HRIDCA
PRAVILNIK O POSTUPCIMA CERTIFICIRANJA

Izdanje 1.3

Status: 08. 06. 2015.

Sadržaj:

Popis izdanja dokumenta:

Izdanje	Datum	Obrazloženje izmjene
PRO-I-91-01	08.06.2015.	Prvo izdanje dokumenta

0. Uvod

0.1. Opseg i namjena dokumenta

Ovaj Pravilnik o postupcima certificiranja (u daljnjem tekstu Pravilnik) definira postupke i mjere koje primjenjuju Agencija za komercijalnu djelatnost d.o.o. (u daljnjem tekstu AKD) i Ministarstvo unutarnjih poslova (u daljnjem tekstu Ministarstvo) prilikom upravljanja postupcima certificiranja za elektroničku osobnu iskaznicu (eOI) kao i fizičke osobe te pouzdajuće strane prilikom korištenja certifikata na eOI.

Pravilnik je usklađen s Općim pravilima davanja usluga certificiranja (engl. *Certificate Policy* – CP, u daljnjem tekstu: Opća pravila) koji izdaje AKD PKI.

Pravilnik odgovara dokumentu „Posebna unutarnja pravila o postupcima izdavanja kvalificiranih certifikata i zaštiti sustava certificiranja“ koji je definiran u Pravilniku o evidenciji davatelja usluga certificiranja [8], odnosno u Pravilniku o izradi elektroničkog potpisa [6].

Prema RFC 3647 [12] Pravilnik odgovara dokumentu „Certification Practice Statement CPS“ kojim se iskazuje praksa po kojoj se izdaju certifikati i po kojoj se upravlja životnim ciklusom certifikata.

Struktura i sadržaj dokumenta su strogo usklađeni sa zahtjevima RFC 3647 [12] tako da je svako poglavlje na odgovarajući način nazvano i numerirano te sadrži informacije za koje je propisano da su sadržane u tom poglavlju.

0.2. Reference

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

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

[5] Zakon o elektroničkom potpisu (NN 10/02, 80/08, 30/14)

[6] Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelja usluga izdavanja vremenskog žiga i certifikata (NN 107/10, 89/13)

[7] Popis normizacijskih dokumenata u području primjene zakona o elektroničkom potpisu i pravilnika o izradi elektroničkog potpisa, uporabi sredstva za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelje usluga izdavanja vremenskog žiga i certifikata u poslovanju davatelja usluga certificiranja u Republici Hrvatskoj (NN 89/13)

[8] Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj (NN 107/2010)

[9] Directive 1999/93/EC of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures

[10] 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

[11] 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

0.2.2. Obvezujuće i buduće norme

Usluge povjerenja:

[12] RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[13] EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

[14] EN 319 411-2 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates (HRN ETSI/EN 319 411-2)

[15] EN 319 411-3 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates

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

Sredstvo za izradu elektroničkog potpisa (SSCD):

[17] EN 419 211-2 Protection profiles for secure signature creation device - Part 2: Device with Key Generation

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

Profili certifikata:

[19] RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile

[20] RFC 3739 Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

[21] RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[22] EN 319 412-5 Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile (HRN ETSI/EN 319 412-5)

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

Sustavi upravljanja:

[24] ISO/IEC 15408 Information technology — Security techniques — Evaluation criteria for IT security Part 1, Part 2, Part 3 (HRN ISO/IEC 15408)

[25] ISO/IEC 9001 Quality Management Systems

[26] ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management System – Requirements (ISMS)

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

[28] ISO/IEC 14298 Graphic technology — Management of security printing processes

0.2.3. Vezane tehničke specifikacije

[29] ISO/IEC 9594-8 ITU-T Recommendation X.509:2000 / ISO/IEC 9594-8:2001: Information technology – Open Systems Interconnection – The Directory: Public-key attribute certificate frameworks

[30] ISO/IEC 9594-2 ITU-T Recommendation X.501:2008/ ISO/IEC 9594-2:2008 – Information technology – Open Systems Interconnection – The Directory: Models

[31] ISO/IEC 19790 ISO/IEC 19790: Information technology - Security techniques - Security requirements for cryptographic modules.

[32] FIPS PUB 140-2 NIST FIPS PUB 140-2:2002 – Security Requirements for Cryptographic Modules

[33] ETSI TS 119 312 V1.1.1 (2014-11) Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

[34] CEN/TS 15480 Identification card systems — European Citizen Card Part 1, Part 2, Part 3, Part 4, Part 5

0.3. Definicije i kratice

0.3.1. Definicije

Za potrebe ovog dokumenta primjenjuju se sljedeće definicije:

e-Osobna iskaznica - je osobna iskaznica fizičkih osoba (osoba), a koja sadrži osobne identifikacijske podatke u elektroničkom obliku te parove ključeva i pripadajuće certifikate.

Elektronička identifikacija - postupak korištenja osobnih identifikacijskih podataka u elektroničkom obliku koji na nedvojben način predstavljaju bilo fizičku ili pravnu osobu ili fizičku osobu koja predstavlja pravnu osobu.

Sredstvo elektroničke identifikacije (*Electronic identification means*) - materijalna i/ili nematerijalna jedinica koja sadrži osobne identifikacijske podatke i koja se koristi za autentikaciju na elektroničku uslugu.

Osobni identifikacijski podaci - skup podataka koji omogućavaju da se utvrdi identitet fizičke ili pravne osobe ili fizičke osobe koja predstavlja pravnu osobu.

Sustav elektroničke identifikacije *(Electronic identification scheme)* - sustav za elektroničku identifikaciju u okviru kojega se izdaju sredstva elektroničke identifikacije fizičkim ili pravnim osobama ili fizičkim osobama koje predstavljaju pravne osobe.

Autentikacija - elektronički postupak koji omogućava da elektronička identifikacija fizičke ili pravne osobe ili izvornost i cjelovitost podataka u elektroničkom obliku budu potvrđeni.

Pouzdajuća strana *(Relying party)* - fizička ili pravna osoba koja se oslanja na elektroničku identifikaciju ili uslugu povjerenja.

Kvalificirani elektronički potpis - napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise.

Podaci za izradu elektroničkog potpisa *(Electronic signature creation data)* - jedinstveni podaci koje potpisnik koristi za izradu elektroničkog potpisa.

Elektronički potpis - skup podataka u elektroničkom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektroničkom obliku i koje potpisnik koristi za potpisivanje.

Napredan elektronički potpis - elektronički potpis koji pouzdano jamči identitet potpisnika i koji udovoljava zahtjevima sadržanim u čl. 4. Zakona o elektroničkom potpisu [5] odnosno koji ispunjava zahtjeve iz čl. 26 Uredbe (EU) [10].

Kvalificirani elektronički potpis - napredan elektronički potpis koji je izrađen pomoću kvalificiranih sredstava za izradu elektroničkog potpisa i temelji se na kvalificiranom certifikatu za elektroničke potpise.

Certifikat - potvrda u elektroničkom obliku koja povezuje podatke za verificiranje elektroničkog potpisa s nekom osobom i potvrđuje identitet te osobe.

Kvalificirani certifikat - certifikat koji udovoljava zahtjevima iz čl. 11. Zakona o elektroničkom potpisu [5], kojeg izdaje davatelj usluga izdavanja kvalificiranog certifikata koji ispunjava uvjete iz čl. 17 Zakona o elektroničkom potpisu [5] odnosno koji ispunjava zahtjeve utvrđene u Prilogu I Uredbe (EU) [10].

Usluga povjerenja (*Trust Service*) - elektronička usluga koja unaprjeđuje povjerenje u elektroničke transakcije.

Pružatelj usluga povjerenja (*Trust Service Provider*) - fizička ili pravna osoba koja pruža jednu ili više usluga povjerenja bilo kao kvalificirani ili nekvalificirani pružatelj usluga povjerenja.

Davatelj usluga certificiranja (Certification-Service-Provider) - pravna ili fizička osoba koja izdaje certifikate ili daje druge usluge povezane s elektroničkim potpisima.

Proizvod - hardver ili softver ili odgovarajuće komponente hardvera ili softvera koji su namijenjeni za korištenje u svrhu pružanja usluga povjerenja.

Sredstvo za izradu elektroničkog potpisa *(Electronic signature creation device - SSCD)* - konfigurirani softver ili hardver koji se koristi za izradu elektroničkog potpisa.

Kvalificirano sredstvo za izradu elektroničkog potpisa - sredstvo za izradu elektroničkog potpisa koje ispunjava zahtjeve utvrđene u Prilogu II Uredbe (EU) [10].

Elektronički pečat - podaci u elektroničkom obliku koji su pridruženi drugim podacima u elektroničkom obliku ili su logički povezani s njima radi osiguravanja izvornosti i cjelovitosti tih podataka.

Certifikat za autentikaciju mrežnih stranica - potvrda pomoću koje je moguće izvršiti autentikaciju mrežnih stranica te kojom se mrežne stranice povezuju s fizičkom ili pravnom osobom kojoj je izdan certifikat.

Podaci za validaciju - podaci koji se koriste za validaciju elektroničkog potpisa ili elektroničkog pečata.

Validacija - postupak verifikacije i potvrđivanja da su elektronički potpis ili pečat valjani.

Subjekt *(Subject)* - osoba ili organizacija koja je u certifikatu navedena kao subjekt.

Potpisnik - fizička osoba koja izrađuje elektronički potpis, a koja djeluje u svoje ime ili u ime pravne osobe koju predstavlja.

Povjerenstvo za upravljanje pravilima certificiranja (*Policy Management Authority - PMA*) - Povjerenstvo imenovano od strane Uprave AKD-a koje je odgovorno za postavljanje, uvođenje i

administriranje politika, sigurnosno operativnih procedura i provedbenih dokumenata vezanih uz djelovanje davatelja usluga certificiranja

Opća pravila certificiranja *(Certificate Policy - CP)* - Imenovani skup pravila koji ukazuje na prikladnost certifikata za određenu zajednicu ili skupinu prema zajedničkim sigurnosnim zahtjevima davatelja usluga certificiranja.

Pravilnik o postupcima certificiranja *(Certification Practice Statement - CPS)* – Posebna unutarnja pravila o postupcima izdavanja certifikata i zaštiti sustava certificiranja.

Ovjerovitelj (*Certification Authority -CA*) – Pravna ili fizička osoba autorizirana od PMA koja izdaje i potpisuje certifikate u skladu s Pravilnikom o postupcima certificiranja.

Krovni ovjerovitelj (*Root Certification Authority - Root CA*) – Ovjerovitelj koji izdaje certifikat samome sebi te podređenim ovjeroviteljima koji djeluju u sklopu hijerarhijske strukture.

Podređeni ovjerovitelj (*Subordinate Certification Authority - Subordinate CA*) – Ovjerovitelj koji izdaje certifikat krajnjim korisnicima tj. vlasnicima certifikata

Izdavatelj eOI - nadležno tijelo državne uprave koje izdaje eOI.

Osoba - fizička osoba, državljanin RH kojoj je Izdavatelj eOI i temeljem podnesenog zahtjeva izdao eOI i koja posjeduje certifikat na eOI.

Evidencija osobnih iskaznica – zbirka podataka koja se vodi na papiru i u elektroničkom obliku koja sadrži podatke i isprave o vlasnicima eOI za koje je upis u evidenciju propisan Zakonom o OI [1].

Tijelo za ocjenjivanje sukladnosti - tijelo u smislu čl. 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.

0.3.2. Kratice

Kratice koje se koriste u dokumentu su:

eOI Elektronička osobna iskaznica
PP Policijska postaja
PU Policijska uprava
OI Osobna iskaznica
EP Elektronički potpis
PKI Public Key Infrastructure
PIN Personal Identification Number
PUK Personal unblocking code
CA Certificate Authority
RA Registration Authority
LRA Local Registration Authority
CP Certificate Policy
CPS Certificate Practice Statement
SSCD Electronic signature creation device
QSCD Qualified electronic signature creation device
PMA Policy Management Authority

1. Uvod

1.1. Pregled

Elektronička osobna iskaznica (eOI) je obavezna isprava za hrvatske državljane starije od 18 godina s prijavljenim prebivalištem u Republici Hrvatskoj, a pravo na hrvatsku osobnu iskaznicu ima svaki državljanin Republike Hrvatske.

Temeljem Zakona o osobnoj iskaznici [1], osobne iskaznice izdaju policijske uprave odnosno policijske postaje Ministarstva dok poslove tehničke izrade osobnih iskaznica koji obuhvaćaju poslove proizvodnje osobnih iskaznica i izdavanja certifikata za osobne iskaznice obavlja AKD kao pravna osoba u državnom vlasništvu koju je Vlada Republike Hrvatske na prijedlog ministra nadležnog za unutarnje poslove odredila za obavljanje tih poslova.

eOI sadrži osobne identifikacijske podatke u grafičkoj formi koje su utisnuti na površini kartice i koji su u elektroničkoj formi pohranjeni u čipu kartice. Osobe, u ovisnosti o njihovoj starosti, na čipu eOI dobivaju par ključeva i odgovarajuće certifikate.

Izdaju se dva tipa certifikata:

a) Identifikacijski certifikat koji je kvalificirani certifikat i koji se koristi za elektroničku identifikaciju i autentikaciju radi pristupa elektroničkim uslugama
b) Potpisni certifikat koji je kvalificirani certifikat, koji se koristi za podršku naprednom elektroničkom potpisu i koji ima istu pravnu snagu i zamjenjuje vlastoručni potpis

Certifikati sadrže identifikacijske podatke osobe i njegov javni ključ u elektroničkom obliku koji omogućava da se na nedvojben način povežu podaci za verificiranje elektroničkog potpisa s fizičkom osobom te potvrdi identitet te osobe.

Certifikati na eOI su kvalificirani i izdaju se u skladu sa Zakonom o elektroničkom potpisu [5], Uredbom EU [10], te vezanim pod-zakonskim aktima i normama.

Certifikati na eOI su značajne razine sigurnosti što znači da pružaju značajni stupanj pouzdanja u odnosu na traženi ili utvrđeni identitet osobe i primijenjeni postupak certificiranja, a čija je svrha značajno smanjenje rizika zlouporabe ili promjene identiteta.

PKI infrastruktura koja omogućuje izdavanje certifikata za eOI uspostavljena je u AKD-u. Ona je uređena hijerarhijski tako da se sastoji od krovnog ovjerovitelja AKDCA Root koji izdaje certifikat samom sebi i podređenom ovjerovitelju HRIDCA, a koji izdaje certifikate fizičkim osobama.

AKD je upisan u evidenciju ministarstva nadležnog za poslove gospodarstva kao davatelj usluga certificiranja koji obavlja usluge izdavanja kvalificiranih certifikata.

Sukladno Uredbi EU [10], svaka 24 mjeseca AKD će angažirati ovlašteno tijelo za ocjenjivanje sukladnosti kako bi u skladu s propisanim postupkom obavilo reviziju AKD-a kao pružatelja kvalificiranih usluga povjerenja, a dobiveno izvješće o rezultatima ocjenjivanja sukladnosti će biti dostavljeno nadzornom tijelu.

Hrvatska elektronička osobna iskaznica ima sve funkcionalnosti europske kartice građana prema CEN/TS 15480 [34] što ju čini interoperabilnom i prikladnom za korištenje u elektroničkom poslovanju na nacionalnom i Europskom nivou.

1.2. Ime dokumenta i identifikacija

Identifikacija dokumenta	
Oznaka	PRO-I-91-01
Naziv	Pravilnik o postupcima certificiranja
Izdanje	1.3
Datum objave	08.06.2015.
Datum stupanja na snagu	08.06.2015.
Autor	AKD, Agencija za komercijalnu djelatnost d.o.o
Tip dokumenta	Certificate Practice Statement
Dostupnost	http://eid.hr/cps

Pravila o postupcima certificiranja koja su navedena u ovome dokumentu identificiraju se kroz sljedeće OID-e:

a) Identifikacijski certifikat: OID 1.3.6.1.4.1.43999.5.1.2.1.2.2
b) Potpisni certifikat: OID 1.3.6.1.4.1.43999.5.1.2.1.2.1
c) Certifikat OSCP usluge: OID 1.3.6.1.4.1.43999.5.2.1.2.1.9

Identifikacijski i potpisni certifikat se izdaju po pravilima koja su ekvivalentna EN 319 411-2 [14], poglavlje 5.2 QCP public + SSCD:

itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1)

1.3. PKI Sudionici

AKD je davatelj usluga povjerenja kako je definirano u Uredbi EU [10]. Usluge povjerenja koje su u opsegu ovoga dokumenta obuhvaćaju usluge certificiranja, usluge registracije i usluge proizvodnje osobnih iskaznica.

Kako bi se jasno razgraničile nadležnosti i odgovornosti sudionika poslovnog procesa, u ovome dokumentu su definirane sljedeće uloge:

a) davatelj usluga certificiranja,
b) davatelj usluga registracije,
c) osobe,
d) pouzdajuće strane,
e) proizvođač i
f) povjerenstvo za upravljanje pravilima certificiranja.

