HRIDCA
PRAVILNIK O POSTUPCIMA CERTIFICIRANJA

Verzija za javnu objavu

Izdanje 2.1

Vrijedi od 20. 04. 2018.

Sadržaj:

Predgovor

Hrvatska elektronička osobna iskaznica (u daljnjem tekstu: eOI) je identifikacijski dokument hrvatskih državljana koju izdaje Ministarstvo unutarnjih poslova (u daljnjem tekstu: MUP) temeljem Zakona o osobnoj iskaznici [1].

eOI je obavezna isprava za hrvatske državljane starije od 18 godina s prijavljenim prebivalištem u Republici Hrvatskoj, a pravo na eOI ima svaki državljanin Republike Hrvatske. Osobe, u ovisnosti o starosti, na čipu eOI dobivaju par ključeva i odgovarajuće certifikate.

Na elektroničkoj osobnoj iskaznici izdaju se dva tipa certifikata:

a) Identifikacijski certifikat koji je sredstvo elektroničke identifikacije i ispunjava zahtjeve za visoku razinu sigurnosti prema čl. 8 točka 2 c) Uredbe (EU) br. 910/2014 [9].
b) Potpisni certifikat koji je kvalificirani certifikat za elektronički potpis i ispunjava zahtjeve utvrđene u Prilogu I Uredbe (EU) br. 910/2014 [9].

Oba certifikata izdaje Agencija za komercijalnu djelatnost d.o.o. (u daljnjem tekstu: AKD) koja je kvalificirani pružatelj usluga povjerenja i kojoj je ministarstvo RH nadležno za gospodarstvo kao nadzorno tijelo odobrilo kvalificirani status.

Elektronička osobna iskaznica je kvalificirano sredstvo za izradu elektroničkog potpisa te ispunjava zahtjeve utvrđene u Prilogu II *Uredbe (EU) br. 910/2014* [9].

1. Uvod

1.1. Pregled dokumenta

Ovaj dokument „HRIDCA Pravilnik o postupcima certificiranja“ (u daljnjem tekstu: pravilnik ili CPS) detaljno specificira organizacijske i tehničke mjere koje se u praksi primjenjuje certifikacijsko tijelo HRIDCA prilikom utvrđivanja identiteta, izdavanja certifikata i upravljanja njihovim životnim ciklusom.

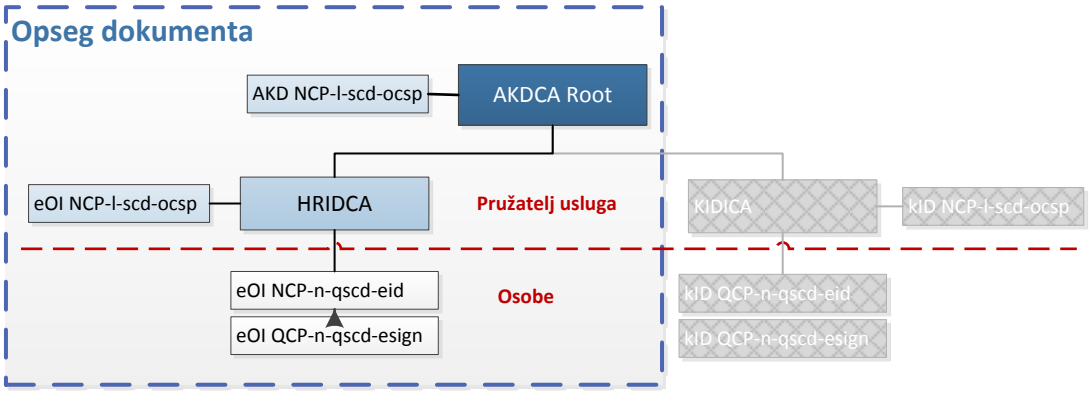
Pravilnik je usklađen s dokumentom „AKD PKI Opća pravila pružanja usluga certificiranja“ (engl. *Certificate Policy* – CP, u daljnjem tekstu: opća pravila ili CP) koji se primjenjuje na cijelu hijerarhijsku infrastrukturu zasnovanu na krovnom certifikacijskim tijelu AKDCA Root koje je izdalo certifikat samom sebi te podređenom certifikacijskom tijelu HRIDCA.

Prema IETF RFC 3647 [33], pravilnik odgovara dokumentu „*Certification Practice Statement – CPS*“ tako da su struktura i sadržaj dokumenta strogo usklađeni sa zahtjevima ove norme.

1.1.1. Opseg dokumenta

Pravila navedena u ovom dokumentu primjenjuju se na podređeno certifikacijsko tijelo HRIDCA kojem je certifikat izdalo krovno certifikacijsko tijelo AKDCA Root.

Slika 1: Opseg dokumenta



HRIDCA izdaje osobne certifikate fizičkim osobama isključivo za potrebe izdavanja eOI, a to su potpisni certifikat (eOI QCP-n-qscd-esign) i identifikacijski certifikat (eOI NCP-n-qscd-eid).

HRIDCA ne izdaje certifikate pravnim osobama osim OCSP certifikata kojeg izdaje sebi i koji je u funkciji pružanja usluga.

1.1.2. Namjena dokumenta

Ovaj je dokument namijenjen:

- pružatelju usluga povjerenja kako bi u praksi osigurao provedbu sigurnosnih zahtjeva koji su definirani u CP i
- tijelima za ocjenjivanje sukladnosti i nadzornim tijelima za procjenu sposobnosti AKD-a da pruža kvalificirane usluge povjerenja i da ima status kvalificiranog pružatelja usluge.

Ova verzija dokumenta objavljena je na internetskim stranicama. Dokument ne sadrži poslovno povjerljive informacije, a omogućuje osobama i pouzdajućim stranama da se detaljnije

upoznaju sa svojim pravima i obvezama i da procijene prikladnost certifikata za određenu namjenu.

Sigurnosni zahtjevi definirani u ovome dokumentu te primijenjeni u praksi, usklađeni su sa strogim zahtjevima za kvalificirane pružatelje usluga povjerenja i kvalificirane usluge povjerenja koje oni pružaju, a koji su propisani Uredbom (EU) br. 910/2014 [9] i Zakonom o elektroničkom potpisu [7].

1.2. Naziv dokumenta i identifikacija

1.2.1. Naziv dokumenta

Tablica 1: Naziv dokumenta

Oznaka :	PRO-I-91-02
Naziv:	HRIDCA Pravilnik o postupcima certificiranja (Verzija za javnu objavu)
Izdanje:	2.1
Datum objave:	20.04.2018.
Autor:	AKD, Agencija za komercijalnu djelatnost d.o.o
OID:	1.3.6.1.4.1.43999.5.1, 1.3.6.1.4.1.43999.5.2
Tip dokumenta:	Certificate Practice Statement
Dostupnost:	http://eid.hr/cps

Tablica 2: Povijest promjena dokumenta

Izdanje	Datum	Obrazloženje izmjene
1.3	08.06.2015.	Prvo objavljeno izdanje dokumenta
1.4	28.06.2016.	Specificirana učestostalost provjere medija u točiki 5.5.3 d).
2.0	26.06.2017.	Usklađivanje s Provedbenim odlukama EU iz 2015 i novim ETSI normama
2.1	20.04.2018.	Ispravci zatipaka i uočenih pogrešaka u dokumentu.

1.2.2. Identifikacijska oznaka

Identifikacijska oznaka (OID) rezerviran od strane AKD je: 1.3.6.1.4.1.43999.

Identifikacijska oznaka krovnog certifikacijskog tijela AKDCA Root je 1.3.6.1.4.1.43999.5.

Identifikacijske oznake koje su pokrivene ovim CPS su:

a) eOI Kvalificirani certifikati

   Pravila po kojima se izdaju eOI QC certifikati ekvivalentna su pravilima **QCP-n-qscd**, prema točki 5.3 ETSI EN 319 411-2 [27] koja se primjenjuju za EU kvalificirane certifikate za fizičke osobe s privatnim ključem na kvalificiranom sredstvu za izradu elektroničkog potpisa. (OID: 0.4.0. 194112.1.2)

b) eOI Normalizirani certifikati

   Pravila po kojima se izdaju eOI NC certifikati ekvivalentna su pravilima **NCP+**, prema točki 5.3 ETSI EN 319 411-1 [26], a koja se primjenjuju za normalizirane certifikate s privatnim ključem na sigurnom kriptografskom uređaju. (OID: 0.4.0.2042.1.2)

Identifikacijske oznake certifikata koje izdaje HRIDCA, a koje su pokrivene ovim CPS su navedene u sljedećoj tablici:

Tablica 3: Identifikacijska oznaka HRIDCA certifikata

Naziv	Oznaka	OID
Naziv	Oznaka	OID
eOI Potpisni certifikat	eOI QCP-n-qscd-esign	1.3.6.1.4.1.43999.5.1.2.1.2.10
eOI Identifikacijski certifikat	eOI NCP-n-qscd-eid	1.3.6.1.4.1.43999.5.1.2.1.2.20
eOI OCSP certifikat*	eOI NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.2.1.2.1.9

*OCSP certifikat je u funkciji pružanja usluga i ne izdaje se javnosti.

1.3. PKI Sudionici

U kontekstu ovoga dokumenta, sudionici AKD PKI su:

a) Povjerenstvo za upravljanje pravilima certificiranja (eng. *Policy Management Authority – PMA*),
b) Certifikacijsko tijelo (eng. *Certification Authority – CA*),
c) Registracijsko tijelo (eng. *Registration Authority –RA*),
d) Osobe,
e) Pouzdajuće strane (*eng. Relying party*) i
f) Proizvođač.

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

1.3.1. Povjerenstvo za upravljanje pravilima certificiranja – PMA

AKD je pružatelj usluga povjerenja koji izdaje certifikate, kojem vjeruju osobe i pouzdajuće strane i koji 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 pružanja usluga certificiranja (CP), uvjeta pružanja usluga certificiranja (PDS), ovog pravilnika o postupcima certificiranja (CPS) te sigurnosno operativnih procedura i provedbenih dokumenata vezanih uz djelovanje 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.

1.3.2. 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 i 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 certifikatima, pravilima i uvjetima certificiranja te ostalim informacijama vezanim uz certifikate i usluge certificiranja.

PKI infrastruktura uspostavljena od strane AKD PKI uređena je hijerarhijski kako je opisano u točki 1.1.1.

1.3.3. Registracijsko tijelo - RA

Ministarstvo unutarnjih poslova (MUP) je nadležno tijelo državne uprave za izdavanje eOI.

MUP je registracijsko tijelo (u daljnjem tekstu: pružatelj usluga registracije ili RA) koji provjerava identitete i identifikacijske podatke fizičkih osoba temeljem kojih HRIDCA izdaje, obnavlja, opoziva i suspendira certifikate.

MUP samostalno upravlja svojim osobljem u policijskim upravama i policijskim postajama (PU/PP) koje djeluju kao lokalni registracijski uredi (eng. Local Registration Authority - LRA) i koji obavljaju poslove registracije osoba u skladu s Zakonom o osobnoj iskaznici [1].

Poslovi PU/PP su:

a) informiranje osoba o postupcima registracije i izdavanja eOI,
b) zaprimanje zahtjeva za izdavanje, opoziv i suspenziju certifikata na eOI,
c) utvrđivanje identiteta osoba i podnositelja zahtjeva,
d) omogućavanje sklapanja ugovora s fizičkim osobama,
e) uručivanje certifikata i eOI.

MUP i AKD sklopili su ugovor kojim se je MUP obvezao da će osigurati provedbu sigurnosnih pravila i postupaka koji su opisani u ovome dokumentu, posebno u poglavlju 3 te točkama 5.3 i 5.5.

1.3.4. Osobe

Osobe su fizičke osobe kojima je izdana OI, koje su dobile certifikat na osobnoj iskaznici i koje su s AKD-om potpisale Ugovor o pružanju usluga certificiranja u skladu sa Zakonom o osobnoj iskaznici [1]. Osoba je direktno odgovorna za djelovanje u skladu s Uvjetima pružanja usluga certificiranja (eng. PKI Disclosure Statement – PDS).

Osoba je ujedno i subjekt koji se imenuje u certifikatu te potpisnik koji izrađuje elektronički potpis i koristi certifikat u svoje osobno ime.

U CA certifikatima, subjekt certifikata je naziv CA sustava pružatelja usluga povjerenja. Slično vrijedi i za OCSP certifikat. Uvijek kada subjekt certifikata nije fizička osoba, autoriziraju se fizičke osobe – skrbnici certifikata koji preuzimaju odgovornosti za zaštitu korespondirajućeg privatnog ključa i SCD.

1.3.5. Pouzdajuće strane

Pouzdajuće strane (eng. *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 osobom odnosno provjeru identiteta osobe i validaciju elektroničkog potpisa.

1.3.6. Proizvođač

AKD je proizvođač eOI i opskrbljuje osobe s eOI na kojoj se pohranjuje privatni ključ.

Proizvođač pruža sljedeće usluge:

a) pripremu i proizvodnju eOI,
b) generiranje parova kriptografskih ključeva osoba te njihov unos u eOI,
c) individualizaciju tijela i čipa eOI,
d) distribuciju eOI osobama posredno korištenjem usluga RA.

Proizvođač je dužan osigurati da je eOI kvalificirano sredstvo za izradu elektroničkog potpisa (eng. *Qualified electronic Signature Creation Device – QSCD*).

1.4. Upotreba certifikata

Detaljne informacije o sadržaju certifikata su dostupne u poglavlju 7 ovog dokumenta.

