AKD PKI
OPĆA PRAVILA DAVANJA USLUGA CERTIFICIRANJA

Izdanje 1.3

Status: 08. 06. 2015.

Sadržaj:

Popis izdanja dokumenta:

Izdanje	Datum	Obrazloženje izmjene
PRO-I-90-01	08.06.2015.	Prvo izdanje dokumenta

0. Uvod u dokument

0.1. Opseg i namjena dokumenta

Ovaj dokument – AKD PKI Opća pravila davanja usluga certificiranja (eng. *Certificate Policy* –CP, u daljnjem tekstu Opća pravila) definira skup pravila i sigurnosnih zahtjeva koji se moraju primjenjivati prilikom upravljanja postupcima certificiranja za elektroničku osobnu iskaznicu (eOI), te prilikom korištenja certifikata na eOI.

Temeljem ovoga dokumenta utvrđuje se prikladnost pojedinog tipa certifikata za određenu namjenu odnosno grupu korisnika i/ili elektroničku uslugu.

Sigurnosni zahtjevi koji su propisani u ovome dokumentu osnova su za donošenje Pravilnika o postupcima certificiranja (eng. *Certification Practice Statement* – CPS, u daljnjem tekstu Pravilnik) koji sudionicima postupka certificiranja detaljno definira pravila i omogućava provedbu ovih sigurnosnih zahtjeva u praksi prilikom utvrđivanja identiteta osoba, upravljanja životnim ciklusom certifikata i korištenja certifikata.

Ovaj dokument odgovara „Općim pravilima davanja usluga certificiranja“ koji je kao obvezan dokument davatelja usluga certificiranje definiran u Pravilniku o evidenciji davatelja usluga certificiranja [8], odnosno u Pravilniku o izradi elektroničkog potpisa [6].

Prema RFC 3647 [12] Opća pravila odgovaraju dokumentu „*Certificate Policy* -CP“ tako da su struktura i sadržaj dokumenta strogo usklađeni sa zahtjevima ovoga standarda.

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

AKD je davatelj usluga povjerenja kako je definirano u Uredbi EU [10], a usluge povjerenja koje pruža i koje su u opsegu ovoga dokumenta obuhvaćaju usluge certificiranja, usluge registracije osoba i usluge proizvodnje kartica.

PKI infrastruktura koja omogućuje izdavanje certifikata uspostavljena je u AKD-u, a namijenjena je isključivo za izdavanje certifikata fizičkim osobama za potrebe izdavanja elektroničke osobne iskaznice (eOI). Pravila vezana uz izdavanje i korištenje certifikata koje izdaje AKD PKI proizlaze iz Zakona o osobnoj iskaznici [1] te Pravilnika o obrascima i evidenciji osobnih iskaznica [2].

AKD PKI izdaje dva tipa certifikata:

a) Identifikacijski certifikat koji je kvalificirani certifikat i koji se koristi za elektroničku identifikaciju i autentikaciju radi pristupa elektroničkim uslugama i
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 koje izdaje AKD PKI su kvalificirani i izdaju se u skladu sa Zakonom o elektroničkom potpisu [5], Uredbom EU [10], te vezanim pod-zakonskim aktima i normama.

Certifikati su usklađeni s pravilima za „QCP public + SSCD“ prema normi EN 319 411-2 [14].

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.

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 je dužan angažirati ovlašteno tijelo za ocjenjivanje sukladnosti kako bi u skladu s propisanim postupkom obavilo reviziju AKD-a kao pružatelja kvalificiranih usluga povjerenja.

Hrvatska elektronička osobna iskaznica je usklađena s tehničkom specifikacijom CEN/TS 15480 (European Citizen Card) [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-90-01
Naziv	AKD PKI Opća pravila davanja usluga 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 Policy
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] za „QCP public + SSCD“.

1.3. PKI Sudionici

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

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

d) davatelj usluga certificiranja,
e) davatelj usluga registracije,
f) osobe,
g) pouzdajuće strane,
h) proizvođač i
i) povjerenstvo za upravljanje pravilima certificiranja.

1.3.1. Davatelj usluga certificiranja

Poslovi davatelja usluga certificiranja su:

a) Voditi registar certifikata ovjerovitelja.
b) Osigurati dostupnosti usluga vezanih uz vođenje registra certifikata ovjerovitelja 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 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

Davatelj usluga registracije provjerava identitet osoba i osigurava podatke temeljem kojih davatelj usluga certificiranja izdaje certifikate.

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.
c) Informirati fizičke osobe o pravilima vezanim uz izdavanje certifikata te postupke 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 i davatelja usluga certificiranja.
f) Upisivati provjerene osobne identifikacijske podatke o osobama i njihovim zahtjevima te odobravati zahtjeve osoba.
g) Slati potrebne podatke za realizaciju zahtjeva proizvođaču i davatelju usluga certificiranja.
h) Uručivati certifikate i aktivacijske podatke osobama.
i) Administrirati SSCD nakon izdavanja.

Detaljnije informacije se mogu naći u poglavlju 9.6.2.

1.3.3. Osobe

Osobe su fizičke osobe kojima je kroz propisani postupak izdan certifikat i koje su dobile u posjed SSCD sa certifikatom i korespondirajućim privatnim ključem.

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

Poslovi proizvođača su:

a) Proizvoditi kartice i osigurati sredstvo za izradu elektroničkog potpisa (SSCD).
b) Informirati osobe o pravilima vezanim uz korištenje kartice.
c) Provoditi pripremu podataka i individualizaciju tijela i čipa kartice.
d) Generirati parove ključeva i aktivacijske podatke, pribaviti certifikate od ovjerovitelja te ih unijeti u SSCD.
e) Generirati podatke za aktivaciju SSCD te izraditi sigurnosne omotnice.
f) Distribuirati kartice i sigurnosne omotnice davatelju usluga registracije.

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 (*Policy Management Authority – PMA*) kao formalno tijelo odgovorno za upravljanje pravilima certificiranja AKD PKI.

Povjerenstvo je odgovorno za upravljanje pravilima rada ovjerovitelja te definiranje i administriranje dokumenata:

a) Opća pravila certificiranja (u daljnjem tekstu: Opća pravila) po kojima djeluje davatelj usluga certificiranja
b) Pravilnika o postupcima certificiranja (u daljnjem tekstu: Pravilnik) s detaljnim pravilima po kojima davatelj usluga certificiranja provodi postupke certificiranja.

Povjerenstvo utvrđuje postupke za kontrolu i nadzor nad radom ovjerovitelja.

Detaljnije informacije se mogu naći u poglavlju 9.6.6.

1.4. 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 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.

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

m) Certifikati se ne mogu i ne smiju koristi za šifriranje podataka i za potpisivanje e-mail poruka.

n) Svaka upotreba certifikata, osim onih koje su navedene u ovom poglavlju, je zabranjena.

o) Ako se identifikacijski certifikat koristi za podršku elektroničkom potpisu takav se potpis neće se smatrati naprednim elektroničkim potpisom.

p) 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

Vrijede pravila:

a) Povjerenstvo je odgovorno za upravljanje pravilima rada ovjerovitelja te definiranje i administriranje Općih pravila i Pravilnikaa.

b) Poštanska adresa povjerenstva:
   - Agencija za komercijalnu djelatnost d.o.o
   - Povjerenstvo za upravljanje pravilima certificiranja
   - Savska cesta 31, 10000 Zagreb, Hrvatska

c) Elektronička adresa povjerenstva: pma@akd.hr

d) Internet stranice davatelja usluga povjerenja: http://eid.hr

e) Povjerenstvo je odgovorno za ažuriranje Općih pravila i vezanih Pravilnika te ocjenu prikladnosti i usklađenosti s primjenjivim zakonskim aktima i normama u području elektroničkog potpisa navedenih u poglavlju 9.15.

f) 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

U strukturi javnog imenika objavljuju se izdani certifikati.

