



AKD PKI
OPĆA PRAVILA PRUŽANJA USLUGA CERTIFICIRANJA

Izdanje 2.5

Vrijedi od 01.07.2021.

SADRŽAJ

PREDGOVOR	8
1. UVOD	9
1.1. PREGLED DOKUMENTA.....	9
1.1.1. <i>Struktura dokumenta</i>	9
1.1.2. <i>Opseg dokumenta</i>	9
1.1.3. <i>Namjena dokumenta</i>	10
1.2. NAZIV DOKUMENTA I IDENTIFIKACIJA	11
1.2.1. <i>Naziv dokumenta</i>	11
1.2.2. <i>Identifikacijska oznaka</i>	11
1.3. PKI SUDIONICI.....	12
1.3.1. <i>Certifikacijska tijelo – CA</i>	13
1.3.2. <i>Pružatelj servisa za serversko potpisivanje - SSASP</i>	13
1.3.3. <i>Povjerenstvo za upravljanje pravilima certificiranja – PMA</i>	14
1.3.4. <i>Registracijsko tijelo – RA</i>	14
1.3.5. <i>Osobe</i>	15
1.3.6. <i>Pouzdajuće strane</i>	15
1.3.7. <i>Ostali</i>	15
1.4. UPORABA CERTIFIKATA.....	16
1.4.1. <i>Primjerene uporabe certifikata</i>	16
1.4.2. <i>Zabranjene uporabe certifikata</i>	17
1.5. ADMINISTRACIJA DOKUMENTA	17
1.5.1. <i>Organizacija odgovorna za održavanje dokumenta</i>	17
1.5.2. <i>Kontakt podaci</i>	17
1.5.3. <i>Ocjenjivanje usklađenosti dokumenta</i>	17
1.5.4. <i>Postupak odobravanja dokumenta</i>	18
1.6. DEFINICIJE I KRATICE	18
2. REPOZITORIJ I OBJAVLJIVANJE INFORMACIJA.....	18
2.1. REPOZITORIJ	18
2.2. PORTAL ZA OBJAVLJIVANJE INFORMACIJA	18
2.3. VRIJEME OBJAVLJIVANJA I UČESTALOST OBJAVE INFORMACIJA	19
2.4. KONTROLE PRISTUPA REPOZITORIJU	19
3. IDENTIFIKACIJA I AUTENTIKACIJA	19
3.1. ODREĐIVANJE IMENA.....	19
3.1.1. <i>Tipovi imena</i>	19
3.1.2. <i>Smislenost imena</i>	20
3.1.3. <i>Anonimnost i pseudonimi osobe</i>	20
3.1.4. <i>Pravila tumačenja imena</i>	20
3.1.5. <i>Jedinstvenost imena</i>	22
3.1.6. <i>Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka</i>	22
3.2. INICIJALNO UTVRĐIVANJE IDENTITETA.....	22
3.2.1. <i>Metoda dokazivanja posjeda privatnog ključa</i>	22
3.2.2. <i>Potvrda identiteta pravnih osoba</i>	22
3.2.3. <i>Potvrda identiteta fizičkih osoba</i>	23
3.2.4. <i>Informacije o osobama koje se ne provjeravaju</i>	23
3.2.5. <i>Provjera ovlasti</i>	23
3.2.6. <i>Kriteriji za interoperabilnost</i>	23
3.2.7. <i>Ostale odredbe prilikom utvrđivanja identiteta</i>	23
3.3. IDENTIFIKACIJA I AUTENTIKACIJA KOD OBNOVE CERTIFIKATA	23
3.3.1. <i>Identifikacija i autentikacija kod redovite obnove certifikata</i>	23
3.3.2. <i>Identifikacija i autentikacija kod izdavanja novog para ključeva</i>	23
3.4. IDENTIFIKACIJA I AUTENTIKACIJA KOD OPOZIVA CERTIFIKATA.....	23
4. PROVEDBENI ZAHTEVI VEZANI UZ ŽIVOTNI CIKLUS CERTIFIKATA	24
4.1. PODNOŠENJE ZAHTEVA ZA IZDAVANJE CERTIFIKATA	24

4.1.1.	Tko može podnijeti zahtjev za izdavanje certifikata	24
4.1.2.	Postupak podnošenja zahtjeva za izdavanje certifikata	24
4.2.	OBRADA ZAHTEVA ZA IZDAVANJE CERTIFIKATA	24
4.2.1.	Provedba identifikacije i autentifikacije	24
4.2.2.	Odobranje ili odbijanje zahtjeva za izdavanje certifikata	24
4.2.3.	Vrijeme obrade zahtjeva za izdavanje certifikata	24
4.3.	POSTUPAK IZDAVANJA CERTIFIKATA	24
4.3.1.	Postupci tijekom izdavanja certifikata	24
4.3.2.	Obavješćivanje o izdavanju certifikata	24
4.4.	PREUZIMANJE CERTIFIKATA	25
4.4.1.	Provedba postupka prihvatanja certifikata	25
4.4.2.	Objava certifikata od strane CA	25
4.4.3.	Obavješćivanje drugih strana o izdavanju certifikata	25
4.5.	KORIŠTENJE KLJUČEVA I CERTIFIKATA	25
4.5.1.	Osobe	25
4.5.2.	Pouzdanje strane	25
4.6.	OBNOVA CERTIFIKATA	26
4.6.1.	Razlozi za obnovu certifikata	26
4.6.2.	Tko može zatražiti obnovu certifikata	26
4.6.3.	Obrada zahtjeva za obnovu certifikata	26
4.6.4.	Obavješćivanje osobe o obnovi certifikata	26
4.6.5.	Provedba prihvatanja obnovljenog certifikata	26
4.6.6.	Objavljanje certifikata po obnovi certifikata	26
4.6.7.	Obavješćivanje drugih strana o obnovi certifikata	26
4.7.	IZDAVANJE NOVOG PARA KLJUČEVA	26
4.7.1.	Razlozi za izdavanje novog para ključeva	26
4.7.2.	Tko može zatražiti izdavanje novog para ključeva	26
4.7.3.	Obrada zahtjeva za izdavanje novog para ključeva	27
4.7.4.	Obavješćivanje osobe o izdavanju novog para ključeva	27
4.7.5.	Provedba prihvatanja novog para ključeva	27
4.7.6.	Objavljanje certifikata po izdavanju novog para ključeva	27
4.7.7.	Obavješćivanje drugih strana o izdavanju novog para ključeva	27
4.8.	PROMJENA CERTIFIKATA	27
4.8.1.	Razlozi za promjenu certifikata	27
4.8.2.	Tko može zatražiti promjenu certifikata	27
4.8.3.	Obrada zahtjeva za promjenu certifikata	27
4.8.4.	Obavješćivanje osobe o promjeni certifikata	27
4.8.5.	Provedba prihvatanja promijenjenog certifikata	27
4.8.6.	Objavljanje certifikata po promjeni certifikata	28
4.8.7.	Obavješćivanje drugih strana o promjeni certifikata	28
4.9.	OPOZIV I SUSPENZIJA CERTIFIKATA	28
4.9.1.	Koji su razlozi za opoziv certifikata	28
4.9.2.	Tko može zahtijevati opoziv certifikata	29
4.9.3.	Postupci kod podnošenja zahtjeva za opoziv certifikata	29
4.9.4.	Vremenski period za podnošenje zahtjeva za opoziv	29
4.9.5.	Vremenski period obrade zahtjeva za opoziv od strane CA	29
4.9.6.	Provjera statusa certifikata	29
4.9.7.	Učestalost izdavanja CRL	29
4.9.8.	Maksimalno kašnjenje objave CRL	30
4.9.9.	Dostupnost on-line provjere statusa certifikata	30
4.9.10.	Zahtjevi za on-line provjeru statusa certifikata	30
4.9.11.	Ostali načini provjere	30
4.9.12.	Specifični zahtjevi vezani uz kompromitaciju ključeva	30
4.9.13.	Razlozi za suspenziju certifikata	30
4.9.14.	Tko može tražiti suspenziju certifikata	31

4.9.15. Postupci kod podnošenja zahtjeva za suspenziju certifikata.....	31
4.9.16. Ograničenje na trajanje suspenzije	31
4.10. USLUGE PROVJERE STATUSA CERTIFIKATA.....	31
4.10.1. Operativna svojstva.....	31
4.10.2. Dostupnost usluga.....	32
4.10.3. Opcionalna svojstva	32
4.11. KRAJ ŽIVOTNOG CIKLUSA CERTIFIKATA	32
4.12. POHRANA KOD TREĆE OSOBE I OPORAVAK PRIVATNOG KLJUČA	32
5. FIZIČKE, ORGANIZACIJSKO-UPRAVLJAČKE I PROVEDBENE MJERE ZAŠTITE.....	32
5.1. MJERE FIZIČKE ZAŠTITE.....	32
5.1.1. Lokacija objekta i konstrukcija	33
5.1.2. Fizički pristup.....	33
5.1.3. Sustavi za klimatizaciju i napajanje.....	33
5.1.4. Opasnost od poplave.....	33
5.1.5. Protupožarna zaštita	33
5.1.6. Pohrana medija	33
5.1.7. Uništavanje	33
5.1.8. Sigurnosne kopije na drugoj lokaciji.....	34
5.2. ORGANIZACIJSKO-UPRAVLJAČKE MJERE ZAŠTITE	34
5.2.1. Povjerljive uloge	34
5.2.2. Broj osoba potrebnih za obavljanje aktivnosti	34
5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu.....	34
5.2.4. Uloge koje zahtijevaju odvajanje zaduženja	34
5.3. PROVJERA OSOBLJA	34
5.3.1. Kvalifikacije, radno iskustvo i sigurnosne provjere.....	34
5.3.2. Postupak provjere prikladnosti radnika	35
5.3.3. Zahtjevi za obukom	35
5.3.4. Periodična obnova znanja i obuka	35
5.3.5. Periodična rotacija i provjera radnika	35
5.3.6. Sankcije	35
5.3.7. Zahtjevi za vanjske suradnike.....	36
5.3.8. Dokumentacija dostupna radnicima	36
5.4. UPRAVLJANJE REVIZIJSKIM ZAPISIMA	36
5.4.1. Tipovi događaja koji se zapisuju.....	36
5.4.2. Učestalost obrade revizijskih zapisa.....	36
5.4.3. Period čuvanja revizijskih zapisa	37
5.4.4. Zaštita revizijskih zapisa	37
5.4.5. Sigurnosne kopije revizijskih zapisa.....	37
5.4.6. Prikupljanje revizijskih zapisa	37
5.4.7. Obavješćivanje i alarmiranje	37
5.4.8. Procjena ranjivosti sustava	37
5.5. ARHIVIRANJE ZAPISA.....	38
5.5.1. Tipovi zapisa koji se arhiviraju.....	38
5.5.2. Period čuvanja arhiviranih zapisa	38
5.5.3. Zaštita arhive.....	38
5.5.4. Postupci izrade sigurnosnih kopija arhive	38
5.5.5. Zahtjevi za zaštitu zapisa vremenskim žigom.....	38
5.5.6. Prikupljanje arhivske građe.....	38
5.5.7. Postupci dobivanja i provjere arhiviranih podataka	39
5.6. PROMJENA CA KLJUČA.....	39
5.7. KOMPROMITACIJA I OPORAVAK.....	39
5.7.1. Incidenti i postupci u slučaju kompromitacije	39
5.7.2. Kvarovi računalnih resursa, softvera i/ili podataka	39
5.7.3. Postupanje u slučaju kompromitacije	39
5.7.4. Upravljanje kontinuitetom poslovanja	40

5.8.	PRESTANAK RADA	40
6.	TEHNIČKE MJERE ZAŠTITE	41
6.1.	GENERIRANJE I DOSTAVA PARA KLJUČEVA	41
6.1.1.	Generiranje ključeva	41
6.1.2.	Dostava privatnog ključa osobama	41
6.1.3.	Dostava javnog ključa CA-u	41
6.1.4.	Dostava javnog ključa CA pouzdajućim stranama	41
6.1.5.	Duljine ključeva	41
6.1.6.	Generiranje i provjera kvalitete parametara javnog ključa	42
6.1.7.	Namjena ključeva (po X.509 v3 polju uporabe ključa)	42
6.2.	ZAŠTITA PRIVATNOG KLJUČA	42
6.2.1.	Norme i upravljačke funkcije kriptografskog modula	42
6.2.2.	Upravljanje privatnim ključem od strane više osoba (n od m)	42
6.2.3.	Pohrana privatnog ključa	43
6.2.4.	Sigurnosno kopiranje privatnog ključa	43
6.2.5.	Arhiviranje privatnog ključa	43
6.2.6.	Prijenos privatnog ključa u kriptografski uređaj ili iz njega	43
6.2.7.	Čuvanje ključa u kriptografskom modulu	43
6.2.8.	Metoda aktivacije privatnog ključa	44
6.2.9.	Deaktivacija privatnog ključa	44
6.2.10.	Postupci uništavanja kriptografskih ključeva	44
6.2.11.	Ocjena kriptografskog modula	45
6.3.	OSTALI VIDOVI UPRAVLJANJA KRIPTOGRAFSKIM KLJUČEVIMA	45
6.3.1.	Arhiviranje javnog ključa	45
6.3.2.	Period važenja certifikata i kriptografskih ključeva	45
6.4.	AKTIVACIJSKI PODACI	46
6.4.1.	Generiranje i instalacija aktivacijskih podataka	46
6.4.2.	Zaštita aktivacijskih podataka	46
6.4.3.	Ostale odredbe o aktivacijskim podacima	46
6.5.	MJERE ZAŠTITE RAČUNALNIH RESURSA	47
6.5.1.	Posebni tehnički zahtjevi za računalnu sigurnost	47
6.5.2.	Ocjena računalne sigurnosti	47
6.6.	ŽIVOTNI CIKLUS I TEHNIČKE KONTROLE	47
6.6.1.	Upravljanje razvojem sustava	47
6.6.2.	Provjera upravljanja sigurnošću	47
6.6.3.	Provjera sigurnosti životnog ciklusa	47
6.7.	KONTROLA MREŽE	48
6.8.	UPOTREBA VREMENSKOG ŽIGA	48
7.	SADRŽAJ CERTIFIKATA I CRL	48
7.1.	PROFILI CERTIFIKATA	48
7.1.1.	Broj verzije	49
7.1.2.	Ekstenzije certifikata	49
7.1.3.	Identifikator objekta (OID) algoritama	52
7.1.4.	Oblici naziva	52
7.1.5.	Ograničenja u nazivima	52
7.1.6.	Identifikator objekata (OID) općih pravila certificiranja	52
7.1.7.	Upotreba ekstenzije Policy Constraints	52
7.1.8.	Sintaksa i semantika kvalifikatora općih pravila	52
7.1.9.	Procesne semantike za kritičnu ekstenziju Certificate Policies	52
7.2.	CRL PROFILI	53
7.2.1.	Broj verzije	53
7.2.2.	CRL ekstenzije	53
7.3.	OCSP PROFIL	53
7.3.1.	Broj verzije	53
7.3.2.	Ekstenzije OCSP	53

