engl. server signing application service provider ili SSASP): pouzdani pružatelj usluge koji upravlja okružjem za serversko potpisivanje;
53. uređaj za kreiranje elektroničkog potpisa (engl. signature creation device ili SCDev): konfigurirani softver ili hardver koji se koristi za kreiranje podataka potrebnih za izradu elektronički potpisa i za kreiranje elektroničkog potpisa;
54. Pravila izdavanja vremenskog žiga ili TSP/PS (engl. Time-Stamp Policy/ Practice Statement): Imenovani skup pravila koji ukazuje na prikladnost vremenskog žiga za određenu skupinu i/ili grupu primjena sa zajedničkim sigurnosnim zahtjevima;
55. Postupci izdavanja vremenskog žiga ili TSP/PS (engl. Time-Stamp Policy/ Practice Statement): Skup operativnih postupaka koje primjenjuje TSA kod izdavanja vremenskog žiga i kod upravljanja postupcima izdavanja vremenskog žiga;
56. Usluga vremenskog žiga (engl. Time-stamping service): Usluga povjerenja za izdavanje vremenskih žigova;
57. Pružatelj usluga vremenskog žiga (engl. Time-Stamping Authority - TSA): Pružatelj usluge izdavanja vremenskog žiga koji koristi jednu ili više jedinica za izradu vremenskog žiga;
58. Jedinica za izradu vremenskog žiga (engl. Time-Stamping Unit - TSU): Skup hardvera i softvera združen u jednu cjelinu koja u danom trenutku ima samo jedan aktivan potpisni ključ za izradu vremenskog žiga;
59. UTC(k): Vremenska skala koja se ostvaruje u laboratoriju „k“ i koja se čuva u bliskom dogovoru s UTC, a s ciljem postizanja ± 100 ns;
60. Aktivacijski podaci: tajni podaci potrebni za pristup ili aktivaciju kriptografskog uređaja. Aktivacijski podatak može biti PIN, zaporka, kod ili elektronički ključ kojeg osoba zna ili posjeduje;
61. Registracijski kodovi: podaci potrebni za registraciju certifikata i postavljanje PINa za privatni ključ u CERTILIA mPotpis servisu koji upravlja udaljenim QSCD uređajem za kreiranje udaljenog elektroničkog potpisa,
62. Pravna osoba: društvena tvorevina kojoj je pravni poredak priznao pravnu i poslovnu sposobnost i za koju se provjerom u nadležnom nacionalnom registru može utvrditi pravna osobnost, pravo za obavljanje gospodarskih djelatnosti ili drugo registrirano djelovanje više osoba pod zajedničkim imenom.

PRILOG 2: Kratice

AKD	AKD d.o.o.
AKDCA	Certifikacijsko tijelo AKD
HRIDCA	Certifikacijsko tijelo za izdavanje certifikata osobama za potrebe elektroničke osobne iskaznice građana Republike Hrvatske
CERTILIA	Certifikacijsko tijelo za izdavanje kvalificiranih certifikata fizičkim i pravnim osobama i organizacijama u komercijalne svrhe
PKI	Public Key Infrastructure
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
CP	Certificate Policy
CPS	Certificate Practice Statement
TSP/PS	Time-stamp Policy/Practice Statement
TSA	Time-Stamping Authority
EUSCP	EU SSASC Policy
SSASC	Server Signing Application Service Component
SSASC PS	SSASC Practice Statement
CERTILIA mPotpis	AKD SSASC
SCP	SSASC Policy
SSASP	Server Signing Application Service Provider
QCP	Qualified Certificate Policy
PMA	Policy Management Authority
CA	Certificate Authority
RA	Registration Authority
LRA	Local Registration Authority
OID	Object Identifier - Identifikacijska oznaka
SCD/ SCDev	Signature Creation Device
SSCD	Secure Signature Creation Device
QSCD	Qualified Electronic Signature Creation Device
IdP	Identity Provider
AKD IDP	AKD Identity Provider
DTBS	Data to be Signed
SAD	Signature Activation Data
CRL	Certificate Revocation List
LDAP	Lightweight Directory Access Protocol
OCSP	On-line Certificate Status Protocol