Lista opozvanih certifikata dostupna je na adresama: http://crl1.eid.hr/hridca.crl, http://crl1.eid.hr/hridca.crl i ldap://ldap.eid.hr.

2.2. Portal za objavljivanje informacije

Sve informacije koje su potrebne osobama i pouzdajućim stranama za korištenje usluga certificiranja i kartica objavljuju se na Portalu eOI (u daljnjem tekstu Portal) koji je dostupan na http://eid.hr.

Osnovne informacije na Portalu su:

a) Certifikati krovnog i podređenog ovjerovitelja
b) Opća pravila certificiranja
c) Pravilnik o postupcima certificiranja
d) Obrazac Ugovora o davanju usluga certificiranja
e) Informacije o vezanim zakonskim i pod-zakonskim propisima
f) Obavijesti vezane uz davanje usluga certificiranja
g) Informacije o postupcima registracije osoba

Registriranim osobama su dostupne dodatne informacije o korištenju kartice, portala i elektroničkih usluga koje pruža davatelj usluga povjerenja.

Pri registraciji na Portal osoba je dužna postupati po uputama koje su dostupne ja javnom dijelu Portala.

2.3. Učestalost objave informacija

Informacije u javnom imeniku objavljuju se odmah nakon njihovog izdavanja.

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

2.4. Kontrola pristupa

Portal i javni imenik HRIDCA su javno dostupni putem Interneta.

Dostupnost Portala i javnog imenika HRIDCA je 24 sata na dan, 7 dana u tjednu.

Davatelj usluga povjerenja će osigurati stalnu raspoloživost portala i javnog imenika 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 osigurao oporavak sustava u najkraćem mogućem roku.

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.

Nema ograničenja vezanih uz prava pristupa osnovnim informacijama na Portalu.

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

Postupci registracije osoba na Portal dostupni su na javnom dijelu Portala.

3. Identifikacija i autentikacija

3.1. Određivanje imena

Vrijede pravila:

a) Ime certifikata određuje se u skladu s pravilima RFC 3739 [20] te preporukama budućeg standarda Draft ETSI EN 319 412-1 [23].
b) Za certifikate ovjerovitelja polje „Subject“ se formira od:
   - commonName
   - organizationIdentifier
   - organizationName
   - countryName
c) Za certifikate osoba polje „Subject“ formira se od:
   - commonName
   - serialNumber
   - givenName
   - Surname
   - organizationalUnitName
   - organizationName
   - countryName
d) U polju „Subject“ svakog certifikata kojeg izdaje davatelj usluga povjerenja upisani su jedinstveni podaci o potpisniku.
e) Za certifikate ovjerovitelja polje „Subject“ identificira pravnu osobu koja izdaje certifikate, a jedinstvenost imena pravne osobe osigurana je atributom „organizationIdentifier“.
f) Za certifikate osoba polje „Subject“ identificira fizičku osobu, a jedinstvenost imena fizičke osobe osigurana je atributom „serialNumber“.

3.2. Inicijalno utvrđivanje identiteta

Prilikom inicijalnog utvrđivanja identiteta potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva:

a) Zahtjev za inicijalno izdavanje osobne iskaznice podnosi se osobno.
b) Inicijalno utvrđivanje identiteta osoba mora se provoditi u skladu sa Zakonom o osobnoj iskaznici [1] i vezanim pod-zakonskim aktima [2].
c) Tijekom postupka predaje zahtjeva za izdavanje osobne iskaznice vrši se inicijalno utvrđivanje identiteta te postupak registracije osoba koji uključuje upis osoba u evidenciju osobnih iskaznica.
d) Dokazi o punom imenu i prezimenu i drugi podaci te specifična fizička obilježja koja dokazuju identitet osobe prikupljaju se izravno uz prisutnost osobe i korištenjem postojećih podataka iz evidencije osobnih iskaznica.
e) Utvrđivanje identiteta osoba vrši se neposrednom identifikacijom u fizičkoj prisutnosti osobe odnosno temeljem predočenih ili dostupnih identifikacijskih podataka ili važeće isprave.

f) 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.

g) Tijekom registracije podnositelja zahtjeva za osobnu iskaznicu prikupljaju se i dodatna fizička obilježja osobe: fotografija osobe te otisak papilarnih linija lijevog i desnog kažiprsta.

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

i) Davatelj usluga registracije odgovoran je za provjeru prikupljenih podataka i nedvojbeno utvrđivanje identiteta osoba kao i za zaštitu podataka koji su prikupljeni u postupku registracije.

j) Davatelj usluga certificiranja dužan je Pravilnikom propisati detaljne postupke inicijalnog utvrđivanja identiteta osoba.

k) Pravila utvrđivanja identiteta koja se primjenjuju prilikom izdavanja osobne iskaznice moraju osigurati značajni stupanj pouzdanja u utvrđeni identitet fizičke osobe.

3.3. Utvrđivanje identiteta kod obnove certifikata

Certifikati na osobnoj iskaznici imaju isti rok važenja kao i osobna iskaznica.

Utvrđivanje identiteta kod obnove certifikata vrši se u fizičkoj prisutnosti osobe kao i kod inicijalnog utvrđivanja identiteta u poglavlju 3.2.

Davatelj usluga certificiranja dužan je Pravilnikom propisati detaljne postupke utvrđivanja identiteta osoba kod obnove certifikata.

3.4. Utvrđivanje identiteta kod opoziva i suspenzije certifikata

Kod opoziva ili suspenzije certifikata potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva:

a) Prilikom osobnog podnošenja zahtjeva vrši se utvrđivanje identiteta neposrednom identifikacijom u fizičkoj prisutnosti osobe temeljem predočenih identifikacijskih podataka ili važeće isprave, odnosno uvidom u postojeće podatke iz evidencije osobnih iskaznica.

b) Kada davatelj usluga registracije unosi zahtjev za opoziv, suspenziju ili povlačenje suspenzije certifikata u informacijski sustav nužno je utvrditi identitet službenika.

c) Kod podnošenja zahtjeva za suspenziju ili povlačenje suspenzije certifikata korištenjem elektroničke usluge potrebno je utvrditi identitet osobe.

d) Davatelj usluga certificiranja dužan je Pravilnikom propisati detaljne postupke utvrđivanja identiteta osoba kod opoziva i suspenzije certifikata.