8.	PROVJERA USKLAĐENOSTI	54
8.1.	UČESTALOST I OKOLNOSTI PROVJERE USKLAĐENOSTI	54
8.2.	IDENTITET/KVALIFIKACIJE REVIZORA	54
8.3.	ODNOS REVIZORA S PREDMETOM REVIZIJE	54
8.4.	PODRUČJA OBUHVAĆENA REVIZIJOM.....	54
8.5.	POSTUPANJE U SLUČAJU NESUKLADNOSTI	54
8.6.	PRIOPĆAVANJE REZULTATA	55
9.	OSTALE POSLOVNE I PRAVNE STAVKE	55
9.1.	NAKNADE ZA USLUGE.....	55
9.1.1.	<i>Naknade za izdavanje ili obnovu certifikata.....</i>	<i>55</i>
9.1.2.	<i>Naknade za pristup certifikatu.....</i>	<i>55</i>
9.1.3.	<i>Naknade za opoziv i pristup informacijama o statusu certifikata.....</i>	<i>55</i>
9.1.4.	<i>Naknade za ostale usluge.....</i>	<i>55</i>
9.1.5.	<i>Povrat naknade.....</i>	<i>55</i>
9.2.	FINANCIJSKA ODGOVORNOST	56
9.2.1.	<i>Pokrivenost osiguranjem.....</i>	<i>56</i>
9.2.2.	<i>Ostala sredstva.....</i>	<i>56</i>
9.2.3.	<i>Osiguranje ili garancije za krajnje korisnike.....</i>	<i>56</i>
9.3.	POVJERLJIVOST POSLOVNIH PODATAKA.....	57
9.3.1.	<i>Opseg povjerljivih poslovnih podataka</i>	<i>57</i>
9.3.2.	<i>Podaci koji se ne smatraju povjerljivim poslovnim podacima.....</i>	<i>57</i>
9.3.3.	<i>Odgovornost za zaštitu povjerljivih poslovnih podataka.....</i>	<i>57</i>
9.4.	ZAŠTITA OSOBNIH PODATAKA	57
9.4.1.	<i>Plan zaštite osobnih podataka</i>	<i>57</i>
9.4.2.	<i>Povjerljivi osobni podaci.....</i>	<i>58</i>
9.4.3.	<i>Osobni podaci koji nisu povjerljivi</i>	<i>58</i>
9.4.4.	<i>Odgovornost za zaštitu osobnih podataka.....</i>	<i>58</i>
9.4.5.	<i>Ovlaštenje za korištenje osobnih podataka.....</i>	<i>58</i>
9.4.6.	<i>Dostupnost podataka mjerodavnim tijelima.....</i>	<i>58</i>
9.4.7.	<i>Ostale okolnosti objave osobnih podataka</i>	<i>58</i>
9.5.	PRAVA INTELEKTUALNOG VLASNIŠTVA	58
9.6.	OBVEZE I ODGOVORNOSTI	59
9.6.1.	<i>Obveze i odgovornosti PMA</i>	<i>59</i>
9.6.2.	<i>Obveze i odgovornosti CA.....</i>	<i>59</i>
9.6.3.	<i>Obveze i odgovornosti RA</i>	<i>59</i>
9.6.4.	<i>Obveze i odgovornosti osoba</i>	<i>60</i>
9.6.5.	<i>Obveze i odgovornosti pouzdajućih strana</i>	<i>61</i>
9.6.6.	<i>Obveze i odgovornosti ostalih sudionika.....</i>	<i>61</i>
9.7.	ODRICANJE OD ODGOVORNOSTI.....	61
9.8.	OGRANIČENJA ODGOVORNOSTI	62
9.9.	NAKNADA ŠTETE	62
9.10.	TRAJANJE I PRESTANAK VAŽENJA	63
9.10.1.	<i>Trajanje</i>	<i>63</i>
9.10.2.	<i>Prestanak važenja</i>	<i>63</i>
9.10.3.	<i>Posljedice prestanka važenja i nastavak djelovanja</i>	<i>63</i>
9.11.	POJEDINAČNE OBAVIJESTI I KOMUNIKACIJA SA SUDIONICIMA.....	63
9.12.	IZMJENE I DOPUNE	64
9.12.1.	<i>Postupak izmjena i dopuna</i>	<i>64</i>
9.12.2.	<i>Način obavještanja i period.....</i>	<i>64</i>
9.12.3.	<i>Okolnosti pod kojima se mora mijenjati OID.....</i>	<i>64</i>
9.13.	POSTUPAK RJEŠAVANJA SPOROVA.....	64
9.14.	VAŽEĆI PROPISI.....	64
9.15.	USKLAĐENOST S VAŽEĆIM PROPISIMA	64
9.16.	OSTALE ODREDBE.....	65
9.16.1.	<i>Sporazum</i>	<i>65</i>

9.16.2. Prijenos odgovornosti	65
9.16.3. Nevaljanost pojedine odredbe	65
9.16.4. Ovrha	65
9.16.5. Viša sila	65
9.17. OSTALE ODREDBE	65
PRILOG 1: DEFINICIJE	66
PRILOG 2: KRATICE	70
PRILOG 3: REFERENCE.....	72
PRILOG 4: POVIJEST PROMJENA DOKUMENTA	75

Predgovor

AKD d.o.o. (u daljnjem tekstu: AKD) je pravna osoba koja djeluje kao pružatelj usluga povjerenja u smislu *Uredbe (EU) br. 910/2014 [1]*.

AKD samostalno ili u suradnji s trećim stranama pruža sljedeće usluge povjerenja:

- Usluga registracije (engl. Registration service),
- Usluga generiranja certifikata (engl. Certificate generation service),
- Usluga upravljanja opozivom certifikata (engl. Revocation management service),
- Usluga provjere statusa certifikata (engl. Revocation status service),
- Usluge informiranja (engl. Dissemination service),
- Usluga opskrbe uređajima (engl. Subject device provision service),
- Usluga izdavanja kvalificiranog vremenskog žiga (engl. Time-stamp issuing), i
- Usluge izrade kvalificiranog udaljenog elektroničkog potpisa i pečata (engl. Remote signature creation service).

AKD je kvalificirani pružatelj usluga povjerenja kojem je ministarstvo Republike Hrvatske nadležno za poslove gospodarstva kao nadzorno tijelo odobrilo kvalificirani status temeljem pozitivnog izvješća tijela za ocjenjivanje sukladnosti.

AKD pruža usluge povjerenja od 2015. godine, kada započinje s izdavanjem elektroničke osobne iskaznice Republike Hrvatske (u daljnjem tekstu: eOI) i certifikata koji se na njoj nalaze izdanih sa HRIDCA sustava. Od 2017. godine AKD izdaje komercijalne certifikate sa KIDCA sustava, a od 2018. godine uspostavlja usluge izdavanja kvalificiranog vremenskog žiga i servisa AKD mPotpis koji upravlja udaljenim QSCD uređajem za kreiranje udaljenog elektroničkog potpisa i pečata u ime potpisnika odnosno autora pečata.

Cilj AKD-a je promovirati korištenje elektroničke identifikacije i doprinijeti izgradnji povjerenja u elektroničko poslovanje u cjelini, što predstavlja ključni čimbenik za gospodarski razvoj društva i dobrobit šire društvene zajednice.

1. Uvod

1.1. Pregled dokumenta

1.1.1. Struktura dokumenta

Ovaj dokument „AKD PKI Opća pravila pružanja usluga certificiranja“ (u daljnjem tekstu: opća pravila ili CP) jasno određuje i opisuje skup općenitih pravila po kojima AKD pruža usluge povjerenja.

Prema IETF RFC 3647 [37], opća pravila odgovaraju dokumentu „Certificate Policy - CP“ te su struktura i sadržaj dokumenta strogo usklađeni sa zahtjevima ove norme.

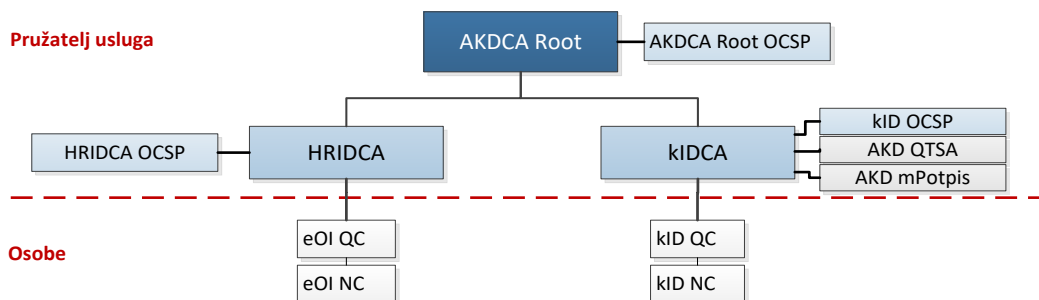
Dokument sadrži:

- poglavlje 1: podaci o sudionicima i uporabi certifikata,
- poglavlje 2: informacije koje objavljuje pružatelj usluga povjerenja,
- poglavlje 3: postupci provjere identiteta i identifikacijskih podataka osobe,
- poglavlje 4: postupci vezani uz izdavanje i upravljanje životnim ciklusom certifikata,
- poglavlje 5: fizičke, organizacijsko-upravljačke i provedbene mjere zaštite i postupci koji se provode u svrhu zaštite sustava izdavanja certifikata,
- poglavlje 6: tehničke mjere zaštite certifikata, privatnog ključa i informacijskih sustava,
- poglavlje 7: sadržaj certifikata i CRL,
- poglavlje 8: nadzor i provjera usklađenosti koja se provodi nad pružanjem usluga certificiranja
- poglavlje 9: ostale poslovne i pravne odredbe vezane uz pružatelja usluga povjerenja i usluge povjerenja koje on pruža.

1.1.2. Opseg dokumenta

Pravila navedena u ovom dokumentu primjenjuju se na hijerarhijsku PKI infrastrukturu zasnovanu na krovnom certifikacijskom tijelu AKDCA Root koji izdaje certifikate podređenim certifikacijskim tijelima HRIDCA i KIDCA.

Slika 1: Hijerarhijski model AKD PKI



AKD izdaje kvalificirane (QC) i normalizirane elektroničke certifikate (NC) te pruža uslugu izdavanja kvalificiranih elektroničkih vremenskih žigova i uslugu kreiranja udaljenog elektroničkog potpisa i pečata u ime potpisnika odnosno autora pečata.

HRIDCA izdaje certifikate isključivo za potrebe izdavanja eOI.

KIDCA izdaje certifikate za komercijalnu namjenu i za potrebe servisa koji izdaje kvalificirane elektroničke vremenske žigove.

KIDCA izdaje i kvalificirane certifikate koji se koriste u servisu AKD mPotpis koji upravlja udaljenim QSCD uređajem za izradu udaljenog elektroničkog potpisa i pečata u ime potpisnika i autora pečata.

Usluga izdavanja kvalificiranih elektroničkih vremenskih žigova nije u opsegu usluga certificiranja predviđenih ovim dokumentom. Pravila i opis pravila po kojima se izdaju kvalificirani elektronički vremenski žigovi dana su u AKD QTSA Pravilima i postupcima pružanja usluge vremenskog žiga (dalje u tekstu: TSP/PS) [56].

1.1.3. Namjena dokumenta

Ovaj dokument namijenjen je:

- osobama kojima su potrebne detaljnije informacije o njihovim vlastitim pravima i obvezama, kao i o pravima i obvezama pružatelja usluga povjerenja,
- pouzdajućim stranama za utvrđivanje prikladnosti pojedinog tipa certifikata za određenu namjenu, grupu osoba i/ili elektroničku uslugu,
- pružatelju usluga povjerenja koji će temeljem ovoga dokumenta za podređena certifikacijska tijela HRIDCA i KIDCA izraditi pravilnike o postupcima certificiranja (engl. Certification Practice Statement – CPS, [54] i [55], u daljnjem tekstu: pravilnik ili CPS) i pravila i postupke pružanja usluga vremenskog žiga – TSP/PS [56], u kojem će detaljnije specificirati postupke i mjere kojima će osigurati provedbu ovih sigurnosnih zahtjeva u praksi,
- tijelima za ocjenjivanje sukladnosti i nadzornim tijelima za procjenu sposobnosti AKD-a da pruža kvalificirane usluge povjerenja i da ima status kvalificiranog pružatelja usluge.

Sigurnosni zahtjevi definirani u ovome dokumentu usklađeni su sa strogim zahtjevima za kvalificirane pružatelje usluga povjerenja i kvalificirane usluge povjerenja koje oni pružaju, a koji su propisani Uredbom (EU) br. 910/2014 [1] i Zakonom o provedbi Uredbe (EU) br. 910/2014 [2].

1.2. Naziv dokumenta i identifikacija

1.2.1. Naziv dokumenta

Oznaka :	PRO-I-90-02
Naziv:	AKD PKI Opća pravila pružanja usluga certificiranja
Izdanje:	2.5
Datum objave:	01.07. 2021.
Autor:	AKD d.o.o.
Tip dokumenta:	Certificate Policy
Dostupnost:	http://eid.hr/cps i http://id.hr/cps

Povijest promjena dokumenta je navedena je u Prilogu 4.

1.2.2. Identifikacijska oznaka

Identifikacijska oznaka (OID) rezervirana od strane AKD je 1.3.6.1.4.1.43999.

Kvalificirani certifikati (QC) se izdaju po pravilima koja su ekvivalentna pravilima **QCP-n-qscd**, prema točki 5.3 ETSI EN 319 411-2 [17], a koja se primjenjuju za EU kvalificirane certifikate za fizičke osobe s privatnim ključem na kvalificiranom sredstvu za izradu elektroničkog potpisa (QSCD). Identifikacijska oznaka tih certifikata je:

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

Kvalificirani certifikati (QC) za pravne osobe se izdaju po pravilima koja su ekvivalentna pravilima **QCP-l-qscd**, prema točki 5.3 ETSI EN 319 411-2 [17], a koja se primjenjuju za EU kvalificirane certifikate za elektroničke pečate. Identifikacijska oznaka tih certifikata je:

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

Normalizirani certifikati (NC) se izdaju po pravilima koja su ekvivalentna pravilima **NCP+**, prema točki 5.3 ETSI EN 319 411-1 [16], a koja se primjenjuju za normalizirane certifikate s privatnim ključem na sigurnom kriptografskom uređaju.

Identifikacijska oznaka tih certifikata je:

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

Tablica 1: OID oznake certifikata

Naziv	Oznaka	OID
OCSP certifikati		
AKDCA Root OCSP certifikat	AKD NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.0.1.2.1.9
HRIDCA OCSP certifikat	eOI NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.2.1.2.1.9
KIDCA OCSP certifikat	KID NCP-l-scd-ocsp	1.3.6.1.4.1.43999.5.5.1.2.1.9
Certifikati za AKD TSA		
KIDCA TSU certifikat	KID QCP-l-scd-tsa	1.3.6.1.4.1.43999.5.4.1.2.2.8

Identifikacijske oznake, pravila, i opis pravila, po kojima certifikacijska tijela izdaju certifikate krajnjim korisnicima odnosno fizičkim osobama su dane u CPS pojedinog CA, [54] i [55].