1.3.1. Davatelj usluga certificiranja

AKD je davatelj usluga certificiranja za eOI (eng. Certification-Service-*Provider* – CSP).

AKD i Ministarstvo imaju sklopljen ugovor kojim se izričito obvezuju na poštivanje i primjenu ovoga Pravilnika koji je usklađen s obvezujućim zakonskim aktima te koji podržava i implementira norme u području elektroničkog potpisa prema poglavlju 9.15.

Poslovi davatelja usluga certificiranja su:

a) Voditi registar certifikata ovjerovitelja HRIDCA.

b) Osigurati dostupnosti usluga vezanih uz vođenje registra certifikata ovjerovitelja HRIDCA uključujući izdavanje i objavu certifikata te upravljanje životnim ciklusom certifikata nakon izdavanja (opoziv, suspenziju ili povlačenje suspenzije).
c) Provoditi izdavanje, opoziv, suspenziju ili povlačenje suspenzije certifikata temeljem dobivenih zahtjeva.
d) Informirati osobe i pouzdajuće strane putem Portala o pravilima vezanim uz korištenje certifikata i davanje usluga certificiranja.

Detaljnije informacije se mogu naći u poglavlju 9.6.1.

1.3.2. Davatelj usluga registracije

Ministarstvo je nadležno tijelo državne uprave za izdavanje eOI. Ministarstvo je ujedno davatelj usluga registracije (eng. *Registration Authority* –RA).

Komunikacija s osobama vrši se u PU/PP Ministarstva (eng. *Local Registration Authorities*-LRA).

Davatelj usluga registracije provjerava identitet osoba i osigurava podatke temeljem kojih ovjerovitelj HRIDCA izdaje certifikate. U tome kontekstu bez suglasnosti AKD-a kao davatelja usluga povjerenja, Ministarstvo kao davatelj usluga registracije nije ovlašten mijenjati pravila registracije niti dozvoliti trećim stranama da za njega obavlja uslugu registracije koja je u opsegu ovoga Pravilnika.

Poslovi davatelja usluga registracije su:

a) Zaprimati zahtjeve osoba za izdavanje, opoziv, suspenziju ili povlačenje suspenzije certifikata.
b) Obavljati poslove registracije fizičkih osoba za potrebe izdavanja certifikata na eOI.
c) Informirati fizičke osobe o pravilima vezanim uz izdavanje eOI te o postupcima certificiranja i korištenja certifikata.
d) Provjeravati i nedvojbeno utvrđivati identitet fizičkih osoba.
e) Osigurati sklapanje Ugovora o davanju usluga certificiranja između fizičkih osoba koji posjeduju certifikat na osobnoj iskaznici i davatelja usluga certificiranja.
f) Upisivati provjerene osobne identifikacijske podatke o osobama i njihovim zahtjevima u evidenciju osobnih iskaznica, te odobravati zahtjeve osoba.
g) Slati potrebne podatke za realizaciju zahtjeva proizvođaču eOI i davatelju usluga certificiranja.
h) Uručivati osobne iskaznice i sigurnosne omotnice osobama.
i) Administrirati SSCD nakon izdavanja (deblokada SSCD).

Detaljnije informacije se mogu naći u poglavlju 9.6.2.

1.3.3. Osobe

Osobe su fizičke osobe kojima je izdavatelj osobnih iskaznica u skladu sa Zakonom o osobnoj iskaznici [1] izdao osobnu iskaznicu i koje su dobile u posjed certifikat i korespondirajući privatni ključ na osobnoj iskaznici.

Pravo na osobnu iskaznicu imaju državljani RH s prebivalištem u RH.

Vrijede pravila:

a) Djeca do 5 godina dobivaju osobnu iskaznicu bez certifikata.

b) Osobama starijim od 5 a mlađim od 18 godina izdaje se samo identifikacijski certifikat.
c) Punoljetnim osobama starijim od 18 godina uz identifikacijski certifikat izdaje se i potpisni certifikat.
d) Osobama starijim od 65 godina izdati će se osobna iskaznica bez certifikata ili s oba certifikata.

Osoba je ujedno subjekt naveden u certifikatu te potpisnik koji koristi certifikat za elektroničku identifikaciju i elektronički potpis isključivo u svoje osobno ime.

Detaljnije informacije se mogu naći u poglavlju 9.6.3.

1.3.4. 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 davatelja usluga povjerenja. Certifikat omogućuje pouzdajućoj strani elektroničku identifikaciju te provjeru certifikata i validaciju elektroničkog potpisa osoba.

Detaljnije informacije se mogu naći u poglavlju 9.6.4.

1.3.5. Proizvođač

Proizvođač osobne iskaznice je AKD.

Proizvođač proizvodi osobne iskaznice, osigurava SSCD kao sredstvo za izradu elektroničkog potpisa, za osobe generira parove ključeva i podatke za aktivaciju te od ovjerovitelja HRIDCA dobiva odgovarajući certifikat.

Poslovi proizvođača su:

a) Izrađivati osobne iskaznice i osigurati sredstvo za izradu elektroničkog potpisa (SSCD)
b) Uspostaviti Portal eOI (u daljnjem tekstu Portal) i informirati osobe o pravilima vezanim uz korištenje eOI kao SSCD.
c) Provoditi pripremu podataka i individualizaciju tijela i čipa eOI
d) Generirati parove ključeva i aktivacijske podatke, pribaviti certifikate od ovjerovitelja HRIDCA te ih unijeti u eOI
e) Generirati podatke za aktivaciju eOI i registraciju na Portal te izraditi sigurnosne omotnice
f) Distribuirati eOI i sigurnosne omotnice u PU/PP

Detaljnije informacije se mogu naći u poglavlju 9.6.5.

1.3.6. Povjerenstvo za upravljanje pravilima certificiranja

AKD je imenovao stručno Povjerenstvo za upravljanje pravilima certificiranja (eng. *Policy Management Authority* – PMA) kao formalno tijelo odgovorno za upravljanje pravilima certificiranja AKD PKI.

Povjerenstvo je ovlašteno za izradu, uvođenje i administriranje općih pravila davanja usluga certificiranja, pravilnika o postupcima certificiranja i pripadne dokumentacije kao i za utvrđivanje postupaka za kontrolu i nadzor nad radom ovjerovitelja.

Detaljnije informacije se mogu naći u poglavlju 9.6.6.

1.4. Upotreba certifikata

1.4.1. Primjerena upotreba certifikata

Osobe i pouzdajuće strane trebaju biti svjesne zakonskih implikacija koje proizlaze iz upotrebe identifikacijskog i potpisnog certifikata:

a) Certifikati se izdaju isključivo fizičkim osobama koje djeluju u svoje osobno ime.
b) Osobe mogu koristiti certifikate u privatne svrhe ali i za poslovnu uporabu kada nije nužno certifikatom dokazivati pripadnost poslovnom subjektu.
c) Certifikati na eOI su značajne razine sigurnosti što znači da pružaju značajan stupanj pouzdanja u odnosu na traženi ili utvrđeni identitet osobe i primijenjeni postupak certificiranja, a čija je svrha značajno smanjenje rizika zlouporabe ili promjene identiteta.
d) Certifikate izdaje davatelj usluga izdavanja kvalificiranih certifikata koji ispunjava uvjete iz čl. 17 Zakona o elektroničkom potpisu [5] i Aneksa II Direktive 1999/93/EC.
e) Oba certifikata se izdaju na sredstvu za izradu naprednog elektroničkog potpisa (SSCD) koji zadovoljava zahtjeve iz čl. 9 Zakona o elektroničkom potpisu [5] i Aneksa I Direktive 1999/93/EC.
f) Oba certifikata su kvalificirani certifikati i udovoljavaju zahtjevima iz čl. 11. Zakona o elektroničkom potpisu [5].
g) Certifikati se mogu koristiti u upravnim postupcima, iako time njihova uporaba nije ograničena. Dozvoljeno ih je koristiti i u građanskim postupcima.
h) Potpisni certifikat se koristi isključivo za podršku elektroničkom potpisu odnosno naprednom elektroničkom potpisu koji ima istu pravnu snagu i zamjenjuje vlastoručni potpis odnosno vlastoručni potpis i otisak pečata sukladno Zakonu o elektroničkom potpisu [5].
i) Identifikacijski certifikat se koristi za autentikaciju osoba na elektroničke usluge.
j) Maloljetne osobe smiju koristiti identifikacijski certifikat za podršku elektroničkom potpisu, no punoljetnim osobama preporučuje se korištenje potpisnog certifikata za takvu namjenu.
k) Preporučeni financijski limit za certifikate na eOI iznosi do 80.000 kn po transakciji.
l) Ako nije posebnim ugovorom ili na drugi način određeno, ukupna odgovornost AKD-a prema osobama i pouzdajućim stranama koje se razumno pouzdaju u certifikat ograničena je iznosom police osiguranja sukladno poglavlju 9.8.

1.4.2. Zabranjena upotreba certifikata

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

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

a) Certifikati se ne mogu i ne smiju koristi za šifriranje podataka i za potpisivanje e-mail poruka.
b) Ako se identifikacijski certifikat koristi za podršku elektroničkom potpisu takav se potpis neće se smatrati naprednim elektroničkim potpisom.
c) Potpisni certifikat se ne može koristiti za bilo koju drugu namjenu osim za podršku elektroničkom potpisu odnosno naprednom elektroničkom potpisu.

1.5. Upravljanje postupcima certificiranja

1.5.1. Administriranje dokumenata

Davatelj usluga certificiranja imenovao je stručno Povjerenstvo za upravljanje pravilima certificiranja (u daljnjem tekstu Povjerenstvo) koje se sastoji od više članova koji posjeduju specijalistička znanja vezana uz regulatorne, poslovne, pravne, formalne i tehničke aspekte davanja usluga certificiranja.

Povjerenstvo je odgovorno za:

a) definiranje Općih pravila certificiranja (u daljnjem tekstu Opća pravila) po kojima djeluje davatelj usluga certificiranja i
b) definiranje detaljnih pravila koja se primjenjuju kod izdavanja certifikata, a koja su sadržana u Pravilniku.

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

Povjerenstvo je dužno na godišnjoj osnovi provesti reviziju Pravilnika o postupcima certificiranja te ocijeniti prikladnost i usklađenost dokumenta sa Općim pravilima davanja usluga certificiranja.

1.5.4. Postupak odobravanja dokumenta

Član Povjerenstva za regulatorni dio odgovoran je za praćenje zakonske regulative i normi vezanih uz elektronički potpis te utvrđivanje potrebe za izmjenom i usklađivanjem dokumenta.

Prije izdavanja dokumenta i početka njegove primjene te nakon svake izmjene dokumenta svi članovi povjerenstva moraju dati suglasnost za prihvaćanje i objavljivanje dokumenta.

2. Objavljivanje informacija

2.1. Repozitorij

Sve informacije koje su potrebne osobama i pouzdajućim stranama za provjeru statusa certifikata sadržane su u certifikatu.

To uključuje:

a) Listu opozvanih certifikata putem HTTP protokola: http://crl2.eid.hr/hridca.crl i http://crl2.eid.hr/hridca.crl
b) Listu opozvanih certifikata putem LDAP protokola: ldap://ldap.eid.hr
c) OCSP uslugu: http://ocsp-hridca.eid.hr/hridca

Certifikati osoba su objavljeni u strukturi javnog imenika.

2.2. Portal za objavljivanje informacije

Sve informacije koje su potrebne osobama i pouzdajućim stranama za korištenje usluga certificiranja i kartice eOI objavljuje HRIDCA na Portalu.

Portal je dostupan na Internet stranici http://eid.hr.

Osnovne informacije na Portalu su:

a) Certifikat krovnog ovjerovitelja AKDCA Root: http://eid.hr/cert/akdcaroot.crt.
b) Certifikat podređenog ovjerovitelja HRIDCA: http://eid.hr/cert/hridca.crt.
c) Opća pravila certificiranja i Pravilnik o postupcima certificiranja: http://eid.hr/cps.
d) Informacije o vezanim zakonskim i pod-zakonskim propisima.
e) Obavijesti vezane uz davanje usluga certificiranja.
f) Informacije o postupcima registracije osoba.
g) Odgovori na često postavljana pitanja.

Dodatne informacije i usluge dostupne registriranim osobama su:

h) Aplikacija i upute za instalaciju i korištenje kartice.
i) Provjera statusa certifikata.
j) Zahtijevanje suspenzije ili povlačenja suspenzije certifikata.
k) Promjena registracijskih podataka.

Postupak registracije osoba na Portal opisan je u poglavlju 2.4.3.

2.3. Učestalost objave informacija

Valjani certifikati objavljuju se na internet stranicama davatelja usluga certificiranja i u javnom imeniku odmah nakon izdavanja certifikata.

Maksimalno vrijeme koje može proteći između objavljivanja liste opozvanih certifikata te obrade zahtjeva za suspenziju/povlačenje suspenzije certifikata su definirani u skladu s točkom 4.9.5 ovoga pravilnika.

Sve informacije koje su potrebne osobama i pouzdajućim stranama za korištenje usluga certificiranja i eOI objavljuju se putem Portala odmah nakon odobrenja dokumenata.

2.4. Kontrola pristupa

2.4.1. Dostupnost

Informacije za provjeru statusa certifikata i Portal su javno dostupni putem Interneta.

Dostupnost informacija je 24 sata na dan, 7 dana u tjednu.

Davatelj usluga povjerenja će osigurati stalnu raspoloživost repozitorija i Portala u skladu s najboljim poslovnim praksama.

Nakon kvara sustava ili drugih čimbenika koji nisu pod kontrolom davatelja usluga certificiranja, primijeniti će se sva raspoloživa sredstva kako bi se osiguralo oporavak sustava u najkraćem mogućem roku.

2.4.2. Ograničenja vezana uz pristup objavljenim informacijama

Nema ograničenja vezanih uz prava pristupa osnovnim informacijama na Portalu.

Dodatne informacije i usluge na Portalu dostupne su samo registriranim osobama.

Nema ograničenja vezanih uz prava pristupa uslugama za provjeru statusa certifikata.

Svim institucijama Republike Hrvatske ovjerovitelj HRIDCA omogućava neograničeno korištenje CRL i OCSP usluga i pretraživanje certifikata objavljenih u javnom imeniku.

AKD zadržava pravo poduzimanja odgovarajućih mjera zaštite od zlouporabe usluga.

2.4.3. Registracija osoba na Portalu

Podaci koji se zahtijevaju od osoba da unesu tijekom postupka registracije na Portal su:

- OIB (korisničko ime)
- Podatak za registraciju (inicijalna zaporka)

Inicijalna zaporka upisana je u sigurnosnu omotnicu koja je osobama uručena s elektroničkom osobnom iskaznicom.

Inicijalna zaporka je automatski generirana, jedinstvena i dovoljno kompleksna te udovoljava smjernicama za izdavanje visoko sigurne zaporke.

Tijekom inicijalne registracije osoba će promijeniti dobiveni podatak za registraciju te upisati zaporku koju će ubuduće koristiti za pristup Portalu.

Tijekom korištenja Portala osoba treba voditi računa o sljedećem:

a) Nakon 5 uzastopnih pokušaja unosa pogrešne zaporke korisnički račun će se privremeno zaključati.
b) Ako je osoba zaboravila zaporku moguće je otvoriti zahtjev za dobivanje nove zaporke putem elektroničke pošte.
c) Registrirane osobe u svakom trenutku mogu same promijeniti svoju e-mail adresu i broj telefona putem Portala.
d) Ako je osoba zaboravila zaporku i ne može koristi registriranu e-mail adresu može doći u registracijski ured gdje će zahtijevati promjenu e-mail adrese.

Registriranim osobama osiguran je za pristup Portalu kroz siguran komunikacijski kanal.

3. Identifikacija i autentikacija

3.1. Određivanje imena

3.1.1. Tipovi imena

U polju „Subject“ svakog certifikata koje izdaje davatelj usluga povjerenja upisani su jedinstveni podaci o potpisniku.

Za certifikate ovjerovitelja polje „Subject“ identificira ime ovjerovitelja koji izdaje certifikate.
Za certifikate osoba polje „Subject“ identificira fizičku osobu.

3.1.2. Smislenost imena

Za certifikate ovjerovitelja polje „Subject“ formira se od:

commonName:	Naziv potpisnika
organizationIdentifier:	Identifikator pravne osobe tj. VAT broj
organizationName:	Naziv prave osobe koja djeluje kao davatelj usluga certificiranja
countryName:	Kod države

Za certifikate osoba polje „Subject“ formira se od:

CommonName:	Naziv potpisnika tj. fizičke osobe
serialNumber:	Serijski broj
givenName:	Ime potpisnika tj. fizičke osobe
Surname:	Prezime potpisnika tj. fizičke osobe
organizationalUnitName:	Naziv tipa certifikata
organizationName:	Naziv ovjerovitelja koji izdaje certifikate
countryName:	Kod države

3.1.3. Anonimnost i pseudonimi

Nije podržano.