Pri određivanju upotrebe certifikata važno je uzeti u obzir ostale odredbe navedene u ovom dokumentu, a posebno kriterije za interoperabilnosti koji su navedeni u točki 3.2.6 te poslovne odredbe navedene u poglavlju 9.

1.4.1. Primjerene upotrebe certifikata

1.4.1.1. CA Certifikati

CA certifikate koristi pružatelj usluga za potpisivanje certifikata i CRL.

Ova grupa obuhvaća:

- AKD Root CA certifikat koji je izdao i potpisao HRIDCA certifikat i
- HRIDCA certifikat kojim je potpisan OCSP Certifikat kao i certifikati izdani krajnjim korisnicima (eOI NCP-n-qscd-eid i eOI QCP-n-qscd-esign).

Korespondirajući privatni ključ CA certifikata čuva se na sigurnom kriptografskom uređaju.

Namjena CA certifikata po X.509 v3 ekstenziji „*Key Usage*“ je *„Certificate Signing, Off-line CRL Signing, CRL Signing“.* Ova je ekstenzija označena kao kritična.

1.4.1.2. OCSP Certifikati

HRIDCA OCSP certifikat izdaje HRIDCA, a koristi ga pružatelj usluga za potpisivanje OCSP odgovora.

Korespondirajući privatni ključ OCSP certifikata čuva se na sigurnom kriptografskom uređaju.

Namjena OCSP certifikata po X.509 v3 ekstenziji „*Key Usage*“ je *„Digital Signature“.* Ova je ekstenzija označena kao kritična.

Namjena OCSP certifikata po X.509 v3 ekstenziji „*Extended Key Usage*“ je „*OCSP Signing*“.

1.4.1.3. eOI NCP-n-qscd-eid eOI identifikacijski certifikat

Osobe i pouzdajuće strane trebaju biti svjesne pravila upotrebe eOI identifikacijskog certifikata:

a) eOI identifikacijski certifikat je sredstvo elektroničke identifikacije visoke razine sigurnosti kako je specificirano u čl. 8 točka 2 c) Uredbe (EU) br. 910/2014 [9].
b) Maloljetne osobe smiju koristiti eOI identifikacijski certifikat za podršku elektroničkom potpisu, no punoljetnim fizičkim osobama preporučuje se korištenje potpisnog certifikata za takvu namjenu.
c) U polju „Subject“ eOI identifikacijskog certifikata je imenovana fizička osoba.
d) eOI osobni certifikati se koriste u privatne svrhe ali i za poslovnu namjenu kada nije nužno certifikatom potvrditi povezanost osobe s poslovnim subjektom.
e) Namjena eOI identifikacijskog certifikata po X.509 v3 ekstenziji *„Key Usage“* je *„Digital Signature“*. Ova je ekstenzija označena kao kritična.

1.4.1.4. eOI QCP-n-qscd-esign eOI potpisni certifikat

Osobe i pouzdajuće strane trebaju biti svjesne pravila upotrebe eOI potpisnog certifikata:

a) eOI potpisni certifikat služi kao podrška pri izradi kvalificiranog elektroničkog potpisa kako je definirano čl. 3 (12) *Uredbe (EU) br. 910/2014* [9].
b) eOI potpisni certifikat se može koristiti i kao podrška u izradi naprednog elektroničkog potpisa baziranog na kvalificiranom certifikatu kako je definirano u čl. 26 i 27 *Uredbe (EU) br. 910/2014* [9].
c) U polju *„Subject“* eOI potpisnog certifikata je imenovana fizička osoba.
d) Namjena eOI potpisnog certifikata po X.509 v3 ekstenziji *„Key Usage“* je *„Non-Repudiation“*. Ova je ekstenzija označena kao kritična.
e) eOI potpisni certifikat se koristi u privatne svrhe ali i za poslovnu namjenu kada nije nužno certifikatom potvrditi povezanost osobe s poslovnim subjektom.
f) eOI potpisni certifikat je EU kvalificirani certifikat, a kvalificirani elektronički potpis učinjen ovim certifikatom ima jednak pravni učinak kao vlastoručni potpis.

1.4.2. Zabranjene upotrebe certifikata

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

a) Svaka upotreba certifikata, osim onih koje su navedene u točki 1.4.1, je zabranjena.
b) Certifikati nisu namijenjeni za šifriranje podataka.
c) Certifikati ne sadrže ekstenziju s e-mail adresom.
d) Ako se eOI identifikacijski certifikat koristi za podršku elektroničkom potpisu takav se potpis neće se smatrati kvalificiranim elektroničkim potpisom.

Pri provjeri valjanosti certifikata koja je opisana u točki 9.6.4 ovog dokumenta, pouzdajuće strane trebaju provjeriti OID certifikata iz točke 1.2.2 kako bi donijele valjanu odluku o prihvaćanju ili odbacivanju certifikata pri upotrebi.

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:

Agencija za komercijalnu djelatnost d.o.o
Povjerenstvo za upravljanje pravilima certificiranja
Savska cesta 31
10000 Zagreb
Hrvatska

e-mail: pma@akd.hr

web: http://eid.hr

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 dokumenta i početka njihove primjene, kao i nakon svake izmjene dokumenta, članovi PMA daju suglasnost za prihvaćanje i objavljivanje dokumenta.

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

2. Repozitorij i objavljivanje informacija

2.1. Repozitorij

CA osigurava repozitorij i stavlja na raspolaganje javnosti informacije koje su potrebne za provjeru statusa certifikata što uključuje:

a) informacije o statusu certifikata koje su dostupne kao OCSP usluga,
b) posljednja izdana CRL putem HTTP i LDAP protokola za AKDCA Root i HRIDCA i
c) CA certifikati.

Podaci u repozitoriju su navedeni u sljedećoj tablici.

Tablica 4: Podaci o repozitoriju

Informacije	AKDCA Root	HRIDCA
CRL: HTTP protokol	http://crl1.eid.hr/akdcaroot.crl http://crl2.eid.hr/akdcaroot.crl	http://crl1.eid.hr/hridca.crl http://crl2.eid.hr/hridca.crl
CRL: LDAP protokol	ldap://ldap.eid.hr	ldap://ldap.eid.hr
OCSP usluga	http://ocsp.eid.hr/akdcaroot	http://ocsp-hridca.eid.hr/hridca
CA certifikati	http://eid.hr/cert/akdcaroot.crt	http://eid.hr/cert/hridca.crt

Podaci za provjeru statusa certifikata sadržani su u certifikatu.

Valjani i važeći certifikati osoba izdani od HRIDCA sadržani su u strukturi javnog imenika, a javnosti mogu biti dostupni pod uvjetima navedenim u točki 2.4.

2.2. Portal za objavljivanje informacija

Sve informacije koje su potrebne osobama i pouzdajućim stranama za korištenje usluga certificiranja objavljuje HRIDCA na portalu elektroničke osobne iskaznice (dalje u tekstu portal).

Javnosti je dostupan javni dio portala http://eid.hr na kojem se objavljuju sljedeće informacije:

a) AKD PKI Opća pravila pružanja usluga certificiranja, http://eid.hr/cps,
b) HRIDCA Pravilnik o postupcima certificiranja, http://eid.hr/cps,
c) eOI Uvjeti pružanja usluga certificiranja, http://eid.hr/cps,
d) obavijesti vezane uz pružanje usluga certificiranja i
e) ostale informacije koje CA i proizvođač smatraju relevantnim za korisnike i pouzdajuće strane.

CA uspostavlja privatni dio portala kojem mogu pristupiti osobe koje su se registrirale.
Na privatnom dijelu portala objavljene su sljedeće informacije:

f) aplikacija i upute potrebne za instalaciju i korištenje eOI,
g) elektronička usluga za provjeru statusa i suspenziju certifikata,
h) pregled i promjena registracijskih podataka i
i) kontakt podaci za pomoć korisnicima.

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 dostupni na hrvatskom jeziku, a dio sadržaja uključujući CP, CPS i PDS može biti dostupan i na hrvatskom i na engleskom jeziku.
c) Certifikati u repozitoriju objavljuju se nakon njihovog izdavanja.
d) Informacije o statusu certifikata dostupne su pod uvjetima navedenim u točki 4.10.
e) Učestalost objave CRL definirana je u točki 4.9.7.

f) HRIDCA OCSP usluga za provjeru statusa izdanih certifikata dostupna je u skladu s točkom 4.9.10.
g) Osigurana je stalna 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) CA certifikati, CP, CPS, PDS i osnovne informacije na portalu dostupne su javnosti bez ograničenja.
b) Dodatne informacije i usluge neposredne provjere statusa i suspenzije certifikata na portalu mogu biti dostupne samo registriranim osobama.
c) HRIDCA ne postavlja nikakva ograničenja vezana uz pristup informacijama koje su potrebne za provjeru statusa certifikata.
d) Pravo pregleda certifikata fizičkih osoba u javnom imeniku HRIDCA će se omogućiti tijelima javnog sektora RH kada je to neophodno.
e) 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 vlasnika certifikata.

Ime certifikata određuje se u skladu s preporuci ITU-T X.520 [46] ili IETF RFC 5280 [35].

Pri određivanju polja „*Subject*“, primjenjuju se pravila navedena u preporuci ITU-T X.501 [47].

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

commonName:	Ime CA certifikata, odnosno OCSP certifikata
organizationIdentifier:	Identifikator pravne osobe - pružatelja usluge povjerenja
organizationName:	Ime pravne osobe - pružatelja usluge povjerenja
countryName:	Kod države

Za certifikate fizičkih osoba polje „Subject“ formira se od:

commonName:	Ime fizičke osobe
serialNumber:	Serijski broj
givenName:	Ime fizičke osobe
Surname:	Prezime fizičke osobe
organizationalUnitName:	Tip certifikata
organizationName:	Naziv organizacije s kojom je osoba povezana
countryName:	Kod države

3.1.2. Smislenost imena

Imena u polju „*Subject*“ moraju biti smislena i trebaju omogućiti nedvojbeno i jedinstveno utvrđivanje identiteta fizičke osobe.

3.1.3. Anonimnost i pseudonimi osobe

Nije podržano.

3.1.4. Pravila tumačenja imena

Pravila tumačenja imena za CA i OCSP certifikate navedena su u sljedećoj tablici.

Tablica 5: Pravila tumačenja imena CA i OCSP certifikata

CA i OCSP certifikati		
Polje	Pojašnjenje	Vrijednost
CommonName (cn)	Ime CA ili OCSP sustava	AKDCA Root AKDCA Root OCSP
		HRIDCA HRIDCA OCSP
organizationName (O)	Ime pravne osobe - pružatelja usluga povjerenja	AKD d.o.o
organizationIdentifier	VATHR-OIB gdje je VAT oznaka da se radi o pravnoj osobi, HR kod države, znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) i OIB porezni identifikacijski broj pravne osobe	VATHR-58843087891
countryName (C)	2 znaka ISO koda države (HR)	HR

Pravila tumačenja imena za certifikate fizičkih osoba navedena su u sljedećoj tablici.

Tablica 6: Pravila tumačenja imena fizičkih osoba

Fizičke osobe		
Polje	Pojašnjenje	Vrijednost
CommonName (cn)	Ime i prezime fizičke osobe iz identifikacijske isprave	Ime i prezime
serialNumber	PNOHR-OIB gdje je PNO oznaka da se radi o fizičkoj osobi, HR kod države, znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) i OIB osobni identifikacijski broj	PNOHR-OIB
givenName (g)	Ime fizičke osobe	Ime
Surname (sn)	Prezime fizičke osobe	Prezime
organizationalUnitName	Tip certifikata	Identification

(OU)		Signature
organizationName (O)	Naziv CA koji izdaje certifikat	AKD d.o.o.
countryName (C)	2 znaka ISO koda države (HR)	HR

3.1.5. Jedinstvenost imena

U polju „*Subject*“ svakog certifikata upisani su jedinstveni podaci o osobi kojoj se izdaje certifikat.

Jedinstvenost imena fizičke osobe osiguran je atributom „*serialNumber*“, dok se jedinstvenost imena pravne osobe osigurava atributom „*organizationIdentifier*“.

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

Vrijede pravila:

a) Privatni ključevi osoba generiraju se u HSM uređaju te se zajedno s pripadnim certifikatima u sigurnom okružju unose u čip eOI.
b) eOI s privatnim ključevima i certifikatima uručuje se osobi direktno nakon utvrđivanja njenog identiteta.
c) Privatni ključevi CA i OCSP certifikata se pod kontrolom autoriziranog osoblja CA generiraju u SCD uređaju u sigurnom okružju i tamo ostaju tijekom njihovog korištenja.

3.2.2. Potvrda identiteta pravnih osoba

Nije primjenjivo.

HRIDCA ne izdaje certifikate pravnim osobama.

3.2.3. Potvrda identiteta fizičkih osoba

3.2.3.1. Prikupljanje informacija o fizičkim osobama

Prikupljanje i provjera podataka o osobama vrši se u skladu s Pravilnikom o obrascima i evidenciji osobnih iskaznica [2].

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

a) Osnovne informacije o osobi koje uključuju:
   - puno ime i prezime,
   - podatak o spolu,
   - državljanstvo,
   - datum rođenja,
   - OIB,

- mjesto i adresa prebivališta.

b) Zahtijeva se fotografija u boji i otisak papilarnih linija lijevog i desnog kažiprsta te se skenira potpis osobe.

c) Zahtijevaju se odgovarajući dokumenti za provjeru imena, identiteta i osnove za izdavanje eOI i certifikata.

d) Dokumenti koji se smatraju mjerodavnim dokazima kod utvrđivanja identiteta fizičkih osoba u skladu s nacionalnim pravom u Republici Hrvatskoj su:
   - ranije izdane javne isprave (osobna iskaznica ili putovnica),
   - domovnica,
   - izvadak iz matice rođenih,
   - rodni list i
   - vjenčani list.