Pravila i opis pravila prema kojima AKD postupa sa privatnim ključevima i pripadajućim certifikatima u AKD mPotpis servisu i udaljenom QSCD uređaju za kreiranje udaljenog kvalificiranog potpisa i pečata u ime potpisnika opisana su u CPS KIDCA [55].

Pravila i opis pravila po kojima se izdaju kvalificirani elektronički žigovi dana su u TSP/PS [56].

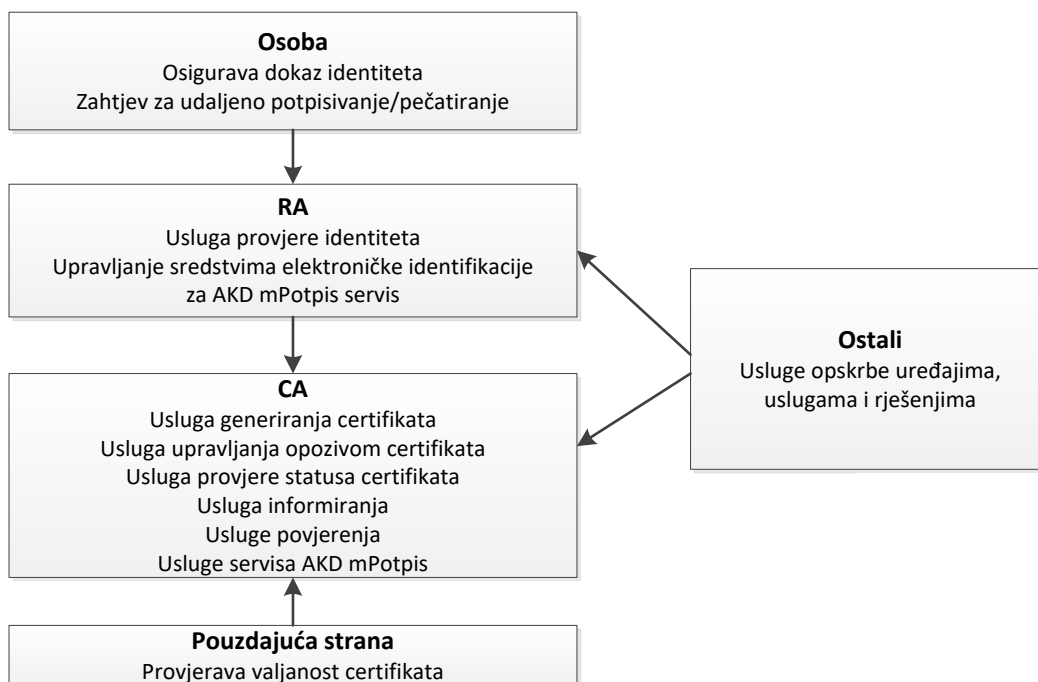
1.3. PKI sudionici

U kontekstu ovoga dokumenta, sudionici AKD PKI su:

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

Sudionici i usluge koje oni pružaju prikazani su na sljedećoj shemi.

Slika 2: Veza između sudionika



Informacije o odgovornostima svih sudionika se mogu naći u točki 9.6 ovog dokumenta te detaljnije u CPS pojedinog CA, [54] i [55].

Usluge AKD-a kao pružatelja servisa za serversko potpisivanje (SSASP) u servisu AKD mPotpis propisane su u KIDCA CPS [55].

1.3.1. *Certifikacijska tijelo – CA*

Certifikacijsko tijelo (u daljnjem tekstu: pružatelj usluga certificiranja ili CA) je tijelo uspostavljeno u AKD-u, koje je autorizirano od PMA da izdaje certifikate u skladu s općim pravilima i pravilnikom.

CA pruža sljedeće usluge povjerenja:

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

1.3.2. *Pružatelj servisa za serversko potpisivanje - SSASP*

AKD upravlja okruženjem AKD mPotpis za izradu udaljenog elektroničkog potpisa i udaljenog elektroničkog pečata. Certifikate koji se koriste u okruženju servisa za udaljeno potpisivanje i pečatanje izdaje KIDCA.

Okruženje AKD mPotpis omogućuje:

- a) **Generiranje privatnog ključa** (engl. signing key generation service) – generira privatne ključeve za potpis u udaljenom QSCD uređaju i prosljeđuje u KIDCA RA dokaz o provedenom uručenju osobi.
- b) **Povezivanje certifikata sa privatnim ključem** (engl. certificate linking service) – povezuje privatni ključ sa pripadajućim certifikatom izdanim od strane KIDCA.
- c) **Povezivanje autentikacijskog sredstva sa privatnim ključem** (engl. eID means linking service) – povezuje autentikacijski mehanizam sa privatnim ključem u svrhu pružanja osobi kontrole nad podacima za kreiranje udaljenog elektroničkog potpisa/pečata.
- d) **Aktiviranje podataka za kreiranje potpisa** (engl. signature activation service) – verificira podatke za aktivaciju potpisnih podataka i aktivira pripadajući privatni ključ za potpisivanje u svrhu kreiranja udaljenog elektroničkog potpisa.
- e) **Brisanje privatnog ključa** (engl. signing key deletion service) – trajno osiguravanje nemogućnosti korištenja potpisnog ključa.
- f) **Dostupnost autentikacijskih sredstava** (engl. eID means provision service) – omogućuje osobama korištenje dozvoljenih autentikacijskih sredstava za pristup AKD mPotpis servisu. AKD omogućuje osobama korištenje dvofaktorskih autentikacijskih

sredstava i mehanizama za pristup AKD mPotpis servisu registriranih u AKD IDP odnosno KID IDP sustavu ili nacionalnom NIAS sustavu.

1.3.3. Povjerenstvo za upravljanje pravilima certificiranja – PMA

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

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

PMA je odgovoran za definiranje, uvođenje i administriranje općih pravila pružanja usluga certificiranja (CP), uvjeta korištenja usluga certificiranja (PDS), pravilnika o postupcima certificiranja (CPS) te sigurnosno operativnih procedura i provedbenih dokumenata vezanih uz djelovanje AKD PKI i pružanje usluga povjerenja.

1.3.4. Registracijsko tijelo – RA

Registracijsko tijelo (u daljnjem tekstu: pružatelj usluga registracije ili RA) pruža usluge registracije osoba odnosno provjerava identitete i identifikacijske podatke osobe temeljem kojih CA izdaje, obnavlja, opoziva i suspendira certifikate.

Poslovi RA su:

- a) informiranje osoba o postupcima registracije i izdavanja certifikata,
- b) zaprimanje zahtjeva za izdavanje, opoziv i suspenziju certifikata,
- c) utvrđivanje identiteta osoba i podnositelja zahtjeva,
- d) sklapanje Ugovora o pružanju usluga certificiranja,
- e) uručivanje certifikata odnosno uređaja s privatnim ključem (QSCD).

AKD može:

- a) samostalno provoditi aktivnosti RA ili
- b) delegirati trećoj strani provedbu svih ili nekih poslova RA.

Ako su svi ili neki poslovi RA delegirani trećoj strani, treća se strana mora ugovorom obvezati da će ispuniti sljedeće zahtjeve:

- a) osigurati da je identitet službenika ovlaštenih za obavljanje poslova registracije nedvojbeno utvrđen te da je takvo osoblje pouzdano i savjesno,
- b) provoditi kontrole vezane uz osoblje ovlašteno za obavljanje poslova registracije u skladu s točkom 5.3 ovog dokumenta,
- c) čuvati dokumentaciju i informacije prikupljene u postupku registracije u skladu s točkom 5.5,
- d) provoditi poslove registracije na način koji je opisan u poglavlju 3,

- e) obvezati se na pridržavanje općih pravila i pravilnika ili osigurati vlastite dokumentirane procedure o provedbi usluge registracije temeljem kojih će nadzorna tijela moći obaviti nadzor i provjeru sukladnosti sa zahtjevima normi.

Osim navedenih poslova RA poslovi pojedinog CA mogu obuhvaćati i druge poslove, detaljnije opisano u CPS pojedinog CA, [54] i [55].

1.3.5. Osobe

Osoba može biti fizička osoba ili pravna osoba.

Fizička Osoba koja se u certifikatu imenuje kao subjekt certificiranja (engl. Subject) može biti:

- a) fizička osoba koja djeluje u svoje osobno ime ili
- b) fizička osoba koja je povezana sa organizacijom.

Kada je subjekt certificiranja fizička osoba tada fizička osoba prihvaća sve obveze i odgovornosti koje su navedene u točki 9.6.4.

Kada je subjekt certificiranja fizička osoba koja je povezana s organizacijom, organizacija je naručitelj i ispunjeni su zahtjevi iz točke 3.2.2 CPS pojedinog CA, [54] i [55], tada se s organizacijom sklapa ugovor i dio odgovornosti navedenih u točki 9.6.4 preuzima organizacija.

Za certifikate za elektronički pečat u certifikatu se imenuje pravna osoba kao subjekt certificiranja (engl. Subject).

Pravna osoba koja izrađuje elektronički pečat je autor pečata.

Ovlašteni predstavnik je osoba ovlaštena za zastupanje pravne osobe i/ili autora pečata ili treća osoba sa punomoći osobe ovlaštene za zastupanje pravne osobe.

Ovlaštenom predstavniku uručuju se izdani certifikati na QSCD i/ili registracijski kodovi za registraciju certifikata za udaljeni pečat u servisu AKD mPotpis te on/ona u ime autora pečata prihvaća primjenjive AKD-ove „Uvjete pružanja usluga certificiranja za pravne osobe“.

Osobe naručitelji (engl. Subscriber) su fizičke osobe ili organizacije koje su podnijele zahtjev za izdavanje certifikata, te su ujedno i vlasnici certifikata.

1.3.6. Pouzdajuće strane

Pouzdanje strane su fizičke ili pravne osobe koje pružaju elektroničke usluge i koje djeluju temeljem razumnog pouzdanja u certifikat i pružatelja usluga povjerenja.

AKD prepoznaje uloge i odgovornosti proizvođača i dobavljača s kojima je sklopio ugovor, a koji isporučuju opremu ili sudjeluju u provedbi usluga povezanih sa PKI.

1.3.7. Ostali

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

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

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

Udaljeni QSCD uređaj je sukladan zahtjevima ISO/IEC 15408 [44] Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5 i prema pravilima definiranim u Prilogu II Uredbe (EU) br. 910/2014 [1].

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

QSCD uređaj je sukladan ISO/IEC 15408 [44] Common Criteria (CC) v3.1 Information Technology Security Evaluation Assurance Level EAL4+ augmented with AVA_VAN.5, ALC_DVS.2 i prema pravilima definiranim u Prilogu II Uredbe (EU) br. 910/2014 [1].

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

- a) pripremu i proizvodnju sigurnih kriptografskih uređaja (kartice, odnosno QSCD) za osobe,
- b) generiranje parova kriptografskih ključeva osoba te njihov unos u sigurne kriptografske uređaje,
- c) distribuciju uređaja osobama i
- d) osigurava da je QSCD kvalificirano sredstvo za izradu elektroničkog potpisa/pečata (engl. Qualified Electronic Signature Creation Device – QSCD) sukladno CC EAL4+.

1.4. Uporaba certifikata

1.4.1. Primjerene uporabe certifikata

Prema svojoj namjeni, certifikati su podijeljeni u sljedeće grupe:

- a) **CA Certifikati** koje koristi pružatelj usluga za potpisivanje certifikata i CRL.

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

Ova grupa obuhvaća:

- **AKD Root CA** certifikat kojim su potpisani certifikati podređenih CA: HRIDCA i KIDCA,
 - **HRIDCA certifikat** kojim su potpisani certifikati izdani osobama za eOI i
 - **KIDCA certifikat** kojim su potpisani certifikati izdani za komercijalnu namjenu,
- b) **OCSP Certifikat** koje koristi pružatelj usluga za potpisivanje OCSP odgovora. Svako certifikacijsko tijelo izdaje svoj OCSP certifikat.
 - c) **TSU Certifikati** koje koristi pružatelj usluga vremenskog žiga za potpisivanje odgovora. TSU certifikat izdaje KIDCA certifikacijsko tijelo isključivo za vlastite potrebe AKD QTSA usluge.

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

- d) **eOI certifikati** koje izdaje HRIDCA krajnjim korisnicima u skladu s Zakonom o osobnoj iskaznici [13]. Primjerena uporaba eOI certifikata eOI opisana je u pravilniku HRIDCA CPS [54].
- e) **KID certifikati** koje izdaje KIDCA krajnjim korisnicima uz naknadu, te punoljetnim korisnicima eOI u skladu s izmjenama i dopunama Zakona o osobnoj iskaznici (NN 144/20) [13]. Primjerena uporaba certifikata KID certifikata opisana je u KIDCA Pravilniku o postupcima certificiranja [55].

Namjena certifikata navedena je u X.509 v3 ekstenzijama certifikata „Key Usage“ i „Extended Key Usage“.

1.4.2. Zabranjene uporabe certifikata

Zabranjena je svaka uporaba certifikata koja nije navedena u točki 1.4.1.

Osobe i pouzdajuće strane trebaju biti svjesne namjene certifikata i ograničenja koja su vezana uz korištenje pojedinog tipa certifikata.

Pri provjeri valjanosti certifikata koja je opisana u točki 9.6.5 ovog dokumenta, pouzdajuće strane trebaju provjeriti OID certifikata iz točke 1.2.2 kako bi donijele valjanu odluku o prihvaćanju ili odbacivanju certifikata za određenu namjenu.

1.5. Administracija dokumenta

1.5.1. Organizacija odgovorna za održavanje dokumenta

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

1.5.2. Kontakt podaci

Poštanska adresa:

AKD d.o.o.

Povjerenstvo za upravljanje pravilima certificiranja

Savska cesta 31

10000 Zagreb

Hrvatska

e-mail: pma@akd.hr

web: <http://eid.hr>, <http://id.hr>

1.5.3. Ocjenjivanje usklađenosti dokumenta

PMA je odgovoran za ocjenjivanje usklađenosti dokumenta s nacionalnom i EU regulativom te tehničkim specifikacijama, normama i postupcima vezanim uz elektroničku identifikaciju i usluge povjerenja.

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

1.5.4. Postupak odobravanja dokumenta

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

Glavni direktor odobrava objavu općih pravila i pravilnika.

1.6. Definicije i kratice

Definicije pojmova i kratice koji se koriste u ovome dokumentu, a koji su navedeni u prilogu 1 i prilogu 2 ovoga dokumenta, usklađeni su s Uredbom (EU) br. 910/2014 [1], ETSI EN 319 411-1 [16], ETSI EN 319 411-2 [17] te ETSI EN 319 422 [23] i ostalim obvezujućim normama i dokumentima.

2. Repozitorij i objavljivanje informacija

2.1. Repozitorij

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

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

Adrese na kojima su dostupni CA certifikati te CRL i OCSP usluge za provjeru statusa certifikata se mogu naći u svakom certifikatu.