3.1.4. Pravila tumačenja imena

Polje „Subject“ svih certifikata koje izdaje davatelj usluga certificiranja certifikata formira se u skladu s RFC 3739 [20] te preporukom budućeg standarda Draft ETSI EN 319 412-1 [23].
Slijede pravila tumačenja imena za certifikate ovjerovitelja:

Korijenski AKDCA Root certifikat		
Polje	Vrijednost	Pojašnjenje
CommonName (cn)	AKDCA Root	AKDCA Root predstavlja naziv krovnog ovjerovitelja
organizationIdentifier	VATHR-58843087891	VAT označava da se radi o pravnoj osobi HR je kod države Znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) 58843087891 je porezni identifikacijski broj AKD-a (pravne osobe)
organizationName (O)	AKD d.o.o	AKD d.o.o je naziv pravne osobe
countryName (C)	HR	HR je kod države

Podređeni HRIDCA certifikat		
Polje	Vrijednost	Pojašnjenje
CommonName (cn)	HRIDCA	HRIDCA predstavlja naziv podređenog ovjerovitelja
organizationIdentifier	VATHR-58843087891	VAT označava da se radi o pravnoj osobi HR je kod države Znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) 58843087891 je porezni identifikacijski broj AKD-a (pravne osobe)
organizationName (O)	AKD d.o.o	AKD d.o.o je naziv pravne osobe
countryName (C)	HR	HR je kod države

Slijede pravila tumačenja imena za certifikate osoba:

Identifikacijski certifikat		
Polje	Vrijednost	Pojašnjenje
CommonName (cn)	Ime Prezime	Ime Prezime predstavlja ime i prezime osobe
serialNumber	PNOHR-OIB	PNO je oznaka da se radi o fizičkoj osobi HR je kod države Znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) OIB je osobni identifikacijski broj
givenName (g)	Ime	Ime predstavlja ime osobe
Surname (sn)	Prezime	Prezime predstavlja prezime osobe
organizationalUnitName (OU)	Identification	Identification predstavlja identifikacijski certifikat
organizationName (O)	HRIDCA	Naziv ovjerovitelja koji izdaje certifikat
countryName (C)	HR	HR je kod države

Potpisni certifikat		
Polje	Vrijednost	Pojašnjenje
CommonName (cn)	Ime Prezime	Ime Prezime predstavlja ime i prezime osobe
serialNumber	PNOHR-OIB	PNO je oznaka da se radi o fizičkoj osobi HR je kod države Znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) OIB je osobni identifikacijski broj

givenName (g)	Ime	Ime predstavlja ime osobe
Surname (sn)	Prezime	Prezime predstavlja prezime osobe
organizationalUnitName (OU)	Signature	Signature predstavlja potpisni certifikat
organizationName (O)	HRIDCA	Naziv ovjerovitelja koji izdaje certifikat
countryName (C)	HR	HR je kod države

3.1.5. Jedinstvenost imena

Polje „Subject“ jedinstveno je za svakog ovjerovitelja certifikata i za svaku osobu.

Za certifikat ovjerovitelja koristi se osobni identifikacijski broj pravne osobe (VAT) koji je jedinstven za svaku pravnu osobu, a koji je sadržan u vrijednosti atributa „organizationIdentifier“.

Za certifikate osoba koristi se osobni identifikacijski broj fizičke osobe (OIB) koji je jedinstven za svaku fizičku osobu, a koji je sadržan u vrijednosti atributa „serialNumber“.

3.2. Inicijalno utvrđivanje identiteta

3.2.1. Metoda dokazivanja posjeda privatnog ključa

Visoki stupanj pouzdanja u identitet osobe koja posjeduje privatni ključ postiže se primjenom sljedećih pravila utvrđivanja identiteta:

a) Zahtjev za izdavanje osobne iskaznice podnosi se osobno.
b) Utvrđivanje identiteta osoba vrši se neposrednom identifikacijom u fizičkoj prisutnosti fizičke osobe odnosno temeljem predočenih ili dostupnih identifikacijskih podataka ili važeće isprave.
c) Maloljetna osoba starija od 12 godina mora biti osobno nazočna prilikom podnošenja zahtjeva za izdavanje osobne iskaznice.
d) Ako maloljetna osoba koja podnosi zahtjev za izdavanje nove osobne iskaznice ne posjeduje javnu ispravu kojom se može provjeriti njezin identitet, prilikom podnošenja zahtjeva mora biti prisutan roditelj ili skrbnik koji će potvrditi identitet maloljetne osobe.

3.2.2. Dokazi identiteta poslovnih subjekata

Nije primjenjivo.

3.2.3. Dokazi identiteta osoba

Prilikom inicijalnog utvrđivanja identiteta prikupljaju se sljedeći dokazi identiteta osoba:

a) Dokazi o identitetu osobe i specifična fizička obilježja koja dokazuju identitet osobe prikupljaju se izravno uz fizičku prisutnost osobe tijekom zaprimanja zahtjeva za izdavanje osobne iskaznice.

b) Podaci o identitetu osoba koji se inicijalno prikupljaju tijekom registracije osoba sadrže: prezime, ime, podatak o spolu, državljanstvu, datum rođenja, osobni identifikacijski broj (OIB) i prebivalište.
c) Ako se zahtjev za izdavanje osobne iskaznice podnosi prvi put, potrebno je priložiti domovnicu, izvadak iz matice rođenih ili rodni list i fotografiju u boji.
d) Ako je osobi već izdana putovnica, ne treba priložiti domovnicu niti izvadak iz matice rođenih ili rodni list.
e) Tijekom postupka registracije podnositelja zahtjeva za osobnu iskaznicu uzima se otisak papilarnih linija lijevog i desnog kažiprsta kao specifično fizičko obilježje osobe.
f) Otisci prstiju ne uzimaju se djeci mlađoj od 12 godina, kao ni osobama kojima to nije moguće uzeti iz medicinskih razloga.
g) Otisci prstiju se ne uzimaju ako su već izuzeti i pohranjeni u elektroničkom obliku u nekom postupku izdavanja javne isprave koji provodi Ministarstvo.
h) Osobi čije se ime i prezime sastoji od više riječi, koje se zbog broja slova koja sadrže ne mogu upisati u prostor za upis imena i prezimena, u obrazac osobne iskaznice upisat će se one riječi osobnog imena koje je osoba izjavom pred matičarom odredila za uporabu u pravnom prometu te prilaže izvadak iz matice rođenih ili rodni list iz kojeg je vidljivo kojim će se imenom služiti u pravnom prometu.
i) Prikupljani dokazi o identitetu osobe se u postupku registracije osoba upisuju u informacijski sustav putem kojeg se vodi evidencija osobnih iskaznica.

3.2.4. Informacije o osobama koje se ne provjeravaju

Informacije o osobama koje se ne provjeravaju su:

a) telefonski broj
b) e-mail adresa

Osobe su odgovorne za točnost i cjelovitost navedenih podataka.

3.2.5. Provjera i odobravanje

Službena osoba koja zaprima zahtjev za izdavanje osobne iskaznice dužna je provjeriti prikupljene podatke i nedvojbeno utvrditi identitet osobe koja podnosi zahtjev.

Provjera se vrši fizičkim uvidom u predočene identifikacijske podatke ili važeću ispravu odnosno uvidom u postojeće podatke u elektroničkom obliku koji su ranije prikupljeni u nekom postupku izdavanja javne isprave koji provodi Ministarstvo.

Bez obzira jesu li podaci u tiskanoj ili elektroničkoj formi, tijekom postupka registracije osoba provjerava se vjerodostojnost prikupljenih podataka.

3.2.6. Kriteriji za interoperabilnost

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

Pitanja vezana uz izdavanje i korištenje osobnih iskaznica uređuju nacionalna zakonodavstva svake zemlje članice Europske unije.

Pravila utvrđivanja identiteta koja se primjenjuje prilikom izdavanja hrvatske osobne iskaznice usklađena su s praksom koja se primjenjuje u drugim europskim državama te pružaju značajan

stupanj pouzdanja u utvrđeni identitet fizičke osobe čime su rizici zlouporabe ili promjene identiteta značajno smanjeni.

3.3. Utvrđivanje identiteta kod obnove certifikata

3.3.1. Identifikacija i potvrđivanje identiteta kod obnove certifikata

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

3.3.2. Identifikacije i potvrđivanje identiteta kod izdavanja novog para ključeva

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

a) Pravila utvrđivanja identiteta kod izdavanja nove osobne iskaznice ista su kao i pravila kod inicijalnog utvrđivanja identiteta (točka 3.2.1)
b) Osobe koje podnose zahtjev jer im je prethodno izdana osobna iskaznica prestala važiti ili iz drugog razloga više ne služi svojoj svrsi, trebaju priložiti staru osobnu iskaznicu koja se poništava i vraća osobi te fotografiju u boji.
c) 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. Utvrđivanje identiteta kod opoziva i suspenzije certifikata

Kod opoziva ili suspenzije certifikata primjenjuju se sljedeće sigurnosne mjere i postupci:

a) Kod osobnog podnošenja zahtjeva za opozivom i suspenzijom certifikata pravila su ista kao kod inicijalnog utvrđivanja identiteta (točka 3.2.1)
b) Kod podnošenja zahtjeva za suspenziju certifikata korištenjem elektroničke usluge identitet osobe utvrđuje se provjerom pristupnih podataka.

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

Elektronička osobna iskaznica je obavezna isprava za hrvatske državljane starije od 18 godina s prijavljenim prebivalištem u Republici Hrvatskoj.

Pravo na hrvatsku osobnu iskaznicu ima svaki državljanin Republike Hrvatske.

Osobe podnose zahtjev za izdavanje osobne iskaznice, a certifikati na osobnoj iskaznici će im biti izdani u skladu s pravilima za izdavanje certifikata koja su definirana Zakonom o osobnoj iskaznici [1]:

a) Pravo na hrvatsku osobnu iskaznicu ima svaki državljanin Republike Hrvatske bez obzira na godine života i bez obzira imaju li ili nemaju prebivalište u Republici Hrvatskoj.

b) eOI je obvezan dokument za državljane RH starije od 18 godina s prebivalištem u RH.
c) Djeci mlađoj od 5 godina se ne izdaju certifikati, a djeci starijoj od 5 godina izdaje se samo identifikacijski certifikat.
d) Za punoljetne osobe od 18 do 65 godina izdaje se identifikacijski i potpisni certifikat.
e) Za osobe starije od 65 godina izdaje se identifikacijski i potpisni certifikat ili se ne izdaju certifikati.

4.1.2. Postupak podnošenja zahtjeva za izdavanje certifikata

Prilikom podnošenja zahtjeva osigurana je provedba sljedećih sigurnosnih mjera:

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.
c) Izgled i sadržaj obrasca zahtjeva za izdavanje osobne iskaznice propisan je provedbenim aktima donesenim temeljem Zakona o osobnoj iskaznici [1].
d) Zahtjev za izdavanje osobne iskaznice podnosi se osobno, a za dijete odnosno osobu lišenu poslovne sposobnosti zahtjev podnosi zakonski zastupnik.
e) Ministarstvo na svojim službenim stranicama objavljuje upute o proceduri izdavanja osobne iskaznice.
f) Zahtjev za izdavanje certifikata će se prihvatiti samo ako je utvrđen identitet podnositelja zahtjeva sukladno proceduri koja je navedena u poglavlju 3.2.
g) Osobe su dužne dostaviti cjelovite i točne osobne identifikacijske podatke u trenutku podnošenja zahtjeva.
h) Prilikom podnošenja zahtjeva osoba sklapa Ugovor o davanju usluga certificiranja s AKD-om kojim prihvaća uvjete koji su navedeni u Općim pravilima.

4.2. Obrada zahtjeva za izdavanje certifikata

4.2.1. Provedba identifikacije i autentikacije

Zahtjev za izdavanje osobne iskaznice će se prihvatiti samo ako je identitet podnositelja zahtjeva utvrđen sukladno proceduri koja je navedena u poglavlju 3.2.

Identitet službenika PU/PP koji prihvaća zahtjev za izdavanje certifikata i unosi ga u evidenciju osobnih iskaznica potvrđen je u postupku autentikacije službenika na informacijskom sustavu davatelja usluge registracije.

4.2.2. Odobravanje ili odbijanje zahtjeva za izdavanje certifikata

Službenici PU/PP utvrđuju identitet podnositelja zahtjeva, provjeravaju sadržaj obrazaca zahtjeva za izdavanje osobne iskaznice i odlučuju o prihvaćanju ili odbijanju zahtjev za izdavanje osobne iskaznice odnosno certifikata na osobnoj iskaznici.

Ako zahtjev nije točno i u cijelosti popunjen te pravilno potpisan, službenik PU/PP mora odbiti zahtjev.

Ako je zahtjev prihvaćen, upisuje se u evidenciju osobnih iskaznica, a podaci potrebni za realizaciju zahtjeva prosljeđuju se proizvođaču eOI kroz siguran komunikacijski kanal.

4.2.3. Vrijeme obrade zahtjeva za izdavanje certifikata

Davatelj usluga certificiranja i proizvođač su poduzeli odgovarajuće mjere kako bi se obrada zahtjeva za izdavanje osobne iskaznice odnosno certifikata na osobnoj iskaznici provela u skladu s rokom koji je propisan Zakonom o osobnoj iskaznici [1]:

a) u roku od 30 dana od dana podnošenja zahtjeva, ako je zahtjev za izdavanje podnesen u redovnom postupku,
b) u roku od 10 dana od dana podnošenja zahtjeva, ako je zahtjev za izdavanje podnesen u ubrzanom postupku,
c) u roku od 3 radna dana od dana podnošenja zahtjeva, ako je zahtjev za izdavanje podnesen u žurnom postupku.

4.3. Postupak izdavanja certifikata

4.3.1. Postupci tijekom izdavanja certifikata

Davatelj usluga certificiranja i proizvođač provode sljedeće sigurnosne mjere i postupke prilikom izdavanja certifikata:

a) Proizvođač eOI ne provjerava cjelovitost, točnost i jedinstvenost podataka zaprimljenih od davatelja usluga registracije već se oslanja na provjeru izvršenu u PU/PP Ministarstva.
b) Postupak izrade kartice i izdavanja certifikata vrši se u sigurnom okružju proizvođača odnosno davatelja usluga certificiranja.
c) Proizvođač izrađuje karticu sa otisnutim dizajnom i ugrađenim zaštitnim elementima koji omogućavaju fizičku zaštitu od krivotvorenja ili promjene u skladu sa zahtjevima Ministarstva kao izdavatelja osobne iskaznice.
d) Nakon učitavanja aplikacije i inicijalizacije eO, proizvođač individualizira tijelo i čip eOI.
e) Tijekom postupka individualizacije eOI, generiraju se privatni i javni ključ te aktivacijski i registracijski podaci, a temeljem zahtjeva zaprimljenih od RA proizvođač kroz siguran komunikacijski kanal pribavlja certifikat od ovjerovitelja HRIDCA.
f) Ovjerovitelj HRIDCA certificira javni ključ, generira certifikat odgovarajućeg profila i objavljuje certifikat u javnom imeniku.
g) Proizvođač u sigurnom okružju unosi privatni i javni ključ osobe i podatke za aktivaciju u čip eOI.
h) Ključevi ovjerovitelja koji se koriste za potpisivanje certifikata kao i privatni ključevi osoba štite se mjerama koje su propisane u točki 6.2
i) Nakon proizvodnje eOI, proizvođač dostavlja eOI u PU/PP.
j) Na paketima koji se transportiraju nisu vidljive oznake koje upućuju na sadržaj paketa.

4.3.2. Obavješćivanje o izdavanju certifikata

Davatelj usluga registracije definira način obavješćivanja osoba te obavješćuje osobu da je njegova osobna iskaznica gotova te da ju može preuzeti.

4.4. Preuzimanje eOI i certifikata

4.4.1. Provedba postupka prihvaćanja certifikata

Kada od davatelja usluga registracije dobije obavijest da je njegova osobna iskaznica gotova, osoba može preuzeti osobnu iskaznicu u PU/PP u kojoj je podnijela zahtjev za njezino izdavanje.

Za redovne i ubrzane osobne iskaznice proizvođač je odgovoran za pravovremenu dostavu osobnih iskaznica i sigurnosnih omotnica na skladište Ministarstva u Zagrebu, a Ministarstvo je odgovorno za dostavu osobnih iskaznica u PU/PP u kojoj je osoba podnijela zahtjev za njezino izdavanje.

Žurne osobne iskaznice i sigurnosne omotnice proizvođač će dostavljati na adrese PU u čijem je sastavu PP u kojoj je osoba podnijela zahtjev za izdavanje osobne iskaznice.

Osobna iskaznica se osobno uručuje fizičkoj osobi nakon provjere identiteta prema točki 3.2.5.