3.2.3.2. Provjera informacija o fizičkim osobama

PU/PP prikuplja i provjerava informacije i dokumente o fizičkoj osobi kako bi se osiguralo da je svaka informacija sadržana u certifikatu provjerena i potvrđena.

Postupci utvrđivanja i provjere identiteta fizičkih osoba provode se u skladu s identifikacijskom praksom u RH za fizičke osobe koja uključuje, ali se ne ograničava na:

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

b) provjeru odgovaraju li prikupljene informacije onima koje su navedene u predočenim dokumentima,

c) kada je primjenjivo,usporedbu prikupljenih informacija s onima koje su prikupljene u nekom ranijem postupku izdavanja javne isprave koji provodi MUP,

d) provjeru vjerodostojnosti priloženih/ predočenih dokumenata,

e) utvrđivanje je li osoba državljanin RH i postoji li osnova za izdavanje eOI,

f) utvrđivanje postoji li osnova za dobivanje certifikata na eOI prema sljedećim kriterijima:
   - djeca do 5 godina dobivaju eOI bez certifikata,
   - osobe starije od 5 a mlađe od 18 godina dobivaju samo identifikacijski certifikat,
   - punoljetne osobe starije od 18 godina dobivaju oba certifikata: identifikacijski i potpisni certifikat i
   - osobe starije od 65 godina dobivaju eOI ili bez certifikata ili s oba certifikata,

g) provjeru o izvršenoj uplati naknade za eOI i

h) provjeru o zasnivanju ugovornog odnosa između korisnika i pružatelja usluga certificiranja o prihvaćanju obveza i odgovornosti.

3.2.4. Informacije o osobama koje se ne provjeravaju

Od osoba se traže kontakt informacije: telefonski broj i e-mail adresa.

PU/PP ne provjerava dodatne informacije za kontakt već je za njihovu točnost odgovorna osoba.

3.2.5. Provjera tijela

3.2.5.1. Provjera RA/LRA službenika

Vrijede pravila:

a) Prije dodjeljivanja zaduženja službenicima PU/PP vrši se provjera te nedvojbeno utvrđivanje identiteta i pouzdanosti službenika u skladu s točkom 5.3.

b) U postupku autentikacije službenika na informacijskom sustavu PU/PP koristi se pouzdana metoda autentikacije.

c) Kako bi se spriječio sukob interesa, subjekt certifikata i službenik PU/PP ne smije biti ista osoba. Službenik koji zahtjeva certifikat ne smije identificirati sam sebe niti unositi zahtjev za izdavanje vlastitog certifikata u informacijski sustav PU/PP.

3.2.5.2. Provjera CA osoblja

Vrijede pravila:

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 formalni postupak identifikacije svih sudionika ceremonije uz fizičku prisutnost osobe temeljem predočenog dokumenta.

c) Kada se izdaju CA i OCSP certifikati, u suradnji s ljudskom resursima provjerava se jesu li koordinator i skrbnici kriptografskog ključa u stalnom radnom odnosu kod CA.

d) Tijekom operativne provedbe softverski modul koji automatizirano prikuplja, provjerava i šalje zahtjeve na obradu, autenticira se informacijskom sustavu CA korištenjem SSL/TLS client autentikacije.

3.2.6. Kriteriji za interoperabilnost

eOI je identifikacijski dokument hrvatskih državljana čije je izdavanje regulirano Zakonom o osobnoj iskaznici [1].

Kriteriji bitni za određivanje interoperabilnosti eOI i certifikata na eOI su:

a) Visoka razina sigurnosti elektroničke identifikacije koja se ostvaruje korištenjem eOI certifikata utemeljena je kriterijima koji su propisani u Uredbi (EU) br. 910/2014 [9] i Provedbenoj odluci komisije (EU) 2015/1502 [11] što znači:
   - da pruža visoku razinu osiguranja identiteta 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 vlasništvo osobe koja je vlasnik,
   - da posjeduje visoko pouzdan mehanizam autentikacije i
   - da ga izdaje pružatelj usluga koji ima uspostavljenu učinkovitu praksu upravljanja informacijskom sigurnošću.

b) Potpisni certifikat je kvalificirani certifikat za elektronički potpis, kako je specificirano u čl. 3 točka 15 Uredbe (EU) br. 910/2014 [9], te ispunjava zahtjeve utvrđene u Prilogu I Uredbe (EU) br. 910/2014 [9].

c) Identifikacijski certifikat se izdaje po istim pravilima koja se primjenjuju za potpisni certifikat, a služi kao sredstvo elektroničke identifikacije visoke razine sigurnosti prema čl. 8 točka 2 c) Uredbe (EU) br. 910/2014 [9].

d) Ministarstvo RH nadležno za upravu kao nadzorno tijelo zaduženo za elektroničku identifikaciju, provodi stručni pregled sustava elektroničke identifikacije u skladu s Provedbenom odlukom komisije (EU) 2015/296 [10].

e) Certifikate izdaje kvalificirani pružatelj usluga povjerenja, kako je specificirano u čl. 3 točka 20 Uredbe (EU) br. 910/2014 [9] kojem ministarstvo RH nadležno za gospodarstvo kao nadzorno tijelo odobrava kvalificirani status.

f) eOI na kojoj se izdaju certifikati je kvalificirano sredstvo za izradu elektroničkog potpisa, kako je specificirano u čl. 3 točka 23 Uredbe (EU) br. 910/2014 [9] i ispunjava zahtjeve utvrđene u Prilogu II Uredbe (EU) br. 910/2014 [9].

g) eOI ima sve potrebne funkcionalnosti europske kartice građana prema CEN/TS 15480 [49] te je interoperabilna i prikladna za korištenje u elektroničkom poslovanju na nacionalnom i Europskom nivou.

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 točki 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) Kod izdavanja novog para ključeva mogu se koristiti informacije i dokumenti koji su osigurani tijekom inicijalnog utvrđivanja identiteta prema točki 3.2.3.

b) Provjera informacija vrši na isti način kao kod inicijalnog utvrđivanja identiteta u točki 3.2.3.

c) Osobe koje podnose zahtjev jer im je prethodno izdana osobna iskaznica prestala važiti ili iz drugog razloga više ne služi svojoj svrsi, trebaju priložiti fotografiju u boji te staru osobnu iskaznicu koja se poništava i vraća osobi.

d) Osobe koje podnose zahtjev zbog promjene osobnog imena ili promjene prezimena dodatno prilažu izvod iz matice rođenih, u kojem je navedena bilješka o novom osobnom imenu ili novom prezimenu kojim se osoba dužna služiti u pravnom prometu, ili vjenčani list.

3.4. Identifikacija i autentikacija kod opoziva certifikata

Provjera identiteta osobe kod podnošenja zahtjeva za opoziv vrši se neposrednom identifikacijom uz fizičku prisutnost osobe temeljem predočenog dokumenta.

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

Prihvatljiva metoda autentikacije na daljinu uključuje autentikaciju na korisnički portal uz korištenje podatka koji se potvrđuje putem e-mail-a.

Podaci za autentikaciju na portal sadržani su u sigurnosnoj omotnici koja se uručuje osobi kod preuzimanja certifikata.

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

Podnošenje zahtjeva za izdavanje OI i certifikata na OI vrši se u skladu s Zakonom o osobnoj iskaznici [1]:

a) Zahtjev za izdavanje certifikata podnosi fizička osoba koje koja je imenovana kao subjekt certifikata.
b) Za dijete odnosno osobu lišenu poslovne sposobnosti zahtjev za izdavanje certifikata podnosi njen zakonski zastupnik.
c) Autorizirani službenik PU/PP unosi zahtjev za izdavanje certifikata u informacijski sustav PU/PP.

Zahtjev za izdavanje CA i OCSP certifikata podnosi autorizirano osoblje CA.

4.1.2. Postupak podnošenja zahtjeva za izdavanje certifikata

Postupak podnošenja zahtjeva za izdavanje osobne iskaznice odnosno certifikata na osobnoj iskaznici definiran je Zakonom o osobnoj iskaznici [1]. Ministarstvo na svojim službenim stranicama objavljuje upute o proceduri izdavanja eOI.

Propisana su sljedeća pravila:

a) Zahtjev za izdavanje osobne iskaznice podnosi se na lokacijama u PU/PP Ministarstva u uredovno radno vrijeme.
b) Zahtjev za izdavanje osobne iskaznice podnosi se na propisanom obrascu čiji je izgled i sadržaj propisan Pravilnikom o obrascima i evidenciji osobnih iskaznica [2].
c) Osobe su dužne potpisom na zahtjevu za izdavanje osobne iskaznice potvrditi da su osobni identifikacijski podaci u trenutku podnošenja zahtjeva cjeloviti i točni.
d) Prilikom podnošenja zahtjeva osoba sklapa Ugovor o pružanju usluga certificiranja s AKD-om te svojim potpisom potvrđuje da prihvaća svoje obveze i odgovornosti.
e) Uz zahtjev za izdavanje osobne iskaznice prilaže se potvrda o izvršenoj uplati naknade prema Pravilniku o cijeni osobnih iskaznica [3].

4.2. Obrada zahtjeva za izdavanje certifikata

4.2.1. Provedba identifikacije i autentikacije

Identitet fizičkih osoba potvrđuje se u postupcima koji su navedeni u točki 3.2.3.

Za autorizirane službenike RA/LRA i osoblje CA primjenjuju se postupci navedeni u točki 3.2.5.

4.2.2. Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Vrijede pravila:

a) Službenici PU/PP odlučuju o prihvaćanju ili odbijanju zahtjeva za izdavanje certifikata osobama.

b) Zahtjev za izdavanje certifikata će biti odbijen:
   - ako postoji sumnja da prikupljene informacije o fizičkim osobama iz točke 3.2.3.1 nisu točne, cjelovite ili vjerodostojne,
   - ako postupak provjere informacija o fizičkim osobama nije uspješno proveden u skladu s točkom 3.2.3.2,
   - ako ne postoji osnova za izdavanje eOI ili certifikata na eOI,
   - ako nije izvršena uplata naknade za eOI,
   - ako je zahtjev za izdavanje certifikata naknadno nakon podnošenja zahtjeva povučen ili
   - ako je tijekom zaprimanja ili naknadno nakon podnošenja zahtjeva utvrđeno da zahtjev za izdavanje certifikata nije bio autoriziran.

c) Ako je zahtjev za izdavanje certifikata odbijen, podnositelj zahtjeva se informira usmenim putem o razlozima odbijanja zahtjeva.

d) Svi podneseni zahtjevi unose se su u informacijski sustav koji ispunjava sigurnosne zahtjeve navedene u točkama 6.5, 6.6 i 6.7.

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

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

4.2.3. Vrijeme obrade zahtjeva za izdavanje certifikata

Obrada zahtjeva za izdavanje certifikata provodi se u skladu s rokom izdavanja osobne iskaznice koji je propisan Zakonom o osobnoj iskaznici [1]:

a) u roku od 30 dana od dana podnošenja zahtjeva, ako je zahtjev podnesen u redovnom postupku,

b) u roku od 10 dana od dana podnošenja zahtjeva, ako je zahtjev podnesen u ubrzanom postupku,

c) u roku od 3 radna dana od dana podnošenja zahtjeva, ako je zahtjev podnesen u žurnom postupku.

4.3. Postupak izdavanja certifikata

4.3.1. Postupci tijekom izdavanja certifikata

a) Fizičkim osobama se mogu izdati certifikati samo ako je autorizirana osoba unijela zahtjev u informacijski sustav PU/PP za evidenciju osobnih iskaznica.

b) Odmah nakon unošenja zahtjeva za izdavanje certifikata u informacijski sustav, podaci potrebni za realizaciju zahtjeva se šalju proizvođaču kroz siguran komunikacijski kanal.

c) CA ne provjerava cjelovitost, točnost i jedinstvenost zaprimljenih podataka za izdavanje eOI i certifikata već se oslanja na provjeru izvršenu u PU/PP.

d) Proizvođač izrađuje eOI s čipom s otisnutim dizajnom i ugrađenim zaštitnim elementima koji omogućavaju fizičku zaštitu od krivotvorenja ili promjene u skladu sa zahtjevima MUP-a kao izdavatelja eOI.
e) Postupak izdavanja certifikata, generiranja parova ključeva i PIN-ova te njihovog unošenja u eOI vrši se u sigurnom okružju koje ispunjava zahtjeve navedene u točkama 6.5, 6.6 i 6.7.
f) Profili izdanih certifikata su u skladu sa zahtjevima navedenim u točki 7.1.
g) Ključevi CA koji se koriste za potpisivanje certifikata kao i ključevi osoba štite se mjerama i postupcima koji su propisani u točki 6.2.
h) Nakon postupka izrade i individualizacije, eOI se propisno pakiraju i dostavljaju u PU/PP u kojoj je osoba podnijela zahtjev za njezino izdavanje.
i) Ako je zahtjev podnesen u žurnom postupku, eOI se dostavlja u PU u čijem je sastavu PP u kojoj je osoba podnijela zahtjev za izdavanje osobne iskaznice.

4.3.2. Obavješćivanje o izdavanju certifikata

Kod podnošenja zahtjeva ovlašteni službenici PU/PP informiraju osobu kada će njegova eOI biti izrađena i kada će ju moći preuzeti.