4. Provedbeni zahtjevi vezani uz životni ciklus certifikata

4.1. Podnošenje zahtjeva za izdavanje certifikata

Potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka prilikom podnošenja zahtjeva za izdavanje certifikata:

a) 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].
b) Zahtjev za izdavanje osobne iskaznice podnosi se osobno, a za dijete odnosno osobu lišenu poslovne sposobnosti zahtjev podnosi zakonski zastupnik.
c) Zahtjev za izdavanje osobne iskaznice treba biti predan na propisanom obrascu na lokacijama davatelja usluga registracije.
d) Zahtjev za izdavanje certifikata će se prihvatiti samo ako je utvrđen identitet podnositelja zahtjeva sukladno proceduri koja je navedena u poglavlju 3.2.
e) Osobe su dužne dostaviti cjelovite i točne osobne identifikacijske podatke u trenutku podnošenja zahtjeva.
f) Potrebno je informirati osobe o proceduri izdavanja osobne iskaznice te o pravilima davanja usluga certificiranja.
g) Prilikom podnošenja zahtjeva osoba mora sklopiti ugovor s davateljem usluga certificiranja kojim prihvaća uvjete davanja usluga certificiranja, koji su navedeni u Općim pravilima te objavljeni na Portalu.

4.2. Obrada zahtjeva za izdavanje certifikata

Potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka prilikom obrade zahtjeva za izdavanje certifikata:

a) Zahtjev za izdavanje osobne iskaznice smije se prihvatiti samo ako je identitet podnositelja zahtjeva utvrđen sukladno proceduri koja je navedena u poglavlju 3.2.
b) Službenici davatelja usluge registracije utvrđuju identitet podnositelja zahtjeva za izdavanje osobne iskaznice i odlučuju o prihvaćanju ili odbijanju zahtjeva.
c) Obrada zahtjeva za izdavanje osobne iskaznice odnosno certifikata na osobnoj iskaznici mora biti provedena u rokovima koji su propisani Zakonom o osobnoj iskaznici [1].

4.3. Postupak izdavanja certifikata

Potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka prilikom izdavanja certifikata:

a) Postupak izrade i izdavanja certifikata te generiranja parova ključeva i njihovog unošenja u SSCD mora se vršiti u sigurnom okružju.
b) Privatni i javni ključ osobe se može generirati i certifikat se može izdati isključivo temeljem zahtjeva zaprimljenog od davatelja usluga registracije.
c) Profil izdanog certifikata mora biti u skladu sa zahtjevima koji su navedeni u poglavlju 7.1.
d) Ključevi ovjerovitelja koji se koriste za potpisivanje certifikata kao i ključevi osoba moraju biti pod dvojnom kontrolom autoriziranih osoba i štititi se mjerama koje su propisane u poglavlju 6.2.

4.4. Preuzimanje certifikata

Potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka prilikom preuzimanja osobne iskaznice i certifikata:

a) Potrebno je obavijestiti osobu da je njegova osobna iskaznica gotova te da ju može preuzeti.
b) Osobna iskaznica se treba osobno uručiti fizičkoj osobi nakon provjere identiteta.
c) Utvrđivanje identiteta osobe prilikom preuzimanja osobne iskaznice vrši se neposrednom identifikacijom u fizičkoj prisutnosti osobe temeljem predočenih identifikacijskih podataka ili važeće isprave, odnosno uvidom u postojeće podatke iz evidencije osobnih iskaznica.
d) Smatra se da je potpisnik prihvatio privatni ključ i certifikat u trenutku uručenja osobne iskaznice.

4.5. Korištenje ključeva i certifikata

Vrijede pravila:

a) Davatelj usluga certificiranja dužan je putem Portala objavljivati sve potrebne informacija za korisnike i pouzdajuće strane te osigurati dostupnost Portala i usluga za provjeru statusa certifikata.
b) Osobe su potpisivanjem Ugovora o davanju usluga certificiranja osobe preuzele odgovornosti i obvezale se da će postupati u skladu s odredbama koje su navedene u ovom dokumentu.
c) Osobama se s osobnom iskaznicom uručuje neoštećena sigurnosna omotnica koja sadrži podatke za registraciju na Portal i aktivaciju eOI.
d) Prije korištenja eOI osobe su dužne na Portalu pronaći odgovarajuće upute te slijedeći upute registrirati se na Portal i aktivirati eOI.
e) Osobe su upućene na Portal gdje se trebaju informirati o svojim odgovornostima i obvezama kao i o pravilima korištenja usluga certificiranja i kartice.
f) Pouzdajuće strane su upućene na Portal gdje se trebaju informirati o sadržaju Općih pravila i Pravilnika, a posebno o svojim odgovornostima i obvezama te prihvatljivom načinu korištenja usluga certificiranja.

Pouzdajuće strane trebaju se pridržavati sljedećih pravila:

g) Koristiti certifikat isključivo u svrhe propisane u poglavlju 1.4.
h) Provjeriti rok važenja certifikata i status certifikata prije ostvarivanja povjerenja u certifikat prema podacima koji su navedeni u certifikatu.
i) Provjeriti certifikat prema postupcima za validaciju certifikacijske staze, sukladno dokumentu RFC 5280 [21].
j) Provjeriti da su svi podaci o identitetu subjekta u certifikatu ispravno prikazani.
k) 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 poglavlju 4.7.

4.7. Izdavanje novog para ključeva

Novi par ključeva i novi certifikat će biti izdan:

a) nakon isteka roka važenja certifikata ili
b) nakon opoziva certifikata.

Opozvani certifikat nije moguće ponovo reaktivirati već je potrebno podnijeti zahtjev za izdavanje nove osobne iskaznice.

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

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

4.8. Promjena certifikata

Nije primjenjivo.

4.9. Opoziv i suspenzija certifikata

Vrijede pravila:

a) Osoba je dužna u trenutno podnijeti zahtjev za opoziv certifikata u slučaju kvara, gubitka ili krađe osobne iskaznice odnosno zlouporabe ili neautoriziranog korištenja privatnog ključa.
b) Ako se promijene podaci o osobnom imenu ili osobnom identifikacijskom broju, osoba je dužna zatražiti opoziv certifikata u roku od 2 dana od dana nastanka promjene.
c) Zahtjev za opoziv certifikata podnosi osoba ili njen zakonski zastupnik na lokacijama Davatelja usluga registracije.
d) Zahtjev za opoziv smije podnijeti i davatelj usluga registracije nakon što se osobna iskaznica proglasi nevažećom zbog razloga propisanih Zakonom o osobnoj iskaznici [1] ili u slučaju izvanrednih okolnosti i više sile.
e) 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.
f) U redovnim uvjetima rada zahtjev za opoziv treba biti proveden odmah nakon podnošenja zahtjeva te objavljen pouzdajućim stranama putem OCSP usluge. Valjanost odgovora usluge OCSP će biti maksimalno 24 sata.
g) Podređeni ovjerovitelj mora izdati CRL barem 1 put u roku od 24 sata, a period važenja CRL je 24 sata od trenutka izdavanja.
h) Maksimalno vrijeme koje može proteći između zaprimanja zahtjeva a opoziv ili suspenziju certifikata i objave nove liste opozvanih certifikata je 24 sata.
i) CRL korijenskog ovjerovitelja mora biti važeća 90 dana od trenutka izdavanja, a status OCSP usluge za podređene ovjerovitelje će se osvježiti svakih 90 dana.

j) Ako osoba sumnja u kvar, gubitak ili krađu osobne iskaznice odnosno zlouporabu ili neautorizirano korištenje privatnog ključa ili ako nije u mogućnosti pravovremeno podnijeti zahtjev za opoziv certifikata, osoba je dužna podnijeti zahtjev za suspenziju certifikata.

k) Suspenzija certifikata se podnosi osobno na lokaciji davatelja usluga registracije ili korištenjem elektroničke usluge na Portalu.

l) Ako je osoba pronašla osobnu iskaznicu ili ako je prestao razlog zbog kojeg je tražena suspenzija certifikata, osoba je dužna povući suspenziju certifikata u roku od 8 dana. Ako to nije učinjeno u navedenom roku suspendirani certifikat će biti trajno opozvan.