Smatra se da je potpisnik prihvatio privatni ključ i certifikat u trenutku uručenja osobne iskaznice.

4.4.2. Objava certifikata od strane ovjerovitelja

Davatelj usluga certificiranja osigurao je sve potrebne preduvjete da ovjerovitelj HRIDCA objavljuje certifikate u javnom imeniku odmah nakon izdavanja certifikata.

4.4.3. Obavješćivanje drugih strana o izdavanju certifikata

Informaciju da je osobna iskaznica izrađena i da je certifikat izdan, proizvođač prosljeđuje davatelju usluga registracije kroz siguran komunikacijski kanal odmah nakon izrade osobne iskaznice.

4.5. Korištenje ključeva i certifikata

4.5.1. Osobe

Osobe su dužne osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka:

a) Prilikom preuzimanja osobne iskaznice osobi se uručuje sigurnosna omotnica s podacima za registraciju na Portal i aktivaciju eOI. Prilikom preuzimanja sigurnosne omotnice osoba je dužna utvrditi da ista nije oštećena.

b) Prije korištenja eOI osoba je dužna registrirati se na Portal korištenjem registracijskog podatka dobivenog u sigurnosnoj omotnici.

c) Temeljem informacija koje su dostupne registriranim osobama na Portalu, osoba treba instalirati čitač kartice i aplikaciju koja omogućava korištenje kartice na računalu.

d) eOI je moguće koristiti tek nakon što se provede postupak aktivacije prema uputama koje su dostupne na Portalu, a korištenjem aktivacijskog podatka dobivenog u sigurnosnoj omotnici.

e) Tijekom aktivacije eOI postavit će se PIN za zaštitu identifikacijskog privatnog ključa te poseban PIN za zaštitu potpisnog privatnog ključa kao i PUK podatak koji će se koristiti u slučaju da je bilo koji PIN zaključan.

f) PIN i PUK vrijednosti osoba može zapisati, ali ih je potrebno pohraniti na sigurno mjesto i čuvati uvijek odvojeno od eOI.
g) Osoba je dužna zaštititi karticu s privatnim ključem, aktivacijski podatak, PIN-ove i PUK od krađe, gubitka, izmjena, kompromitiranja i neovlaštene uporabe.

Tijekom korištenja eOI osoba treba voditi računa o sljedećem:

h) Nakon 6 uzastopnih pokušaja unosa pogrešnog PIN-a kartica će se zaključati.
i) Zaključana kartica se može otključati korištenjem PUK vrijednosti.
j) Nakon 6 uzastopnih pokušaja unosa pogrešnog PUK-a kartica će se blokirati i osoba mora doći u PU/PP gdje će autorizirana osoba izvršiti deblokadu kartice.

4.5.2. Pouzdajuće strane

Pouzdajuće strane koje namjeravaju ostvariti pouzdanje u certifikat dužne su osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka:

a) Informirati se o sadržaju ovoga dokumenta a posebno o svojim odgovornostima iz točke 9.6.4 i prihvatljivom načinu korištenja usluga certificiranja iz točke 1.4.
b) Koristiti certifikat isključivo u svrhe propisane u točki 1.4.
c) Provjeriti rok važenja certifikata i status certifikata prije ostvarivanja povjerenja u certifikat prema podacima koji su navedeni u certifikatu.
d) Provjeriti certifikat prema postupcima za validaciju certifikacijske staze, sukladno dokumentu RFC 5280 [21].
e) Provjeriti da su svi podaci o identitetu subjekta u certifikatu ispravno prikazani.
f) Pri verificiranju elektroničkog potpisa, provjeriti da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu i da je u vrijeme izrade elektroničkog potpisa certifikat bio valjan.

4.6. Obnova certifikata

Svaka obnova certifikata podrazumijeva izdavanje novog para ključeva i novog certifikata.

Nije moguće obnoviti certifikat zadržavajući pri tome stare ključeve.

Postupak obnove certifikata podrazumijeva postupke navedene u točki 4.7.

4.7. Izdavanje novog para ključeva

Nakon isteka roka važenja certifikata ili nakon opoziva certifikata izdaje se novi certifikat.

Davatelj usluga certificiranja ne čuva privatne ključeve osoba niti može reaktivirati opozvani certifikat već će se osobi izdati nova osobna iskaznica s novim parom ključa i certifikatom.

Postupci podnošenja i obrade zahtjeva u slučaju izdavanja novog para ključeva provode se kako je opisano u točkama 4.1 i 4.2.

Postupci izdavanja odnosno preuzimanja certifikata u slučaju izdavanja novog para ključeva provode se kako je opisano u točkama 4.3 i 4.4.

4.8. Promjena certifikata

Nije primjenjivo.

4.9. Opoziv i suspenzija certifikata

4.9.1. Koji su razlozi za opoziv certifikata

Razlozi za opoziv certifikata su:

a) Promjena podataka u certifikatu odnosno promjena u osobnom imenu ili osobnom identifikacijskom broju.
b) Kvar, gubitak ili krađa osobne iskaznice odnosno zlouporaba ili neautorizirano korištenje privatnog ključa.
c) Prestanak važenja certifikata prije isteka roka na koji je certifikat izdan zbog razloga koji su propisani u čl. 15 Zakona o osobnoj iskaznici [1].
d) 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.

4.9.2. Tko može tražiti opoziv certifikata

Zahtjev za opoziv certifikata podnosi osoba ili njen zakonski zastupnik.

Zahtjev za opoziv može podnijeti i davatelj usluga registracije nakon što se evidentira status nevažeće osobne iskaznice u evidenciji osobnih iskaznica zbog razloga koji su navedeni u točki 4.9.1.

Zahtjev za opoziv će podnijeti davatelj usluga registracije ako nastupe izvanredne okolnosti i u slučaju 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.

4.9.3. Procedura opoziva certifikata

Zahtjev za opoziv certifikata se podnosi se u policijskoj upravi odnosno policijskim postajama Ministarstva.

Zahtjev za opoziv certifikata će se prihvatiti samo ako je identitet podnositelja zahtjeva utvrđen sukladno pravilima za utvrđivanje identiteta kod opoziva i suspenzije certifikata, prema poglavlju 3.4.

Ako je zahtjev prihvaćen, prosljeđuje se na daljnju obradu kroz siguran komunikacijski kanal.

Davatelj usluga certificiranja osigurava sigurno okružje u kojem ovjerovitelj HRIDCA provodi postupak opoziva certifikata.

4.9.4. Rok za podnošenje zahtjeva za opoziv

Podnositelji zahtjeva za opozivom certifikata iz točke 4.9.2. ovog Pravilnika trebaju u najkraćem razumnom roku od nastanka razloga za opoziv navedenih u točki 4.9.1. ovog Pravilnika podnijeti zahtjev za opoziv certifikata.

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. Rok obrade zahtjeva za opoziv

Zahtjev za opoziv biti će provjeren i putem informacijskog sustava te poslan ovjerovitelju HRIDCA na provedbu u roku od 60 minuta.

Ovjerovitelj HRIDCA osvježava OCSP odmah po dobivanju zahtjeva za opoziv certifikata.

Maksimalno vrijeme koje može proteći između zaprimanja zahtjeva za opoziv, suspenziju ili povlačenje suspenzije certifikata i objave statusa certifikata je 24 sata.

Sustav za opoziv i suspenziju certifikata raspolaže s pouzdanim izvorom vremena i osigurava važeću zabilješku datuma i vremena. Maksimalno dozvoljeno odstupanje u vremenu je 1 sekunda.

4.9.6. Provjera statusa certifikata

Informacija o statusu certifikata sadrži informaciju o opozvanim certifikatima kojima nije istekao rok važenja.

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 odbiti uporabu certifikata.

4.9.7. Učestalost izdavanja CRL

HRIDCA se obvezuje da će CRL izdati barem 1 put u roku od 24 sata i da će novu CRL izdati barem 10 minuta prije isteka važenja CRL.

U redovnim uvjetima rada CRL se izdaje svakih 12 sati.

Period važenja CRL ovjerovitelja HRIDCA je 24 sata od trenutka izdavanja CRL.

CRL ovjerovitelja AKDCA je važeća 90 dana od trenutka izdavanja CRL.

4.9.8. Maksimalno kašnjenje CRL

S obzirom na to da se nova CRL izdaje barem 10 minuta prije isteka važenja CRL, maksimalno dozvoljeno kašnjenje od trenutka izdavanja CRL do trenutka objave CRL u javnom imeniku ili putem interneta je 10 minuta.

4.9.9. On line provjera

Ovjerovitelj HRIDCA omogućava on-line provjeru statusa certifikata putem OCSP usluge.

OCSP usluga dostupna je preko protokola HTTP na adresi objavljenoj u polju authorityInformationAccess svakog certifikata.

Valjanost odgovora usluge OCSP će biti maksimalno 24 sata.

Status OCSP usluge za provjeru statusa certifikata podređenih ovjerovitelja će se osvježiti svakih 90 dana.

Odgovor OCSP usluge će biti potpisan certifikatom izdanog od istog ovjerovitelja koji je izdao certifikat za kojeg se traži provjera statusa.

4.9.10. Zahtjevi za on-line provjeru

U redovnim uvjetima rada ovjerovitelj HRIDCA osvježava OCSP odmah po dobivanju zahtjeva za opoziv certifikata.

4.9.11. Ostali načini provjere

Nisu podržani.

4.9.12. Specifični zahtjevi za ponovno izdane ključeve

Nije primjenjivo.

4.9.13. Razlozi za suspenziju certifikata

Razlozi za suspenziju certifikata je:

a) Sumnja u kvar, gubitak ili krađu osobne iskaznice odnosno zlouporabu ili neautorizirano korištenje privatnog ključa.
b) Nemogućnost pravovremenog dolaska u PU/PP radi podnošenja zahtjeva za opoziv certifikata.

Razlog za povlačenje suspenzije certifikata je:

c) Pronalazak eOI odnosno prestanak razloga zbog kojeg je tražena suspenzija certifikata.

4.9.14. Tko može tražiti suspenziju certifikata

Zahtjev za suspenziju certifikata podnosi osoba ili njen zakonski zastupnik.

4.9.15. Procedura suspenzije certifikata

U slučaju nastanka razloga za suspenziju certifikata navedenih u točki 4.9.1. ovog Pravilnika, osoba je dužna trenutno zahtijevati suspenziju certifikata.

Davatelj usluga registracije dužan je osigurati zaprimanje zahtjeva za suspenziju certifikata u svojim PU/PP tijekom uredovnog radno vremena.

Davatelj usluga certificiranja osigurava potrebne preduvjete kako bi osobe mogle zahtijevati suspenziju ili povlačenje suspenzije certifikata korištenjem elektroničke usluge na Portalu.

Zahtjev za suspenziju certifikata će se prihvatiti samo ako je identitet utvrđen sukladno pravilima za utvrđivanje identiteta kod opoziva i suspenzije certifikata, prema poglavlju 3.4.

Ako je zahtjev prihvaćen, prosljeđuje se na daljnju obradu kroz siguran komunikacijski kanal.

Postupak suspenzije certifikata provodi ovjerovitelj HRIDCA u sigurnom okružju.

4.9.16. Ograničenje na trajanje suspenzije

U slučaju prestanka razloga za suspenziju certifikata navedenih u točki 4.9.13., osoba može u roku od 8 dana od podnošenja zahtjeva za suspenziju zahtijevati povlačenje suspenzije certifikata na način koji je opisan u točki 4.9.15.

Ako nije zahtijevano povlačenje suspenzije certifikata, a istekao je rok za povlačenje suspenzije certifikata, suspendirani certifikat će biti opozvan nakon 8 dana.

4.10. Servisi za provjeru statusa certifikata

4.10.1. Operativna svojstva

Obveza davatelja usluge certificiranja je osigurati informacije temeljem kojih će pouzdajuće strane moći obaviti provjeru valjanosti certifikata.

Osigurano je:

a) Dostupnost usluga provjere CRL putem HTTP i LDAP protokola te OCSP provjera statusa certifikata.
b) Dostupnost usluga za provjeru statusa certifikata putem Interneta.
c) Adresa za provjeru statusa korištenjem OCSP usluge je: http://ocsp-hridca.eid.hr/hridca.
d) Adrese za dohvat CRL na web poslužitelju su: http://crl2.eid.hr/hridca.crl i http://crl2.eid.hr/hridca.crl.
e) Adresa za dohvat CRL putem javnog imenika dostupna treba biti: ldap://ldap.eid.hr/cn=HRIDCA,o=AKD d.o.o.,c=HR?certificateRevocationList;binary.

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

4.10.2. Dostupnost usluga

Davatelj usluga certificiranja osigurava redundantnu informacijsku infrastrukturu koja će osigurati dostupnost usluga za CRL i OCSP provjeru opozvanih certifikata 24 sata na dan, 7 dana u tjednu.

U slučaju ispada sustava usluga će biti dostupna u najkraćem mogućem roku i u skladu s pozitivnim poslovnim praksama.

Kako bi se skratilo vrijeme obrade i provjere statusa certifikata preporuka je koristiti OCSP protokol.

4.10.3. Opcionalna svojstva

Nije predviđeno.

4.11. Kraj životnog ciklusa certifikata

Rok važenja certifikata na osobnoj iskaznici je 5 godina koliko vrijedi i osobna iskaznica.

Certifikat će prestati biti valjan i prije isteka roka važenja od 5 godina ako se ranije opozove.

Ugovor o davanju usluga certificiranja sa osobom se sklapa na rok od 5 godina od dana izdavanja certifikata, a otkazuje se opozivom certifikata.

4.12. Pohrana i oporavak privatnog ključa

Informacijska infrastruktura je konfigurirana tako da je onemogućena pohrana i oporavak privatnih ključeva osoba.

5. Organizacijske, provedbene i fizičke mjere zaštite

U ovom poglavlju definirane organizacijske, provedbene i fizičke mjere koje se primjenjuju u svrhu zaštite sustava izdavanja eOI i certifikata na eOI.

5.1. Mjere fizičke zaštite

5.1.1. Lokacija objekta i konstrukcija

PKI infrastruktura i proizvodni pogoni smješteni su u poslovnom kompleksu AKD-a koji je zbog svoje namjene i značaja posebno važan za nacionalnu sigurnost. Objekti i prostori AKD-a ustrojeni su u 4 sigurnosne zone prema vrsti, namjeni i značaju aktivnosti koja se u pojedinoj zoni provodi: Pristupna, Administrativna, Djelatna i Sigurna zona. PKI infrastruktura je smještena u Sigurnoj zoni gdje se primjenjuju najstrože fizičke, tehničke i proceduralne mjere zaštite.

5.1.2. Fizički pristup

Prostor sigurne zone opremljen je sljedećim sustavima tehničke zaštite: video nadzor, kontrola pristupa, sustav protupožarne zaštite i protuprepadna zaštita.

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

Pristup sigurnoj zoni ograničen je na ovlašteno osoblje koje obavlja administratorske aktivnosti i nadzor. Prisutnost vanjskog osoblja kao i ostalih radnika AKD-a moguća je isključivo uz pratnju ovlaštenog osoblja.

Kontrola pristupa sigurnoj zoni ostvaruje se korištenjem ID kartice uz primjenu biometrijskih metoda za identifikaciju osoba tj. prepoznavanje zjenice oka.

Fizički pristup svoj računalnoj opremi sigurne zone (hardveru) ostvaruje se isključivo uz dvojnu kontrolu.

5.1.3. Sustavi za klimatizaciju i napajanje

Prostor sigurne zone propisno je klimatiziran. Sva oprema spojena je na izvor neprekinutog napajanja, a za slučaj prestanka napajanja gradske energetske mreže na duži period osiguran je i agregat rezervnog napajanja.

5.1.4. Opasnost od poplave

Prostor sigurne zone smješten je mjestu koje je osigurano od poplave.

5.1.5. Protupožarna zaštita

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

5.1.6. Pohrana medija

Mediji se čuvaju u sigurnosnim spremnicima.

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.

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 materijala vrši se komisijski uz prisutnost najmanje 2 osobe.

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

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

5.1.8. Sigurnosne kopije na drugoj lokaciji

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

5.2. Organizacijske mjere zaštite

5.2.1. Povjerljive uloge

Poslovi upravljanja informacijskim sustavom i operativni poslovi vezani uz rad sustava certificiranja obavljaju se unutar odvojenih organizacijskih jedinica u sklopu AKD-a prema detaljno utvrđenim pravilima koji su opisani u internim procedurama i uputama.

Radom ovjerovitelja AKDCA Root i HRIDCA upravlja Povjerenstvo za upravljanje pravilima certificiranja.

Ovlaštenim radnicima koji sudjeluju u provedbi aktivnosti ovjerovitelja dodijeljene su odgovarajuće korisničke uloge s jasno definiranim i dokumentiranim odgovornostima i ovlaštenjima.