4.4. Preuzimanje certifikata

4.4.1. Provedba postupka prihvaćanja certifikata

Vrijede pravila:

a) eOI s certifikatima se uručuje osobi u PU/PP nakon utvrđivanja identiteta neposrednom identifikacijom u fizičkoj prisutnosti osobe.
b) Provjera identiteta vrši se temeljem predočenih identifikacijskih podataka ili važeće isprave, odnosno uvidom u postojeće podatke iz evidencije osobnih iskaznica.
c) Smatra se da je potpisnik prihvatio privatni ključ i certifikat u trenutku uručenja eOI.
d) U trenutku preuzimanja eOI , osoba je informirana o uvjetima korištenja certifikata i već je potpisala ugovor (prema poglavlju 4.1.2).
e) Ako osoba ne preuzme eOI u roku od 90 dana, smatra se da nije prihvatila certifikat.
f) Certifikati koji nisu prihvaćeni se opozivaju po proceduri koja je opisana u toči 4.9.3.

4.4.2. Objava certifikata od strane CA

Certifikati se objavljuju u javnom imeniku odmah nakon izdavanja certifikata.

Certifikati osobe neće biti dostupni javnosti za pretraživanje osim kada je osigurana suglasnost osobe.

4.4.3. Obavješćivanje drugih strana o izdavanju certifikata

Informaciju da je certifikat izdan i da je eOI izrađena CA prosljeđuje informacijskom sustavu PU/PP kroz siguran komunikacijski kanal.

CA ne obavještava druge strane o izdavanju certifikata.

Osoba može dostaviti svoj certifikat drugim stranama, kada je to potrebno.

4.5. Korištenje ključeva i certifikata

4.5.1. Osobe

Osobama se uručuje neoštećena sigurnosna omotnica koja sadrži podatke za registraciju na portal eOI i aktivaciju eOI.

Svaka osoba kojoj je izdan certifikat na eOI dužna je potpisati ugovor o pružanju usluga certificiranja kako je propisano u čl.9. st. 3. Zakona o osobnoj iskaznici [1] te se obvezati da će postupati u skladu s eOI uvjetima pružanja usluga certificiranja odnosno da će ispuniti svoje obveze navedene u točki 9.6.4.

eOI uvjeti pružanja usluga certificiranja sadrže:

a) informacije o pružatelju usluga certificiranja, o opsegu usluga koje on pruža i o pravilima pružanja usluga,
b) tipove, namjenu i ograničenja certifikata te način provjere certifikata,
c) obveze i odgovornosti fizičkih osoba, pružatelja usluga i pouzdajućih strana,
d) poslovne informacije vezane uz jamstva, cijene, sklapanje i raskid ugovora,
e) odredbe vezane uz zaštitu podataka i privatnosti,
f) komunikacija s korisnicima, pritužbe, rješavanje sporova i mjerodavno pravo i
g) primjenjivi zakoni i nadzor nad pružateljem usluga certificiranja.

4.5.2. Pouzdajuće strane

Pouzdajuće strane, koje se oslanjaju na eOI certifikate i usluge certificiranja poje pruža HRIDCA dužne su postupati u skladu s eOI uvjetima pružanja usluga certificiranja te ispuniti svoje obveze navedene u točki 9.6.5.

4.6. Obnova certifikata

4.6.1. Razlozi za obnovu certifikata

Certifikat treba obnoviti ako ističe period važenja certifikata.

Svaka obnova certifikata podrazumijeva izdavanje novog para ključeva (vidi točku 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 osobe 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 i novi certifikat će biti izdan:

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

HRIDCA ne čuva privatne ključeve osoba niti može reaktivirati opozvani certifikat već će se osobi izdati nova eOI s novim parom ključa i novim certifikatom.

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 osobe 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 osobnom imenu ili osobnom identifikacijskom broju ili
b) utvrđeno je da informacije sadržane u certifikatu nisu ispravne.

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 osobe 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

Razlozi za opoziv certifikata fizičkih osoba su:

a) Podnesen je autorizirani zahtjev za opoziv certifikata.
b) Prijavljena je promjena podataka u certifikatu odnosno došlo je do promjene u osobnom imenu ili osobnom identifikacijskom broju fizičke osobe koji su sadržani u polju „Subject“ certifikata.
c) Prijavljen je gubitak, krađa ili kvar eOI.
d) Prijavljena je zlouporaba ili neautorizirano korištenje eOI ili uvijek kada je moguća kompromitacija privatnog ključa.

e) Utvrđen je prestanak važenja certifikata prije isteka perioda na koji je certifikat izdan zbog razloga koji su propisani u čl. 15 Zakona o osobnoj iskaznici [1].

f) 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.

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

h) Certifikat se zbog operativnih razloga ukida ili mijenja. To uključuje sljedeće situacije:
   - Utvrđeno je da privatni ključ ne odgovara javnom ključu u certifikatu ili je naknadno utvrđeno da podaci u certifikatu nisu ispravni.
   - Utvrđeno je da zahtjev za izdavanje certifikata nije bio autoriziran ili je naknadno povučen.
   - Utvrđeno je da certifikat nije izdan u skladu s HRIDCA pravilnikom ili AKD PKI općim pravilima.

i) HRIDCA certifikat je opozvan.

HRIDCA certifikat će biti opozvan u sljedećim situacijama:

j) 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.

k) Utvrđena je kompromitacija HRIDCA privatnog ključa.

l) AKDCA Root certifikat je opozvan.

m) Ako HRIDCA 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 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 d),

b) autorizirani službenici PU/PP, zbog razloga koji su navedeni u točkama 4.9.1 a) do g) i

c) autorizirano osoblje CA, zbog razloga koji su navedeni u točki 4.9.1 h) do m).

4.9.3. Postupci kod podnošenja zahtjeva za opoziv certifikata

Na portalu su dostupne jasne upute o postupcima koje treba poduzeti u slučaju nastanka razloga za opoziv certifikata koji su navedeni u 4.1.9.

Kod podnošenja zahtjeva za opoziv certifikata, primjenjuju se sljedeći postupci:

a) Osobe podnose zahtjev za opoziv svoga certifikata:
   - u uredima PU/PP u radno vrijeme ili
   - putem portala po proceduri za suspenziju certifikata koja je navedena u točki 4.9.15. kontinuirano 24/7.

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

c) Ako je zahtjev za opoziv odobren proslijedit će se na daljnju obradu CA.

d) Postupak opoziva CA i OCSP certifikata 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 o osobnom imenu ili osobnom identifikacijskom broju, osoba je dužna zatražiti opoziv u roku od 2 dana 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 zahtjev za opoziv ne može biti potvrđen u roku od 24 sata, tada se status certifikata neće mijenjati.
d) Maksimalno vrijeme koje može proteći između zaprimanja zahtjeva za opoziv certifikata i objave statusa certifikata je 24 sata.
e) Certifikat koji je trajno opozvan (tj. koji nije suspendiran), ne može se reaktivirati i njegov status se više ne može promijeniti.
f) 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.
g) CA osigurava sigurno okružje u kojem se provodi postupak opoziva certifikata u skladu s točkama 6.5, 6.6 i 6.7.

4.9.6. Provjera statusa certifikata

Usluge za provjeru informacije o statusu certifikata dostupne su putem Interneta.

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 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) Svaka CRL sadrži informaciju o vremenu izdavanja i o periodu važenja CRL.
b) HRIDCA se obvezuju da će CRL izdati barem 1 put u roku od 24 sata.
c) Nova CRL će se izdati barem 10 minuta prije isteka važenja prethodne CRL.
d) U redovnim uvjetima rada, KRIDCA generira i izdaje CRL svakih 12 sati.
e) Period važenja CRL koju izdaje HRIDCA je 24 sata od trenutka izdavanja CRL.

f) Za AKDCA Root period važenja CRL je 90 dana od trenutka izdavanja CRL.
g) U slučaju opoziva HRIDCA ili AKDCA Root certifikata, AKDCA Root će izdati CRL u roku od 24 sata.
h) Ako je istekao period važenja certifikata koji je opozvan, informacija o opozivu certifikata se može biti maknuti s CRL.
i) Kako bi se osigurala dostupnost CRL u skladu s pravilima koja su navedena u ovom poglavlju, pravovremenost izdavanja CRL se kontinuirano nadzire.

4.9.8. Maksimalno kašnjenje objave CRL

Maksimalno kašnjenje od trenutka izdavanja CRL do trenutka objave CRL putem interneta je 10 minuta u redovnim uvjetima rada.

4.9.9. Dostupnost on line provjere statusa certifikata

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

OCSP odgovor mora biti u skladu s IETF RFC 6960 [36] i IETF RFC 5019 [37].

OCSP certifikat sadrži ekstenziju *id-pkix-ocsp-nocheck*, kako je zahtijevano u CA/Browser Forum BRG [16] i kako je definirano u IETF RFC 6960 [36].

4.9.10. Zahtjevi za on-line provjeru statusa certifikata

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

a) OCSP usluga dostupna je preko protokola HTTP na adresi objavljenoj u polju authorityInformationAccess svakog certifikata.
b) HRIDCA će osvježiti informacije koje se objavljuju preko OCSP barem svaka 24 sata.
c) U redovnim uvjetima rada HRIDCA će osvježiti informacije koje se objavljuju preko OCSP odmah po dobivanju zahtjeva za opoziv certifikata.
d) Valjanost odgovora usluge HRIDCA OCSP je maksimalno 24.
e) AKDCA će osvježiti informacije koje se objavljuju preko OCSP barem svakih 90 dana.
f) U slučaju opoziva certifikata HRIDCA, AKDCA Root će osvježiti informacije koje se objavljuju preko OCSP u roku od 24 sata.
g) 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.
h) Ako OCSP usluga zaprimi zahtjev za provjeru statusa certifikata koji još nije izdan, tada neće odgovoriti sa statusom „good“.
i) Odgovor OCSP usluge o statusu certifikata neće biti „*good*“ ako status CA certifikata nije provjeren ili ako CA certifikat nije valjan.
j) 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

Registriranim osobama na privatnom dijelu portala HRIDCA osigurava neposrednu provjeru statusa svoga certifikata (vidi točku 2.2).

4.9.12. Specifični zahtjevi vezani uz kompromitaciju ključeva

HRIDCA, sukladno točki 4.9.1, opoziva certifikat ako je potvrđena kompromitacija privatnog ključa.

4.9.13. Razlozi za suspenziju certifikata

Razlozi za suspenziju certifikata osobe su:

a) Podnesen je autorizirani zahtjev za suspenziju certifikata.
b) Prijavljen je nestanak eOI.
c) Postoji mogućnost da zahtjev za opoziv certifikata bude naknadno 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, posljedice koje mogu nastati uslijed neopoziva certifikata nisu zanemarive.

Razlozi za povlačenje suspenzije certifikata osobe su:

f) Podnesen je autorizirani zahtjev za povlačenje suspenzije certifikata.
g) Pronalazak eOI.
h) Prestanak razloga zbog kojeg je tražena suspenzija certifikata.

4.9.14. Tko može tražiti suspenziju certifikata

Zahtjev za suspenziju ili povlačenje suspenzije certifikata može zahtijevati:

a) fizička osoba koja je imenovana kao subjekt certifikata ili njen zakonski zastupnik,
b) autorizirani službenik PU/PP i
c) autorizirano osoblje CA.

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 podnose zahtjev za suspenziju svoga certifikata:
   - u uredima PU/PP u radno vrijeme ili
   - na daljinu korištenjem elektroničke usluge za suspenziju certifikata.
b) Zahtjev za suspenziju certifikata će se prihvatiti samo ako je identitet podnositelja zahtjeva utvrđen sukladno pravilima za utvrđivanje identiteta prema točki 3.4.
c) Ako je zahtjev za suspenziju ili povlačenje suspenzije odobren proslijedit će se na daljnju obradu CA.
d) Maksimalno vrijeme koje može proteći između zaprimanja zahtjeva za suspenziju ili povlačenje suspenzije certifikata i objave statusa certifikata je 24 sata.
e) 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 jedan puta dnevno.

f) 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.

Povlačenjem zahtjeva za suspenziju, certifikat se reaktivira, miče se s CRL i ponovo postaje valjan.

Ako u roku od 8 dana od podnošenja zahtjeva za suspenziju nije zahtijevano povlačenje suspenzije certifikata, suspendirani certifikat će biti trajno 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 i LDAP protokola te OCSP uslugu provjere statusa certifikata.

b) Informacije o opozvanim certifikatima kojima je istekao period važenja (osnovno polje certifikata „*Valid to*“) brišu se s javno dostupnih CRL i OCSP usluge, ali ostaju arhivirani kod CA.

c) Javna adresa za provjeru statusa HRIDCA certifikata korištenjem OCSP usluge je: http://ocsp-hridca.eid.hr/hridca.

d) Javne adrese za dohvat HRIDCA CRL na web poslužitelju su: http://crl1.eid.hr/hridca.crl i http://crl2.eid.hr/hridca.crl.

e) Javna adresa za dohvat CRL putem javnog imenika je: ldap://ldap.eid.hr/cn=HRIDCA,o=AKD d.o.o.,c=HR?certificateRevocationList;binary.

f) Redoslijed kojim pouzdajuća stana dohvaća informaciju o statusu certifikata je:
   1) OCSP usluga: http://ocsp-hridca.eid.hr/hridca
   2) HTTP CRL: http://crl1.eid.hr/hridca.crl
   3) HTTP CRL: http://crl2.eid.hr/hridca.crl
   4) LDAP CRL:
      ldap://ldap.eid.hr/cn=HRIDCA,o=AKD d.o.o.,c=HR?certificateRevocationList;binary

g) Integritet i autentičnost informacije o statusu certifikata je osigurana elektroničkim potpisom : CRL je potpisana HRIDCA certifikatom, a OCSP odgovor certifikatom HRIDCA OSCP.