U strukturi javnog imenika sadržani su certifikati izdani od podređenih CA, a javnosti mogu biti dostupni pod uvjetima navedenim u točki 2.4.

2.2. Portal za objavljivanje informacija

Sve informacije koje su potrebne osobama i pouzdajućim stranama za korištenje usluga povjerenja objavljuju se na portalima pružatelja usluga povjerenja; na <http://eid.hr> za certifikate koje izdaje HRIDCA odnosno na <http://id.hr> za certifikate koje izdaje KIDCA.

Osnovne informacije koje se objavljuju na portalu obuhvaćaju, ali se ne ograničavaju na:

- a) Opća pravila pružanja usluga (CP),
- b) Pravilnici o postupcima certificiranja (CPS, [54] i [55]),
- c) Uvjeti pružanja usluga certificiranja (PDS),
- d) obavijesti vezane uz pružanje usluga certificiranja i
- e) ostale informacije koje su relevantne za osobe i pouzdajuće strane.

CA će registriranim osobama omogućiti dodatne informacije i usluge kao što su:

- a) informacije i aplikacije za korištenje uređaja (QSCD),
- b) informacije i aplikacije za korištenje AKD mPotpis servisa i za upravljanje dvofaktorskim identifikacijskim sredstvima za pristup AKD mPotpis servisu i

- c) usluga neposredne provjere statusa i suspenzije certifikata.

2.3. Vrijeme objavljivanja i učestalost objave informacija

Vrijede pravila:

- a) Informacije na portalu dostupne su odmah nakon njihovog formalnog odobrenja.
- b) Svi sadržaji na portalu su na hrvatskom jeziku, a dio sadržaja može biti dostupan i na engleskom jeziku.
- c) Opća pravila, pravilnici [54] i [55] i uvjeti pružanja usluga certificiranja dostupni su na hrvatskom i na engleskom jeziku.
- d) U slučaju nepodudaranja u sadržaju dokumenata na engleskom jeziku sa sadržajem dokumenata na hrvatskom jeziku, važeća je verzija dokumenta na hrvatskom jeziku.
- e) Podaci vezani za status certifikata u repozitoriju se objavljuju nakon njihovog izdavanja
- f) Informacije o statusu certifikata dostupne su pod uvjetima navedenim u točki 4.10.
- g) Učestalost objave CRL definirana je u točki 4.9.7.
- h) OCSP usluga za provjeru statusa izdanih certifikata dostupna je u skladu s točkom 4.9.10.
- i) CA je dužan osigurati stalnu raspoloživost repozitorija 24 sata na dan, 7 dana u tjednu u skladu s najboljim poslovnim praksama.
- j) Nakon kvara sustava ili drugih čimbenika koji nisu pod kontrolom CA, potrebno je primijeniti sva raspoloživa sredstva kako bi se osigurao oporavak sustava u najkraćem mogućem roku.

2.4. Kontrole pristupa repozitoriju

Vrijede pravila:

- a) Osnovne informacije na portalu dostupne su javnosti bez ograničenja.
- b) Dodatne informacije i usluge na portalu dostupne su samo registriranim osobama.
- c) CA ne postavlja nikakva ograničenja vezano uz korištenje CRL i OCSP usluga.
- d) Certifikati osobe mogu biti dostupni javnosti za pretraživanje ako je osigurana suglasnost osobe. Suglasnost se daje sukladno pravilima propisanim u CPS pojedinog CA, [54] i [55].
- e) CA zadržava pravo poduzimanja odgovarajućih mjera zaštite repozitorija i portala od zlouporabe.

3. Identifikacija i autentikacija

3.1. Određivanje imena

3.1.1. Tipovi imena

U svakom certifikatu su u polju „Subject“ upisani podaci o imenu osobe.

Ime certifikata određuje se u skladu s preporuci ITU-T X.520 [51] ili IETF RFC 5280 [39].

Pri određivanju polja „Subject“, primjenjuju se pravila navedena u preporuci ITU-T X.501 [52].

Za certifikate koji sadrže polje „Subject Alternative Name“, primjenjuju se pravila koja su navedena u preporuci IETF RFC 5280 [39].

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

commonName:	Ime CA certifikata, OCSP usluge ili TSA usluge
organizationIdentifier:	Identifikator pravne osobe – pružatelja usluge povjerenja
organizationName:	Ime pravne osobe – pružatelja usluge povjerenja
countryName:	ISO kod države

Za certifikate fizičkih osoba polje „Subject“ formira se sukladno pravilima koja su definirana u CPS pojedinog CA, [54] i [55].

Za certifikate koji se izdaju pravnim osobama za komercijalnu namjenu polje „Subject“ formira se sukladno pravilima koja su definirana u KIDCA CPS [55].

3.1.2. Smislenost imena

Imena u polju „Subject“ moraju biti smisljena i trebaju omogućiti utvrđivanje identiteta fizičke ili pravne osobe.

3.1.3. Anonimnost i pseudonimi osobe

Nije podržano.

3.1.4. Pravila tumačenja imena

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

Tablica 2: Pravila tumačenja imena CA i OCSP certifikata

Pravne osobe (CA, TSU i OCSP certifikati)	
Polje	Pojašnjenje
CommonName (cn)	Ime CA ili OCSP ili TSA sustava
organizationName (O)	Ime pravne osobe - pružatelja usluga povjerenja
organizationIdentifier	VATHR-OIB gdje je VAT oznaka da se radi o pravnoj osobi, HR kod države, znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) i OIB porezni identifikacijski broj pravne osobe
countryName (C)	Dvoslovni ISO kod države pružatelja usluga povjerenja (HR)

Pravila tumačenja imena za certifikate fizičkih osoba navedena su u sljedećim tablicama.

Tablica 3: Pravila tumačenja imena fizičkih osoba

Fizičke osobe		
Polje	Tip certifikata	Pojašnjenje
CommonName (cn)	Korisnički	Ime i prezime fizičke osobe iz identifikacijske isprave
serialNumber	Korisnički	3 znaka za tip reference identiteta osobe, dvoslovni ISO kod države, znak minus "-", identifikacijski broj, npr: PNOHR-OIB, sukladno točki 5.1.3 ETSI EN 319 412-1 [18]
givenName (g)	Korisnički	Ime fizičke osobe subjekta certificiranja
Surname (sn)	Korisnički	Prezime fizičke osobe subjekta certificiranja
organizationalUnitName (OU)	Korisnički	Tip certifikata (RSignature za udaljeni potpisni, Sigature za potpisni ili Identification za Identifikacijski)
organizationName (O)	HRIDCA korisnički	Naziv CA koji izdaje certifikat
	KIDCA korisnički	Naziv organizacije s kojom je fizička osoba povezana
organizationIdentifier	HRIDCA korisnički	Ne koristi se.
	KIDCA korisnički	VATHR-OIB gdje je VAT oznaka da se radi o pravnoj osobi, HR kod države, znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) i OIB porezni identifikacijski broj organizacije, za fizičke osobe povezane s organizacijom
countryName (C)	Korisnički	Dvoslovni ISO kod države osobe subjekta certificiranja

Tablica 4: Pravila tumačenja imena pravnih osoba (elektronički pečat)

Pravne osobe (elektronički pečat)		
Polje	Tip certifikata	Pojašnjenje
CommonName (cn)	KIDCA korisnički	Naziv certifikata za pečat kojim se pravna osoba, autor pečata, predstavlja.
organizationalUnitName (OU)	KIDCA korisnički	Tip certifikata (Seal ili RSeal (za udaljeni certifikat))
organizationName (O)	KIDCA korisnički	Naziv pravne osobe, autora pečata

organizationIdentifier	KIDCA korisnički	VATHR-OIB gdje je VAT oznaka da se radi o pravnoj osobi, HR kod države, znak minus "-" (0x2D (ASCII), U+002D (UTF-8)) i OIB porezni identifikacijski broj pravne osobe
countryName (C)	KIDCA korisnički	Dvoslovni ISO kod države u kojoj je registrirana pravna osoba

3.1.5. Jedinstvenost imena

U polju „Subject“ svakog certifikata upisani su jedinstveni podaci o osobi kojoj se izdaje certifikat. Jedinstvenost imena fizičke osobe osiguran je atributom „serialNumber“, dok se jedinstvenost imena pravne osobe osigurava atributom „organizationIdentifier“.

3.1.6. Prepoznavanje, potvrđivanje identiteta i uloga zaštitnog znaka

Nije primjenjivo.

3.2. Inicijalno utvrđivanje identiteta

3.2.1. Metoda dokazivanja posjeda privatnog ključa

Vrijede pravila:

- Privatni ključevi svih fizičkih i pravnih osoba generiraju se u HSM uređaju te se zajedno s pripadnim certifikatima u sigurnom okruženju unose na kvalificirano sredstvo (QSCD) ili generiraju i koriste unutar udaljenog kvalificiranog sredstva za izradu elektroničkog potpisa (udaljeni QSCD).
- QSCD koji se isporučuje u posjed osobe s privatnim ključevima i certifikatima uručuje se osobi direktno nakon utvrđivanja njenog identiteta.
- Registracijski kodovi za registraciju certifikata i postavljanje aktivacijskih podataka u servisu AKD mPotpis za privatne ključeve kojima upravlja kvalificirani pružatelj usluge povjerenja u ime potpisnika ili autora pečata dostavljaju se fizičkoj osobi ili ovlaštenom predstavniku pravne osobe prema proceduri opisanoj u KIDCA CPS [55].
- Privatni ključevi CA, OCSP i TSU certifikata se pod kontrolom autoriziranih osoba CA generiraju u SCD uređaju u sigurnom okruženju i tamo ostaju tijekom njihovog korištenja.

3.2.2. Potvrda identiteta pravnih osoba

U postupku registracije pravne osobe moraju se prikupiti i provjeravati informacije o pravnoj osobi u skladu s nacionalnim pravom RH te u skladu s točkom 6.2.2 norme ETSI EN 319 411-2 [17].

3.2.3. Potvrda identiteta fizičkih osoba

Pri izdavanju certifikata RA provjerava identitet i, ako je to primjenjivo, posebna obilježja fizičke osobe kojoj se izdaje certifikat, a u skladu s nacionalnim pravom RH.

Primjenjuju se pravila potvrđivanja identiteta fizičkih osoba u skladu s točkom 6.2.2 norme ETSI EN 319 411-2 [17].

3.2.4. Informacije o osobama koje se ne provjeravaju

RA/LRA ne provjerava dodatne informacije za kontakt već je za njihovu točnost odgovorna osoba.

3.2.5. Provjera ovlasti

Primjenjuju se relevantna pravila koja su definirana u CPS pojedinog CA, [54] i [55].

3.2.6. Kriteriji za interoperabilnost

Nije određeno.

3.2.7. Ostale odredbe prilikom utvrđivanja identiteta

Postupci koji se primjenjuju prilikom utvrđivanja identiteta detaljno su opisani u CPS pojedinog CA, [54] i [55].

3.3. Identifikacija i autentikacija kod obnove certifikata

3.3.1. Identifikacija i autentikacija kod redovite obnove certifikata

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

3.3.2. Identifikacija i autentikacija kod izdavanja novog para ključeva

Vrijede pravila:

- a) Kod izdavanja novog para ključeva mogu se koristiti informacije i dokumenti koji su osigurani tijekom inicijalnog utvrđivanja identiteta prema točki 3.2.3.
- b) Provjera informacija vrši na isti način kao kod inicijalnog utvrđivanja identiteta u točki 3.2.3.
- c) Potrebno je voditi računa da su informacije i dokumenti koji su prikupljeni kod inicijalnog utvrđivanja identiteta još uvijek valjani te da se obnove kada je to potrebno.

3.4. Identifikacija i autentikacija kod opoziva certifikata

Identifikacija i autentikacija kod opoziva se provode u skladu s točkom 6.2.4 norme ETSI EN 319 411-2 [17].

4. Provedbeni zahtjevi vezani uz životni ciklus certifikata

4.1. Podnošenje zahtjeva za izdavanje certifikata

4.1.1. *Tko može podnijeti zahtjev za izdavanje certifikata*

Zahtjev za izdavanje certifikata može podnijeti:

- a) fizička osoba koja je imenovana kao subjekt certifikata,
- b) zakonski zastupnik organizacije s kojom je osoba subjekt certificiranja povezana,
- c) ovlašteni predstavnik autora pečata ili
- d) autorizirano osoblje CA za CA, OCSP i TSU certifikate.

Pravila za podnošenje zahtjeva su detaljnije definirana u CPS pojedinog CA, [54] i [55].

4.1.2. *Postupak podnošenja zahtjeva za izdavanje certifikata*

Pravila za podnošenje zahtjeva su detaljnije definirana u CPS pojedinog CA, [54] i [55].

4.2. Obrada zahtjeva za izdavanje certifikata

4.2.1. *Provedba identifikacije i autentikacije*

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

Za fizičke osobe koje su povezana s organizacijom, dodatno se provodi postupak potvrđivanja identiteta pravne osobe kako je navedeno u točki 3.2.3.

Identitet pravnih osoba potvrđuje se u postupcima koji su navedeni u točki 3.2.2.

4.2.2. *Odobranje ili odbijanje zahtjeva za izdavanje certifikata*

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

4.2.3. *Vrijeme obrade zahtjeva za izdavanje certifikata*

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

4.3. Postupak izdavanja certifikata

4.3.1. *Postupci tijekom izdavanja certifikata*

Tijekom izdavanja certifikata moraju se primjenjivati postupci u skladu s točkom 6.3.3 norme ETSI EN 319 411-1 [16].

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

4.3.2. *Obavješćivanje o izdavanju certifikata*

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

4.4. Preuzimanje certifikata

4.4.1. *Provedba postupka prihvaćanja certifikata*

Postupci prihvaćanja certifikata se provode u skladu s točkom 6.3.4 norme ETSI EN 319 411-2 [17].

Primjenjuju se pravila koja su definirana u CPS pojedinog CA, [54] i [55].

4.4.2. *Objava certifikata od strane CA*

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

4.4.3. *Obavješćivanje drugih strana o izdavanju certifikata*

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

4.5. Korištenje ključeva i certifikata

4.5.1. *Osobe*

Privatni ključevi su isključivo pod kontrolom fizičke osobe koja je imenovana kao subjekt certificiranja ili ovlaštenog predstavnika pravne osobe kada je u certifikatu imenovana pravna osoba autor pečata.

Fizičke osobe i ovlašteni predstavnik pravne osobe su prihvatile uvjete pružanja usluga certificiranja te su se obvezale da će do kraja životnog ciklusa certifikata (vidu točku 4.9 ovog dokumenta) ispunjavati svoje obveze navedene u točki 9.6.4 ovog dokumenta.

Uvjeti pružanja usluga certificiranja sadrže:

- a) informacije o pružatelju usluga certificiranja, o opsegu usluga koje on pruža i o pravilima pružanja usluga,
- b) tipove, namjenu i ograničenja certifikata te način provjere certifikata,
- c) informacije o postupanju s autentikacijskim i PIN podacima za pristup servisu AKD mPotpis i korištenje privatnih ključeva i pripadajućih certifikata za udaljeni potpis ili pečat,
- d) obveze i odgovornosti fizičkih osoba, pružatelja usluga i pouzdajućih strana,
- e) poslovne informacije vezane uz jamstva, cijene i sl.,
- f) odredbe vezane uz zaštitu podataka i privatnosti,
- g) komunikacija, pritužbe, rješavanje sporova i
- h) primjenjivi ugovori, CP, CPS, zakoni i nadzor nad pružateljem usluga certificiranja.