Uloge vezane uz administriranje informacijskog sustava su:

a) administrator sigurnosti
b) administrator informacijskog sustava
c) operater
d) kontrolor

Uloge vezane uz upravljanje kriptografskim ključevima su:

e) koordinatori upravljanja kriptografskim ključevima
f) skrbnici kriptografskih ključeva

Nositelj uloge koordinator upravljanja kriptografskim ključevima je ujedno i administrator sigurnosti.

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

Princip dijeljenog znanja uključen je u sve aktivnosti upravljanja kriptografskim ključevima i administriranja kritičnih informacijskih sustava ovjerovitelja.

Pri dodjeli uloga strogo se poštuju principi segregacije zaduženja.

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

Princip dvojne kontrole uključen je u sve aktivnosti upravljanja kriptografskim ključevima i administriranja kritičnih informacijskih sustava ovjerovitelja.

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

5.2.4. Uloge koje zahtijevaju odvajanje dužnosti

Pri dodjeli korisničkih uloga i fizičkoj kontroli pristupa sigurnosnim spremnicima i opremi, strogo se poštuju principi segregacije zaduženja tako da jedna osoba ne može raspolagati kriptografskim materijalima i zaporkama za samostalno obavljanje sigurnosno osjetljive aktivnosti, već je uvijek nužno osigurati prisutnost barem dvije osobe.

5.3. Osoblje

5.3.1. Kvalifikacije, iskustvo i sigurnosne provjere

Članovi Povjerenstva su specijalisti za područje kriptografije i informacijske sigurnosti te regulatorna i pravna pitanja vezana uz područje elektroničkog potpisa i sigurnosti.

Članovi Povjerenstva i svi radnici koje sudjeluju u provedbi aktivnosti ovjerovitelja imaju odgovarajuću stručnu spremu, znanja i iskustvo potrebno za izvršavanje povjerene uloge. Također su potpisali ugovor o radu, u stalnom su radnom odnosu s AKD-om i nisu u poslovnom odnosu s drugim davateljima usluga certificiranja.

Za svakog radnika kojem je povjerena neka od navedenih uloga definiran je adekvatna zamjena.

Uloge se dodjeljuju u skladu s opisom radnog mjesta, kvalifikacijama i znanjima radnika.

Pri zapošljavanju radnika koji sudjeluju u provedbi aktivnosti ovjerovitelja provodi se strogi selekcijski postupak.

Standardna procedura pri zapošljavanju uključuje provjere stručne spreme, prethodnih zaposlenja, zdravstvene sposobnosti, prilaganje potvrde o nekažnjavanju i sl.

Pri zapošljavanju radnici se upoznaju sa sigurnosnim procedurama i pravilima i obvezuju se da će poštivati utvrđena pravila.

5.3.2. Provjera prikladnosti radnika za korisničku ulogu

Pri dodjeljivanju uloga i odabiru radnika koje će sudjelovati provedbi aktivnosti ovjerovitelja provodi se formalna procedura procjene prikladnosti radnika za određenu ulogu prema unaprijed definiranim kriterijima:

a) da su dobro upoznati internim propisima i postupaju u skladu s njima,
b) da imaju uredan osobni dosje,
c) da su pouzdani i savjesni radnici i
d) da nisu kažnjavani.

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

5.3.3. Informiranje o pravilima rada

Radnici koji sudjeluju u provedbi aktivnosti ovjerovitelja su informirani o pravilima rada prije nego preuzmu svoje obveze. Cilj informiranja je:

a) osigurati da su radnici svjesni vlastite uloge i odgovornosti u poslovnom procesu,
b) omogućiti da radnici prepoznaju sigurnosne probleme i incidente te da reagiraju u skladu s potrebama njihove poslovne funkcije i
c) pružiti podršku i pomoć u razumijevanju internih procedura i sigurnosnih zahtjeva.

5.3.4. Periodično osnaživanje i osvješćivanje

Osim informiranja o pravilima rada koje se provodi pri preuzimanju radnih obveza, na godišnjoj osnovi se provodi program osnaživanja i osvješćivanja radnika.

5.3.5. Periodična provjera prikladnosti radnika za korisničku ulogu

Ponovna procjena prikladnosti radnika za korisničku ulogu i informiranje o pravilima rada za nosioce kriptografskih uloga vrši se na godišnjoj osnovi uz formalno potpisivanje izjava o prihvaćanju odgovornosti.

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 nisu nosioci definiranih korisničkih uloga.

Zahtjevi za vanjske suradnike opisani su internim procedurama.

5.3.8. Dokumentacija

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

5.4. Procedure upravljanja revizijskim zapisima

5.4.1. Tipovi događaja koji se zapisuju

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

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 tiskani dokazi o ispunjenju sigurnosnih zahtjeva koji su navedeni u ovome dokumentu.

Revizijski zapisi vezani uz upravljanje životnim ciklusom certifikata uključuju, ali se ne ograničavaju na:

a) registracija korisnika,
b) izdavanje certifikata,
c) priprema podataka i izrada SSCD,
d) opoziv, suspenzija, povlačenje suspenzije certifikata i
e) izdavanje i objava CRL.

Revizijski zapisi vezani uz aktivnosti administriranja i održavanja sustava uključuju, ali se ne ograničavaju na:

f) pokretanje i zaustavljanje aplikacija,
g) praćenje rada sustava (upozorenja, alarmi, zastoji, greške, korištenje resursa i sl),
h) promjene konfiguracija kritičnih sustava,
i) spas i povrat podataka i
j) prava pristupa podacima.

Revizijski zapisi sadrže barem sljedeće zapise:

k) identifikacija korisnika,
l) tip događaja,
m) datum i vrijeme događaja,
n) uspješne i neuspješne događaje,
o) ishodište događaja i
p) identifikacija podataka, komponenti sustava ili resursa kojima se pristupilo.

5.4.2. Učestalost obrade revizijskih zapisa

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

Za manje kritične aktivnosti provodi se periodična kontrola.

5.4.3. Period čuvanja revizijskih zapisa

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

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

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

5.4.4. Zaštita revizijskih zapisa

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

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

5.4.5. Sigurnosne kopije revizijskih zapisa

Implementirana je oprema za izradu sigurnosnih kopija te su utvrđene redovite i automatizirane aktivnosti vezane uz osiguranje neprekinutost poslovanja.

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

Sigurnosne kopije se rade u više kopija i pohranjuju se na on site ili off site lokacije.

5.4.6. Prikupljanje revizijskih zapisa

Uspostavljen je sustav upravljanja revizijskim zapisima (eng. *Log Management System*) koji vrši automatsku pohranu i zaštitu revizijskih zapisa u realnom vremenu.

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

5.4.7. Obavješćivanje i alarmiranje

Sustav upravljanja revizijskim zapisima vrši 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

Analiza ranjivosti sustava provodi se korištenjem odobrenih softverskih alata i to za sve informacijske sustave u djelatnoj i sigurnoj zoni.

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

Implementirani su sustavi koji ispituju mogućnost upada u sustav (eng. *Intrusion Detection System*) i koji alarmiraju pojavu ranjivosti u realnom vremenu.

Odmah po otkrivanju ranjivosti poduzimaju se aktivnosti za njihovo rješavanje.

5.5. Arhiviranje

5.5.1. Tipovi podataka koji se arhiviranju

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

a) podatke o osobama prikupljene u postupku registracije,
b) podatke o postupcima obrade zahtjeva za izdavanje certifikata,
c) podatke o postupcima izrade, distribucije i uručenja eOI,
d) podatke o postupcima obrade zahtjeva za opoziv, suspenzije i povlačenje suspenzije certifikata,
e) podatke o izdavanju i objavi CRL ,
f) revizijske zapise kritičnih sustava i
g) ostale podatke sukladno važećim propisima.

5.5.2. Period čuvanja arhiviranih podataka

Davatelj usluga registracije i davatelj usluga certificiranja osiguravaju dugoročno čuvanje informacija kako bi se osigurala pravna valjanost elektroničkih potpisa tijekom duljih razdoblja i jamče mogućnost njihove validacije neovisno o budućim tehnološkim promjenama.

Svi arhivirani podaci i dokumentacija čuvaju se najmanje 10 godina.

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 barem 2 kopije medija koje se pohranjuju na različitim lokacijama.
d) Mediji s arhivskim podacima se povremeno provjeravaju te prepisuju na drugi medij kako bi se osigurala zaštite od starenja ili tehnološkog zastarijevanja.

AKD kao stvaratelj i imatelj javnoga arhivskog i registraturnoga gradiva postupa u skladu s odredbama Zakona o arhivskom gradivu i arhivima (NN 105/97, 64/00, 65/09, 125/11).

5.5.4. Postupci izrade sigurnosnih kopija arhive

Postupak izrade sigurnosnih kopija arhive odnosno povrata podataka iz sigurnosnih kopija je poznat, testiran i pouzdan, a postupak oporavka se može realizirati u prihvatljivom vremenu, ako za to nastane potreba.

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

Uključene su opcije automatske provjere medija i postupka izrade sigurnosnih kopija, a uspješnost provođenja aktivnosti izrade sigurnosnih kopija podataka se provjerava.

5.5.5. Zahtjevi za zaštitu zapisa vremenskim žigom

Nije primjenjivo.

5.5.6. Prikupljanje arhivske građe

Prikupljanje arhivske građe vrši se interno. Radnik zadužen za pismohranu provodi evidentiranje prikupljenog arhivskog gradiva te dostavlja potrebne podatke o jedinicama gradiva u državni arhiv.

5.5.7. Procedure dobivanja i provjere arhiviranih podataka

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

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

5.6. Promjena ključa

Davatelj usluga certificiranja treba voditi računa da se procedura za promjenu ključa ovjerovitelja vrši pravovremeno prije isteka roka važenja ključa.

Osobe trebaju voditi računa da se procedura promjene osobne iskaznice vrši pravovremeno prije isteka roka važenja.

Procedura promjene ključa za osobe je ista kao procedura dobivanja postojećeg ključa.

Procedura promjene ključa ovjerovitelja ista je kao procedura generiranja postojećeg ključa.

5.7. Kompromitacija i oporavak

5.7.1. Tipovi incidenata i sigurnosnih događaja

Tipovi incidenata koji se bilježe i obrađuju su zatajenje hardverske opreme i softvera, nepravilnosti u radu, preopterećenja kapaciteta ili degradacija usluge, nedostupnost servisa, mreže ili aplikacije i sl.

Primjeri sigurnosnih događaja koji se bilježe i obrađuju su kompromitacija resursa, privatnog ključa, softvera i/ili podataka, nekontrolirane promjene sigurnosnih postavki sustava, povreda prava pristupa na računalnoj opremi, odstupanja od propisanog načina rada, slabosti kriptografskih algoritama i sl.

5.7.2. Postupanje u slučaju incidenta

AKD ima definiran i dobro dokumentiran poslovni proces i određene formalne odgovornosti u slučaju pojave incidenta.

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

Tijekom obrade incidenata moguće je inicirati pokretanje postupka upravljanja promjenama, odnosno postupiti po proceduri za hitne situacije.

5.7.3. Postupanje u slučaju sigurnosnog događaja

AKD ima definiran i dobro dokumentiran poslovni proces i određene formalne odgovornosti koje osiguravaju adekvatno i pravovremeno reagiranje na sigurnosne događaje.

Postupci obrade sigurnosnih događaja uključuju definiranje opsega, prikupljanje i osiguranje dokaza te provedba forenzičke analize.

Nakon utvrđivanja uzroka nastanka sigurnosnog događaja te analize potencijalnih posljedica, odlučuje se o daljim aktivnostima.

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

a) prestaje s izdavanjem certifikata na kompromitiranom ovjerovitelju,
b) pokreće se postupak opoziva certifikata ovjerovitelja,
c) pokreće se postupak opoziva certifikata osoba izdanih od strane kompromitiranog ovjerovitelja,
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 ključa ovjerovitelja.

5.7.4. Upravljanje kontinuitetom poslovanja

AKD ima utvrđen i dobro dokumentiran Plan neprekinutosti poslovanja i Plan oporavka sustava kako bi se ostvarili preduvjeti za neprekinuto poslovanje u slučaju zastoja u radu IT sustava kao i u slučaju prirodnih katastrofa, nesreća, velikih kvarova opreme i namjernih akcija.

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

Plan neprekinutosti poslovanja uključuje procedure za postupanje u hitnim situacijama.

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

5.8. Prestanak rada

U slučaju prestanka sporazuma s Ministarstvom, davatelj usluga povjerenja će konzultirati nadležna državna tijela o daljnjim postupcima koji će se poduzeti vezano uz prestanak davanja usluga certificiranja.

Postupci prestanka rada će uključivati:

a) tranziciju sustava na novog davatelja usluga certificiranja,
b) predaju prikupljene dokumentacije i arhivske građe,
c) prestanak izdavanja certifikata za eOI i
d) propisno uništenje kriptografskih ključeva i podataka davatelja usluga certificiranja.

6. Tehničke mjere zaštite

6.1. Generiranje i dostava para ključeva

6.1.1. Generiranje ključeva ovjerovitelja

Vrije pravila:

a) Postupak inicijalnog generiranja para ključeva ovjerovitelja provodi se formalnom ceremonijom generiranja koju organizira i nadzire Povjerenstvo.
b) Ceremonija se provodi u fizički sigurnom okružju tj. u prostoru sigurne zone.
c) Ceremoniji prisustvuju radnici kojima su povjerene uloge (poglavlje 5.2), interni i vanjski revizori, javni bilježnik te ostali pozvani svjedoci.
d) Prije početka ceremonije u nazočnosti javnog bilježnika provodi se formalna identifikacija osoba te dodjela uređaja, sigurnosnih omotnica i obrazaca za pohranu.
e) Postupak generiranja ključa ovjerovitelja 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 ključeva ovjerovitelja 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 ovjerovitelja (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, ispis certifikata ovjerovitelja, zapisnik o provedbi ceremonije te video zapis ceremonije generiranja ključa ovjerovitelja pohranjuju se u arhivu.
k) Prije isteka potpisnog ključa ovjerovitelja, novi par ključeva će se generirati uz istu proceduru kao kod inicijalne generacije ključa ovjerovitelja.
l) Davatelj usluga povjerenja će voditi računa da postupak generiranja novog para ključeva ovjerovitelja ne uzrokuje neugodnosti ili zastoje osobama, pouzdajućim stranama i ostalim sudionicima koji su povezani s davateljem usluga povjerenja.

6.1.2. Generiranje i dostava privatnog ključa osoba

Vrijede pravila:

a) Postupak generiranja ključeva za osobe vrši proizvođač osobne iskaznice u fizički sigurnom okružju tj. u prostoru sigurne zone.
b) U sigurnom okružju centra za individualizaciju vrši se unos ključeva u SSCD.
c) Privatni ključ osobe u informacijskom sustavu je cijelo vrijeme šifriran kriptografskim ključem koji je pohranjen na HSM-u.

d) Dešifriranje privatnog ključa osobe vrši se samo kroz minimalno vrijeme potrebno za njegov unos u čip eOI.
e) Šifrirani privatni ključevi osoba čuvaju se u informacijskom sustavu maksimalno 30 dana nakon njihovog generiranja nakon čega se automatski brišu.
f) Po završetku proizvodnog procesa proizvođač čuva osobne iskaznice u trezoru do njihove otpreme davatelju usluga registracije.
g) Davatelj usluga registracije osigurava sve potrebne preduvjete za sigurnu pohranu osobnih iskaznica i sigurnosnih omotnica koje čekaju na uručenje osobama.

6.1.3. Dostava javnog ključa osoba ovjerovitelju

Odmah po generaciji ključeva osoba, proizvođač pribavlja certifikat od ovjerovitelja HRIDCA šaljući mu javni ključ. Ovaj se proces odvija putem sigurnog komunikacijskog kanala kako bi se osigurala zaštita izvornosti javnog ključa i certifikata.

6.1.4. Dostava javnog ključa ovjerovitelja pouzdajućim stranama

Javni ključevi ovjerovitelja AKDCA Root i HRIDCA su dostupni na Portalu (vidi poglavlje 2.2). Kako bi se omogućila provjera izvornosti certifikata ovjerovitelja, sažetak certifikata se na zahtjev može dostaviti sigurnim kanalom pouzdajućim stranama.

6.1.5. Duljine ključeva

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

Ključevi osoba su duljine 2048 bita, RSA 256 algoritam.

6.1.6. Generiranje i provjera kvalitete parametara javnog ključa

AKDCA Root i HRIDCA ključevi kao i ključevi osoba generirani su na HSM uređaju sukladno poglavlju 6.2.1.

Davatelj usluga certificiranja osigurava da su za generaciju ključeva ovjerovitelja i osoba korišteni kriptografski algoritmi i parametri koji su prikladni za korištenje tijekom perioda važenja certifikata i koji su usklađeni s preporukama norme ETSI TS 119 312 [33].

6.1.7. Namjena ključeva

Izdani certifikati su X.509 v3, a njihova namjena je definirana kroz vrijednost polja „keyUsage“.