4.10.2. Dostupnost usluga

Vrijede pravila:

a) Usluga zaprimanja zahtjeva za opoziv ili suspenziju certifikata uredima PU/PP dostupna je u radno vrijeme.

b) U redovnim uvjetima rada, zahtjev za suspenziju certifikata može se podnijeti elektroničkim putem, kontinuirano 24 sata na dan, 7 dana u tjednu.

c) U redovnim uvjetima rada, dostupnost usluga CRL i OCSP provjere statusa certifikata je 24 sata na dan, 7 dana u tjednu.
d) Odzivno vrijeme za CRL i OCSP provjeru statusa certifikata od maksimalno 10 sekundi.
e) Kako bi se skratilo vrijeme obrade i provjere statusa certifikata preporuka je koristiti OCSP protokol.
f) U slučaju ispada sustava, usluga će biti dostupna u najkraćem mogućem roku i u skladu s najboljim poslovnim praksama.

4.10.3. Opcionalna svojstva

Nije predviđeno.

4.11. Kraj životnog ciklusa certifikata

eOI certifikati se izdaju na period od 5 godina.

Tijekom perioda važenja certifikata osoba se obvezuje postupati u skladu s eOI uvjetima pružanja usluga certificiranja.

Certifikat prestaje biti valjan ako je:

a) istekao period važenja certifikata (osnovno polje certifikata „*Valid to*“) ili
b) ako je opozvan.

4.12. Pohrana i oporavak privatnog ključa

Nije primjenjivo.

CA ne obavlja pohranu i oporavak privatnih ključeva osoba.

5. Fizičke, organizacijsko-upravljačke i provedbene mjere zaštite

5.1. Mjere fizičke zaštite

AKD kontrolira fizički pristup cjelokupnoj PKI infrastrukturi, podacima i svim komponentama sustava vezanim uz pružanje usluga povjerenja te provodi aktivnosti procjene i suzbijanja rizika.

Mjere fizičke sigurnosti primjenjuju se u skladu su s ETSI EN 319 401 [24] i poglavljem 11 ISO/IEC 27002 [42].

Detaljnije informacije o mjerama fizičke sigurnosti koje provodi pružatelj usluga dostupne su u pravilnicima.

5.1.1. Lokacija objekta i konstrukcija

Informacijski sustav CA te proizvodni pogoni u kojima se izrađuje i individualizira eOI, 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 protu prepadna 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, klasificirani 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 [42].

5.1.7. Uništavanje

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 udaljenim lokacijama 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 [24] i CEN TS 419 261 [23].

Povjerljive uloge uključuju ali se ne ograničavaju na:

a) **Administratori sigurnosti:** Odgovorni za implementaciju i provedbu sigurnosnih pravila u praksi.
b) **RA službenici**: Osoba 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 principi:

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 definiranih sigurnosnih pravila te onemogućava provedbu aktivnosti bez prethodne autentikacije autoriziranih 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 navedenim u točki 3.2.5.

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.

Kod promjene zaduženja i nakon prestanka radnog odnosa, osoblju CA se ukidaju prava pristupa prostorima CA kao i korisnička prava na informacijskom sustavu CA.

Registracijsko tijelo će službenicima PU/PP se kod promjene zaduženja i nakon prestanka radnog odnosa ukinuti sva korisnička prava na informacijskom sustavu PU/PP.

5.3.2. Postupak provjere prikladnosti radnika za korisničku ulogu

Pri dodjeljivanju povjerljivih uloga i odabiru radnika koje će sudjelovati provedbi aktivnosti certificiranja provodi se formalni 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.

Prije dodjeljivanja zaduženja osoblju CA i službenicima PU/PP provjerava se i potvrđuje identitet, sposobnost i pouzdanost radnika.

Osoblje koji sudjeluju u provedbi aktivnosti CA mora biti u stalnom radnom odnosu kod pružatelja usluga certificiranja.

Službenici PU/PP su državni službenici i u radnom su odnosu u registracijskom tijelu (MUP).

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

Osoblje CA raspolaže s internim sigurnosnim pravilima te je primjereno educirano o sigurnosnim zahtjevima i svojoj ulozi u provedbi postupaka certificiranja.

MUP osigurava upute te provodi edukaciju službenika PU/PP kako bi se osiguralo da su oni upoznati sa svojim obvezama, da ih razumiju te da su svjesni svojih odgovornosti.

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 u dvije godine.

Cilj informiranja je:

a) osigurati razumijevanje sigurnosnih zahtjeva, internih sigurnosnih pravila ili uputa,
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.

5.3.5. Periodična rotacija i provjera radnika

Osoblje CA kojem su dodijeljene povjerljive uloge vezane uz upravljanje kriptografskim ključevima svake se tri godine podvrgava ponovnoj procjeni prikladnosti prema točki 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

Revizijske 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,
   - izdavanje certifikata,
   - priprema podataka i izrada SSCD,
   - opoziv, suspenzija, povlačenje suspenzije certifikata i
   - izdavanje i objava CRL.

b) zapisi o postupcima upravljanja kriptografskim ključevima što uključuje, ali se ne ograničava na
   - generiranje,
   - korištenje,
   - učitavanje,
   - pohranu,
   - oporavak i
   - uništavanje kriptografskih ključeva.

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.

d) 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 generiranje izvještaja i alarmiranje pojave sigurnosnih događaja za kritične aktivnosti.

Za manje kritične aktivnosti provodi se periodična kontrola.

5.4.3. Period čuvanja revizijskih zapisa

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

Svi revizijski zapisi arhiviraju se u skladu s pravilima arhiviranja koja su opisana u točki 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) Onemogućena je konfiguracija sustava koja će deaktivirati bilježenje aktivnosti u revizijskim zapisima.
f) Revizijski zapisi se ne smiju brisati niti se smiju automatski zapisivati preko postojećih podataka.

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 (eng. *Log Management System*) koji provodi automatsko prikupljanje, pohranu, zaštitu i obradu revizijskih zapisa u realnom vremenu.

Revizijski zapisi svih kritičnih sustava uključeni su u sustav upravljanja revizijskim zapisima.

Događaji u revizijskim zapisima se mogu pretraživati po tipu i po vremenu događaja.

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.

5.4.8. Procjena ranjivosti sustava

Procjena ranjivosti sustava provodi se temeljem pregleda revizijskih zapisa u sustavu upravljanja revizijskim zapisima.

Ispitivanje i analiza ranjivosti informacijskog sustava provodi se periodično korištenjem odobrenih softverskih alata, a prema internim sigurnosnim pravilima.

Odmah po otkrivanju ranjivosti poduzimaju se aktivnosti za njihovo rješavanje.

5.5. Arhiviranje zapisa

5.5.1. Tipovi zapisa koji se arhiviranju

Arhiviraju se svi podaci bitni za pružanje usluga što uključuje ali se ne ograničava na:

a) revizijske zapise kako je navedeno u točki 5.4.1,
b) dokumentaciju i informacije prikupljene u postupku registracije fizičkih i pravnih osoba kako je navedeno u točkama 3.2.2.1 i 3.2.3.1,
c) dokumentaciju s ceremonije generiranja CA ključeva kako je navedeno u točki 6.1.1,
d) certifikate i podatke o upravljanju životnim ciklusom certifikata,
e) podatke o upravljanju kriptografskim ključevima i QSCD,
f) dokumentacija o pravilima pružanja usluga (CP, CPS, PDS) i
g) ostali podaci i dokumentaciju sukladno zakonskim propisima.

5.5.2. Period čuvanja arhiviranih zapisa

Svi arhivirani podaci i dokumentacija navedena u točki 5.5.1 čuva se najmanje 10 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 provjeravaju najmanje dva puta godišnje, te po potrebi prepisuju na drugi medij kako bi se osigurala zaštita 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 105/97, 64/00, 65/09, 125/11).

5.5.4. Postupci izrade sigurnosnih kopija arhive

Postupci izrade sigurnosnih kopija arhive provode se u prostorima sigurne zone, a sigurnosne kopije arhive se čuvaju na udaljenoj lokaciji.

5.5.5. Zahtjevi za zaštitu zapisa vremenskim žigom

Nije primjenjivo.

5.5.6. Prikupljanje arhivske građe

Prikupljanje arhivske građe vrši se interno na način koji ovisi o vrsti zapisa.

Prikupljanje i arhiviranje podataka i dokumentacije koja nastaje u postupku registriranja osoba u PU/PP regulirano je ugovorom.

5.5.7. Postupci dobivanja i provjere arhiviranih podataka

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

Pristup podacima iz arhive imaju samo autorizirane osobe.

Provjera podataka iz arhive uključuje provjeru zaštite izvornosti podataka.

5.6. Promjena CA ključa

Prije isteka perioda važenja 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 važenja svakog izdanog certifikata uvijek bude kraći od perioda važenja 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 [32].

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 pružateljem usluga certificiranja.

5.7. Kompromitacija i oporavak

5.7.1. Incidenti i postupci u slučaju kompromitacije

U slučaju kvarova ili kompromitacije računalnih resursa, softvera i/ili podataka postupa se u skladu s poglavljem 16 ISO/IEC 27002 [42].

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 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 informacijskog sustav kao i u slučaju prirodnih katastrofa, nesreća, velikih kvarova opreme i namjernih akcija.

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

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

Upravljanje kontinuitetom poslovanja se provodi u skladu s poglavljem 17 ISO/IEC 27002 [42].

AKD osigurava visoku dostupnost i neprekinuto odvijanje aktivnosti za slijedeće usluge

- usluge upravljanja opozivom certifikata,
- usluge provjere statusa certifikata i
- usluge informiranja.

Usluge generiranja certifikata, registracije i opskrbe uređajima provode se u radno vrijeme.

5.8. Prestanak rada

U slučaju prestanka pružanja usluga, AKD će konzultirati MUP i ministarstvo RH nadležno za gospodarstvo i upravu kako bi se potvrdili daljnji postupci vezani uz prekid rada.

Prekid pružanja usluga certificirana provoditi će se u skladu s CP i donesenim eOI planom prekida pružanja usluga certificiranja.

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 formalnom 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 (točka 5.2), interni i vanjski revizori, javni bilježnik te ostali pozvani svjedoci.
d) Prije početka ceremonije u nazočnosti javnog bilježnika provodi se formalna 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 njihov unos u eOI vrši proizvođač u fizički sigurnom okružju u zoni visoke sigurnosti.
l) CA ključevi kao i ključevi osoba se generiraju, koriste i čuvaju u HSM uređaju koji implementira norme i upravljačke funkcije kako je navedeno u točki 6.2.1.

6.1.2. Dostava privatnog ključa osobama

eOI s privatnim ključevima osoba otpremaju se u PU/PP po završetku proizvodnog procesa gdje se uručuje osobi nakon utvrđivanja identiteta neposrednom identifikacijom u fizičkoj prisutnosti osobe.

6.1.3. Dostava javnog ključa CA-u

Odmah po generaciji ključeva osoba, proizvođač pribavlja certifikat od HRIDCA korištenjem elektroničke usluge.

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

Autentikacija proizvođača 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 HRIDCA su dostupni u certifikatima na portalu (vidi točku 2.2), a sadržani su i u eOI.

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

6.1.5. Duljine ključeva

AKDCA Root i HRIDCA ključevi su duljine 4096 bita, RSA 256 algoritam.

Ključevi OCSP su duljine 2048 bita, RSA 256 algoritam.

Ključevi osoba su duljine 2048 bita, RSA 256 algoritam.

6.1.6. Generiranje i provjera kvalitete parametara javnog ključa

CA i OCSP ključevi kao i ključevi osoba generirani su korištenjem generatora slučajnih brojeva u HSM uređaju. Parametri javnog ključa za RSA algoritam su u skladu s normom FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf) ili drugom ekvivalentnom normom koju odobri PMA.

Općenito, za generaciju CA i OCSP ključeva te ključeva osoba koriste se kriptografski algoritmi i parametri u skladu s preporukama ETSI TS 119 312 [32].

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

Osobama se izdaju X.509 v3 certifikati u skladu s IETF RFC 5280 [35], a njihova namjena definirana je kroz vrijednost ekstenzije „*Key Usage*“.

Ekstenzija „*Key Usage“* svih certifikata označena je kao kritična ekstenzija.

Ekstenzija „*Key Usage“* ima vrijednost:

a) za CA certifikate: „Certificate Signing, Off-line CRL Signing i CRL Signing“,
b) za OCSP certifikate: „*Digital Signature“,*
c) za eOI potpisni certifikat: „*Non-Repudiation*“ i
d) za eOI identifikacijski certifikat: „*Digital Signature“* .

OCSP certifikati imaju dodatno ekstenziju „*Extended Key Usage*“ koja ima vrijednost „*OCSP Signing“.*

6.2. Zaštita privatnog ključa

6.2.1. Norme i upravljačke funkcije kriptografskog modula

Vrijede pravila:

a) CA i OCSP ključevi kao i ključevi osoba generiraju se u HSM uređaju koji demonstrira sukladnost s FIPS PUB 140-2 level 3 [38] standardom.

b) Inicijalizacija HSM uređaja i generiranje ključeva CA provodi se tijekom ceremonije generiranja CA ključa kako je opisano u točki 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) Privatni ključevi osoba se nakon generiranja unose u eOI koja kao kvalificirano sredstvo za izradu elektroničkog potpisa (QSCD), koja zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 [39] te demonstrira sukladnost s obrascima zaštite iz serije EN 419 211 [17], [18], [19], [20], [21] i [22].