4.5.2. *Pouzdajuće strane*

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

4.6. Obnova certifikata

4.6.1. Razlozi za obnovu certifikata

Certifikat treba obnoviti ako ističe period važenja certifikata.

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

4.6.2. Tko može zatražiti obnovu certifikata

Vrijede pravila iz točke 4.1.

4.6.3. Obrada zahtjeva za obnovu certifikata

Vrijede pravila iz točke 4.2.

4.6.4. Obavještanje osobe o obnovi certifikata

Vrijede pravila iz točke 4.3.

4.6.5. Provedba prihvatanja obnovljenog certifikata

Vrijede pravila iz točke 4.4.1.

4.6.6. Objavljivanje certifikata po obnovi certifikata

Vrijede pravila iz točke 4.4.2.

4.6.7. Obavještanje drugih strana o obnovi certifikata

Vrijede pravila iz točke 4.4.3.

4.7. Izdavanje novog para ključeva

4.7.1. Razlozi za izdavanje novog para ključeva

Novi par ključeva i novi certifikat će biti izdani:

- a) ako certifikat treba obnoviti (vidi točku 4.6) ili
- b) ako certifikat treba promijeniti (vidi točku 4.8) ili
- c) ako treba izdati novi certifikat nakon opoziva (vidi točku 4.9).

CA ne može reaktivirati opozvani certifikat već će se osobi izdati novi par ključeva i novi certifikat. Detaljnija pravila su definirana u CPS pojedinog CA, [54] i [55].

4.7.2. Tko može zatražiti izdavanje novog para ključeva

Vrijede pravila iz točke 4.1.

4.7.3. Obrada zahtjeva za izdavanje novog para ključeva

Vrijede pravila iz točke 4.2.

4.7.4. Obavještavanje osobe o izdavanju novog para ključeva

Vrijede pravila iz točke 4.3.

4.7.5. Provedba prihvatanja novog para ključeva

Vrijede pravila iz točke 4.4.1.

4.7.6. Objavljivanje certifikata po izdavanju novog para ključeva

Vrijede pravila iz točke 4.4.2.

4.7.7. Obavještavanje drugih strana o izdavanju novog para ključeva

Vrijede pravila iz točke 4.4.3.

4.8. Promjena certifikata**4.8.1. Razlozi za promjenu certifikata**

Razlozi za promjenu certifikata su:

- a) došlo je do promjene podataka koji su sadržani u certifikatu ili
- b) utvrđeno je da informacije sadržane u certifikatu nisu ispravne.

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

Dodatni razlozi i pravila su definirana u CPS pojedinog CA, [54] i [55].

4.8.2. Tko može zatražiti promjenu certifikata

Vrijede pravila iz točke 4.1.

4.8.3. Obrada zahtjeva za promjenu certifikata

Vrijede pravila iz točke 4.2.

4.8.4. Obavještavanje osobe o promjeni certifikata

Vrijede pravila iz točke 4.3.

4.8.5. Provedba prihvatanja promijenjenog certifikata

Vrijede pravila iz točke 4.4.1.

4.8.6. Objavljivanje certifikata po promjeni certifikata

Vrijede pravila iz točke 4.4.2.

4.8.7. Obavješćavanje drugih strana o promjeni certifikata

Vrijede pravila iz točke 4.4.3.

4.9. Opoziv i suspenzija certifikata

4.9.1. Koji su razlozi za opoziv certifikata

Razlozi za opoziv certifikata su:

- a) Podnesen je autorizirani zahtjev za opoziv certifikata.
- b) Prijavljena je promjena podataka u certifikatu odnosno došlo je do promjene u imenu ili identifikacijskom broju fizičke ili pravne osobe koji su sadržani u polju „Subject“ certifikata.
- c) Utvrđene su greške u podacima u certifikatu ili na tijelu QSCD uređaja tijekom obrade zahtjeva, izdavanja certifikata, personalizacije QSCD uređaja, personalizacije PIN omotnica ili drugih aktivnosti pružatelja usluga certificiranja, prije uručenja ili prihvaćanja certifikata.
- d) Prijavljen je gubitak, krađa ili kvar QSCD.
- e) Prijavljena je zlouporaba ili neautorizirano korištenje QSCD, privatni ključ ili aktivacijski podaci nisu u isključivom posjedu subjekta certificiranja ili ovlaštenog predstavnika ili uvijek kada je moguća kompromitacija privatnog ključa. Trajno je izgubljen PIN za aktivaciju privatnog ključa certifikata za udaljeno potpisivanje ili pečatiranje izdan u sklopu servisa AKD mPotpis.
- f) Prijavljen je prestanak povezanosti osobe subjekta certificiranja sa organizacijom.
- g) Utvrđen je prestanak važenja certifikata prije isteka perioda na koji je certifikat izdan zbog smrti osobe ili ako više ne postoji osnova po kojoj je izdan certifikat.
- h) Nastupile su izvanredne okolnosti i slučaj više sile, uključujući elementarne vremenske i prirodne nepogode, odron zemlje, poplave, požar, rat, vojne operacije, terorizam, upade u fizički prostor, upade u informacijski sustav ili građanske nemire.
- i) Sud, javno tužiteljstvo ili institucija koja provodi sudsku ili kriminalističku obradu zahtjeva opoziv certifikata kako bi se spriječilo kazneno djelo.
- j) Utvrđeno je da privatni ključ ne odgovara javnom ključu u certifikatu ili je naknadno utvrđeno da podaci u certifikatu nisu ispravni.
- k) Utvrđeno je da zahtjev za izdavanje certifikata nije bio autoriziran ili je naknadno povučen.
- l) Utvrđeno je da certifikat nije izdan u skladu s pravilnikom ili općim pravilima.
- m) CA certifikat je opozvan.

CA certifikat će biti opozvan u sljedećim situacijama:

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

- b) Utvrđena je kompromitacija CA privatnog ključa.
- c) Ako pružatelj usluga certificiranja zbog tehničkog, ugovornog ili bilo kojeg drugog razloga prestane izdavati certifikate ili prestane pružati usluge certificiranja.

Dodatni razlozi i pravila za opoziv certifikata mogu biti definirani u CPS pojedinog CA, [54] i [55].

4.9.2. Tko može zahtijevati opoziv certifikata

Opoziv certifikata može zahtijevati:

- a) fizička osoba koja je imenovana kao subjekt certifikata ili njen zakonski zastupnik,
- b) ovlaštenu predstavnik ili zakonski zastupnik u ime pravne osobe,
- c) autorizirani službenik RA/LRA,
- d) PMA, ili
- e) autorizirano osoblje CA.

4.9.3. Postupci kod podnošenja zahtjeva za opoziv certifikata

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

4.9.4. Vremenski period za podnošenje zahtjeva za opoziv

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

Dodatni kriteriji mogu biti definirani u CPS pojedinog CA, [54] i [55].

4.9.5. Vremenski period obrade zahtjeva za opoziv od strane CA

Obrada zahtjeva za opoziv certifikata se provodi u razumnom vremenu u skladu s CPS pojedinog CA, [54] i [55].

4.9.6. Provjera statusa certifikata

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

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

4.9.7. Učestalost izdavanja CRL

CRL se izdaje po sljedećim pravilima:

- a) Svaka CRL sadrži informaciju o vremenu izdavanja i o periodu važenja CRL.
- b) Podređeni CA se obvezuju da će CRL izdati barem 1 put u roku od 24 sata.
- c) Period važenja CRL koju izdaje podređeni CA je 24 sata od trenutka izdavanja CRL.
- d) Za AKDCA Root period važenja CRL je 90 dana od trenutka izdavanja CRL.
- e) U slučaju opoziva CA certifikata, AKDCA Root će izdati CRL u roku od 24 sata.

- f) Ako je istekao period važenja certifikata koji je opozvan i koji je na CRL, isti može biti maknut s CRL.
- g) Kako bi se osigurala dostupnost CRL u skladu s propisanim pravilima pravovremenost izdavanja CRL se nadzire.

4.9.8. Maksimalno kašnjenje objave CRL

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

4.9.9. Dostupnost on-line provjere statusa certifikata

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

OCSP odgovor mora biti u skladu s IETF RFC 6960 [36] i IETF RFC 5019 [41].

OCSP certifikat sadrži ekstenziju *id-pkix-ocsp-nocheck*, kako je definirano u IETF RFC 6960 [36].

4.9.10. Zahtjevi za on-line provjeru statusa certifikata

Omogućena je on-line provjera statusa certifikata putem OCSP usluge po pravilima opisanim u CPS pojedinog CA, [54] i [55], pri čemu se najmanje primjenjuje:

- a) OCSP usluga dostupna je preko protokola HTTP na adresi objavljenoj u polju „*Authority Information Access*“ svakog certifikata.
- b) Svaki odgovor OCSP usluge je elektronički potpisan certifikatom koji je izdan od istog CA koji je izdao certifikat za kojeg se traži provjera statusa certifikata.
- c) Ako OCSP usluga zaprimi zahtjev za provjeru statusa certifikata koji još nije izdan, tada neće odgovoriti sa statusom „*good*“.
- d) Odgovor OCSP usluge o statusu certifikata neće biti „*good*“ ako status CA certifikata nije provjeren ili ako CA certifikat nije valjan.
- e) Kako bi se osigurala dostupnost usluge u skladu s pravilima koja su navedena u ovom poglavlju, rad OCSP usluge se kontinuirano nadzire.

4.9.11. Ostali načini provjere

Ostali načini provjere mogu biti definirani u CPS pojedinog CA, [54] i [55].

4.9.12. Specifični zahtjevi vezani uz kompromitaciju ključeva

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

4.9.13. Razlozi za suspenziju certifikata

Razlozi za suspenziju certifikata osobe su:

- a) Podnesen je autorizirani zahtjev za suspenziju certifikata.
- b) Prijavljen je nestanak QSCD ili sumnja osobe na prestanak isključivog posjeda privatnog ključa ili aktivacijskih podataka.
- c) Postoji mogućnost da zahtjev za opoziv certifikata bude naknadno povučen.

- d) Nije moguće pravovremeno podnijeti zahtjev za opoziv certifikata zbog bilo kojeg razloga navedenog u točki 4.9.1.
- e) Nije moguće pravovremeno donijeti odluku o opozivu certifikata, a posljedice koje mogu nastati uslijed neopoziva certifikata nisu zanemarive.
- f) Nisu ispunjene ugovorne obaveze primatelja usluga certificiranja.

Razlozi za povlačenje suspenzije certifikata osobe su:

- g) Podnesen je autorizirani zahtjev za povlačenje suspenzije certifikata.
- h) Pronalazak QSCD ili prestanak razloga navedenih pod b).
- i) Prestanak razloga zbog kojeg je tražena suspenzija certifikata.

4.9.14. Tko može tražiti suspenziju certifikata

Zahtjev za suspenziju ili povlačenje suspenzije certifikata može zahtijevati:

- a) fizička osoba koja je imenovana kao subjekt certifikata ili njen zakonski zastupnik,
- b) ovlašteni predstavnik ili zakonski predstavnik pravne osobe autora pečata,
- c) autorizirani službenik RA/LRA,
- d) PMA i
- e) autorizirano osoblje CA.

4.9.15. Postupci kod podnošenja zahtjeva za suspenziju certifikata

Primjenjuju se postupci su definirani u CPS pojedinog CA, [54] i [55].

4.9.16. Ograničenje na trajanje suspenzije

U slučaju prestanka razloga za suspenziju certifikata navedenih u točki 4.9.13., moguće je zahtijevati povlačenje zahtjeva za suspenziju certifikata u roku definiranom u CPS pojedinog CA, [54] i [55].

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

Ako nije zahtijevano povlačenje suspenzije certifikata u definiranom roku, suspendirani certifikat će biti trajno opozvan.

4.10. Usluge provjere statusa certifikata

4.10.1. Operativna svojstva

Javne adrese za CRL i OCSP usluge provjere statusa certifikata su sadržane u svakom certifikatu. Usluge provjere statusa certifikata provode u skladu s točkom 6.3.10 norme ETSI EN 319 411-2 [17].

Primjenjuju se postupci definirani u CPS pojedinog CA, [54] i [55].

4.10.2. Dostupnost usluga

Primjenjuju se pravila koja su definirana u CPS pojedinog CA, [54] i [55], pri čemu se osigurava najmanje:

- a) Usluga zaprimanja zahtjeva za opoziv ili suspenziju certifikata uredima RA/LRA dostupna je u radno vrijeme.
- b) U redovnim uvjetima rada, zahtjev za suspenziju certifikata može se podnijeti elektroničkim putem, kontinuirano 24 sata na dan, 7 dana u tjednu.
- c) U redovnim uvjetima rada, dostupnost usluga CRL i OCSP provjere statusa certifikata je 24 sata na dan, 7 dana u tjednu.
- d) Kako bi se skratilo vrijeme obrade i provjere statusa certifikata preporuka je koristiti OCSP protokol.
- e) U slučaju ispada sustava, usluga će biti dostupna u najkraćem mogućem roku i u skladu s najboljim poslovnim praksama.

4.10.3. Opcionalna svojstva

Nije predviđeno.

4.11. Kraj životnog ciklusa certifikata

Certifikat će prestati važiti ako je :

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

4.12. Pohrana kod treće osobe i oporavak privatnog ključa

CA ne obavlja pohranu kod trećih osoba i oporavak privatnih ključeva osoba koji se nalaze na QSCD uređaju koji se uručuje u posjed osoba.

Privatni ključevi koji se koriste u sklopu servisa AKD mPotpis za udaljeno potpisivanje i pečatiranje pohranjuju se u sigurnom okruženju udaljenog QSCD uređaju sukladno pravilima definiranim u KIDCA CPS [55]. AKD ne omogućuje osobama oporavak privatnih ključeva koji se koriste u sklopu servisa AKD mPotpis.

5. Fizičke, organizacijsko-upravljačke i provedbene mjere zaštite

5.1. Mjere fizičke zaštite

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

Mjere fizičke sigurnosti primjenjuju se u skladu su s ETSI EN 319 401 [14] i s poglavljem 11 ISO/IEC 27002 [47].

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

5.1.1. Lokacija objekta i konstrukcija

Radi postizanja propisane razine sigurnosti, objekti i prostori u kojima je smješten informacijski sustav i u kojima se odvijaju aktivnosti pružanja usluga certificiranja ustrojavaju se u sigurnosne zone.

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

Produkcijski CA sustavi smješteni su u zoni visoke sigurnosti gdje se primjenjuju najstrože fizičke, tehničke i proceduralne mjere zaštite.