4.10. Usluge za provjeru statusa certifikata

Vrijede pravila:

a) Obveza davatelja usluge certificiranja je javno putem Interneta objaviti informacije temeljem kojih će pouzdajuće strane moći obaviti provjeru valjanosti certifikata.

b) Obveza pouzdajuće strane je obaviti provjeru valjanosti svakog certifikata prije ostvarenja povjerenja u certifikat.

c) Redoslijed kojim pouzdajuća stana dohvaća informaciju o statusu certifikata je:

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

d) Dostupnost usluga za CRL i OCSP provjeru opozvanih certifikata je 24 sata na dan, 7 dana u tjednu, a u slučaju ispada sustava usluga će biti dostupna u najkraćem mogućem roku i u skladu s pozitivnim poslovnim praksama.

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 s osobom se sklapa na rok od 5 godina od dana izdavanja certifikata, a otkazuje se opozivom certifikata.

4.12. Pohrana i oporavak privatnog ključa

Jednom kada je certifikat opozvan privatni ključ se više se ne može oporaviti niti koristiti.

AKD PKI ne obavlja pohranu i oporavak privatnih ključeva osoba.

5. Organizacijske, provedbene i fizičke mjere zaštite

5.1. Mjere fizičke zaštite

PKI infrastruktura i proizvodni pogoni smješteni su u poslovnom kompleksu AKD-a koji je zbog svoje namjene i značaja posebno važan za nacionalnu sigurnost.

PKI infrastruktura je smještena u prostorima sigurne zone gdje se primjenjuju najstrože fizičke, tehničke i proceduralne mjere zaštite.

Prostor sigurne zone opremljen je kompleksnim sustavima tehničke zaštite, a zaštitari su stalno prisutni na objektu 24/7. Cijeli poslovni kompleks neprekidno je nadziran iz centralnog nadzornog sustava.

Pristup sigurnoj zoni ograničen je na ovlašteno osoblje koje obavlja administrativne aktivnosti i nadzor.

Fizički pristup sigurnosnim spremnicima i svoj fizičkoj opremi povezanoj s kriptografskim aktivnostima ostvaruje se isključivo uz dvojnu kontrolu.

Prostor sigurne zone propisno je klimatiziran i smješten na mjestu koje je osigurano od poplave, a sva oprema spojena je na izvor neprekinutog napajanja.

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

Mediji se čuvaju u sigurnosnim spremnicima na dvije odvojene lokacije.

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.

AKD implementira off-site backup na izdvojenoj udaljenoj lokaciji u prostoru koji udovoljava jednakim ili višim sigurnosnim zahtjevima.

5.2. Organizacijske mjere zaštite

Poslovi upravljanja informacijskim sustavom i operativni poslovi vezani uz rad sustava certificiranja obavljaju se prema detaljno utvrđenim pravilima.

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

Princip dijeljenog znanja i 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.

Pri dodjeli uloga strogo se poštuju principi segregacije zaduženja.

5.3. Osoblje

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 im 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.

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

Osim informiranja o pravilima rada koje se provodi pri preuzimanju radnih obveza, na godišnjoj osnovi se provodi program osnaživanja i osvješćivanja radnika te osiguravaju potrebna sredstva za njihovu edukaciju.

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

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

Vanjski suradnici nisu nosioci definiranih korisničkih uloga.

Svim radnicima koji sudjeluju u provedbi aktivnosti ovjerovitelja dostupna je dokumentacija potrebna za obavljanje svakodnevnih radnih zadataka.

5.4. Procedure upravljanja revizijskim zapisima

Potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka:

a) Revizijski zapisi kao dokazi o ispunjenju sigurnosnih zahtjeva moraju biti dostatni kako bi se mogao provoditi nadzor odnosno kako bi se neovlaštena uporaba informacijskog sustava mogla adekvatno istražiti ako za to nastane potreba.

b) Revizijski zapisi moraju biti dostupni u elektroničkom obliku, a tamo gdje to nije moguće, potrebno je osigurati dokaze u tiskanoj formi.

c) Revizijski zapisi vezani uz aktivnosti administriranja i održavanja sustava moraju uključivati promjene konfiguracije i ovlasti, pokretanje i zaustavljanje aplikacija, zastoje i kvarove, promjene na mrežnoj opremi i vatrozidima, uspješne i neuspješne pokušaje pristupa.

d) Potrebno je osigurati revizijske zapise vezane uz upravljanje životnim ciklusom certifikata koji moraju uključivati podatke o registraciji korisnika, izdavanju certifikata, pripremi podataka i izradi SSCD, opoziv, suspenzija i povlačenje suspenzije certifikata te izdavanje i objava CRL.

e) Kritični revizijski zapisi se pregledavaju u realnom vremenu, a za manje kritične aktivnosti provodi se periodična kontrola.

f) Revizijski zapisi vezani uz aktivnosti administriranja i održavanja sustava čuvaju se najmanje 1 godinu dok se revizijski zapisi vezani uz upravljanje životnim ciklusom certifikata čuvaju barem 10 godina u skladu s pravilima arhiviranja koja su opisana u poglavlju 5.5.

g) Revizijski zapisi moraju biti adekvatno zaštićeni i vjerodostojni tako da se mogu prezentirati kao materijalni dokazi u kasnijim eventualnim sudskim postupcima.

h) Svi sistemski satovi i vremena moraju biti točni i usklađeni, kako bi revizijski zapisi sadržavali važeću zabilješku datuma i vremena.

i) Potrebno je utvrditi redovite i automatizirane aktivnosti vezane uz izradu sigurnosnih kopija i osiguranje neprekinutost poslovanja. Postupak povrata podataka iz sigurnosnih kopija mora biti poznat, testiran i pouzdan tako da osigura povrat podataka u razumnom vremenu.

j) Potrebno je uspostaviti sustav upravljanja revizijskim zapisima (*log management system*) koji će vršiti automatsku pohranu i zaštitu revizijskih zapisa svih kritičnih sustava u realnom vremenu. Manje kritični zapisi mogu se prikupljati ručnim ili djelomično ručnim procesima.

k) Potrebno je osigurati automatsku obradu revizijskih zapisa u realnom vremenu i automatsko generiranje alarma u slučaju pojave sigurnosnih događaja za sve kritične aktivnosti.

l) Analiza ranjivosti sustava treba se provoditi periodično korištenjem odobrenih softverskih alata.