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

Pravila pohrane privatnih ključeva CA i OCSP usluge:

a) Nakon njihove generacije privatni ključevi CA i OCSP usluge ostaju pohranjeni u HSM uređaju i pod kontrolom barem 2 osobe.

b) Sustav koji upravlja s privatnim ključem AKDRoot CA pokreće se samo kada je to potrebno.

c) Sustav koji upravlja s privatnim ključem HRIDCA je stalno dostupan i koristi se isključivo za potpisivanje certifikata osoba i CRL. Isto vrijedi i za pripadne 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 osoba:

e) Pojedinačni privatni ključevi osoba se odmah nakon generacije šifriraju kriptografskim ključevima čija je snaga jednaka ili veća od ključa koji se štiti.

f) Dodatno, privatni ključevi se šifriraju u sklopu skupne datoteke koja se prenosi proizvođaču u njegov centar za individualizaciju.

g) Dešifriranje privatnog ključa osobe vrši se u sigurnom prostoru proizvođača i to samo kroz minimalno vrijeme potrebno za njihov unos u čip eOI.

h) 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 [38] standardom.

i) AKD ne vrši trajnu pohranu privatnih ključeva osoba, već se oni brišu nakon postupka individualizacije eOI.

6.2.4. Sigurnosno kopiranje privatnog ključa

Sigurnosno kopiranje CA i OCSP privatnog ključa provodi se u 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 u sigurnosnom spremniku u štićenom prostoru sigurne zone kao i na sekundarnoj lokaciji gdje je osiguran isti ili veći nivo zaštite privatnog ključa.

Privatni ključevi osoba se ne kopiraju.

6.2.5. Arhiviranje privatnog ključa

CA privatni ključevi se ne arhiviranju.

OCSP privatni ključevi se ne arhiviraju.

Privatni ključevi osoba 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 [38] standardom.

Kada je CA privatni ključ izvan HSM uređaja 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 [38] standardom.

Uvijek kada je privatni ključ CA izvan HSM uređaja zbog prijenosa na drugi uređaj ili zbog potrebe sigurnosne pohrane jamči se isti ili veći nivo sigurnosti privatnog ključa.

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

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

Privatni ključevi osoba koji se šalju proizvođaču šifrirani su se u skladu s pravilima navedenim u točki 6.2.3.

6.2.7. Čuvanje ključa u kriptografskom modulu

Privatni ključ CA i OCSP 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 eOI.

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

Aktivacija privatnih ključeva na HSM uređaju odnosno na eOI 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 i OCSP koji su u HSM uređaju provodi se isključivo pod dvojnom kontrolom autoriziranih osoba.
b) Aktivacija se provodi korištenjem hardverskog sredstva za aktivaciju i pripadajućeg tajnog PIN-a.
c) Jednom aktiviran, privatni ključ u HSM uređaju ostaje aktiviran sve dok je HSM uređaj uključen.
d) Nakon isključivanja i ponovnog uključivanja HSM uređaja ponovo se provodi aktivacija privatnih ključeva.

Aktivacija privatnog ključa osobe u eOI:

e) Aktivacija privatnog ključa osobe provodi se jednokratno unosom PIN-a.
f) Aktivacija privatnih ključeva u eOI moguća je tek nakon aktivacije eOI koja se provodi u skladu s pravilima navedenim u točki 6.4.1

6.2.9. Deaktivacija privatnog ključa

Deaktivacija privatnog ključa u HSM uređaju:

a) Privatni ključ CA je deaktiviran ako HSM uređaj ili sustav koji upravlja privatnim ključem nije aktivan ili nije u funkciji. Isto vrijedi i za privatni ključ OCSP.

Deaktivacija privatnog ključa osobe na eOI:

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

6.2.10. Postupci uništavanja kriptografskih ključeva

Postupak uništavanja privatnog ključa CA odnosno OCSP usluge:

a) Uništavanje privatnog ključa CA odnosno OCSP usluge vrši se:
   - ako se HSM uređaj iznosi iz sigurne zone radi popravka ili zamjene opreme ili
   - nakon isteka perioda važenja certifikata ili
   - nakon prestanka rada CA odnosno OCSP.
b) Kada za to nastane potreba, uništavanje privatnog ključa na HSM uređaju, vrši 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 vrši se postupkom koji je opisan u točki 5.1.7.

Postupak uništavanja privatnih ključeva osoba:

f) Uništavanje datoteka s šifriranim privatnim ključevima osoba na informacijskom sustavu provodi se automatiziranim postupkom, nakon postupka individualizacije i stavljanja privatnih ključeva osoba na eOI.

g) Uništavanje šifriranih privatnih ključeva na informacijskom sustavu vrši se korištenjem provjerene sigurne metode te uz osiguran revizijski zapis o uništenju.

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 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 točki 5.5.

6.3.2. Period važenja certifikata i kriptografskih ključeva

Period važenja certifikata naveden je u sljedećoj tablici.

Tablica 7: Period važenja certifikata

Certifikat	Period važenja
Certifikat krovnog certifikacijskog tijela AKDCA Root	do 2038-01-19 03:14:07+00:00
Certifikat podređenog certifikacijskog tijela HRIDCA	do 15 godina
Certifikat za potpis OCSP odgovora	do 3 godine
eOI osobni certifikati	do 5 godina

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

Period važenja svakog certifikata je sadržan svakom certifikatu. Certifikat je važeći od datuma izdavanja (osnovno polje certifikata „*Valid from*“) do datuma isteka roka perioda važenja (osnovno polje certifikata „*Valid to*“).

Tijekom perioda važenja 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 vrši 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 vršiti se samo kroz minimalno vrijeme potrebno za njihov unos u eOI odnosno za njihov ispis u sigurnosne omotnice.
c) Odmah nakon stavljanja aktivacijskih podataka osoba na eOI odnosno nakon ispisa aktivacijskih podataka u sigurnosne omotnice, vrši 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.

Osobe vrše aktivaciju eOI u skladu sa sljedećim pravilima:

e) Aktivaciju eOI osoba provodi samostalno nakon preuzimanja eOI korištenjem podataka za aktivaciju dobivenih u sigurnosnoj omotnici, a prema uputi za aktivaciju eOI koja je dostupna na portalu eOI.
f) Tijekom aktivacije eOI postavljaju se PINovi za zaštitu privatnih ključeva kao i PUK vrijednost za otključavanje eOI.
g) Osobe su informirane o svojim obvezama vezanim uz zaštitu aktivacijskih podataka odnosno PINova.

6.4.2. Zaštita aktivacijskih podataka

Proizvođač poduzima sljedeće mjere zaštite aktivacijskih podataka:

a) Generiranje aktivacijskih podataka te njihov unos u eOI i ispis u sigurnosne omotnice vrši se pod dvojnom kontrolom u sigurnom okružju proizvođača eOI.
b) Sigurnosne omotnice s aktivacijskim podacima pakiraju se u odvojenim paketima i šalju u PU/PP neovisno o slanju eOI.
c) Sigurnosne omotnice s aktivacijskim podacima se uručuju osobama u PU/PP.

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

d) Nakon 6 uzastopnih pokušaja unosa pogrešnog PIN-a eOI se zaključava.
e) Zaključanu eOI osoba može otključati samostalno korištenjem PUK vrijednosti koja je postavljena tijekom aktivacije eOI.
f) Nakon 6 uzastopnih pokušaja unosa pogrešnog PUK-a eOI se blokira.
g) Blokiranu eOI može deblokirati samo službenik PU/PP u sigurnom okružju korištenjem elektroničke usluge za deblokadu eOI.
h) Deblokada eOI vrši se u fizičkoj prisutnosti osobe, a nakon utvrđivanje identiteta osobe.

6.4.3. Ostale odredbe o aktivacijskim podacima

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

U skladu s dokumentiranim internim procedurama AKD provodi zaštitu aktivacijskih podataka od generiranja, instalacije, ispisa u sigurnosne omotnice i uništavanja aktivacijskih podataka do transporta i uručivanja sigurnosnih omotnica osobama.

Nakon što im je uručena sigurnosna omotnica, osobe su odgovorne za zaštitu aktivacijskih podataka.

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 [41] i ISO/IEC 27002 [42] normama.

Pored toga implementirani su tehnički zahtjevi vezani uz računalnu sigurnost u skladu s zahtjevima norme ETSI EN 319 401 [24] kao i sa zahtjevima koji su navedeni u dokumentu CA/Browser Forum NetSec [15] odnosno CEN TS 419 261 [23].

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

6.6.1. Upravljanje razvojem sustava

U skladu s poglavljem 14 ISO/IEC 27002 [42] 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.

6.6.2. Provjera upravljanja sigurnošću

U skladu s poglavljem 12 ISO/IEC 27002 [42] 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 [44] 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.

6.6.3. Provjera sigurnosti životnog ciklusa

Tijekom životnog ciklusa provode se periodične kontrole i nadzor nad sigurnošću informacijskog sustava.

U skladu s poglavljem 15 ISO/IEC 27002 [42] uspostavljene su kontrole vezane uz poslovne odnose i dobavljače što uključuje:

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

6.7. Kontrola mreže

Uspostavljene su kontrole mreže kako je definirano u poglavlju 13 ISO/IEC 27002 [42], prilogu B CEN TS 419 261 [23] i CA/Browser Forum NetSec [15].

To obuhvaća 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:
   - PKI CA zona gdje su smješteni računalni resursi za provedbu usluge generiranje i upravljanja opozivom certifikata,
   - PKI uslužna zona gdje su smješteni računalni resursi za provedbu usluge informiranja i provjeru statusa certifikata,
   - Perso uslužna zona gdje su smješteni računalni resursi unos kriptografskih ključeva u eOI i ispis aktivacijskih podataka na sigurnosne omotnice,
   - 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 točkom 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 vatrozidima, 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:
l) sigurnoj zoni se može pristupiti samo iz uslužne i djelatne zone,
m) uslužnoj i djelatnoj zoni se može pristupiti samo iz nadzorne i pristupne zone.
n) Automatizirano se generiraju izvještaji o svakoj promjeni konfiguracije vatrozida.
o) Implementiran je sustav za otkrivanje napada (eng. *Intrusion Detection System - IDS*), koji nadzire mrežni promet te alarmira sve sumnjive aktivnosti u realnom vremenu.
p) Ispitivanje ranjivosti se provodi periodično i kod svake značajnije promjene konfiguracije, a sve kritične ranjivosti se rješavaju u najkraćem mogućem roku.

q) Kod značajnih promjena, a barem jedan puta godišnje provodi se ispitivanje mogućnosti upada u sustav (*eng. Penetration test*).

6.8. Upotreba vremenskog žiga

Sva informacijska oprema ima usklađeno sistemske satove i raspolaže s pouzdanim izvorom vremena tako da svi revizijski zapisi sadržavaju važeću zabilješku datuma i vremena. Maksimalno dozvoljeno odstupanje u vremenu je 1 sekunda.

7. Sadržaj certifikata i CRL

7.1. Profili certifikata

Obrasci (profili) svih certifikata usklađeni su s IETF RFC 5280 [35] i preporukama ITU-T X.509 [45].

Pri određivanju profila certifikata primjenjuju se sljedeće norme:

- ETSI EN 319 412-1 [28] općenito za sve certifikate,
- ETSI EN 319 412-2 [29]za fizičke osobe,
- ETSI EN 319 412-3 [30] za CA i OCSP certifikate i
- ETSI EN 319 412-5 [31] za EU kvalificirane certifikate

Osnovna polja svih certifikata navedena su u sljedećoj tablici.

Tablica 8: 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 32 bit-a
Signature Algorithm	SHA256RSA, 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
Signature Value	Potpis izdavatelja certifikata, generiran i kodiran prema IETF RFC 5280 [35]

7.1.1. Broj verzije

Koristi se X.509 verzija V3.

7.1.2. Ekstenzije certifikata

7.1.2.1. Ekstenzije CA certifikata

Ekstenzije HRIDCA certifikata navedene su u sljedećoj tablici.

Tablica 9: Ekstenzije HRIDCA certifikata

Polje	Vrijednost
Key Usage*	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints*	Subject Type=CA Path Length Constraint=None
Subject Key Identifier	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	Derived using the SHA-1 hash of the public key.
Authority Info Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eid.hr/cert/akdcaroot.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.eid.hr/akdcaroot
Certificate Policies	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
CRL Distribution Points	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.eid.hr/akdcaroot.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.eid.hr/akdcaroot.crl [3]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://ldap.eid.hr/cn=AKDCA Root,o=AKD d.o.o.,c=HR?certificateRevocationList;binary (ldap://ldap.eid.hr/cn=AKDCA%20Root,o=AKD%20d.o.o.,c=HR?certificateRevocationList%3Bbinary)

*Kritično polje

7.1.2.1. Ekstenzije certifikata osoba

Ekstenzije certifikata osoba koje izdaje HRIDCA navedene su u sljedećoj tablici.