5.1.2. Fizički pristup

Fizički pristup objektima i prostorima u kojima se smješta informacijska infrastruktura i u kojima se odvijaju aktivnosti generiranja i opoziva certifikata kontroliran je i nadziran, a pravo pristupa ograničeno je na ovlašteno osoblje.

Pristup prostorima zone visoke sigurnosti provodi se isključivo uz istovremenu prisutnost najmanje dvije autorizirane osobe.

5.1.3. Sustavi za klimatizaciju i napajanje

Prostori u kojima se smješta informacijska infrastruktura su propisno klimatizirani, a sva oprema je spojena na izvor neprekinutog napajanja.

5.1.4. Opasnost od poplave

Poduzimaju se odgovarajuće mjere zaštite od poplave.

5.1.5. Protupožarna zaštita

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

5.1.6. Pohrana medija

Mediji s podacima, revizijskim zapisima, arhivske ili sigurnosne kopije podataka pohranjuju se u prostorima i sigurnosnim spremnicima koji se štite fizičkim i logičkim mjerama zaštite.

Kako bi se spriječilo neautorizirano otkrivanje, modifikacija, premještanje ili uništavanje informacija koje su pohranjeni na medijima, uspostavljene su sigurnosne mjere u skladu s poglavljem 8 ISO/IEC 27002 [47].

5.1.7. Uništavanje

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

5.1.8. Sigurnosne kopije na drugoj lokaciji

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

5.2. Organizacijsko-upravljačke mjere zaštite

Detaljnije informacije o organizacijsko upravljачkim mjerama zaštite dostupne su u pravilnicima.

5.2.1. Povjerljive uloge

Ovlaštenim radnicima koji sudjeluju u provedbi aktivnosti certificiranja dodijeljene su odgovarajuće povjerljive uloge s jasno definiranim odgovornostima i ovlaštenjima u skladu s normama ETSI EN 319 401 [14] i CEN TS 419 261 [32] i ETSI TS 119 431-1 [24] odnosno CEN EN 419 241-1 [33].

Povjerljive uloge CA osoblja uključuju, ali se ne ograničavaju na administratore sigurnosti, RA službenike, službenike za opoziv, administratore informacijskih sustava, operatere i kontrolore.

5.2.2. Broj osoba potrebnih za obavljanje aktivnosti

Princip dijeljenog znanja i dvojne kontrole uključen je u sve aktivnosti upravljanja kriptografskim ključevima i administriranje kritičnih informacijskih sustava.

5.2.3. Identifikacija i potvrđivanje identiteta za svaku ulogu

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

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

Provjera RA službenika obavlja se prema pravilima definiranim u CPS pojedinog CA, [54] i [55].

5.2.4. Uloge koje zahtijevaju odvajanje zaduženja

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

5.3. Provjera osoblja

Provjera osoblja provodi se u skladu s ETSI EN 319 401 [14] i poglavljem 7 ISO/IEC 27002 [47].

5.3.1. Kvalifikacije, radno iskustvo i sigurnosne provjere

Pri zapošljavanju radnika provodi se strogi selekcijski postupak sukladno dokumentiranim internim pravilima.

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

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

5.3.2. Postupak provjere prikladnosti radnika

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

Prije dodjeljivanja zaduženja osoblju CA i službenicima RA/LRA potrebno je provjeriti te nedvojbeno utvrditi identitet, sposobnost i pouzdanost radnika.

Osoblje koje sudjeluje u provedbi aktivnosti CA mora biti u stalnom radnom odnosu kod pružatelja usluga certificiranja.

Kada su poslovi registracijskog tijela delegirani trećoj strani, službenici RA/LRA moraju biti u radnom odnosu kod registracijskog tijela s kojim je AKD sklopio ugovor o pružanju usluga registracije.

5.3.3. Zahtjevi za obukom

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

Potrebno je osigurati interna pravila i upute te provoditi edukacije službenika RA/LRA i osoblja CA kako bi se osiguralo da su radnici upoznati sa svojim obvezama, da ih razumiju te da su svjesni svojih odgovornosti.

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

5.3.4. Periodična obnova znanja i obuka

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

Kako bi se osiguralo da su radnici upoznati sa svojim obvezama, da ih razumiju te da su svjesni svojih odgovornosti, provodi se informiranje radnika o pravilima rada, prilikom uvođenja novih internih pravila i kod značajnijih promjena, a najmanje jednom u dvije godine.

5.3.5. Periodična rotacija i provjera radnika

Osoblje CA kojem su dodijeljene povjerljive uloge vezane uz upravljanje kriptografskim ključevima svake se tri godine podvrgava ponovnoj procjeni prikladnosti prema točki 5.3.2.

5.3.6. Sankcije

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

5.3.7. Zahtjevi za vanjske suradnike

Vanjski suradnici ne sudjeluju u provedbi aktivnosti CA i nisu im dodijeljene povjerljive uloge. Zahtjevi za posjetitelje, konzultante i vanjske suradnike koji sudjeluju u provedbi održavanja sustava opisani su internim procedurama.

Registracijsko tijelo će osigurati i jamčiti dosljednu primjenu ovih općih pravila i pravilnika u određenim okolnostima kada vanjskim suradnicima dozvoli sudjelovanje u provedbi usluge registracije.

5.3.8. Dokumentacija dostupna radnicima

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

5.4. Upravljanje revizijskim zapisima

5.4.1. Tipovi događaja koji se zapisuju

Vrijede pravila:

- a) Revizijski zapisi moraju biti dostupni u elektroničkom obliku, a tamo gdje to nije moguće, potrebno je osigurati dokaze u tiskanoj formi.
- b) Revizijski zapisi uključuju, ali se ne ograničavaju na zapise o:
 - registraciji fizičke i pravne osobe, upravljanju životnim ciklusom certifikata uključujući izdavanje, opoziv, suspenziju i reaktivaciju certifikata,
 - upravljanju kriptografskim ključevima i QSCD,
 - rad servisa i usluga u sklopu pružanja usluga certificiranja,
 - administriranju i održavanju sustava.
- c) Revizijski zapisi moraju biti dostatni kako bi se mogao provoditi nadzor i kako bi se neovlaštena uporaba informacijskog sustava mogla adekvatno istražiti, ako za to nastane potreba.
- d) Revizijski zapisi moraju biti u prikladnom obliku kako bi se mogli interpretirati i prezentirati kao dokazi o ispunjenju sigurnosnih zahtjeva.
- e) Svi sustavi koji generiraju revizijske zapise raspolažu s pouzdanim izvorom vremena i osiguravaju važeću zabilješku datuma i vremena događaja.

Detaljnija pravila vezana uz tipove događaja koji se zapisuju opisana su u CPS pojedinog CA, [54] i [55].

5.4.2. Učestalost obrade revizijskih zapisa

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

Za manje kritične aktivnosti provodi se periodična kontrola.

5.4.3. Period čuvanja revizijskih zapisa

Revizijski zapisi za kritične sustave su kopirani, zaštićeni i sačuvani najmanje tri mjeseca on-line. Svi revizijski zapisi arhiviraju se u skladu s pravilima arhiviranja koja su opisana u točki 5.5.

5.4.4. Zaštita revizijskih zapisa

Revizijski zapisi se ne smiju brisati niti se smiju automatski zapisivati preko postojećih podataka. Revizijski zapisi su adekvatno zaštićeni i vjerodostojni te se mogu prezentirati kao materijalni dokazi u kasnijim eventualnim sudskim postupcima.

Zaštita revizijskih zapisa uključuje zaštitu od neautoriziranog čitanja, modifikacije, uništavanja i narušavanja integriteta.

5.4.5. Sigurnosne kopije revizijskih zapisa

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

Postupak povrata podataka iz sigurnosnih kopija je poznat, testiran i pouzdan, te se može provesti u razumnom vremenu.

5.4.6. Prikupljanje revizijskih zapisa

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

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

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

5.4.7. Obavješćivanje i alarmiranje

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

Ako su osobe uzrokovale bilježenje revizijskog zapisa u informacijskom sustavu, AKD će ih informirati samo kada je to nužno.

5.4.8. Procjena ranjivosti sustava

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

Ispitivanje i analiza ranjivosti informacijskog sustava provodi se periodično korištenjem odobrenih softverskih alata.

5.5. Arhiviranje zapisa

5.5.1. Tipovi zapisa koji se arhiviraju

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

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

Detaljnija pravila vezana uz tipove zapisa koji se arhiviraju opisana su u CPS pojedinog CA, [54] i [55].

5.5.2. Period čuvanja arhiviranih zapisa

Svi arhivirani podaci i dokumentacija navedena u točki 5.5.1 čuva se najmanje 10 godina nakon isteka valjanosti certifikata.

5.5.3. Zaštita arhive

Arhivirani podaci su adekvatno zaštićeni i vjerodostojni te se mogu prezentirati kao materijalni dokazi u kasnijim eventualnim sudskim postupcima.

Zaštita arhive uključuje zaštitu od neautoriziranog čitanja, modifikacije, uništavanja i narušavanja integriteta.

5.5.4. Postupci izrade sigurnosnih kopija arhive

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

Mediji s arhivskim podacima se povremeno provjeravaju te prepisuju na drugi medij kako bi se osigurala zaštita od starenja ili tehnološkog zastarijevanja.

5.5.5. Zahtjevi za zaštitu zapisa vremenskim žigom

Svi revizijski zapisi i arhiva imaju zabilježenu pouzdanu informaciju o datumu i vremenu.

5.5.6. Prikupljanje arhivske građe

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

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

5.5.7. *Postupci dobivanja i provjere arhiviranih podataka*

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

Pristup podacima iz arhive imaju samo autorizirane osobe.

Provjera podataka iz arhive uključuje provjeru zaštite izvornosti podataka.

5.6. Promjena CA ključa

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

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

- da period važenja svakog izdanog certifikata uvijek bude kraći od perioda važenja CA certifikata koji ga je izdao i
- da su kriptografski algoritmi i parametri uvijek prikladni za korištenje i u skladu s preporukama ETSI TS 119 312 [22].

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

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

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

5.7. Kompromitacija i oporavak

5.7.1. *Incidenti i postupci u slučaju kompromitacije*

U slučaju kvarova ili kompromitacije računalnih resursa, softvera i/ili podataka postupa se u skladu s poglavljem 16 ISO/IEC 27002 [47].

5.7.2. *Kvarovi računalnih resursa, softvera i/ili podataka*

Svi kvarovi računalnih resursa, softvera i/ili podataka se bilježe kao incidenti te se na njih pravovremeno i na adekvatan način reagira u skladu s internim sigurnosnim pravilima.

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

5.7.3. *Postupanje u slučaju kompromitacije*

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

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

- a) prestaje s izdavanjem certifikata na kompromitiranom CA sustavu,

- b) pokreće se postupak opoziva CA certifikata,
- c) pokreće se postupak opoziva certifikata osoba koje je izdao kompromitirani CA,
- d) informiraju se osobe i pouzdajuće strane putem portala,
- e) informira se RA odnosno treća strana kojoj su delegirani poslovi RA,
- f) informiraju se nadležna državna i nadzorna tijela i ostale zainteresirane strane,
- g) u slučaju sumnje da postoje elementi kaznenog djela izvješćuje se policija radi pokretanje istražnog postupka i
- h) pokreće se postupak generiranja novog CA ključa.

5.7.4. Upravljanje kontinuitetom poslovanja

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

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

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

Upravljanje kontinuitetom poslovanja se provodi u skladu s poglavljem 17 ISO/IEC 27002 [47].

5.8. Prestanak rada

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

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

- a) informirati sve sudionike o mogućem planiranom prestanku pružanja usluga certificiranja ili pojedinog servisa,
- b) ukinuti autorizacije i otkazati ugovore dobavljačima, vanjskom osoblju i delegiranim trećim stranama kojima je povjerena provedba poslova vezanih uz pružanje usluga,
- c) informirati nadležna državna tijela i konzultirati se o daljnjim postupcima koji će se poduzeti vezano uz prestanak pružanja usluga certificiranja,
- d) provesti tranziciju sustava na novog pružatelja usluga certificiranja kada je to potrebno i ako je moguće,
- e) nastaviti održavati ili predati prikupljenu dokumentaciju i arhivsku građu,
- f) prestati izdavati certifikate ili pružati pojedinu uslugu ili servis,
- g) propisno uništiti kriptografske ključeve i sve njihove kopije.

6. Tehničke mjere zaštite

Detaljnije informacije o tehničkim mjerama zaštite koje provodi pružatelj usluga dostupne su u pravilnicima.

6.1. Generiranje i dostava para ključeva

6.1.1. Generiranje ključeva

Vrijede pravila:

- a) Postupak inicijalnog generiranja para CA ključeva provodi se službenom ceremonijom generiranja CA ključeva koju organizira i nadzire PMA.
- b) Ceremonija se provodi u fizički sigurnom okružju u zoni visoke sigurnosti prema definiranoj proceduri i unaprijed pripremljenoj tehničkoj skripti.
- c) Ceremoniji prisustvuju radnici kojima su povjerene uloge (točka 5.2), interni i vanjski revizori, javni bilježnik te ostali pozvani svjedoci.
- d) Zapisnik o provedbi ceremonije generiranja CA ključa, video zapis ceremonije i sva pripadna dokumentacija koja uključuje tehničku skriptu i ispis CA javnog ključa, pohranjuju se u arhivi.
- e) Postupak generiranja ključeva i njihov unos u QSCD provodi se u fizički sigurnom okružju u zoni visoke sigurnosti.
- f) CA ključevi kao i ključevi osoba se generiraju, koriste i čuvaju u HSM uređaju koji implementira norme i upravljačke funkcije kako je navedeno u točki 6.2.1. vodeći računa da su kriptografski algoritmi i parametri uvijek prikladni za korištenje i u skladu s preporukama ETSI TS 119 312 [22].
- g) Ključevi certifikata za udaljeni potpis i udaljeni pečat se generiraju, čuvaju i koriste u HSM modulu koji implementira norme i upravljačke funkcije kako je navedeno u poglavlju 6.2.1., u sigurnom okruženju AKD mPotpis servisa za kreiranje udaljenog elektroničkog potpisa i pečata u ime potpisnika i autora pečata.

6.1.2. Dostava privatnog ključa osobama

Primjenjuju se postupci definirani u CPS pojedinog CA, [54] i [55].

6.1.3. Dostava javnog ključa CA-u

Dostava javnog ključa CA-u provodi se u skladu s točkom 6.5.1 norme ETSI EN 319 411-2 [17]. Primjenjuju se postupci su definirani u CPS pojedinog CA, [54] i [55].

6.1.4. Dostava javnog ključa CA pouzdajućim stranama

Javni ključevi CA dostupni su u certifikatima na web portalu (vidi točku 2.2).

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

6.1.5. Duljine ključeva

CA ključevi su duljine 4096 bita, RSA algoritam.

Ključevi OCSP i TSU su duljine 2048 bita, RSA algoritam.

Ključevi osoba i certifikata za elektronički pečat su duljine 2048 bita, RSA algoritam.

Duljine ključeva koji se koriste u servisu AKD mPotpis za udaljeno potpisivanje i pečatiranje definirane su u KIDCA CPS [55].