5.5. Arhiviranje

Potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka:

a) Arhiviraju se podaci o svim aktivnostima vezanim uz upravljanje životnim ciklusom certifikata što uključuje podatke o registraciji korisnika, izdavanju certifikata, pripremi podataka i izradi SSCD, opozivu, suspenzijama i povlačenjima suspenzije certifikata te izdavanju i objavi CRL.

b) Potrebno je osigurati dugoročno čuvanje informacija kako bi se osigurala pravna valjanost elektroničkih potpisa tijekom duljih razdoblja i jamči mogućnost njihove validacije neovisno o budućim tehnološkim promjenama.

c) Svi arhivirani podaci i dokumentacija moraju se čuvati najmanje 10 godina.

d) Potrebno je implementirati mjere zaštite arhivskog i registraturnoga gradiva te osigurati postupanje u skladu s odredbama Zakona o arhivskom gradivu i arhivima (NN 105/97, 64/00, 65/09, 125/11).

e) Postupci izrade i testiranja sigurnosnih kopija arhive moraju se provoditi periodično kako bi se osigurala pouzdanost povratka podataka iz sigurnosnih kopija.

f) Nije potrebno osigurati zaštitu zapisa vremenskim žigom.

g) Potrebno je osigurati prikupljanje arhivske građe, evidentiranje i dostavljanje potrebnih podataka o jedinicama gradiva u državni arhiv.

h) Postupci izdvajanja podataka iz arhive moraju biti kontrolirani i evidentirani.

i) Potrebno je osigurati periodičnu provjeru arhivske građe.

5.6. Promjena ključa

Certifikati na osobnoj iskaznici imaju rok važenja kao i osobna iskaznica.

Osobe trebaju voditi računa da se procedura promjene osobne iskaznice vrši pravovremeno i prije isteka važenja certifikata na njoj.

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

5.7. Kompromitacija i oporavak

U slučaju kompromitiranja privatnog ključa ovjerovitelja potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka:

a) 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.

b) 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.

c) Potrebno je definirati i dobro dokumentirati poslovni proces i odrediti formalne odgovornosti u slučaju pojave incidenta ili sigurnosnog događaja.
d) Potrebno je osigurati dokaze da se incidenti bilježe i da se njih pravovremeno i na adekvatan način reagira.
e) Postupci obrade sigurnosnih događaja trebaju uključiti prikupljanje i osiguranje dokaza te provedbu forenzičke analize te utvrđivanje uzroka nastanka sigurnosnog događaja, potencijalnih posljedica i način njihove sanacije.
f) U slučaju kompromitiranja privatnog ključa ovjerovitelja, prestaje s izdavanjem certifikata na kompromitiranom ovjerovitelju te se pokreće postupak opoziva certifikata kompromitiranog ovjerovitelja i svih certifikata koje je izdao kompromitirani ovjerovitelj.
g) Potrebno je odmah informirati osobe i pouzdajuće strane, kao i ostale sudionike navedene u poglavlju 1.3. ako je došlo do kompromitiranja privatnog ključa ovjerovitelja.
h) Potrebno je utvrditi i dokumentirati 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.

5.8. Prestanak rada

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

6. Tehničke mjere zaštite

6.1. Generiranje i dostava para ključeva

Pri generiranju privatnih ključeva potrebno je osigurati provedbu sljedećih sigurnosnih zahtjeva i postupaka:

a) Postupak inicijalnog generiranja para ključeva ovjerovitelja i pripadnog certifikata mora se provoditi formalnom ceremonijom.
b) Ceremonija mora biti strogo formalan postupak koji uključuje identifikaciju svih sudionika ceremonije i provedbu postupka generiranja ključa ovjerovitelja po dokumentiranoj proceduri.
c) Ceremoniji mora svjedočiti javni bilježnik koji će ovjeriti zapisnik o provedbi ceremonije s potvrđenim identitetom i izjavama sudionika.
d) Tijekom ceremonije potrebno je osigurati nazočnost internog i vanjskog revizora koji će potvrditi da je postupak generiranja ključa korektno obavljen i da je osigurana izvornost generiranih ključeva.
e) Potrebno je osigurati da se za generaciju ključeva ovjerovitelja i osoba koriste 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].
f) Izdani certifikati su X.509 v3, a njihova namjena je definirana kroz vrijednost polja „keyUsage“ prema poglavlju 7.1.

g) Postupak generiranja ključeva ovjerovitelja i osoba vrši se u fizički sigurnom okružju na HSM uređaju ili SSCD.

h) Prije isteka roka važenja privatnog ključa ovjerovitelja i osoba, novi par ključeva se mora generirati uz istu proceduru kao kod inicijalnog generanja privatnog ključa.

i) Davatelj usluga certificiranja mora 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.

j) Javni ključevi ovjerovitelja su dostupni na Portalu, a kako bi se omogućila provjera njihove izvornosti, sažetak certifikata se na zahtjev može dostaviti sigurnim kanalom pouzdajućim stranama.

k) Javni ključevi osoba su dostupni putem javnog imenika.

6.2. Zaštita privatnog ključa

Vrijede pravila:

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

b) Sve aktivnosti upravljanja privatnim ključevima ovjerovitelja provode se isključivo u sigurnoj zoni pod dvojnom kontrolom te uz primjenu principa dijeljenog znanja „n od m“ čime se osigurava da je privatni ključ uvijek pod kontrolom više osoba.

c) Privatni ključevi ovjerovitelja stalno ostaju u HSM uređaju u sigurnoj zoni te se koriste u za potpisivanje certifikata osoba i CRL.

d) 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].

e) Kada je ključ 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.

f) Pri prijenosu privatni ključevi se šifriraju isključivo kriptografskim ključevima čija je snaga jednaka ili veća od ključa koji se štiti.

g) 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.

h) Ne vrši se pohrana niti arhiviranje privatnih ključeva osoba.

i) Sigurnosna kopija ključeva ovjerovitelja pohranjena je i na sekundarnoj lokaciji gdje je osiguran isti ili veći nivo zaštite ključa.

j) Uništavanje kriptografskih ključeva vrši se ako se HSM uređaj iznosi iz sigurne zone radi popravka ili otpisa opreme odnosno nakon isteka perioda važenja ključeva ovjerovitelja ili nakon prestanka rada davatelja usluga certificiranja.

k) Uništavanje kriptografskih ključeva vrši se korištenjem sigurne metode koju osigurava proizvođač HSM-a.

l) Svi postupci upravljanja privatnim ključevima ovjerovitelja moraju biti dokumentirani i potrebno je voditi uredne evidencije koje osiguravaju dokaze o provedbi.

6.3. Ostali vidovi upravljanja kriptografskim ključevima

Vrijede pravila:

a) Javni ključevi ovjerovitelja i osoba 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.
b) Postupci arhiviranja provode se u skladu s pravilima koji su navedeni u poglavlju 5.5.
c) Rok važenja certifikata korijenskog ovjerovitelja AKDCA Root je do 2038-01-19 03:14:07+00:00.
d) Rok važenja certifikata podređenog ovjerovitelja HRIDCA je 15 godina.
e) Rok važenja certifikata osoba je 5 godina.
f) Certifikat je važeći od datuma izdavanja do isteka roka važenja i ne smije se koristiti nakon isteka roka važenja.
g) Tijekom perioda važenja certifikata, certifikat može biti suspendiran ili trajno opozvan nakon čega prestaje biti valjan i ne smije se više koristiti.

6.4. Aktivacijski podaci

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

U sigurnom okružju centra za individualizaciju vrši se generiranje aktivacijskih podataka te njihov unos u SSCD.

Ispis aktivacijskih podataka u sigurnosne omotnice vrši se pod dvojnom kontrolom te od strane osoba koje nisu uključene u individualizaciju kartica.