Tablica 10: Ekstenzije certifikata osoba

Polje	Tip certifikata	Vrijednost
Key Usage*	eOI NCP-n-qscd-eid	Digital Signature
	eOI QCP-n-qscd-esign	Non-Repudiation
Basic Constraints*	All End Entity	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	All End Entity	Derived using the SHA-1 hash of the public key.
Authority Info Access	All End Entity	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://eid.hr/cert/hridca.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp-hridca.eid.hr/hridca
Certificate Policies	eOI NCP-n-qscd-eid	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.1.2.1.2.20 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
	eOI QCP-n-qscd-esign	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.1.2.1.2.10 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
CRL Distribution Points	All End Entity	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl1.eid.hr/hridca.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl2.eid.hr/hridca.crl [3]CRL Distribution Point Distribution Point Name: Full Name: URL= ldap://ldap.eid.hr/cn=HRIDCA,o=AKD d.o.o.,c=HR?certificateRevocationList;binary (ldap://ldap.eid.hr/cn=AKDCA%20Root,o=AKD%20d.o.o.,c=HR?certificateRevocationList%3Bbinary)
qcStatements	eOI NCP-n-qscd-eid	N/P
	eOI QCP-n-qscd-esign	id-etsi-qcs-QcCompliance(1) (0.4.0.1862.1.1)

		id-etsi-qcs-QcSSCD(4) (0.4.0.1862.1.4) id-etsi-qcs-QcPDS (5) (0.4.0.1862.1.5) PdsLocation: url= https://eid.hr/cps/HRIDCA-pds2-0-en.pdf language=en PdsLocation: url= https://eid.hr/cps/HRIDCA-pds2-0-hr.pdf language=hr id-etsi-qcs-QcType (6) (0.4.0.1862.1.6) Type= id-etsi-qct-esign(1) (0.4.0.1862.1.6.1)

*Kritično polje

7.1.3. Identifikator objekta (OID) algoritama

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koje izdaje HRIDCA prikazani su u sljedećoj tablici.

Tablica 11: Algoritmi i pripadni identifikatori objekta

Algoritam	OID
Sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

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 točki 3.1.1. ovog dokumenta.

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

7.1.5. Ograničenja u nazivima

Ne koristi se.

7.1.6. Identifikator objekata (OID) općih pravila certificiranja

U svakom certifikatu koji sadrže ekstenziju *„Certificate Policies“* naveden je odgovarajući OID identifikator kako je navedeno u točki 1.2.2 ovog dokumenta.

7.1.7. Upotreba ekstenzije Policy Constraints

Ne koristi se.

7.1.8. Sintaksa i semantika kvalifikatora općih pravila

U svakom certifikatu koji sadrže ekstenziju *„Certificate Policies“* stavljena je adresa na kojoj se mogu naći CP i CPS kako je navedeno u točki 2.2. ovog dokumenta.

7.1.9. Procesne semantike za kritičnu ekstenziju Certificate Policies

Ne koristi se.

7.2. CRL profili

Profili CRL koji izdaje HRIDCA podržava X.509 verziju 2 sukladno zahtjevima definiranim u IETF RFC 5280 [35]. U sljedećoj tablici su osnovna polja HRIDCA CRL.

Tablica 12: Osnovna polja HRIDCA CRL

Polje	Vrijednost/Ograničenja vrijednosti
Version	X.509 V2, vidi točku 7.2.1
Signature Algorithm	SHA256RSA, 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

Ekstenzije CRL koji izdaje HRIDCA navedene su u sljedećoj tablici.

Tablica 13: Ekstenzije HRIDCA CRL

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

7.3. OCPS profil

Certifikat OCSP usluge je sukladan IETF RFC 6960 [36].
U sljedećoj tablici su osnovna polja HRIDCA OCSP.

Tablica 14: Osnovna polja HRIDCA OCSP

Polje	Vrijednost/Ograničenja vrijednosti
Version	X.509 V3, vidi točku 7.3.1
Serial Number	Jedinstven pozitivan broj s entropijom od 32 bit-a
Signature Algorithm	SHA256RSA, 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
Signature Value	Potpis izdavatelja certifikata, generiran i kodiran prema IETF RFC 5280 [35]

7.3.1. Broj verzije

Koristi se X.509 verzija V3.

7.3.2. Ekstenzije OCSP certifikata

Ekstenzije HRIDCA OCSP certifikata navedene su u sljedećoj tablici.

Tablica 15: Ekstenzije HRIDCA OCSP certifikata

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

	(1.3.6.1.5.5.7.48.1.5)

*Kritično polje

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 [9] provodi se svaka 24 mjeseca.

Redovni nadzor sustava upravljanja s ciljem provjere usklađenosti s ISO/IEC 9001 [43], ISO/IEC 27001 [41] i ISO/IEC 14298 [40] 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 državno 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 [9] provodi tijelo za ocjenjivanje sukladnosti koje je u skladu s Uredbom (EZ) br. 765/2008 [13] ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža.

Kvalifikacije i zahtjevi koji se odnose na tijela za ocjenjivanja sukladnosti definirani su u normi ETSI EN 319 403 [25].

Nadzor sustava upravljanja sukladno normama ISO/IEC 9001 [43], ISO/IEC 27001 [41] i ISO/IEC 14298 [40] vrše ovlaštene revizijske kuće.

Interni revizori moraju

- raspolagati znanjima iz područja PKI i informacijske sigurnosti,
- raspolagati znanjima i razumijevanjem ETSI EN 319 401 [24], ETSI EN 319 411 [26] i [27] i ostalih normi i tehničkih specifikacija koje su referencirane u ovom dokumentu,
- 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.

Interna revizija se vrši sukladno normama ISO/IEC 9001 [43] i ISO/IEC 27001 [41].

8.3. Odnos revizora s predmetom revizije

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

Internu reviziju u AKD-u provodi 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,
- dostupnost i sadržaj usluga informiranja,
- dokumentaciju i sporazume vezane uz uslugu registracije i
- provedbu propisanih postupaka i mjera zaštite u skladu s odredbama CP i CPS.

8.5. Postupanje u slučaju nesukladnosti

U slučaju nesukladnosti provode se sljedeće aktivnosti:

a) Provodi se ispitivanje okolnosti vezanih uz nesukladnost, određuje se uzrok nesukladnosti i predlažu se korektivne radnje.
b) PMA analizira prijedloge i izrađuje operativni plan otklanjanja nesukladnosti koji uključuje opis aktivnosti i planirane rokove.
c) Dodjeljuju se zaduženja vezana uz provedbu i praćenje provedbe operativnog plana.
d) Ako je utvrđena nesukladnost koja značajno utječe na sigurnost pružanja usluga povjerenja ili onemogućuje ispunjenje zakonom propisanih zahtjeva, PMA će zahtijevati prekid pružanja usluge.
e) AKD će poduzeti sve potrebne radnje kako bi spriječio nepovoljan utjecaj prekida pružanja usluga na osobe i pouzdajuće strane.
f) AKD će nastaviti pružati usluge kada PMA utvrdi da razlog zbog kojeg je došlo do prekida usluga više ne postoji.

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 zakonskim odredbama, ministarstvu RH nadležnom za gospodarstvo kao nadzornom tijelu podnosi izvješće o ocjenjivanju sukladnosti.

9. Ostale poslovne i pravne stavke

9.1. Naknade za usluge

9.1.1. Naknade za izdavanje ili obnovu certifikata

Naknada za izdavanje ili obnovu certifikata uključena je u cijenu eOI u skladu s točkom 9.1.4.

9.1.2. Naknade za pristup certifikatu

Tijelima javnog sektora Republike Hrvatske omogućeno je pretraživanje certifikata u javnom imeniku HRIDCA bez naknade.

9.1.3. Naknade za opoziv i pristup informacijama o statusu certifikata

Usluga opoziva certifikata se ne naplaćuje.

Osobe i pouzdajuće strane bez naknade mogu koristiti usluge za provjeru statusa certifikata.

9.1.4. Naknade za ostale usluge

Usluga registracije fizičkih osoba te usluge izrade i individualizacije kartice naplaćuju se kroz cijenu eOI.

Cijena eOI je određena provedbenim aktima koji proizlaze iz Zakona o osobnoj iskaznici [1].

Informacije i usluge dostupne putem portala eOI se ne naplaćuju.

9.1.5. Povrat naknade

Nema odredbi.

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.

AKD je odgovoran za štete koje nanese svakoj fizičkoj ili pravnoj osobi zbog neispunjavanja svojih obveza u skladu s ovim dokumentom i Uredbom (EU) br. 910/2014 [9].

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

Pravila sudionika pružanja usluga certificiranja uređena su u skladu s Zakonom o obveznim odnosima [8].

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 2.000.000,00 kuna.

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

Povjerljivi poslovni podaci smatraju se podaci koji su označeni kao poslovna tajna ili su kao poslovna tajna određeni zakonom o tajnosti podataka [5], na zakonu utemeljenim propisom ili internim pravilom, 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) osobni podaci i dokumentacija prikupljena u postupku registracije u skladu s poglavljem 9.4,
b) zbirke podataka, revizijski zapisi i arhiva pružatelja usluga,
c) izvještaji o provedbi aktivnosti i postupci pružanja usluga,
d) poslovna komunikacija između sudionika postupka certificiranja i
e) ostali podaci različitog tipa značajni za poslovanje ili interese sudionika.

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

f) svi privatni ključevi, aktivacijski podaci i podaci za registraciju na portal,
g) svi simetrični ključevi, PIN-ovi, zaporke, kodovi i sva šifrirana komunikacija između sudionika, mreže ili komponenata PKI infrastrukture,
h) specifični podaci vezani uz sigurnost i provedbu mjera zaštite podataka, informacijskih sustava, poslovne suradnje, radnika i lokacije obavljanja djelatnosti i
i) planovi zaštite i nacrti objekata i prostora te planovi 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:

a) certifikati, lista opozvanih certifikata i informacije o statusu certifikata,
b) informacije i dokumenti koji su objavljeni na portalu,
c) podaci čije priopćavanje neće narušiti Ustavom i zakonima propisana prava i slobode fizičkih i pravnih osoba,
d) podaci koje AKD objavljuje na svojim službenim stranicama ili koje je dužan objaviti radi ispunjenja obveza iz Zakona o pravu na pristup informacijama [6],
e) 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.

Osoblje CA i službenici RA/LRA 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 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 MUP poduzimaju 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 MUP-a 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

MUP prikuplja i obrađuje osobne podatke za potrebe izdavanja osobnih iskaznica.

U skladu sa Zakonom o osobnoj iskaznici [1] MUP vodi evidencije čiji je sadržaj propisan Pravilnikom o obrascima i evidenciji osobnih iskaznica [2].

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 objavljuje certifikate u javnom imeniku pod uvjetima koji su definirani u točki 4.4.2.

Osobni podaci sadržani u certifikatu nisu povjerljivi.

9.4.4. Odgovornost za zaštitu osobnih podataka

AKD i MUP su odgovorni za zaštitu osobnih podataka.

Osigurana je zakonita obrada osobnih podataka u skladu s odredbama Zakona o zaštiti osobnih podataka [4] i vezanih pod-zakonskih akata odnosno Direktive 95/46/EC [14].

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.

Potpisivanjem Ugovora o pružanju usluga certificiranja osobe su dale privolu pružatelju usluga certificiranja za korištenje 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 i Republika Hrvatska koja je vlasnik AKD-a posjeduju i rezerviraju 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, 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 eOI (AKD-eID-Card 1.0) kao i aplikaciju (middleware) za korištenje eOI.

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 eOI i aplikacije za korištenje eOI bez naknade, a po 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

PMA je odgovoran za:

a) definiranje, uvođenje i administriranje CP, CPS, PDS, sigurnosno operativnih procedura i provedbenih dokumenata vezanih uz djelovanje AKD PKI i pružanje usluga povjerenja

b) održavanje kontinuirane prikladnosti i usklađenosti dokumentacije s Uredbom (EU) br. 910/2014 [9] te obvezujućim nacionalnim, europskim ili međunarodnim normama i
c) nadzor provedbom sigurnosnih zahtjeva koji su propisni ovim dokumentom.

9.6.2. Obveze i odgovornosti CA

Certifikacijsko tijelo je odgovorno za:

a) osiguranje provedbe Uredbe (EU) br. 910/2014 [9] te primjenu 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 kao i usluga informiranja u skladu s ovim dokumentom,
c) pravovremenu obradu 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) primjenu 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 CA, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge,
h) zakonitu obradu osobnih podataka u skladu s Zakonom o zaštiti osobnih podataka [4] i Direktivom 95/46/EC [14] i
i) osiguranje ISO/IEC 9001 [43] i ISO/IEC 27001 [41] certifikata kao dokaza kvalitete i sigurnosti pružanje usluga certificiranja.

9.6.3. Obveze i odgovornosti RA

Registracijsko tijelo je odgovorno za:

a) prikupljanje i provjeru podataka o identitetima fizičkih osoba u skladu s Zakonom o osobnoj iskaznici [1],
b) zaprimanje zahtjeva osoba uključujući zahtjeve za izdavanje eOI i certifikata, zahtjeva za opoziv i suspenziju certifikata te zahtjeva za deblokadu eOI te uručivanje eOI,
c) izravnu provjeru i nedvojbeno utvrđivanje identiteta fizičkih osoba neposrednom identifikacijom u fizičkoj prisutnosti osobe prilikom zaprimanja zahtjeva osoba, kao i prilikom uručivanja eOI,
d) upis cjelovitih, točnih i provjerenih osobnih identifikacijskih podataka o fizičkim osobama i njihovim zahtjevima u informacijski sustav te njihovo prosljeđivanje na daljnju obradu proizvođaču odnosno CA,
e) osiguranje da poslove registracije provode isključivo pouzdani i savjesni službenici PU/PP čiji je identitet nedvojbeno utvrđen i koji su adekvatno educirani prije nego što su im dodijeljena ovlaštenja,
f) primjenu odgovarajućih fizičkih, organizacijsko-upravljačkih i provedbenih mjera zaštite informacijskog sustava RA i podataka,

g) bilježenje i dugoročno arhiviranje podataka i dokumentacije prikupljene u postupku registracije i svih bitnih informacije u vezi s podacima koje izdaje i prima RA, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge i
h) provedbu zakonite obrade i zaštite osobnih podataka u skladu s Zakonom o zaštiti osobnih podataka [4] i Direktivom 95/46/EC [14].