6.1.6. Generiranje i provjera kvalitete parametara javnog ključa

CA, OCSP i TSU ključevi kao i ključevi fizičkih i pravnih osoba generirani su korištenjem generatora slučajnih brojeva u HSM uređaju. Parametri javnog ključa za RSA algoritam su u skladu s normom FIPS 186-4 [43] ili drugom ekvivalentnom normom koju odobri PMA.

Općenito, za generaciju CA, OCSP i TSU ključeva te ključeva fizičkih i pravnih osoba koriste se kriptografski algoritmi i parametri u skladu s preporukama ETSI TS 119 312 [22].

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

CA, OCSP, TSU i korisnički X.509 v3 certifikati se izdaju u skladu s IETF RFC 5280 [39], a njihova namjena definirana je kroz vrijednosti ekstenzija „Key Usage“ i „Enhanced Key Usage“ kako je definirano u profilima certifikata (točka 7).

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

6.2. Zaštita privatnog ključa

6.2.1. Norme i upravljačke funkcije kriptografskog modula

CA, OCSP i TSU ključevi, kao i ključevi osoba generiraju se u HSM uređaju koji demonstrira sukladnost s FIPS PUB 140-2 level 3 [42] standardom.

AKD kombinira fizičke, logičke i proceduralne kontrole kako bi osigurao adekvatnu zaštitu HSM-a i privatnih ključeva.

Kada se privatni ključevi dostavljaju u posjed osobe subjekta certificiranja ili ovlaštenog predstavnika autora pečata, isti se nakon generiranja unose u kvalificirano sredstvo za izradu elektroničkog potpisa (QSCD) koje zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 [44] te demonstrira sukladnost s obrascima zaštite iz serije CEN EN 419 211 [26], [27], [28], [29], [30] i [31].

U slučajevima kada kvalificirani pružatelj usluga povjerenja upravlja podacima za izradu elektroničkih potpisa u ime osobe subjekta certificiranja ili autora pečata, isti se generiraju i koriste isključivo unutar HSM uređaja (udaljeni QSCD) u sklopu servisa AKD mPotpis koji zadovoljava zahtjeve EAL4+ augmented with AVA_VAN.5 prema ISO/IEC 15408 [44] i prema pravilima definiranim u Prilogu II Uredbe (EU) br. 910/2014 [1].

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

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

6.2.3. *Pohrana privatnog ključa*

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

Vrijede pravila:

- a) Nakon njihove generacije privatni ključevi CA, TSU i OCSP usluge ostaju pohranjeni u HSM uređaju i pod kontrolom barem 2 osobe.
- b) HSM particija u kojoj se čuva privatni ključ AKD Root CA aktivira se samo kada je to potrebno.
- c) Sustavi koji upravljaju s privatnim ključem podređenih CA su stalno dostupni i koriste se isključivo za potpisivanje certifikata osoba i CRL. Isto vrijedi i za pripadne OCSP sustave koji potpisuju odgovore na upit o statusu certifikata.
- d) Kriptografski ključevi izvan HSM uređaja mogu biti isključivo u šifriranom obliku u skladu s pravilima navedenim u točki 6.2.6.
- e) AKD ne vrši trajnu pohranu privatnih ključeva fizičkih/pravnih osoba u slučaju kada se certifikati izdaju na QSCD uređaju koji se uručuje u posjed osobama. Detaljna pravila za pohranu privatnih ključeva koji se koriste u AKD mPotpis servisu za udaljeno potpisivanje i pečatiranje opisana su u KIDCA CPS [55]

6.2.4. *Sigurnosno kopiranje privatnog ključa*

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

Sigurnosne kopije CA privatnih ključeva pohranjene su u sigurnosnom spremniku u prostoru sigurne zone kao i na sekundarnoj lokaciji gdje je osiguran isti ili veći nivo zaštite privatnog ključa. Privatni ključevi osoba se ne kopiraju.

6.2.5. *Arhiviranje privatnog ključa*

CA, OCSP i TSU privatni ključevi se ne arhiviraju. Privatni ključevi osoba također se ne arhiviraju.

6.2.6. *Prijenos privatnog ključa u kriptografski uređaj ili iz njega*

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

Prijenos privatnih ključeva osoba na QSCD uređaju koji se isporučuje u posjed osobama nije moguć.

Prijenos privatnih ključeva osoba u AKD mPotpis servisu za udaljeno potpisivanje i pečatiranje opisan je u KIDCA CPS [55].

6.2.7. *Čuvanje ključa u kriptografskom modulu*

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

Nakon proizvodnje QSCD uređaja koji se uručuje u posjed osobama, privatni ključ osoba u izvornom čitljivom obliku nalazi se samo unutar QSCD. Svoje privatne ključevi osobe mogu koristiti tek nakon što se provedu postupak aktivacije QSCD.

Čuvanje privatnog ključa kojim upravlja kvalificirani pružatelj usluga povjerenja u ime subjekta certificiranja ili autora pečata unutar servisa AKD mPotpis opisano je u KIDCA CPS [55].

Aktivacija privatnih ključeva na provodi se u skladu s točkom 6.2.8.

6.2.8. Metoda aktivacije privatnog ključa

Aktivacija privatnog CA ključa u HSM uređaju provodi se isključivo pod dvojnomo kontrolom ovlaštenih osoba

Jednom aktiviran CA, OCSP ili TSU privatni ključ, ostaje aktiviran sve dok je HSM uređaj uključen. Nakon isključivanja i ponovnog uključivanja HSM uređaja ponovo se provodi aktivacija privatnih ključeva.

Aktivacija privatnog ključa osobe provodi se jednokratno mehanizmom koji osigurava QSCD.

Aktivacija privatnih ključeva na QSCD moguća je tek nakon aktivacije samog QSCD uređaja.

Aktivacija privatnog ključa kojim upravlja kvalificirani pružatelj usluga povjerenja u ime subjekta certificiranja ili autora pečata provodi se dvofaktorskom autentikacijom na AKD mPotpis servis i PIN-om za aktivaciju privatnog ključa, u trenutku kreiranja elektroničkog potpisa ili elektroničkog pečata, opisano u KIDCA CPS [55].

6.2.9. Deaktivacija privatnog ključa

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

Privatni ključ osobe se deaktivira vađenjem QSCD iz čitača odnosno mehanizmom koji osigurava sam uređaj.

Deaktivacija privatnog ključa u servisu AKD mPotpis kojim upravlja kvalificirani pružatelj usluga povjerenja u ime subjekta certificiranja ili autora pečata provodi se automatski nakon kreiranja elektroničkog potpisa ili elektroničkog pečata, opisano u KIDCA CPS [55].

6.2.10. Postupci uništavanja kriptografskih ključeva

Uništavanje privatnog ključa CA vrši se provjerenom metodom koju osigurava proizvođač HSM uređaja.

Uništavanje privatnog ključa CA iz HSM uređaja vrši se:

- ako se HSM uređaj iznosi iz sigurne zone radi popravka ili zamjene opreme ili
- nakon isteka perioda važenja certifikata ili
- nakon prestanka rada CA, OCSP usluge ili TSA usluge.

Isto vrijedi i za privatni ključ OCSP i TSU.

Uništavanje datoteka s šifriranim privatnim ključevima osoba na informacijskom sustavu provodi se automatski nakon individualizacije i stavljanja privatnih ključeva osoba na QSCD.

Uništavanje privatnog ključa u AKD mPotpis servisu kojim upravlja kvalificirani pružatelj usluga povjerenja u ime subjekta certificiranja ili autora pečata provodi se provjerenom metodom koju osigurava proizvođač HSM uređaja. U slučaju kada je opozvan pripadajući certifikat za udaljeni potpis ili pečat provodi se automatski koristeći metodu koju osigurava proizvođač udaljenog HSM uređaja.

Uništavanje privatnog ključa uvijek se provodi provjerenom metodom koja jamči da se uništeni privatni ključ ni na koji način ne može oporaviti ili ponovo koristiti.

6.2.11. Ocjena kriptografskog modula

Vidjeti točku 6.2.1.

6.3. Ostali vidovi upravljanja kriptografskim ključevima

6.3.1. Arhiviranje javnog ključa

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

Primjenjuju se pravila arhiviranja koja su navedena u točki 5.5.

6.3.2. Period važenja certifikata i kriptografskih ključeva

Period važenja certifikata naveden je u sljedećoj tablici.

Tablica 5: Period važenja certifikata

Certifikat	Period važenja
Certifikat krovnog certifikacijskog tijela AKDCA Root	do 2038-01-19 03:14:07+00:00
Certifikat podređenih certifikacijskih tijela	15 godina
Certifikat za potpis OCSP odgovora	3 godine
Certifikat TSU, za potpis AKD QTSA odgovora	5 godina

Period važenja svakog certifikata je sadržan u svakom certifikatu. Certifikat je važeći od datuma izdavanja „Valid from” do datuma isteka perioda važenja “Valid to”.

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

Period važenja privatnog ključa jednak je periodu važenja korespondirajućeg certifikata.

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

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

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

Periodi važenja certifikata koje se izdaju fizičkim i pravnim osobama definirani su u CPS pojedinog CA, [54] i [55].

6.4. Aktivacijski podaci

6.4.1. *Generiranje i instalacija aktivacijskih podataka*

Aktivacijski podaci, generiranje i instalacija AKD CA privatnih ključeva su izvedeni prema korisničkim uputama HSM uređaja.

Aktivacijski podaci se koriste za zaštitu pristupa privatnim ključevima na QSCD.

Generiranje aktivacijskih podataka u HSM uređaju, njihov unos u QSCD i ispis u sigurnosne omotnice provodi se pod dvojnog kontrolom i u sigurnom okružju.

Aktivaciju QSCD i postavljenje PIN-ova za zaštitu privatnih ključeva na QSCD osobe provode samostalno prema uputi za aktivaciju QSCD koja je dostupna na portalu.

Kada kvalificirani pružatelj usluga povjerenja upravlja podacima za kreiranje elektroničkog potpisa ili pečata u ime osobe subjekta certificiranja ili autora pečata registracijski kodovi generiraju se i njima se upravlja u sigurnom okruženju AKD mPotpis servisa. Registracijski kodovi se koriste za registraciju certifikata te postavljanje PIN-a za korištenje privatnog ključa i dostavljaju se subjektu certificiranja ili ovlaštenom predstavniku autora pečata.

Primjenjuju se pravila koja su definirana u CPS pojedinog CA, [54] i [55].

6.4.2. *Zaštita aktivacijskih podataka*

Primjenjuju se pravila koja su definirani u CPS pojedinog CA, [54] i [55].

6.4.3. *Ostale odredbe o aktivacijskim podacima*

Ostale mjere zaštite aktivacijskih podataka i registracijskih kodova od gubitka, modifikacije, otkrivanja i neautoriziranog korištenja provode se u skladu s dokumentiranim internim procedurama.

Osobe su odgovorne za zaštitu aktivacijskih podataka i registracijskih kodova nakon što su im uručeni.

6.5. Mjere zaštite računalnih resursa

6.5.1. Posebni tehnički zahtjevi za računalnu sigurnost

Računalni resursi se štite mjerama sigurnosti prema ISO/IEC 27001 [46] i ISO/IEC 27002 [47] normama.

Pored toga, implementirani su tehnički zahtjevi vezani uz računalnu sigurnost u skladu s zahtjevima norme ETSI EN 319 401 [14], kao i sa zahtjevima koji su navedeni u CEN TS 419 261 [32] i te ETSI TS 119 431-1 [24] odnosno CEN EN 419 241-1 [33].

6.5.2. Ocjena računalne sigurnosti

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

6.6. Životni ciklus i tehničke kontrole

6.6.1. Upravljanje razvojem sustava

Upravljanje postupkom razvoja i cjelokupnim životnim ciklusom softvera provodi se u skladu s poglavljem 14 ISO/IEC 27002 [47].

6.6.2. Provjera upravljanja sigurnošću

Upravljanje računalnim resursima provodi se u skladu s poglavljem 12 ISO/IEC 27002 [47].

To obuhvaća ali se ne ograničava na:

- a) upravljanje zaštitom od virusa malicioznog koda i neautoriziranog softvera,
- b) spašavanje podataka i zaštita medija od uništenje, oštećenja i neautoriziranog pristupa,
- c) dugoročno čuvanje arhive i zapisa te zaštita od tehnološkog zastarijevanja,
- d) upravljanje autorizacijama,
- e) primjena sigurnosnih zakrpa i održavanje sustava u skladu s preporukama proizvođača i
- f) testiranje ranjivosti informacijskih sustava.

6.6.3. Provjera sigurnosti životnog ciklusa

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

Upravljanje poslovnim odnosima i dobavljačima provodi se u skladu poglavljem 15 ISO/IEC 27002 [47].

6.7. Kontrola mreže

Uspostavljene su kontrole mreže kako je definirano u poglavlju 13 ISO/IEC 27002 [47], prilogu B CEN TS 419 261 [32] te u skladu s ETSI TS 119 431-1 [24] odnosno CEN EN 419 241-1 [33].

6.8. Upotreba vremenskog žiga

Vrijeme u sustavu certificiranja AKD-a usklađeno je s UTC točnim vremenom. Revizijski zapisi AKD PKI sustava sadržavaju točan podatak o datumu i vremenu njihovog nastanka, uz odstupanje manje od +/- 1 s.

7. Sadržaj certifikata i CRL

7.1. Profili certifikata

Obrasci (profili) svih certifikata usklađeni su sa IETF RFC 5280 [39] i preporukama ITU-T X.509 [50].

Pri određivanju profila certifikata primjenjuju se sljedeće norme:

- ETSI EN 319 412-1 [18] općenito za sve certifikate,
- ETSI EN 319 412-2 [19] za fizičke osobe,
- ETSI EN 319 412-3 [20] za CA, OCSP i certifikate za pravne osobe (pečat) i
- ETSI EN 319 412-5 [21] za EU kvalificirane certifikate.

Profili za TSU certifikate usklađeni su sa normom ETSI EN 319 422 [23] i IETF RFC 3161 [40].

Osnovna polja svih certifikata navedena su u sljedećoj tablici.

Tablica 6: Osnovna polja svih certifikata

Polje	Vrijednost/Ograničenja vrijednosti
Version	X.509 V3, vidi točku 7.1.1
Serial Number	Jedinstven pozitivan broj s entropijom od 32 bit-a
Signature Algorithm	SHA256RSA, vidi točku 7.1.3.
Issuer DN	Vidi točku 7.1.4.
Valid from	utcTime
Valid to	utcTime(Valid from + period važenja certifikata u skladu s točkom 6.3.2).
Subject DN	Vidi točku 7.1.4.
Subject Public Key	Javni ključ subjekta
SignatureValue	Potpis izdavatelja certifikata, generiran i kodiran prema IETF RFC 5280 [39].

7.1.1. Broj verzije

Koristi se X.509 verzija V3.

7.1.2. Ekstenzije certifikata

7.1.2.1. Ekstenzije CA certifikata

Ekstenzije CA certifikata navedene su u sljedećoj tablici.