Sigurnosna omotnica s aktivacijskim podatkom se uručuje osobi u PU/PP s eOI.

6.5. Mjere zaštite računalnih resursa

Vrijede pravila:

a) Računalne resurse je potrebno štititi mjerama sigurnosti prema ISO/IEC 27001 [26] i ISO/IEC 27002 [27] normi.
b) Potrebno je uspostaviti i održavati interne standarde sigurnosti te definirati procedure i upute koje će osigurati djelotvornu provedbu zahtjeva Općih pravila i Pravilnika.
c) Potrebno je uspostaviti organizacijsku i upravljačku strukturu s jasno definiranim ulogama i odgovornostima.
d) Dokumentirane procedure trebaju obuhvatiti pravila vezana uz radnike, zaštitare, posjetitelje i vanjske servisere prije zapošljavanja, tijekom ugovornog odnosa i nakon isteka ugovora.
e) Dokumentirane procedure trebaju obuhvatiti administriranje i korištenje informacijskih resursa.
f) Upravljane autorizacijama i pravima pristupa podacima mora biti restriktivno.
g) Potrebno je uspostaviti posebne kontrole vezane uz postupanje s kriptografskim sadržajima i materijalima.
h) Potrebno je uspostaviti adekvatne mjere zaštite objekata i prostora u kojima su smješteni informacijski resursi.

i) Potrebno je uspostaviti interna pravila vezana uz održavanje sigurnosti računalne opreme koji trebaju uključivati zaštitu od malicioznog koda, pravila pohrane podataka, upravljanje revizijskim zapisima, nadzor i kontrola izdanja, testiranje softvera i testove ranjivosti sustava.

j) Potrebno je provoditi redovite mjere održavanja sigurnosti mreže i računalnih resursa.

k) Potrebno je uspostaviti pravila upravljanja incidentima, promjenama, zahtjevima i neprekinutošću poslovanja.

l) Potrebno je osigurati provedbu internih i vanjskih revizija radi provjere sukladnosti sa zakonskim propisima, normama i internim procedurama.

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

m) ispitivanje proizvoda u laboratoriju,

n) podvrgavanje proizvoda opsežnim testovima ranjivosti,

o) vrednovanje procesa istraživanja i razvoja aplikacije,

p) vrednovanje fizičke sigurnosti lokacije i prostora u kojima se provodi razvoj i proizvodnja.

6.6. Upravljanje životnim ciklusom

Nužno je uspostaviti sustav upravljanja utemeljen na procesnom pristupu i kontinuiranom unapređenju te uspostaviti jasna pravila poslovanja.

Potrebno je osigurati certifikate kao dokaze da je sustav upravljanja usklađen 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, potrebno je osigurati 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 treba se vršiti prema ISO/IEC 12207 normi.

6.7. Kontrola mreže

Vrijede pravila:

a) Sve računalne resurse je potrebno odijeliti u logički razdvojene, posebne funkcionalne cjeline koje se nazivaju mrežne zone.

b) Potrebno je uspostaviti sljedeće mrežne zone:
   - javna mreža,
   - pristupna zona (DMZ),
   - administrativna zona,
   - djelatna zona i

- sigurna zona.

c) Mreže je potrebno odijeliti vatrozidima, a između mrežnih zona je potrebno strogo regulirati mrežni promet.

d) Potrebno je definirati i uspostaviti jasna pravila pristupa, postupanja i održavanja za svu opremu unutar određene mrežne zone.

e) Pri prijenosu podataka iz jedne mrežne zone u drugu, podaci se moraju šifrirati.

f) Podaci se, ovisno o stupnju njihove tajnosti smiju dešifrirati samo u odgovarajućoj sigurnosnoj zoni.

g) Za svu opremu potrebno je definirati dozvoljeni softver, dozvoljene korisničke račune i dozvoljene sigurnosne postavke opreme, a za opremu u djelatnoj i sigurnoj zoni potrebno je uspostaviti nadzor nad promjenama sigurnosnih postavki.

h) Informacijski sustav ovjerovitelja mora biti u sigurnoj zoni.

6.8. Oznaka vremena

U opsegu davanja usluga certificiranja nije usluga vremenske ovjere (time stamp).

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 (*Global Positioning System*) kao primarni izvor vremena.

7. Sadržaj certifikata i CRL

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

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].

7.1. Profili certifikata ovjerovitelja

Zajednička polja i ekstenzije AKDCA Root i HRIDCA certifikata:

Polje	Atribut	Vrijednost AKDCA Root
Osnovna polja		
version	Version	V3, vrijednost="2"
serialNumber	CertificateSerialNumber	Jedinstven pozitivan broj
signature	AlgorithmIdentifier	SHA256RSA
issuer	commonName	AKDCA Root
	organizationIdentifier	VATHR-58843087891
	organizationName	AKD d.o.o.
	countryName	HR
validity	notBefore	Vrijeme izdavanja certifikata
	notAfter	Vrijeme izdavanja certifikata + vrijeme važenja certifikata (UTC format zapisa)
subject	commonName	AKDCA Root

	organizationIdentifier	VATHR-58843087891
	organizationName	AKD d.o.o.
	countryName	HR
subjectPublicKeyInfo	AlgorithmIdentifier	RSA (4096)
	subjectPublicKey	Javni ključ subjekta
Ekstenzije		
subjectKeyIdentifier	KeyIdentifier	Derived using the SHA-1 hash of the public key.
authorityKeyIdentifier	KeyIdentifier	Derived using the SHA-1 hash of the public key.
keyUsage*	keyCertSign	Certificate Signing
	cRLSign	Off-line CRL Signing
	cRLSign(o6)	CRL Signing
basicConstraints*	Subject Type	CA
	Path Length Constraint	None

*Kritično polje

Specifičnosti AKDCA Root certifikata:

Polje	Atribut	Vrijednost AKDCA Root
Osnovna polja		
subject	commonName	AKDCA Root
	organizationIdentifier	VATHR-58843087891
	organizationName	AKD d.o.o.
	countryName	HR

Specifičnosti HRIDCA certifikata:

Polje	Atribut	Vrijednost HRIDCA
Osnovna polja		
subject	commonName	HRIDCA
	organizationIdentifier	VATHR-58843087891
	organizationName	AKD d.o.o.
	countryName	HR
Ekstenzije		
certificatePolicies	policyIdentifier	2.5.29.32.0 (Any policy)
	Policy Qualifier Id	CPS
	policyQualifiers	http://eid.hr/cps
cRLDistributionPoints	Distribution Point	http://crl1.eid.hr/akdcaroot.crl
	Distribution Point	http://crl2.eid.hr/akdcaroot.crl
	Distribution Point	ldap://ldap.eid.hr/cn= AKDCA Root,o=AKD d.o.o.,c=HR?certificateRevocationList;binary

authorityInfoAccess	Access Method	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	Alternative Name	http://eid.hr/cert/akdcaroot.crt
	Access Method	id-ad-ocsp (1.3.6.1.5.5.7.48.1)
	accessLocation	http:// ocsp.eid.hr/akdcaroot

7.2. Profili certifikata osoba

Zajednička polja i ekstenzije Identifikacijskog i Potpisnog certifikata:

Field	End Entity DS/NR	Comments
Osnovna polja		
version	Version	Integer Value of "2" for Version 3 certificate
serialNumber	CertificateSerialNumber	Unique positive integer.
signature	AlgorithmIdentifier	SHA256RSA
issuer	commonName	HRIDCA
	organizationIdentifier	VATHR-58843087891
	organizationName	AKD d.o.o.
	countryName	HR
	notBefore	Vrijeme izdavanja certifikata
validity	notAfter	Vrijeme izdavanja certifikata + vrijeme važenja certifikata (UTC format zapisa)
subject	serialNumber	PNOHR-OIB
	givenName	Ime
	Surname	Prezime
	CommonName	Ime Prezime
	organizationalUnitName	Identification
	organizationName	HRIDCA
	countryName	HR
subjectPublicKeyInfo	AlgorithmIdentifier	RSA (2048)
	subjectPublicKey	Javni ključ subjekta
Ekstenzije		
authorityKeyIdentifier	keyIdentifier	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	keyIdentifier	Derived using the SHA-1 hash of the public key.
basicConstraints*	Subject Type	End Entity
	Path Length Constraint	None
cRLDistributionPoints	Distribution Point	http://crl1.eid.hr/hridca.crl
	Distribution Point	http://crl2.eid.hr/hridca.crl

	Distribution Point	ldap://ldap.eid.hr/cn= HRIDCA, o=AKD d.o.o.,c=HR?certificateRevocationList;binary
authorityInfoAccess	Access Method	Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
	Alternative Name	http://eid.hr/cert/hridca.crt
	Access Method	id-ad-ocsp (1.3.6.1.5.5.7.48.1)
	accessLocation	http://ocsp-hridca.eid.hr/hridca
qcStatements	qcStatement	id-etsi-qcs-QcCompliance (0.4.0.1862.1.1)
	qcStatement	id-etsi-qcs-QcSSCD (0.4.0.1862.1.4)
	qcStatement	id-etsi-qcs-SemanticsId-Natural (0.4.0.194121.1.1)

*Kritično polje

Specifičnosti Identifikacijskog certifikata:

Field	End Entity DS/NR	Comments
Ekstenzije		
keyUsage*	digitalSignature	Digital Signature
extKeyUsage	Client Authentication	Client Authentication
certificatePolicies	policyIdentifier	1.3.6.1.4.1.43999.5.1.2.1.2.2
	Policy Qualifier Id	User Notice
	policyQualifiers	none
	Policy Qualifier Id	CPS
	policyQualifiers	http://eid.hr/cps

*Kritično polje

Specifičnosti Potpisnog certifikata:

Field	End Entity DS/NR	Comments
Ekstenzije		
keyUsage*	Non-Repudiation	Non-Repudiation
certificatePolicies	policyIdentifier	1.3.6.1.4.1.43999.5.1.2.1.2.1
	Policy Qualifier Id	User Notice
	policyQualifiers	none
	Policy Qualifier Id	CPS
	policyQualifiers	http://eid.hr/cps

*Kritično polje

7.3. Profil CRL

Zajednička polja AKDCA Root i HRIDCA CRL:

Field	Comments
version	Integer Value of "1" for Version 2 CRL.
signature (AlgorithmIdentifier)	SHA256RSA
thisUpdate	utcTime
revokedCertificates	
userCertificate	serial number of certificate being revoked
revocationDate	utcTime
crlEntryExtensions	
reasonCode	
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	GeneralizedTime This extension may be included if the invalidity date precedes the revocation date.
crlExtensions	
authorityKeyIdentifier	
keyIdentifier	Derived using the SHA-1 hash of the public key.
cRLNumber	Monotonically increasing sequential number.

Specifičnosti AKDCA Root CRL:

Field	Comments
Issuer	X.500 Distinguished name of the issuer of the certificate. cn=AKDCA Root, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
nextUpdate	utcTime (thisUpdate+90d)

Specifičnosti HRIDCA CRL:

Field	Comments
Issuer	X.500 Distinguished name of the issuer of the certificate. cn=HRIDCA, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o.,

	c=HR
nextUpdate	utcTime (thisUpdate+24h)

7.4. OCSP profil

Profil HRIDCA OCSP responder:

Polje	Vrijednost
Osnovna polja	
version	Integer Value of "2" for Version 3 certificate.
serialNumber	Unique positive integer.
signature (AlgorithmIdentifier)	SHA256RSA
issuer	X.500 Distinguished name of the issuer of the certificate. cn=HRIDCA, organizationIdentifier=VATHR-58843087891 o=AKD d.o.o., c=HR
validity	5 years
subject	cn=HRIDCA OCSP, organizationIdentifier=VATHR-58843087891, o=AKD d.o.o., c=HR
subjectPublicKeyInfo	RSA (2048)
extensions	
authorityKeyIdentifier	Derived using the SHA-1 hash of the public key.
subjectKeyIdentifier	Derived using the SHA-1 hash of the public key.
keyUsage*	Digital Signature
extKeyUsage	OCSPSigning
basicConstraints*	Subject Type=End Entity Path Length Constraint=None
certificatePolicies	[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	[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	[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

*Kritično polje

8. Provjera usklađenosti

8.1. Učestalost provjere usklađenosti

Provjera usklađenosti sa Zakonom o elektroničkom potpisu [5], Uredbom EU [10] te vezanim pod-zakonskim aktima i vezanim normama provodi se najmanje svaka 24 mjeseca.

Inspekcijski nadzor sustava upravljanja vrši se najmanje svakih 12 mjeseci.

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

Interne revizije vrše se na godišnjoj osnovi.

8.2. Identitet/kvalifikacije revizora

Ocjenjivanje sukladnosti mora provoditi 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.

Inspekcijski nadzor sustava upravljanja 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 može provoditi ministarstvo nadležno za unutarnje poslove.

Nadležna državna tijela mogu ovlastiti treću stranu za provedbu revizije.

Interni revizori moraju raspolagati dostatnim znanjima i razumijevanjem normi 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 osoba koja nije uključena u dnevnu provedbu aktivnosti, a 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

Rezultati provedene revizije i utvrđene nesukladnosti moraju biti dokumentirani te sa njima moraju biti upoznati odgovorne osobe i predstavnici revidiranog područja.

Jedan put godišnje potrebno je izraditi opću ocjenu o stanju sigurnosti i kvaliteti pružanja usluga.

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 bez ikakve naknade mogu koristiti sljedeće usluge AKD-a:

a) opoziv certifikata,
b) suspenzija/povlačenje suspenzije certifikata,
c) objavljivanje certifikata,
d) objavljivanje CRL,
e) objavljivanje ostalih informacija na Portalu i
f) OCSP provjera statusa certifikata

AKD PKI omogućava neograničeno korištenje OCSP provjere statusa certifikata i pristup javnom imeniku svim institucijama Republike Hrvatske, zadržavajući pri tome pravo poduzimanja odgovarajućih mjera zaštite od zlouporabe usluga tako što će ograničiti broj mogućih zahtjeva po danu.