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

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

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

6.2. Zaštita privatnog ključa

6.2.1. Norme i kontrole kriptografskih modula

CA ključevi kao i ključevi osoba se generiraju u HSM modulu koji demonstrira sukladnost s FIPS PUB 140-2 level 3 [32] standardu.

Svi postupci upravljanja kriptografskim ključevima uključujući generiranje, korištenje, učitavanje, pohranu, oporavak i uništavanje kriptografskih ključeva, provode se isključivo u sigurnoj zoni pod dvojnom kontrolom.

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

Privatni ključevi osoba se unose u osobnu iskaznicu koja kao sredstvo za izradu elektroničkog potpisa (SSCD), zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 [24] te demonstrira sukladnost s obrascima zaštite iz serije EN 419211-2 [17] i EN 419211-3 [18].

6.2.2. Princip dijeljenog znanja

Formalnom ceremonijom generiranja koje je opisano u poglavlju 6.1.1 provodi se postupak inicijalizacije HSM uređaja i generacije ključeva pri čemu svaki skrbnik dobiva samo jednu komponentu ključa.

Postupci upravljanja kriptografskim ključevima provode se uz strogo poštivanje principa dijeljenog znanja n od m, čime se osigurava da je privatni ključ uvijek pod kontrolom više osoba pri čemu jedna osoba ne može doći u posjed kriptografskih materijala kojim se kriptografski ključevi mogu regenerirati.

6.2.3. Pohrana privatnog ključa

Privatni ključ ovjerovitelja stalno ostaje u HSM uređaju u sigurnoj zoni te se koristi isključivo za potpisivanje certifikata osoba i CRL.

Pojedinačni ključevi osoba se odmah nakon generacije šifriraju kriptografskim ključevima čija je snaga jednaka ili veća od ključa koji se štiti. Dodatna zaštita se ostvaruje šifriranjem skupne datoteke koja se tako pripremljena odmah šalje u centar za individualizaciju gdje će se unositi u čip osobne iskaznice.

Ne vrši se pohrana privatnih ključeva osoba.

6.2.4. Kopiranje privatnog ključa

Kada je ključ ovjerovitelja izvan HSM modula za potrebe sigurnosne pohrane, koriste se hardverski mehanizmi zaštite ključa koje osigurava proizvođač opreme, a koji jamče isti ili veći nivo sigurnosti.

Sigurnosne kopije ključeva ovjerovitelja pohranjene su i na sekundarnoj lokaciji gdje je osiguran isti ili veći nivo zaštite ključa.

Privatni ključevi osoba se ne kopiraju.

6.2.5. Arhiviranje privatnog ključa

Svi kriptografski sadržaji pohranjuju se u odijeljenim sigurnosnim spremnicima u omotnicama s detekcijom neovlaštenog otvaranja, vodeći računa da niti jedna osoba ne može doći u posjed ostalih komponenti ključa.

Privatni ključevi osoba se ne arhiviraju.

6.2.6. Prijenos privatnog ključa

Kada je privatni ključ ovjerovitelja izvan HSM uređaja za potrebe sigurnosne pohrane ili prijenosa na drugi HSM uređaj, koriste se hardverski mehanizmi zaštite ključa koje osigurava proizvođač opreme, a koji jamče isti ili veći nivo sigurnosti.

Privatni ključevi osoba šifrirani pojedinačno i u skupnoj datoteci prenose u centar za individualizaciju putem šifriranog komunikacijskog kanala.

U individualizacijskom centru se skupna datoteka dešifrira, a dešifriranje privatnog ključa osobe događa se samo u memoriji računala neposredno prije unošenja ključa u čip eOI.

6.2.7. Zaštita ključa u kriptografskom modulu

Privatni ključ ovjerovitelja u izvornom čitljivom obliku nalazi se samo unutar HSM uređaja.

Privatni ključ osoba u izvornom čitljivom obliku nalazi se samo unutar SSCD.

6.2.8. Metoda aktivacije privatnog ključa

Aktivacija privatnog ključa ovjerovitelja u HSM uređaju provodi se isključivo pod dvojnom kontrolom ovlaštenih osoba. Jednom aktiviran, privatni ključ ovjerovitelja ostaje aktiviran sve dok je HSM uređaj upaljen. Nakon ponovnog paljenja HSM uređaja ponovo se vrši aktivacija ključa ovjerovitelja.

Aktivaciju privatnog ključa osoba izvodi samo osoba u toku postupka aktivacije eOI odnosno SSCD. Tijekom aktivacije osobne iskaznice postavljaju se PINovi za zaštitu identifikacijskog privatnog i potpisnog privatnog ključa kao i PUK za otključavanje kartice.

Privatni ključ osobe ostaje aktivan sve dok se eOI ne zaključa nakon 6 uzastopnih pokušaja unosa pogrešnog PIN-a ili blokira nakon 6 uzastopnih pokušaja unosa pogrešnog PUK-a.

Zaključana eOI se može otključati korištenjem PUK vrijednosti, a blokirana kartica se može oporaviti tek nakon deblokade. Blokada se vrši u sigurnom okružju tek nakon međusobne autentikacije SSCD i HSM-a korištenjem namjenskog administratorskog ključa u SSCD i u HSM uređaju.

6.2.9. Deaktivacija privatnog ključa

CA privatni ključ je deaktiviran ukoliko HSM uređaj nije aktivan.

Privatni ključ osobe se deaktivira vađenjem SSCD iz čitača.

6.2.10. Uništavanje kriptografskog ključa

Uništavanje privatnog ključa ovjerovitelja vrši se ako se HSM uređaj iznosi iz sigurne zone radi popravka ili otpisa opreme odnosno nakon isteka perioda važenja certifikata ovjerovitelja ili nakon prestanka rada davatelja usluga certificiranja.

Uništavanje privatnog ključa ovjerovitelja, ako za to nastane potreba, vrši se korištenjem sigurne metode koju osigurava proizvođač HSM-a. Uništavanje sigurnosnih kopija i arhiva privatnog ključa ovjerovitelja vrši se metodama koje su opisane u točki 5.1.7.

Šifrirana skupna datoteka s privatnim ključevima osoba čuva se u informacijskom sustavu maksimalno 30 dana nakon njihovog generiranja nakon čega se automatski briše metodama koje su opisane u točki 5.1.7.

6.3. Ostali vidovi upravljanja kriptografskim ključevima

6.3.1. Arhiviranje javnog ključa

Javni ključevi AKDCA Root i HRIDCA te ključevi svih osoba kojima su izdani certifikati arhiviraju se kroz period od 10 godina nakon njihovog izdavanja kako bi se omogućila naknadna provjera elektroničkog potpisa te osigurali dokazi u sudskim, upravnim i drugim postupcima.

Postupci arhiviranja provode se u skladu s pravilima koja su navedena u poglavlju 5.5.

6.3.2. Rok važenja certifikata

Rok važenja certifikata korijenskog ovjerovitelja AKDCA Root je do 2038-01-19 03:14:07+00:00.

Rok važenja certifikata podređenog ovjerovitelja HRIDCA je 15 godina.

Rok važenja certifikata osoba je 5 godina.

Certifikat je važeći od datuma izdavanja do isteka roka važenja i ne smije se koristiti nakon isteka roka važenja.

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

6.4. Aktivacijski podaci

6.4.1. Generiranje i instalacija aktivacijskih podataka

Za zaštitu pristupa privatnim ključevima na eOI koriste se aktivacijski podaci odnosno PIN.

Vrijede pravila:

a) Generiranje aktivacijskih podataka te njihov ispis i unos u SSCD vrši se u sigurnom okružju proizvođača eOI.
b) Aktivacijski podaci se ispisuju u sigurnosne omotnice odvojeno od eOI u sigurnom okružju proizvođača eOI.
c) Dvojna kontrola je forsirana na logičkom nivou tako da se zahtijeva autentikacija 2 osobe na informacijskom sustavu za ispis aktivacijskih podataka i za unos aktivacijskih podataka u SSCD.
d) Aktivacijski podatak u informacijskom sustavu je cijelo vrijeme šifriran kriptografskim ključem koji je pohranjen na HSM-u.

e) Dešifriranje aktivacijskih podataka u informacijskom sustavu vršiti se samo kroz minimalno vrijeme potrebno za njihov ispis odnosno unos u eOI.
f) Šifrirani aktivacijski podaci čuvaju se u informacijskom sustavu maksimalno 30 dana nakon njihovog generiranja nakon čega se automatski brišu metodama koje su opisane u točki 5.1.7.

6.4.2. Zaštita aktivacijskih podataka

Proizvođač eOI poduzima sljedeće mjere zaštite aktivacijskih podataka:

a) Ispis aktivacijskih podataka u sigurnosne omotnice vrši se u zasebnoj prostoriji.
b) U postupku ispisa aktivacijskih podataka ne sudjeluju radnici koje su uključeni u proces individualizacije eOI.
c) Ispis aktivacijskih podataka u sigurnosne omotnice vrši se pod dvojnom kontrolom.
d) Dvojna kontrola je forsirana na sustavu kontrole pristupa kroz generiranje alarma ako je samo jedna osoba prisutna u prostoriji za ispis aktivacijskih podataka.
e) Sigurnosne omotnice i eOI pakiraju se u odvojenim paketima.
f) Na paketima koji se transportiraju nisu vidljive oznake koje upućuju da se radi o eOI ili aktivacijskim podacima.

6.4.3. Ostale odredbe o aktivacijskim podacima

Vrijede pravila:

a) Poslovni proces je organiziran tako da se ispis aktivacijskih podataka vrši vremenski nezavisno o individualizaciji eOI.
b) Poslovni proces je organiziran tako da se distribucija aktivacijskih podataka u PU/PP vrši vremenski nezavisno o distribuciji eOI.
c) Uparivanje sigurnih omotnica i eOI vrši službenik MUP-a u PU/PP neposredno prije njihovog uručivanja osobama.

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 [26] i ISO/IEC 27002 [27] normi. To znači:

a) Dokumentirani su interni standardi sigurnosti te postoji niz procedura i uputa koje se redovito ažuriraju.
b) Uspostavljena je organizacijska i upravljačka struktura s jasno definiranim 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.
g) Propisane su i implementirane stroga pravila upravljanja kriptografskom materijalima.
h) Provode se redovite mjere nadzora i održavanja sigurnosti mrežne i računalne opreme koje uključuju zaštitu od malicioznog koda, upravljanje revizijskim zapisima i sigurnosna testiranja i nadzor.
i) Izrađuju se i pohranjuju sigurnosne kopije, te su uspostavljene procedure upravljanja neprekinutošću poslovanja.
j) Uspostavljena su pravila upravljanja incidentima, promjenama i zahtjevima.

6.5.2. Ocjena računalne sigurnosti

Ocjena sustava upravljanja:

a) Kroz interne i vanjske revizije vrši se provjera sukladnosti sa zakonskim propisima, normama ISO/IEC 27001 [26] i ISO/IEC 27002 [27] i internim procedurama.

Procjena proizvoda (SSCD) provodi se prema kriterijima ISO/IEC 15408 [24] što obuhvaća:

b) ispitivanje proizvoda u laboratoriju,
c) podvrgavanje proizvoda opsežnim testovima ranjivosti,
d) vrednovanje procesa istraživanja i razvoja aplikacije i
e) vrednovanje fizičke sigurnosti lokacije i prostora u kojima se provodi razvoj i proizvodnja.

6.6. Upravljanje životnim ciklusom

U AKD-u je uspostavljen Integrirani sustav upravljanja koji je utemeljen na procesnom pristupu i kontinuiranom unapređenju, a uspostavljena pravila poslovanja realiziraju se na fizičkoj, logičkoj ili organizacijskoj razini.

Integrirani sustav upravljanja je usklađen je s međunarodno priznatim normama:

a) Sustav upravljanja kvalitetom – ISO/IEC 9001 [24] norma;
b) Sustav upravljanja informacijskom sigurnošću – ISO/IEC 27001 [26] norma;
c) Sustav upravljanja sigurnošću zaštićenog tiska – ISO/IEC 14298 [28] norma;
d) Sustav upravljanja proizvodnjom eOI - PCI CPS;
e) Sustav upravljanja zaštitom okoliša – ISO/IEC 14001 norma.

Osim certifikata koji potvrđuju usklađenost integriranog sustava upravljanja s gore navedenim normama, AKD posjeduje certifikat poslovne sigurnosti za postupanje s podacima do stupnja tajnosti VRLO TAJNO, EU SECRET i NATO SECRET.

Upravljanje životnim ciklusom softvera koji se razvija u AKD-u vrši se u skladu sa najboljim poslovnim praksama.

6.7. Kontrola mreže

Svi računalni resursi odijeljeni su u logički razdvojene, posebne funkcionalne cjeline koje se nazivaju mrežne zone.

Postoje sljedeće zone:

a) Javna mreža

b) Pristupna zona (DMZ)
c) Administrativna zona
d) Djelatna zona
e) Sigurna zona

Mreže su odijeljene vatrozidima i nadzirane sustavima za otkrivanje napada (eng. *Intrusion Detection System* - IDS). Između zona se strogo regulira mrežni promet, a pravila postupanja i održavanja unutar određene mrežne zone su jasno definirana. Pri prijenosu podataka iz jedne zone u drugu podaci se šifriraju s tim da se podaci smiju dešifrirati samo u odgovarajućoj sigurnosnoj zoni.

Za svu opremu definiran je dozvoljeni softver, dozvoljeni korisnički računi i dozvoljene sigurnosne postavke opreme, a za opremu u djelatnoj i sigurnoj zoni uspostavljen je automatizirani nadzor nad promjenama sigurnosnih postavki.

6.8. Oznaka vremena

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.

Koristi se GPS (eng. *Global Positioning System*) kao izvor vremena.

7. Sadržaj certifikata i CRL

Ovo poglavlje specificira profile certifikata ovjerovitelja, certifikate osoba kao i profile CRL i OCSP.

7.1. Profili certifikata

7.1.1. Certifikat korijenskog ovjerovitelja AKDCA Root

Field	Root CA	Value	Comments
version	M	2	Integer Value of "2" for Version 3 certificate.
serialNumber	M	INTEGER	Unique positive integer.
signature (AlgorithmIdentifier)	M		SHA256RSA
issuer	M		X.500 Distinguished name of the issuer of the certificate. cn=AKDCA Root, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
validity	M		2038-01-19 03:14:07+00:00
subject	M		cn= AKDCA Root, organizationIdentifier=VATHR-58843087891

			o=AKD d.o.o., c=HR
subjectPublicKeyInfo	M		RSA (4096)
extensions			
authorityKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
keyUsage	MC		Certificate Signing, Off-line CRL Signing, CRL Signing
basicConstraints	MC		This extension must appear in all CA certificates. Subject Type=CA Path Length Constrain=None

7.1.2. Certifikat podređenog ovjerovitelja HRIDCA

Field	Sub CA	Value	Comments
version	M	2	Integer Value of "2" for Version 3 certificate.
serialNumber	M	INTEGER	Unique positive integer.
signature (AlgorithmIdentifier)	M		SHA256RSA
issuer	M		X.500 Distinguished name of the issuer of the certificate. cn=AKDCA Root, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
validity	M		15 years
subject	M		cn=HRIDCA, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
subjectPublicKeyInfo	M		RSA (4096)
extensions			
authorityKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
keyUsage	MC		Certificate Signing, Off-line CRL Signing, CRL Signing
basicConstraints	MC		Subject Type=CA Path Length Constraint=None
certificatePolicies	M		[1]Certificate Policy: Policy dentifier= 2.5.29.32.0 (Any policy) [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS

			Qualifier: http://eid.hr/cps
cRLDistributionPoints	M		[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
authorityInfoAccess	M		[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=id-ad-ocsp (1.3.6.1.5.5.7.48.1) accessLocation: URL= http://ocsp.eid.hr/akdcaroot

7.1.3. Identifikacijski certifikat

Field	End Entity DS/NR	Value	Comments
version	M	2	Integer Value of "2" for Version 3 certificate
serialNumber	M	INTEGER	Unique positive integer.
signature (AlgorithmIdentifier)	M		SHA256RSA
issuer	M		X.500 Distinguished name of the issuer of the certificate. cn=HRIDCA, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
validity	M		5 years
subject	M		serialNumber =PNOHR-OIB, g=Ime, sn=Prezime, cn=Ime Prezime, ou=Identification, o=HRIDCA,c=HR
subjectPublicKeyInfo	M		RSA (2048)
extensions			
authorityKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	M		Derived using the SHA-1 hash of the public key.

keyUsage	MC		Digital Signature
extKeyUsage	M		Client Authentication
basicConstraints	MC		Subject Type=End Entity Path Length Constraint=None
certificatePolicies	M		[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.1.2.1.2.2 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=none [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
cRLDistributionPoints	M		[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
authorityInfoAccess	M		[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=id-ad-ocsp (1.3.6.1.5.5.7.48.1) accessLocation: URL= http://ocsp-hridca.eid.hr/hridca
qcStatements	M		id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-SemanticsId-Natural (0.4.0.194121.1.1)

7.1.4. Potpisni certifikat

Field	End Entity QC+SSCD	Value	Comments
version	M	2	Integer Value of "2" for Version 3 certificate.
serialNumber	M	INTEGER	Unique positive integer.

signature (AlgorithmIdentifier)	M		SHA256RSA
issuer	M		X.500 Distinguished name of the issuer of the certificate. cn=HRIDCA, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
validity	M		5 years
subject	M		serialNumber =PNOHR-OIB, g=Ime, sn=Prezime, cn=Ime Prezime, ou= Signature, o=HRIDCA,c=HR
subjectPublicKeyInfo	M		RSA (2048)
extensions			
authorityKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
keyUsage	MC		Non-Repudiation
basicConstraints	MC		Subject Type=End Entity Path Length Constraint=None
certificatePolicies	M		[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.1.2.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=none [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
cRLDistributionPoints	M		[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
authorityInfoAccess	M		[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=id-ad-ocsp (1.3.6.1.5.5.7.48.1) accessLocation: URL= http://ocsp-hridca.eid.hr/hridca
qcStatements	M		id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) id-etsi-qcs-SemanticsId-Natural (0.4.0.194121.1.1)

7.2. Profil CRL

7.2.1. CRL AKDCA Root

Field		Value	Comments
version	M	1	Integer Value of "1" for Version 2 CRL.
signature (AlgorithmIdentifier)	M		SHA256RSA
issuer	M		X.500 Distinguished name of the issuer of the certificate. cn=AKDCA Root, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
thisUpdate	M	YYMMDDHHMMSSZ	utcTime
nextUpdate	M	YYMMDDHHMMSSZ	utcTime (thisUpdate+24h)
revokedCertificates	M		
userCertificate		INTEGER	serial number of certificate being revoked
revocationDate		YYMMDDHHMMSSZ	utcTime
crlEntryExtensions	M		
reasonCode	M		
CRLReason			Any one of these CRL reasons may be asserted: keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL. If the revocation reason is unspecified, then the reasonCode extension should not be included. The removeFromCRL reason code may only be used in delta CRLs and the use certificateHold is deprecated.
invalidtyDate	O	YYYYMMDDHHMMSSZ	GeneralizedTime This extension may be included if the invalidity date precedes the revocation date.

crlExtensions			
authorityKeyIdentifier	M		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
cRLNumber	M	INTEGER	Monotonically increasing sequential number.