9.6.4. Obveze i odgovornosti osoba

Osoba je odgovorna:
a) da u postupku identifikacije predoči vjerodostojne dokaze kojima potvrđuje svoj identitet,
b) da u postupku registracije dostavi točne i istinite podatke,
c) da pregleda i provjeri da su podaci u certifikatu ispravni,
d) da isključivo osoba koja je navedena u certifikatu koristiti privatni ključ koji odgovara javnom ključu u certifikatu,
e) da certifikat u trenutku njegovog korištenja nije istekao i da nije opozvan,
f) da certifikat koristi samo za legalne i autorizirane svrhe te u skladu s njihovom namjenom,
g) da odgovorno koristi i čuva eOI, privatne ključeve i aktivacijske podatke te da poduzima odgovarajuće mjere zaštite od neovlaštenog pristupa i uporabe i
h) da odmah zatraži opoziv ili suspenziju certifikata ako je došlo do promjene osobnih identifikacijskih podataka u certifikatu ili ako sumnja u gubitak, krađu, zlouporabu ili neautorizirano korištenje privatnog ključa.

9.6.5. Obveze i odgovornosti pouzdajućih strana

Pouzdajuće strane su odgovorne:
a) da se prije korištenja usluga informiraju o CP, CPS i PDS, 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 [35] i IETF RFC 3739 [34].

9.6.6. Obveze i odgovornosti proizvođača

Proizvođač je odgovoran za:
a) izradu eOI čiji je sadržaj, oblik i način zaštite propisan Zakonom o osobnoj iskaznici [1] i vezanim pravilnikom [2],
b) pripremu podataka i individualizaciju eOI temeljem zahtjeva i nepromijenjenih podataka dobivenih od RA,

c) generiranje parova ključeva i aktivacijskih podataka, pribavljanje certifikata od HRIDCA te njihovo unošenje u eOI,
d) generiranje podataka za aktivaciju eOI i registraciju na portal te izrada sigurnosnih omotnica,
e) primjenu odgovarajućih fizičkih, organizacijsko-upravljačkih i provedbenih mjera zaštite informacijskog sustava proizvođača i podataka u skladu s ovim dokumentom,
f) zakonitu obradu i zaštitu osobnih podataka u skladu s Zakonom o zaštiti osobnih podataka [4] i Direktivom 95/46/EC [14],
g) osiguranje ISO/IEC 9001 [43], ISO/IEC 27001 [41] i ISO/IEC 14298 [40] certifikata kao dokaza kvalitete upravljanja poslovanjem i proizvodnjom zaštićenog tiska te sigurnošću informacijskih sustava i
h) osiguranje eOI koji zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 15408 [39] te da demonstrira sukladnost s obrascima zaštite iz serije EN 419 211 [17], [18], [19], [20], [21] i [22].

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 upotrebom certifikata,
b) štete prouzročene lažnom ili nemarnom uporabom eOI, privatnih ključeva, certifikata ili CRL,
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.

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.

AKD nije odgovoran za bilo koji gubitak koji može nastati kao posljedica djelovanja više sile i ostalih okolnosti koje su izvan kontrole AKD-a, kako je definirano u točki 9.16.5.

9.8. Ograničenja odgovornosti

Ukupna financijska odgovornost za transakcije obavljene na temelju pouzdavanja u certifikate izdane prema ovom dokumentu iznosi najviše 2.000.000 kuna.

Prema osobama i pouzdajućim stranama koje primjereno koriste certifikate visina financijske odgovornosti za transakcije se ograničava, sukladno preporučenom financijskom limitu koji iznosi do 80.000 kn po transakciji.

9.9. Naknada štete

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

Osoba odgovara oštećenoj strani ako:

a) stekne certifikat temeljem prijevarno danih podataka u zahtjevu za izdavanje eOI ili
b) djeluje ili se predstavlja u ime druge fizičke osobe.

Pouzdajuća strana odgovara oštećenoj strani ako:

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

AKD je odgovoran ako je ta odgovornost jasno uspostavljena ugovorom, općim pravilima, pravilnikom ili zakonskom regulativom Republike Hrvatske.

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

Primjena pravila koja su navedena u ovome dokumentu počinju datumom objavljivanja dokumenta na 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 važenja

Dokument prestaje važiti kad ga zamijeni novije izdanje dokumenta ili kad se objavi prestanak važenja dokumenta.

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

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

9.10.3. Posljedice prestanka važenja 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 nastaviti važiti sve do isteka perioda važenja certifikata ili do opoziva certifikata.

9.11. Pojedinačne obavijesti i komunikacija sa sudionicima

Informiranje osoba i pouzdajućim stranama se provodi putem portala.

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

Tablica 16: Kontakt podaci AKD-a

Kontakt podaci AKD-a:
Agencija za komercijalnu djelatnost d.o.o, Adresa: Savska cesta 31, 10000 Zagreb, Hrvatska web: http://akd.hr, e-mail: akd@akd.hr Portal: http://eid.hr Služba za korisnike: Helodesk-eOI@akd.hr Povjerenstvo za upravljanje pravilima certificiranja: 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 [9], zakoni koji su referencirani u ovom dokumentu, pod zakonski 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 [9], AKD je kvalificirani pružatelj usluga povjerenja kojem je ministarstvo RH nadležno za gospodarstvo kao nadzorno tijelo odobrilo kvalificirani status.

9.16. Ostale odredbe

9.16.1. Sporazum

Ako to nije protivno zakonskim propisima, odredbama općih pravila ili pravilnika, AKD kao pružatelj usluga povjerenja može s ostalim sudionicima sklopiti dodatni ugovor u kojem će se dodatno zaštititi svoje interese.

9.16.2. Prijenos odgovornosti

Nije primjenjivo.

9.16.3. Nevaljanost pojedine odredbe

U slučaju da se neka točka ili odredba ovog dokumenta smatra neprovedivom od strane suda ili drugog arbitražnog tijela, ostali dio dokumenta ostaje na snazi.

U slučaju proturječnosti, nesuglasica i eventualnih sporova oko tumačenja, primjene ili izvršenja usluga certificiranja, primjenjuju se odredbe sadržane u CP odnosno u primjenjivoj zakonskoj regulativi i obvezujućim normama.

9.16.4. Ovrha

Nije primjenjivo.

9.16.5. Viša sila

AKD ne snosi nikakvu odgovornost za bilo koji gubitak koji može nastati kao posljedica djelovanja više sile uključujući elementarne vremenske i prirodne nepogode, odron zemlje, poplave, požar, rat, vojne operacije, terorizam, poremećaji u komunikacijskoj infrastrukturi i opskrbi električnom energijom, zabrane, prisile i nepovoljni utjecaji zakona, građanski nemiri i ostale okolnosti koje su izvan kontrole AKD-a.

9.17. Ostale odredbe

Nije primjenjivo.

PRILOG 1: Definicije

Za potrebe ovog dokumenta primjenjuju se sljedeće definicije koje su preuzete iz Čl. 3 Uredbe (EU) br. 910/2014 [9] odnosno ETSI EN 319 411-1 [26]:

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 online 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 elektronički potpis;
9. „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;
10. „napredan elektronički potpis" znači elektronički potpis koji ispunjava zahtjeve navedene u članku 26. Uredbe (EU) br. 910/2014 [9];
11. „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;
12. „podaci za izradu elektroničkog potpisa" znači jedinstveni podaci koje potpisnik koristi za izradu elektroničkog potpisa;
13. „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;
14. „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 [9];
15. „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;

16. „kvalificirana usluga povjerenja" znači usluga povjerenja koja ispunjava odgovarajuće zahtjeve utvrđene u ovoj Uredbi;
17. „tijelo za ocjenjivanje sukladnosti" znači tijelo u smislu članka 2. točke 13. Uredbe (EZ) br. 765/2008 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;
18. „pružatelj usluga povjerenja" znači fizička ili pravna osoba koja pruža jednu ili više usluga povjerenja bilo kao kvalificirani ili nekvalificirani pružatelj usluga povjerenja;
19. „kvalificirani pružatelj usluga povjerenja" znači pružatelj usluga povjerenja koji pruža jednu ili više kvalificiranih usluga povjerenja i kojemu je nadzorno tijelo odobrilo kvalificirani status;
20. „proizvod" znači hardver ili softver ili odgovarajuće komponente hardvera ili softvera koji su namijenjeni za korištenje u svrhu pružanja usluga povjerenja;
21. „sredstvo za izradu elektroničkog potpisa" znači konfigurirani softver ili hardver koji se koristi za izradu elektroničkog potpisa;
22. "certifikat": javni ključ korisnika koji je zajedno s ostalim informacijama šifriran privatnim ključem CA koji ga je izdao, tako da se ne može krivotvoriti;
23. "Opća pravila pružanja usluga certificiranja (CP)": imenovani skup pravila koja ukazuju na prikladnost certifikata za određenu zajednicu i/ili skupinu sa zajedničkim sigurnosnim zahtjevima;
24. "Lista opozvanih certifikata CRL": potpisana lista s nizom certifikata koje izdavatelj više ne smatra valjanim;
25. "Certifikacijsko tijelo (CA)": tijelo kojem vjeruje jedan ili više korisnika, a koje kreira i dodjeljuje certificate;

    Napomena: 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.
26. "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;
27. "koordinirano svjetsko vrijeme (UTC)": vremenska skala koja je definirana u ITU-R TF.460-6 [47];
28. „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;
29. "zona visoke sigurnost": specifična fizička lokacija gdje se čuva privatni ključ krovnog CA;

30. “Registracijsko tijelo (RA)”: tijelo koje je prvenstveno odgovorno za identifikaciju i autentikaciju subjekta certifikata

    Napomena: RA pomaže u postupku podnošenja zahtjeva za izdavanje i opoziv certifikata;

31. “službenik RA”: radnik odgovoran za provjeru informacija i pripremu podataka koja se nužno provodi pri izdavanju certifikata i odobrenje zahtjeva za izdavanje certifikata;
32. “službenik za opoziv”: radnik odgovoran za provedbu zahtjeva za promjenu statusa certifikata;
33. “krovno certifikacijsko tijelo (krovni CA)”: certifikacijsko tijelo koje na najvišem nivou djeluju u sklopu hijerarhijske strukture i koje potpisuje certifikat podređenim CA;
34. “siguran kriptografski uređaj”: uređaj koji čuva privatni ključ korisnika, štiti taj ključ od kompromitacije i provodi operacije potpisivanja ili dešifriranja u ime korisnika;
35. „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;
36. “subjekt”: osoba identificirana u certifikatu kao vlasnik privatnog ključa koji odgovara javnom ključu u certifikatu.
37. “podređeno certifikacijsko tijelo (podređeni CA): certifikacijsko tijelo čiji je certifikat potpisan korovnim CA;

    Napomena: Podređeni CA izdaje certifikat krajnjim korisnicima.

PRILOG 2: Kratice

Kratice koje se koriste u dokumentu su:

eOI	Elektronička osobna iskaznica
MUP	Ministarstvo unutarnjih poslova
RH	Republika Hrvatska
AKD	Agencija za komercijalnu djelatnost
AKDCA	Certifikacijsko tijelo AKD
HRIDCA	Certifikacijsko tijelo za izdavanje certifikata osobama za potrebe elektroničke osobne iskaznice Republike Hrvatske
PKI	Public Key Infrastructure
CP	Certificate Policy
CPS	Certificate Practice Statement
QCP	Qualified Certificate Policy
PMA	Policy Management Authority
CA	Certificate Authority
RA	Registration Authority
OID	Object Identifier - Identifikacijska oznaka
PU/PP	Policijska uprava/Policijska postaja
LRA	Local Registration Authority

SCD Signature Creation Device

SSCD Secure Signature Creation Device

QSCD Qualified Electronic Signature Creation Device

NIAS	Nacionalni identifikacijski i autentifikacijski sustav
CRL	Certificate Revocation List
CARL	Certification Authority Revocation List
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
HTTP	Hypertext Transfer Protocol
UTC	Coordinated Universal Time
RSA	Rivest, Shamir and Adleman algorithm
HSM	Hardware security module
FIPS	Federal Information Processing Standard
x.509v3	Public Key Infrastructure Standard
PIN	Personal Identification Number
PUK	Personal Unblocking Code
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
EULA	End User Licence Agreement
PDS	Policy Disclosure Statement
PTC	Publicly-Trusted Certificate

PRILOG 3: Reference

Zakoni:

[1] Zakon o osobnoj iskaznici (NN 62/2015).

[2] Pravilnik o obrascima i evidenciji osobnih iskaznica te organizacijskim, tehničkim i sigurnosnim mjerama u postupku izdavanja osobnih iskaznica (NN 63/2015).

[3] Pravilnik o cijeni osobnih iskaznica (NN 62/2015).

[4] Zakon o zaštiti osobnih podataka (NN 103/03, 118/06, 41/08, 130/11, 106/12).

[5] Zakon o tajnosti podataka (NN 79/07, 86/12).

[6] Zakon o pravu na pristup informacijama (NN 25/13, 85/15).

[7] Zakon o elektroničkom potpisu (NN 10/02, 80/08, 30/14) ili Zakon o provedbi uredbe eIDAS.

[8] Zakon o obveznim odnosima (NN 35/05, 41/08, 125/11, 78/15).

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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. 339/93.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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