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 upotrebu 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 dokumentu 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

Vrijede pravila:

a) Povjerljivim poslovnim podacima smatraju se podaci koji su kao poslovna tajna određeni zakonom, na zakonu utemeljenim propisima kao i drugi podaci zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za interese sudionika.
b) Povjerljivim poslovnim podacima smatraju se podaci u bilo kojem obliku koje na bilo koji način između sebe razmjene sudionici u svezi provedbe Općih pravila ili Pravilnika.
c) Povjerljivi poslovni podaci se ne smatraju certifikati i sadržaj certifikata, informacija o statusu certifikata kao i podaci objavljeni na Portalu.
d) Pri dodjeljivanju prava pristupa podacima davatelj usluga povjerenja mora voditi računa o potrebi održavanja rasprostranjenosti podataka na najmanjoj mogućoj razini.
e) Uvid u povjerljive podatke potrebno je omogućiti autoriziranim i ovlaštenim službenicima državnih i javnih tijela ili pravnim osobama koje vrše nadzor ili ako je to nužno za realizaciju poslovne suradnje.
f) 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.
g) Davatelj usluga povjerenja dužan je Pravilnikom detaljno propisati pravila postupanja s poslovno povjerljivim podacima kao i pravila vezana uz objavljivanje podataka.

9.4. Zaštita osobnih podataka

Vrijede pravila:

a) Zaštita osobnih podataka zajamčena je svakoj osobi kojoj se izdaje osobna iskaznica i certifikat na osobnoj iskaznici, a posebno maloljetnim osobama.
b) Osobni podaci koji se prikupljaju za potrebe izdavanja osobnih iskaznica i certifikata na njima smiju se obrađivati samo u svrhu u koju su prikupljeni, odnosno u svrhu koja je podudarna sa svrhom prikupljanja.
c) Prikupljaju se isključivo osobni podaci čije je prikupljanje nužno za ispunjenje obveza iz Zakona o osobnoj iskaznici [1] i vezanim Pravilnikom o obrascima i evidenciji osobnih iskaznica [2] te u opsegu koji je nužan da bi se postigla utvrđena svrha.
d) Davatelj usluga povjerenja dužan je definirati interne procedure koje će osigurati ispravnu obradu osobnih podataka.
e) Pri utvrđivanju mjera zaštite osobnih podataka davatelj usluga certificiranja dužan je djelovati u skladu s odredbama Zakona o zaštiti osobnih podataka [2] i vezanih pod-zakonskih akata.
f) Davatelj usluga registracije obrađuje sve podatke koji su prikupljeni za potrebe izdavanja osobnih iskaznica.
g) Davatelj usluga certificiranja obrađuje samo osobne podatke koji su sadržani u certifikatu i kontakt podatke osobe.
h) Davatelj usluga proizvodnje obrađuje sve osobne podatke koji su nužni za izradu osobne iskaznice te ih u roku od 30 dana nakon izdavanja osobnih iskaznica briše iz svojih evidencija.
i) Davatelj usluga certificiranja dužan je voditi registar certifikata i uz privolu osoba koja je dobivena sklapanjem Ugovora o davanju usluga certificiranja, objaviti certifikate u javnom imeniku.
j) Pri dodjeljivanju prava pristupa osobnim podacima vodi se računa o potrebi održavanja rasprostranjenosti osobnih podataka na najmanjoj mogućoj razini.
k) 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.

9.5. 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 davanja usluga certificiranja, Pravilnik o postupcima certificiranja kao i sve upute informacije i ostale objavljene sadržaje te u skladu s važećim zakonima u Republici Hrvatskoj zadržava sva autorska prava nad njima.

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 Pravilnikom o izradi elektroničkog potpisa [6].
e) Osiguranje dostatnih financijskih sredstva potrebnih za nesmetano pružanje usluga certificiranja u skladu sa zahtjevima koji su utvrđeni ovim Općim pravilima i za cijelo vrijeme obavljanja usluga certificiranja.
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 Općim pravilima.
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 osobnoj iskaznici.
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 Općim pravilima.

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, kao i prilikom uručivanja i deblokade osobne iskaznice.

b) Upis cjelovitih, točnih i provjerenih osobnih identifikacijskih podataka o fizičkim osobama i njihovim zahtjevima u evidenciju osobnih iskaznica, te odobravanje zahtjeva fizičkih osoba.

c) Prosljeđivanje cjelovitih, točnih i provjerenih podataka davatelju usluga certificiranja i proizvođaču.

d) Osiguranje dokaza da je fizička osoba u trenutku izdavanja osobne iskaznice dobila u posjed odgovarajuću osobnu iskaznicu, pripadne aktivacijske podatke te odgovarajući privatni ključ i pripadni certifikat na osobnoj iskaznici.

e) Vođenje evidencija osobnih iskaznica i upravljanje životnim ciklusom osobnih iskaznica kao i pohrana, arhiviranje i zaštita evidencija, potpisanih Ugovora o davanju usluga certificiranja te svih relevantnih informacija koje se odnose na identitet osobe najmanje 10 godina

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 Pravilnikom o postupcima certificiranja.

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 osobnih iskaznica, 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 kao i primjerenom načinu aktiviranja i korištenja kartice te certifikata na njoj.

c) Pažljivo koristiti i čuvati osobnu iskaznicu kao sredstvo za izradu elektroničkog potpisa, privatne ključeve, certifikate, aktivacijske i registracijske podatke, te poduzeti odgovarajuće mjere zaštite od neovlaštenog pristupa i uporabe.

d) Trenutno zatražiti opoziv ili suspenziju certifikata u slučaju kvara, gubitka, krađe ili zlouporabe eOI, privatnog ključa i aktivacijskih podataka.

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 osobnom iskaznicom 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. ovog dokumenta
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 važeći.
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 ovih Općih pravila odnosno ako prekorače ograničenja vezana uz korištenje certifikata i usluge certificiranja koje su navedene u ovim Općim pravilima.
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 osobnih iskaznica su:

a) Izrada osobnih iskaznica čiji je sadržaj, oblik i način zaštite propisan Zakonom o osobnoj iskaznici[1] i vezanim pravilnikom [2].
b) Proizvodnja osobne iskaznice s 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 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 osobnih iskaznica u skladu s Općim pravilima i 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 Pravilniku.
c) Održavanje kontinuirane prikladnost i usklađenost Općih pravila i Pravilnika s primjenjivim zakonskim aktima.
d) Održavanje kontinuirane prikladnosti i usklađenosti Općih pravila i Pravilnika s normama u području elektroničkog potpisa.
e) 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 poglavlju 9.6.

To znači da AKD ne daje jamstvo za:

a) štete koje su prouzročene neprimjerenom upotrebom certifikata prema poglavlju 1.4,
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, ovih 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

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

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

Vrijede pravila:

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

b) Značajnije promjene koje utječu na sudionike će se objavljivati kroz izdavanje novih izdanja dokumenta.
c) Izdanje dokumenta se označava prvim brojem u oznaci izdanja dokumenta, dok su inačice naznačene drugim brojem iza točke.
d) Svaki sudionik može inicirati promjenu dokumenta, a Povjerenstvo će razmotriti prijedlog i odlučiti hoće li prijedlog prihvatiti ili odbiti.
e) 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.
f) Prihvaćeni prijedlozi sudionika će se uvrstiti u novo izdanje dokumenta.
g) O pojavi novog izdanja dokumenta sudionici će biti obaviješteni putem Portala odmah po objavljivanju dokumenta.
h) O pojavi novije inačice dokumenta sudionici se neće obavještavati.

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 ovih Općih pravila mjerodavni su obvezujući zakonski propisi.

9.15. Usklađenost s važećim propisima

Ovim Općim pravilima 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 Općim pravilima 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.