7.2.2. CRL HRIDCA

Field		Value	Comments
version	M	1	Integer Value of "1" for Version 2 CRL.
signature (AlgorithmIdentifier)	M		SHA256RSA
issuer	M		X.500 Distinguished name of the issuer of the certificate. cn=HRIDCA, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
thisUpdate	M	YYMMDDHHMMSSZ	utcTime
nextUpdate	M	YYMMDDHHMMSSZ	utcTime (thisUpdate+90d)
revokedCertificates	M		
userCertificate		INTEGER	serial number of certificate being revoked
revocationDate		YYMMDDHHMMSSZ	utcTime
crlEntryExtensions	M		
reasonCode	M		
CRLReason			Any one of these CRL reasons may be asserted: keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold, removeFromCRL. If the revocation reason is unspecified, then the reasonCode extension should not be included. The removeFromCRL reason code may only be used in delta CRLs and the use certificateHold is deprecated.
invalidtyDate	O	YYYYMMDDHHMMSSZ	GeneralizedTime This extension may be included if the invalidity date precedes the revocation date.
crlExtensions			
authorityKeyIdentifier	M		

keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the public key.
cRLNumber	M	INTEGER	Monotonically increasing sequential number.

7.3. OCSP profil

7.3.1. HRIDCA OCSP responder

Field	End Entity DS/NR	Value	Comments
version	M	2	Integer Value of "2" for Version 3 certificate.
serialNumber	M	INTEGER	Unique positive integer.
signature (AlgorithmIdentifier)	M		SHA256RSA
issuer	M		X.500 Distinguished name of the issuer of the certificate. cn=HRIDCA, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
validity	M		5 years
subject	M		cn=HRIDCA OCSP, organizationIdentifier=VATHR-58843087891, o=AKD d.o.o., c=HR
subjectPublicKeyInfo	M		RSA (2048)
extensions			
authorityKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	M		Derived using the SHA-1 hash of the public key.
keyUsage	MC		Digital Signature
extKeyUsage	M		OCSPSigning
basicConstraints	MC		Subject Type=End Entity Path Length Constraint=None
certificatePolicies	M		[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.2.1.2.1.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=none [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps

cRLDistributionPoints	M		[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
authorityInfoAccess	M		[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

8. Provjera usklađenosti

8.1. Učestalost i okolnosti provjere usklađenosti

Ovaj Pravilnik omogućava reviziju s ciljem provjere usklađenosti sa zakonskom regulativom i normama koji su navedeni u poglavlju 9.15.

Revizija s ciljem potvrđivanja da je AKD kvalificirani pružatelj usluga povjerenja i da su usluge koje pruža kvalificirane, provodi se svaka 24 mjeseca prema pravilima utvrđenim u Uredbi EU [10].

Davatelj usluga povjerenja nadzornom tijelu podnosi izvješće o ocjenjivanju sukladnosti u roku od tri radna dana od njegova primitka.

Davatelj usluga povjerenja će podnijeti izvješće o ocjenjivanju sukladnosti nadzornom tijelu što je prije moguće, no najkasnije do 1. srpnja 2017.

Inspekcijski nadzor sustava upravljanja s ciljem provjere usklađenosti s ISO/IEC 9001 [24], ISI/IEC 27001 [26] i ISO/IEC 14298 [28] normama vrši se najmanje svakih 12 mjeseci.

Nadzor u području zaštite osobnih podataka i proizvodnje osobnih iskaznica vrši se povremeno.

Interne revizije s ciljem provjere postupanja prema ovome Pravilniku i internim procedurama vrši se najmanje svakih 12 mjeseci.

8.2. Identitet/kvalifikacije revizora

Ocjenjivanje sukladnosti sa Uredbom EU [10] provodi tijelo koje je u skladu s Uredbom (EZ) br. 765/2008 [11] ovlašteno kao nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža.

Ministarstvo nadležno za gospodarstvo je nadležno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje on pruža.

Inspekcijski nadzor sustava upravljanja sukladno normama ISO/IEC 9001 [24], ISI/IEC 27001 [26] i ISO/IEC 14298 [28] vrše ovlaštene revizijske kuće.

Nadzor u području zaštite osobnih podataka provode državna te druga tijela određena zakonom i drugim propisima koji uređuju zaštitu osobnih podataka.

Nadzor nad radom AKD-a kao proizvođača osobnih iskaznica može provoditi ministarstvo nadležno za unutarnje poslove.

Nadležna državna tijela mogu ovlastiti treću stranu za provedbu revizije.

Interni revizori su položiti tečajeve za interne revizore za informacijsku sigurnost te raspolažu dostatnim znanjima i razumijevanjem norma i zakona u području elektroničkog potpisa.

8.3. Odnos revizora s predmetom revizije

Vanjski revizori su posve neovisni i delegirani od nadležnog ministarstva odnosno ovlaštene vanjske revizijske kuće.

Internu reviziju provodi Savjetnik Uprave za informacijsku sigurnost ili druga neovisna osoba koju imenuje Povjerenstvo.

8.4. Postupanje u slučaju nesukladnosti

AKD poduzima odgovarajuće tehničke i organizacijske mjere za upravljanje rizicima koji prijete sigurnosti davanja usluga certificiranja i proizvodnje eOI. Primjenom najnovijih tehnoloških rješenja osigurava se da razina sigurnosti odgovara stupnju rizika. Posebno se poduzimaju mjere za sprječavanje i smanjivanje utjecaja sigurnosnih incidenata te za obavješćivanje zainteresiranih strana o neželjenim učincima incidenta.

AKD će informirati nadzorna tijela unutar 24 sata u slučaju nastanka incidenta ili opravdane sumnje u incident koji imaju značajan utjecaj na sigurnost informacijskog sustava, davanje usluga certificiranja ili proizvodnog procesa.

Ako je izgledno da bi povreda sigurnosti ili gubitak cjelovitosti mogli nepovoljno utjecati na osobu ili pouzdajuću stranu, AKD će ih informirati bez odgađanja.

U slučaju manjih nesukladnosti AKD će reagirati na prikladan način, odrediti prirodu i uzroke nesukladnosti te implementirati korekcije ili poduzeti odgovarajuće korektivne ili preventivne radnje.

8.5. Priopćavanje rezultata

Izvještaj o provedenoj reviziji odnosno utvrđenoj nesukladnosti dostavit će se predstavnicima revidiranog područja i odgovornim osobama koje su dužne osigurati provedbu korektivne radnje i priložiti odgovarajuće dokaze o tome.

Jedan put godišnje izrađuje se ocjena uprave koja sadrži sve relevantne podatke o stanju sigurnosti i kvalitete, a koja omogućuje razumno planiranje i učinkovito rukovođenje.

9. Ostale poslovne i pravne stavke

9.1. Naknade za usluge

Cijena koju osobe plaćaju za osobnu iskaznicu je određena aktima koji proizlaze iz Zakona o osobnoj iskaznici [1].

Osobe i pouzdajuće strane će bez ikakve naknade moći koristiti sljedeće usluge AKD-a:

a) opoziv certifikata,
b) suspenzija/povlačenje suspenzije certifikata,
c) provjera statusa certifikata u CRL,
d) usluge i informacije dostupne na Portalu i
e) OCSP provjera statusa certifikata.

AKD zadržava pravo poduzimanja odgovarajućih mjera zaštite od zlouporabe navedenih usluga tako što će ograničiti broj mogućih upita po danu.

Svim institucijama Republike Hrvatske AKD PKI omogućava neograničeno korištenje navedenih usluga uključujući pristup i pretraživanje certifikata u javnom imeniku.

9.2. Financijska odgovornost

AKD kao davatelj usluga certificiranja koji izdaje kvalificirane certifikate, a sukladno odredbama Zakona o elektroničkom potpisu [5], ima osiguran rizik od odgovornosti za štete koje nastanu obavljanjem usluga izdavanja kvalificiranih certifikata, a posebno ako se ustanovi:

a) da nisu točni svi podaci sadržani u kvalificiranom certifikatu u vrijeme izdavanja tog certifikata,
b) da je u vrijeme izdavanja certifikata, potpisnik identificiran u kvalificiranom certifikatu posjedovao podatke za izradu potpisa koji odgovaraju podacima za provjeru potpisa koji su navedeni ili identificirani u certifikatu i
c) da se podaci za izradu potpisa i podaci za provjeru potpisa mogu rabiti na sličan način u slučajevima u kojima davatelj usluga certificiranja pohranjuje i izdaje oboje, osim ako davatelj usluga certificiranja dokaže kako je djelovao s dužnom pažnjom.

AKD je odgovoran za štetu nastalu upotrebom certifikata bilo kojem tijelu, odnosno pravnoj ili fizičkoj osobi zbog toga što je propustio opozvati taj certifikat, osim ako dokaže da je djelovao s dužnom pažnjom.

AKD je u ovom Pravilniku naznačio ograničenja vezana uz upotrebu certifikata i davanja usluga certificiranja i ne odgovara za štetu prouzročenu upotrebom certifikata i usluga certificiranja koja prekoračuje navedena ograničenja.

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. Zaštita tajnosti podataka

9.3.1. Poslovna tajna

Poslovnom tajnom smatraju se podaci zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za interese sudionika.

Poslovnom tajnom se smatraju:

a) revizijski zapisi koji se odnose na proizvodnju i davanje usluga certificiranja,
b) izvještaji s revizija,
c) svi osobni podaci osim onih koji su sadržani u certifikatu,

d) razlog za opoziv ili suspenziju certifikata,
e) ostali podaci različitog tipa značajni za poslovanje ili interese sudionika.

Posebna kategorija poslovne tajne su:

f) privatni ključevi ovjerovitelja te privatni ključevi osoba,
g) svi simetrični javni asimetrični ključevi kao i ključevi, PIN-ovi, zaporke, sigurnosni kodovi koji ih štite,
h) aktivacijski podaci i podaci za registraciju na Portal,
i) komunikacija između komponenata PKI infrastrukture,
j) komunikacija između davatelja sluga certificiranja, registracijskog ureda i proizvođača,
k) komunikacija između elektroničkog dijela osobne iskaznice i vanjskih informacijskih sustava i
l) specifični podaci vezani uz provedbu posebnih mjera zaštite informacijskih sustava, poslovne suradnje, radnika te prostora i objekata koji se koriste za obavljanje djelatnosti.

9.3.2. Podaci koji nisu poslovna tajna

Povjerljivi poslovni podaci se ne smatraju:

a) certifikati i sadržaj certifikata,
b) status certifikata te
c) dokumentacija i ostali podaci objavljeni na Portalu.

9.3.3. Odgovornost za zaštitu poslovne tajne

Pri dodjeljivanju prava pristupa podacima vodi se računa o potrebi održavanja rasprostranjenosti podataka na najmanjoj mogućoj razini. Radnicima kojima nije nužan pristup podatku za obavljanje svojih radnih zadataka, ne smije biti odobren pristup tom podatku.

Svaki radnik koji, tijekom obavljanja poslova iz svoga djelokruga, može doći u doticaj s poslovnom tajnom, dužan je potpisati izjavu o čuvanju tajnosti podataka kojom potvrđuje da je upoznat sa svojim pravima i obvezama čuvanja poslovne tajne te odredbama internih propisa kojima se uređuje područje zaštite podataka.

Uvid u povjerljive podatke moći će ostvariti autorizirani i ovlašteni službenici državnih i javnih tijela ili pravna osoba koja vrši nadzor ili ako je to nužno za realizaciju poslovne suradnje. Ako nije potpisan sporazum u kojem su sadržane odredbe o tajnosti tada se od službenika ili osobe može zahtijevati potpisivanje izjave o tajnosti.

Pravo pristupa tajnim 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.

Ako je za potrebe nadzora potrebno ostvariti pristup podacima koje je državno tijelo, u postupku koji propisan Zakonom o tajnosti podataka [4] klasificiralo, takvim označilo i za kojeg je utvrđen jedan od stupnjeva tajnosti, postupat će se u skladu s navedenim zakonom.

9.4. Zaštita osobnih podataka

9.4.1. Plan zaštite osobnih podataka

Zaštita osobnih podataka osigurana je svakoj fizičkoj osobi.

Pri utvrđivanju mjera zaštite osobnih podataka davatelj usluga certificiranja djeluje u skladu s odredbama Zakona o zaštiti osobnih podataka [3] i vezanih pod-zakonskih akata.

Povjerljivi osobni podaci će se tretirati kao poslovna tajna prema poglavlju 9.3.1.

9.4.2. Povjerljivi osobni podaci

Davatelj usluga registracije prikuplja i obrađuje osobne podatke za potrebe izdavanja osobnih iskaznica. U tu svrhu vodi evidenciju čiji je sadržaj propisan Zakonom o osobnoj iskaznici [1] odnosno vezanim Pravilnikom o obrascima i evidenciji osobnih iskaznica [2].

Evidencija osobnih iskaznica sadrže sljedeće podatke:

a) broj osobne iskaznice,
b) ime i prezime,
c) spol,
d) državljanstvo,
e) datum rođenja,
f) rok važenja osobne iskaznice,
g) fotografija,
h) potpis,
i) podaci o prebivalištu,
j) naziv PU/PP koja izdaje osobnu iskaznicu,
k) osobni identifikacijski broj,
l) kontakt broj mobilnog telefona,
m) kontakt e-mail adresa i
n) otisak papilarnih linija lijevog i desnog kažiprsta.

Davatelj usluge proizvodnje dobiva sve podatke iz evidencije osobnih iskaznica te ih u roku od 30 dana nakon izdavanja osobnih iskaznica briše iz svojih evidencija.

Davatelj usluga certificiranja dobiva osobne podatke koji su sadržani u certifikatu, te kontakt podatke, a to su:

o) ime i prezime,
p) osobni identifikacijski broj,
q) kontakt broj mobilnog telefona i
r) kontakt e-mail adresa.

9.4.3. Osobni podaci koji nisu povjerljivi

Davatelj usluga certificiranja vodi registar certifikata te objavljuje certifikate u javnom imeniku.

9.4.4. Odgovornost za zaštitu osobnih podataka

Ministarstvo kao davatelj usluga registracije te AKD kao davatelj usluga certificiranja i proizvođač eOI odgovorni su za zaštitu osobnih podataka sukladno odredbama Zakona o zaštiti osobnih podataka [3].

Pri dodjeljivanju prava pristupa osobnim podacima vodi se računa o potrebi održavanja rasprostranjenosti osobnih podataka na najmanjoj mogućoj razini.

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 potpisnika.

Potpisivanjem Ugovora o davanju usluga certificiranja osobe su dale privolu davatelju 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 i prava intelektualnog vlasništva.