HTTP	Hypertext Transfer Protocol
UTC	Coordinated Universal Time
RSA	Rivest, Shamir and Adleman algorithm
ECDSA	Elliptic-curve Digital Signature algoritam
ECDH	Elliptic-curve Diffie–Hellman protokol
AES	Advanced Encryption Standard
HSM	Hardware security module
FIPS	Federal Information Processing Standard
X.509	Public Key Infrastructure Standard
PIN	Personal Identification Number
PUK	Personal Unblocking Code
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
EULA	End User Licence Agreement
PDS	PKI Disclosure Statement
PTC	Publicly-Trusted Certificate
TSU	Time-Stamping Unit

PRILOG 3: Reference

EU i nacionalni akti:

[1] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ, *koju je izmijenila Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. i Uredba (EU) 2024/1183 Europskog parlamenta i Vijeća od 11. travnja 2024. koju je ispravio Ispravak Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014*.

[2] Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnje tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/2017).

[3] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ.

[4] Zakon o provedbi opće Uredbe o zaštiti podataka (NN 42/2018).

[5] Provedbena odluka komisije (EU) 2015/1502 od 8. rujna 2015. o utvrđivanju minimalnih tehničkih specifikacija i postupaka za razine osiguranja identiteta koje se pripisuju sredstvima elektroničke identifikacije u skladu s člankom 8. stavkom 3. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.

[6] Provedbena odluka komisije (EU) 2016/650 od 25. travnja 2016. o utvrđivanju normi za ocjenu sigurnosti kvalificiranih sredstava za izradu potpisa i pečata u skladu s člankom 30. stavkom 3. i člankom 39. stavkom 2. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.

[7] Provedbena odluka komisije (EU) 2015/296 od 24. veljače 2015. o utvrđivanju postupovnih aranžmana za suradnju među državama članicama u području elektroničke identifikacije u skladu s člankom 12. stavkom 7. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.

[8] Provedbena odluka komisije (EU) 2015/1501 od 8. rujna 2015. o okviru za interoperabilnost u skladu s člankom 12. stavkom 8. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.

[9] Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/1993.

[10] Zakon o javnom bilježništvu (NN 78/1993, 29/1994, 162/1998, 16/2007, 75/2009, 120/2016).

[11] Zakon o pravu na pristup informacijama (NN 25/2013, 85/2015).

[12] Zakon o obveznim odnosima (NN 35/2005, 41/2008, 125/2011, 78/2015, 29/2018).

Normizacijski dokumenti:

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

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

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

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

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

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

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

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

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

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

[23] ETSI TS 119 431-1: „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev“.

[24] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

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

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

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

[28] CEN EN 419 211-4: "Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application“.

[29] CEN EN 419 211-5: "Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application“.

[30] CEN EN 419 211-6: "Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted communication with signature creation application“.

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

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

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

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

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

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

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

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

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

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

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

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

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

[44] ISO/IEC 14298: "Graphic technology - Management of security printing processes".

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

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

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

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

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

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

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

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

AKD dokumenti:

[53] AKD PKI Opća pravila pružanja usluga certificiranja.

[54] AKD QTSA Pravila i postupci pružanja usluga vremenskog žiga.

[55] AKD Upute za rad RA ureda.

PRILOG 4: Povijest promjena dokumenta

Izdanje	Datum	Obrazloženje izmjene
0.1	02.05.2023.	Nacrt 1. izdanja CERTILIA Pravilnik o postupcima certificiranja
1.0	24.05.2023.	Usvojena i odobrena verzija dokumenta.
1.1	01.06.2025	Usklađivanje roka čuvanja zapisa s EN 319 411, na 7 godina od isteka valjanosti certifikata. Izmjene u regulativi i u algoritmu za potpisivanje certifikata izdanih na pametnim karticama i prestanak korištenja sigurnosnih omotnica. Dodan atribut Key Agreement u polje Key Usage i Smart Card Logon atribut u polje Extended Key Usage korisničkog identifikacijskog certifikata.