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 certifikate ovjerovitelja, Opća pravila i ovaj Pravilnik.

U skladu s važećim zakonima u Republici Hrvatskoj AKD zadržava sva autorska prava nad ovim dokumentom kao i na svim dokumentima koji su objavljeni na Portalu, uključujući certifikate ovjerovitelja.

AKD je razvio vlastiti izvorni kod te posjeduje i rezervira neograničena autorska prava i prava intelektualnog vlasništva na aplikaciju za SSCD (AKD-eID-Card 1.0) kao i aplikaciju (middleware) za korištenje SSCD.

AKD kao autor i vlasnik navedenih aplikacija te Republika Hrvatska kao vlasnik AKD-a raspolažu s neograničenim pravima raspolaganja i korištenja istih.

Osobe imaju pravo korištenja SSCD i aplikacije za korištenje SSCD bez naknade, a po uvjetima korištenja licenci za krajnje korisnike (*End User Licence Agreement EULA*).

9.6. Obveze i odgovornosti

9.6.1. Obveze i odgovornosti davatelja usluga certificiranja

Obveze i odgovornosti davatelja usluga certificiranja su:

a) Osiguranje primjene Zakona o elektroničkom potpisu [5].
b) Osiguranje dostupnosti usluga vezanih uz vođenje registra certifikata ovjerovitelja HRIDCA uključujući izdavanje i objavu certifikata te upravljanje životnim ciklusom certifikata nakon izdavanja (opoziv, suspenziju ili povlačenje suspenzije).
c) Pravovremeno izdavanje, opoziv, suspenziju ili povlačenje suspenzije certifikata temeljem zahtjeva i cjelovitih, točnih i provjerenih podataka dobivenih od davatelja usluga registracije.
d) Osiguranje osoblja zadovoljavajuće razine specijalističkih znanja i iskustva potrebnog za pružanje usluga certificiranja u skladu sa zahtjevima koji su utvrđeni ovim Pravilnikom.
e) Osiguranje dostatnih financijskih sredstva potrebnih za pružanje usluga certificiranja u skladu sa zahtjevima koji su utvrđeni ovim Pravilnikom.
f) Objavljivanje informacija na Portalu o pravilima vezanim uz korištenje certifikata i davanje usluga certificiranja.
g) Provedba svih poslova koji su u nadležnosti davatelja usluga certificiranja u skladu s ovim Pravilnikom.
h) Osiguranje ISO/IEC 9001 [18] i ISO/IEC 27001 [19] certifikata kao dokaza kvalitete i sigurnosti davanja usluga certificiranja.
i) Pohrana, arhiviranje i zaštita svih relevantnih informacija koje se odnose na certifikate najmanje 10 godina od dana isteka zadnjeg certifikata na eOI.
j) Provedba organizacijskih i tehničkih mjera za zaštitu svih relevantnih informacija koje se odnose na certifikate, posebice u svrhu pružanja dokaza i provjere u sudskim, upravnim i drugim postupcima.
k) Davatelj usluga certificiranja je odgovoran za štetu koja je namjerno ili nepažnjom prouzročena svakoj fizičkoj ili pravnoj osobi zbog nepoštovanja svojih obveza koje su preuzete ovim Pravilnikom.

9.6.2. Obveze i odgovornosti davatelja usluga registracije

Obveze i odgovornosti davatelja usluga registracije su:

a) Provjera i nedvojbeno utvrđivanje identiteta fizičkih osoba neposrednom identifikacijom u fizičkoj prisutnosti osobe prilikom predaje zahtjeva za izdavanje, opoziv i suspenziju certifikata odnosno eOI, kao i prilikom uručivanja i deblokade eOI.
b) Upis cjelovitih, točnih i provjerenih osobnih identifikacijskih podataka o fizičkim osobama i njihovim zahtjevima za izdavanje, opoziv i suspenziju certifikata odnosno eOI u evidenciju osobnih iskaznica, te odobravanje zahtjeva fizičkih osoba.
c) Prosljeđivanje cjelovitih, točnih i provjerenih podataka potrebnih za proizvodnju i individualizaciju kartica, izdavanje certifikata te realizaciju zahtjeva za opoziv i suspenziju certifikata kroz siguran komunikacijski kanal.

d) Osiguranje dokaza da je fizička osoba u trenutku izdavanja eOI dobio u posjed odgovarajuću eOI, pripadne aktivacijske podatke za eOI te odgovarajući privatni ključ i pripadni certifikat na eOI.
e) Vođenje evidencije osobnih iskaznica i upravljanje životnim ciklusom eOI kao i pohrana, arhiviranje i zaštita evidencije osobnih iskaznica, potpisanih Ugovora o davanju usluga certificiranja te svih relevantnih informacija koje se odnose na identitet osobe najmanje 10 godina od dana isteka zadnjeg certifikata na eOI.
f) Provedba poslova registracije fizičkih osoba za potrebe izdavanja certifikata za osobnu iskaznicu u skladu sa Zakonom o elektroničkom potpisu [5], provedbenim propisima [6], [7], [8] donesenim na temelju Zakona o elektroničkom potpisu kao i Općim pravilima te Pravilnika.
g) Provedba organizacijskih i tehničkih mjera za zaštitu osobnih podataka kao i svih podataka koji se prikupljaju, razmjenjuju, generiraju, obrađuju i uništavaju tijekom obavljanja poslova registracije fizičkih osoba i izdavanja eOI, posebice u svrhu pružanja dokaza i provjere u sudskim, upravnim i drugim postupcima.
h) Provedba organizacijskih i tehničkih mjera za zaštitu evidencija te informacija koje se odnose na identitet osoba, posebice u svrhu pružanja dokaza i provjere u sudskim, upravnim i drugim postupcima.

9.6.3. Obveze i odgovornosti osoba

Potpisivanjem Ugovora o davanju usluga certificiranja osobe preuzimaju sljedeće odgovornosti:

a) Identificirati se i dostaviti cjelovite i točne osobne identifikacijske podatke u postupku registracije.
b) Informirati se na Portalu o svojim obvezama i odgovornostima, o uvjetima koji se odnose na uporabu certifikata kao i primjerenom načinu korištenja elektroničkog dijela osobne iskaznice.
c) Pažljivo koristiti i čuvati osobnu iskaznicu, te poduzeti odgovarajuće mjere zaštite od zlouporabe ili neautoriziranog korištenja privatnog ključa.
d) Trenutno zatražiti opoziv ili suspenziju certifikata u slučaju kvara, gubitka ili krađe osobne iskaznice odnosno zlouporabe ili neautoriziranog korištenja privatnog ključa.
e) Ako se promijene podaci o osobnom imenu ili osobnom identifikacijskom broju, zatražiti opoziv ili suspenziju certifikata u roku od 2 dana od dana nastanka promjene.
f) Koristiti certifikate samo za legalne i autorizirane svrhe, sve u skladu s odredbama Zakona o elektroničkom potpisu [5].
g) Koristiti certifikate i usluge certificiranja u skladu s odredbama Općih pravila vodeći računa o primjerenoj i zabranjenoj upotrebi certifikata.
h) Nije dozvoljeno davati drugim osobama na korištenje niti se služiti tuđom eOI kao sredstvom za elektroničku identifikaciju ili izradu elektroničkog potpisa.
i) Fizička osoba je odgovorna za štetu koja je namjerno ili nepažnjom prouzročena svakoj fizičkoj ili pravnoj osobi ako ne ispunjava svoje obveze ili ne djeluje u skladu s odredbama Općih pravila.

9.6.4. Obveze i odgovornosti pouzdajućih strana

Obveze i odgovornosti pouzdajućih strana su:

a) Koristiti certifikat isključivo u svrhe propisane u poglavlju 1.4.1. ovog Pravilnika
b) Provjeriti rok važenja certifikata prije ostvarivanja povjerenja u certifikat
c) Provjeriti status certifikata prije ostvarivanja povjerenja u certifikat koristeći valjanu CRL odnosno ili korištenjem OCSP usluge za on-line provjeru opozvanih certifikata, a prema podacima koji su navedeni u certifikatu.
d) Provjeriti certifikat prema postupcima za validaciju certifikacijske staze, sukladno dokumentu RFC 5280 [21].
e) Provjeriti da su svi podaci o identitetu subjekta u certifikatu ispravno prikazani.
f) Pri verificiranju elektroničkog potpisa, provjeriti da je elektronički potpis izrađen privatnim ključem koji odgovara javnom ključu u certifikatu i da je u vrijeme izrade elektroničkog potpisa certifikat bio valjan.
g) Kada se koristi aplikacija za provjeru gore navedenih odredbi, pouzdajuće strane moraju koristiti aplikaciju u koju se mogu pouzdati.
h) Pouzdajuće strane odgovorne su za štetu koja je namjerno ili nepažnjom prouzročena svakoj fizičkoj ili pravnoj osobi ako ne ispunjavaju svoje obveze ili ne djeluju u skladu s odredbama ovoga Pravilnika odnosno ako prekorače ograničenja vezana uz korištenje certifikata i usluge certificiranja koje su navedene u ovome Pravilniku.
i) Pouzdajuća strana snosi sve rizike pouzdanja u certifikat ako zna ili ima razloga smatrati da postoje činjenice koje mogu uzrokovati bilo kakvu štetu uslijed korištenja certifikata.

9.6.5. Obveze i odgovornosti proizvođača

Obveze i odgovornosti proizvođača su:

a) Izrada eOI čiji je sadržaj, oblik i način zaštite propisan Zakonom o osobnoj iskaznici[1] i vezanim pravilnikom [2].
b) Proizvodnja tijela kartice eOI sa otisnutim dizajnom i s ugrađenim zaštitnim elementima koji omogućavaju fizičku zaštitu od krivotvorenja ili promjene u skladu sa zahtjevima Ministarstva kao izdavatelja dokumenta.
c) Priprema podataka i individualizacija tijela i čipa eOI temeljem zahtjeva i nepromijenjenih podataka dobivenih od Ministarstva.
d) Generiranje parova ključeva/aktivacijskih podataka, te pribavljanje certifikata od ovjerovitelja HRIDCA kao i njihovo unošenje u sredstvo za izradu elektroničkog potpisa (SSCD) u sigurnom okružju temeljem zahtjeva zaprimljenih od Ministarstva.
e) Generiranje podataka za aktivaciju eOI i registraciju na Portal te izrada sigurnosnih omotnica.
f) Provedba svih poslova koji su u nadležnosti proizvođača eOI u skladu s ovim Pravilnikom.
g) Osiguranje ISO/IEC 9001 [18], ISO/IEC 27001 [19] i ISO/IEC 14298 [28] certifikata kao dokaza kvalitete upravljanja poslovanjem i proizvodnjom zaštićenog tiska te sigurnošću informacijskih sustava.
h) Osiguranje EAL 4+ certifikata kao dokaza sukladnosti eOI sa standardnim obrascima zaštite sredstava za izradu naprednog elektroničkog potpisa EN 419 211-2 [17] i EN 419 211-3 [18].
i) Provedba organizacijskih i tehničkih mjera za zaštitu svih kriptografskih ključeva i svih podataka koji se razmjenjuju, generiraju, obrađuju i uništavaju tijekom proizvodnog

procesa, posebice u svrhu pružanja dokaza i provjere u sudskim, upravnim i drugim postupcima.

9.6.6. Obveze i odgovornosti Povjerenstva

Obveze i odgovornosti Povjerenstva su:

a) Definiranje Općih pravila certificiranja po kojima djeluje davatelj usluga certificiranja.
b) Definiranje specifičnih pravila certificiranja koja se primjenjuju kod izdavanja certifikata za eOI, a koja su sadržana u ovome Pravilniku.
c) Održavanje kontinuirane prikladnosti i usklađenosti Općih pravila i Pravilnika sa primjenjivim zakonskim aktima i normama u području elektroničkog potpisa navedenih u poglavlju 9.15.
d) Nadzor nad radom ovjerovitelja.

9.7. Odricanje od odgovornosti

AKD daje jamstvo samo za ono za što je kao davatelj usluga certificiranja odgovoran, a što je navedeno u točki 9.6.

To znači da AKD ne daje jamstvo za:

a) štete koje su prouzročene neprimjerenom upotrebom certifikata prema poglavlju 1.4.2,
b) štete prouzročene lažnom ili nemarnom uporabom SSCD, certifikata ili CRL-a,
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 s odredbama Općih pravila davanja usluga certificiranja.

Davatelj usluga registracije 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 davatelja usluga certificiranja.

AKD nije odgovoran za indirektne štete koje mogu proizaći iz korištenja certifikata davatelja usluga elektroničkih servisa.

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 određenom u poglavlju 1.4.

9.9. Naknada štete

Svaki sudionik koji je prouzročio štetu zbog nepoštivanja odredbi primjenjivih zakona, normi, Općih pravila i Pravilnika odgovarat će oštećenom sudioniku.

Fizička osoba odgovara oštećenoj strani ako:

a) stekne certifikat na eOI izdan od ovjerovitelja HRIDCA 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.

Davatelj usluga povjerenja je odgovoran ako je ta odgovornost jasno uspostavljena ugovorom, Općim pravilima, Pravilnikom ili hrvatskom zakonskom regulativom.

9.10. Prestanak važenja ovjerovitelja

9.10.1. Trajanje dokumenta

Primjena pravila koja su navedena u ovome dokumentu počinju datumom stupanja na snagu dokumenta.

9.10.2. Prestanak važenja dokumenta

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

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 dokumenta

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

9.11. Pojedinačne obavijesti i komunikacija sa sudionicima

Komunikacija davatelja usluga certificiranja s osobama i pouzdajućim stranama se provodi putem Portala.

Komunikacija s davateljem usluga certificiranja se provodi se pisanim putem ili elektroničkom poštom korištenjem kontaktnih podataka koji su objavljeni na Portalu.

9.12. Izmjene i dopune dokumenta

9.12.1. Postupak izmjena i dopuna

Zatipci, manje ispravke ili promjene koje ne utječu na sudionike će se objavljivati kroz inačice dokumenta.

Značajnije promjene koje utječu na sudionike će se objavljivati kroz izdavanje novih 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, a Povjerenstvo će razmotriti prijedlog i odlučiti hoće li prijedlog prihvatiti ili odbiti.

Ako Povjerenstvo procijeni da predložena promjena nije u skladu sa zakonskim propisima i normama ili može umanjivati kvalitetu davanja 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.

9.13. 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 hrvatskog prava.

9.14. Važeći propisi

Za tumačenje odredbi ovoga dokumenta mjerodavni su obvezujući zakonski propisi navedeni u poglavlju 9.15.

9.15. Usklađenost s važećim propisima

Ovim dokumentom demonstrira se striktna usklađenost sa sljedećim zakonima:

a) Zakon o osobnoj iskaznici [1],
b) Pravilnik o obrascima i evidenciji osobnih iskaznica [2],
c) Zakon o zaštiti osobnih podataka [3],
d) Zakon o tajnosti podataka [4],
e) Zakon o elektroničkom potpisu [5],
f) Pravilnik o izradi elektroničkog potpisa, uporabi sredstava za izradu elektroničkog potpisa, općim i posebnim uvjetima poslovanja za davatelja usluga izdavanja vremenskog žiga i certifikata [6],
g) Popis normizacijskih dokumenata [7],
h) Pravilnik o evidenciji davatelja usluga certificiranja u Republici Hrvatskoj [8] te

i) 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].

Ovim dokumentom demonstrira se striktna usklađenost sa sljedećim normama:

j) Ovaj dokument je u skladu s RFC 3647 [12].

k) Certifikati se izdaju se sukladno pravilima izdavanja kvalificiranih certifikata EN 319 401 [13], Draft ETSI EN 319 411-1 [16] i EN 319 411-2 [14] za QCP+.

l) Obrasci (profili) certifikata usklađeni su s RFC 3739 [20] i RFC 5280 [21] te Draft EN 319 412-2 [23] i EN 319 412-5 [22].

m) Certifikati se izdaju na sredstvu za izradu elektroničkog potpisa koje zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 [24] te je evaluirano i demonstrira sukladnost s obrascima zaštite EN 419 211-2 [17] i EN 419 211-3 [18].

n) Sustav upravljanja kvalitetom i sigurnošću davatelja usluga certificiranja usklađen je s ISO/IEC 9001 [16] i ISO/IEC 27001 [17] standardima.

o) Sustav upravljanja kvalitetom, sigurnošću poslovanja i tiska proizvođača usklađen je s ISO/IEC 9001 [24], ISO/IEC 27001 [26] i ISO/IEC 14298 [28].

9.16. Ostale odredbe

Ako to nije protivno zakonskim propisima, odredbama Općih pravila ili Pravilnika, AKD kao davatelj usluga povjerenja može s ostalim sudionicima sklopiti ugovor u kojem će se ugovorne strane obvezati na poštivanje obvezujućih zakonskih propisa i normi koji su navedeni u poglavlju 9.16, kao i Pravilnika o postupcima certificiranja i Općih pravila davanja usluga certificiranja