Tablica 7: Ekstenzije CA certifikata

Polje	Tip certifikata	Vrijednost
Key Usage*	All CA	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
Basic Constraints*	All CA	Subject Type=CA Path Length Constraint=None
Subject Key Identifier	All CA	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	All CA	Derived using the SHA-1 hash of the public key.
Authority Info Access	AKDCA Root	N/A
	HRIDCA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://eid.hr/cert/akdcaroot.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.eid.hr/akdcaroot
	KIDCA	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://id.hr/cert/akdcaroot.crt [2]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.id.hr/akdcaroot
Certificate Policies	AKDCA Root	N/A
	HRIDCA	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
	KIDCA	[1]Certificate Policy: Policy Identifier=All issuance policies [1,1]Policy Qualifier Info:

		Policy Qualifier Id=CPS Qualifier: http://id.hr/cps
CRL Distribution Points	AKDCA Root	N/A
	HRIDCA	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl1.eid.hr/akdcaroot.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.eid.hr/akdcaroot.crl [3]CRL Distribution Point Distribution Point Name: Full Name: URL= ldap://ldap.eid.hr/cn=AKDCA Root,o=AKD d.o.o.,c=HR?certificateRevocationList;binary (ldap://ldap.eid.hr/cn=AKDCA%20Root,o=AKD%20d.o.o.,c=HR?certificateRevocationList%3Bbinary)
	KIDCA	[1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl1.id.hr/akdcaroot.crl [2]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl2.id.hr/akdcaroot.crl [3]CRL Distribution Point Distribution Point Name: Full Name: URL= ldap://ldap.id.hr/cn=AKDCA Root,o=AKD d.o.o.,c=HR?certificateRevocationList;binary (ldap://ldap.id.hr/cn=AKDCA%20Root,o=AKD%20d.o.o.,c=HR?certificateRevocationList%3Bbinary)

*Kritično polje

7.1.2.2. Ekstenzije OCSP certifikata

Ekstenzije OCSP certifikata navedene su u sljedećoj tablici.

Tablica 8: Ekstenzije OCSP certifikata

Polje	Tip certifikata	Vrijednost
Key Usage*	All OCSP	Digital Signature (80)
Enhanced Key Usage	All OCSP	OCSP Signing (1.3.6.1.5.5.7.3.9)
Basic Constraints*	All OCSP	Subject Type=End Entity Path Length Constraint=None
Subject Key Identifier	All OCSP	Derived using the SHA-1 hash of the public key.
Authority Key Identifier	All OCSP	Derived using the SHA-1 hash of the public key.
Authority Info Access	AKDCA Root OCSP	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://eid.hr/cert/akdcaroot.crt
	HRIDCA OCSP	[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
	KIDCA OCSP	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://id.hr/cert/kidca.crt
Certificate Policies	AKDCA Root OCSP	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.0.1.2.1.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://eid.hr/cps
	HRIDCA OCSP	[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=CPS Qualifier: http://eid.hr/cps
	KIDCA OCPS	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1.43999.5.5.1.2.1.9 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://id.hr/cps
OCSP No Revocation Checking	All OCSP	id-pkix-ocsp-nocheck 05 00 (1.3.6.1.5.5.7.48.1.5)

*Kritično polje

7.1.2.3. **Ekstenzije certifikata osoba**

Ekstenzije certifikata osoba su definirane u CPS pojedinog CA, [54] i [55].

Pri određivanju profila certifikata osoba moraju se primjenjivati :

- ETSI EN 319 412-1 [18] općenito za sve certifikate,
- ETSI EN 319 412-2 [19] za fizičke osobe,
- ETSI EN 319 412-3 [20] za CA i OCSP i certifikate za pravne osobe (pečat) i
- ETSI EN 319 412-5 [21] za EU kvalificirane certifikate.

7.1.2.4. **Ekstenzije TSU certifikata**

Ekstenzije TSU certifikata su definirane u KIDCA CPS [55].

7.1.3. **Identifikator objekta (OID) algoritama**

Algoritmi s pripadajućim OID identifikatorima za sve certifikate koji se izdaju u AKD PKI sustavu zasnovanom na AKD Root CA su definirani u CPS pojedinog CA, [54] i [55].

7.1.4. **Oblici naziva**

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

Oblici naziva za certifikate koji su izdani u AKD PKI sustavu detaljnije su definirani u CPS pojedinog CA, [54] i [55].

7.1.5. **Ograničenja u nazivima**

Ne koristi se.

7.1.6. **Identifikator objekata (OID) općih pravila certificiranja**

U svakom certifikatu koji sadrže ekstenziju „Certificate Policies“ naveden je odgovarajući OID identifikator u skladu s pravilima navedenim u točki 1.2.2 ovog dokumenta.

7.1.7. **Upotreba ekstenzije Policy Constraints**

Ne koristi se.

7.1.8. **Sintaksa i semantika kvalifikatora općih pravila**

U svakom certifikatu koji sadrže ekstenziju „Certificate Policies“ biti će stavljena adresa na kojoj se mogu naći CP i CPS, [54] i [55] kako je navedeno u točki 2.2. ovog dokumenta.

7.1.9. **Procesne semantike za kritičnu ekstenziju Certificate Policies**

Ne koristi se.

7.2. CRL profili

CRL profili AKDCA Root, HRICDA i KIDCA izdavatelja podržavaju X.509 verziju 2 sukladno zahtjevima definiranim u IETF RFC 5280 [39]. U nastavku su dani CRL profili koje izdaju AKDCA Root, HRIDCA i KIDCA.

Osnovna polja CRL navedena su u sljedećoj tablici.

Tablica 9: Osnovna polja CRL

Polje	Vrijednost/Ograničenja vrijednosti
Version	X.509 V2, vidi točku 7.2.1
Signature Algorithm	SHA256RSA, vidi točku 7.1.3.
Issuer DN	X.500 Distinguished name of the issuer of the CRL.
Effective Date	utcTime
Next Update	utcTime (thisUpdate+24h)
Revoked Certificates	Lista opozvanih certifikata koja uključuje serijski broj certifikata koji je opozvan, datum opoziva i razlog opoziva (keyCompromise, cAcompromise, affiliationChanged, superseded, cessationOfOperation, certificateHold).

7.2.1. Broj verzije

Koristi se X.509 verzija V2.

7.2.2. CRL ekstenzije

Ekstenzije CRL navedene su u sljedećoj tablici.

Tablica 10: Ekstenzije CRL

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

7.3. OCSP profil

7.3.1. Broj verzije

Koristi se OCSP verzija v1.

7.3.2. Ekstenzije OCSP

Poruka OCSP usluge je sukladna RFC 6960 [36].

8. Provjera usklađenosti

8.1. Učestalost i okolnosti provjere usklađenosti

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

Nadzor sustava upravljanja s ciljem provjere usklađenosti s ISO/IEC 9001 [48], ISO/IEC 27001 [46] i ISO/IEC 14298 [45] normama provodi se najmanje svakih 12 mjeseci.

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

8.2. Identitet/kvalifikacije revizora

Ocjenjivanje sukladnosti s *Uredbom (EU) br. 910/2014* [1] provodi tijelo ovlašteno za provedbu ocjenjivanja sukladnosti kvalificiranog pružatelja usluga povjerenja i kvalificiranih usluga povjerenja koje je osigurano akreditacijom prema ETSI EN 319 403 [15].

Nadzor sustava upravljanja sukladno normama ISO/IEC 9001 [48], ISO/IEC 27001 [46] i ISO/IEC 14298 [45] vrše ovlaštene revizijske kuće.

Interne revizije provode osobe koje raspolažu potrebnim znanjima i vještinama za provedbu revizije, u skladu s pravilima koja su navedena u CPS, [54] i [55].

8.3. Odnos revizora s predmetom revizije

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

Internu reviziju provodi osoba koju imenuje PMA.

8.4. Područja obuhvaćena revizijom

Vanjske revizije sustava upravljanja obuhvaćaju cjelokupno poslovanje AKD-a.

Interne revizije PKI obuhvaćaju provedbu usluga certificiranja i servisa koji proizlaze iz usluga certificiranja, propisanih postupaka i mjera zaštite u skladu s odredbama općih pravila i pravilnika.

8.5. Postupanje u slučaju nesukladnosti

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

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

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

Nakon što ocjenitelj utvrdi da je postignuta propisana usklađenost, PMA će odobriti nastavak pružanja usluga certificiranja ili pojedinog servisa povezanog sa uslugama certificiranja.

8.6. Priopćavanje rezultata

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

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

9. Ostale poslovne i pravne stavke

9.1. Naknade za usluge

9.1.1. *Naknade za izdavanje ili obnovu certifikata*

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

AKD naplaćuje uslugu izdavanja i obnove KID certifikata u skladu s utvrđenim cjenikom ili ugovorom.

9.1.2. *Naknade za pristup certifikatu*

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

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

9.1.3. *Naknade za opoziv i pristup informacijama o statusu certifikata*

Za eOI certifikate usluga opoziva i pristupa informacijama o statusu certifikata se ne naplaćuje.

Za KID certifikate AKD može odrediti cijenu i naplaćivati naknadu za opoziv i pristup informacijama o statusu certifikata.

9.1.4. *Naknade za ostale usluge*

Za osobne certifikate, usluga registracije fizičkih osoba te usluge dizajna, izrade i individualizacije kartice naplaćuju se kroz cijenu eOI. Cijena eOI je određena provedbenim aktima koji proizlaze iz Zakona o osobnoj iskaznici [13].

Za KID certifikate, AKD može samostalno ili u suradnji s trećim stranima odrediti cijenu i naplaćivati naknadu za ostale usluge.

Za ostale usluge i servise koji proizlaze iz KIDCA, AKD može samostalno ili u suradnji s trećim stranima odrediti cijenu i naplaćivati naknadu.

9.1.5. *Povrat naknade*

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

Uvjeti povrata naknade za usluge i proizvode vezane za izdavanje certifikata objavljeni su na web portalu, a službenici RA ureda informiraju korisnike u uredima.

Dodatno, uvjeti mogu detaljno biti navedeni u CPS pojedinog CA, [54] i [55] i uvjetima pružanja usluga certificiranja.

9.2. Financijska odgovornost

9.2.1. Pokrivenost osiguranjem

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

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

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

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

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

9.2.2. Ostala sredstva

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

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

9.2.3. Osiguranje ili garancije za krajnje korisnike

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

Polica osiguranja glasi na ukupan iznos od 2.000.000,00 kuna.

Maksimalan iznos financijske odgovornosti koju AKD kao pružatelj usluga certificiranja prihvaća po pojedinačnoj transakciji, iskazan je identifikatorom koji se nalazi u svakom certifikatu osobe. Identifikator se nalazi u polju „Certificate Policies“, iskazan predzadnjom znamenkom OID broja (npr: Policy Identifier=1.3.6.1.4.1.43999.5.4.2.1.2.1).

Pravila tumačenja identifikatora su dana u poglavlju 9.8.

AKD dodatno osigurava imovinu policom osiguranja koja pokriva osiguranje od rizika požara, vremenskih nepogoda, poplava, eksplozija i slično, te osiguranja od loma stroja (industrijski lom)

i loma stakla, kojima se pokrivaju moguće nastale štete od ispada ili oštećenja instalacija i/ili strojne opreme.

9.3. Povjerljivost poslovnih podataka

9.3.1. Opseg povjerljivih poslovnih podataka

Povjerljivim poslovnim podacima smatraju se podaci koji su označeni kao poslovna tajna ili su kao poslovna tajna određeni Zakonom o tajnosti podataka [10] te na zakonu utemeljenom propisu ili internim pravilom, a zbog čijeg bi priopćavanja neovlaštenoj osobi mogle nastupiti štetne posljedice za sudionike postupka certificiranja.

Povjerljivi poslovni podaci obuhvaćaju podatke različitog tipa značajnih za poslovanje, pružanje usluga ili interese sudionika.

Detaljnije informacije o opsegu povjerljivih podataka su dostupne u pravilnicima.

9.3.2. Podaci koji se ne smatraju povjerljivim poslovnim podacima

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

To obuhvaća: certifikate, listu opozvanih certifikata, informacije o statusu certifikata te sve informacije i dokumente koji su objavljeni na portalu.

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

9.3.3. Odgovornost za zaštitu povjerljivih poslovnih podataka

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

Dužnost čuvanja tajne odnosi se na sve sudionike postupka certificiranja koji su na bilo koji način saznali povjerljive poslovne podatke navedene u točki 9.3.1.

9.4. Zaštita osobnih podataka

9.4.1. Plan zaštite osobnih podataka

Zaštita osobnih podataka zajamčena je svakoj fizičkoj osobi.

Osobe su informirane da AKD i pravne osobe kojima su povjereni poslovi RA obrađuju osobne podatke kako bi ispunili zakonom propisane zahtjeve vezane uz provedbu usluge, te da jamče zakonito postupanje i obradu svih osobnih podataka s kojima raspolažu.

AKD i pravne osobe kojima su povjereni poslovi RA poduzimaju odgovarajuće tehničke i organizacijske mjere zaštite od neautorizirane ili nezakonite obrade kao i od slučajnog gubitka, uništenja ili oštećenja osobnih podataka.

9.4.2. Povjerljivi osobni podaci

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

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

9.4.3. Osobni podaci koji nisu povjerljivi

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

Osobni podaci sadržani u certifikatu nisu povjerljivi.

9.4.4. Odgovornost za zaštitu osobnih podataka

AKD i ugovoreni RA odgovorni su za zaštitu osobnih podataka.

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

9.4.5. Ovlaštenje za korištenje osobnih podataka

Osim za potrebe ispunjenja zakonskih, odnosno ugovornih obveza po ugovorima kojima se uređuju usluge certificiranja, osobni podaci će se koristiti samo temeljem pisane privole osobe. Potpisivanjem Ugovora o pružanju usluga certificiranja osobe su upoznate s korištenjem osobnih podataka za potrebe vođenja evidencija te za objavu certifikata u javnom imeniku.

9.4.6. Dostupnost podataka mjerodavnim tijelima

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

9.4.7. Ostale okolnosti objave osobnih podataka

Nema odredbi.

9.5. Prava intelektualnog vlasništva

Kao autor i vlasnik svih sadržaja na portalu uključujući CP, CPS, PDS, certifikate, CRL i aplikacije za QSCD, AKD raspolaže neograničenim pravima korištenja, a osobito pravima umnožavanja, distribucije, objavljivanja i prerade.

Softver i sva ostala dobra koja se koriste u pružanju usluga povjerenja, a koja su u vlasništvu AKD-a, sudionika postupka certificiranja ili bilo koje treće strane, koriste se prema uvjetima korištenja licenci za krajnje korisnike (End User Licence Agreement - EULA) ili drugim odredbama o pravu korištenja.

Svi sudionici su dužni poštovati autorska i srodna prava kao i prava intelektualnog vlasništva.

9.6. Obveze i odgovornosti

9.6.1. Obveze i odgovornosti PMA

PMA je odgovoran za:

- a) definiranje, uvođenje i administriranje CP, CPS, PDS, sigurnosno operativnih procedura i provedbenih dokumenata vezanih uz djelovanje AKD PKI i pružanje usluga povjerenja,
- b) održavanje kontinuirane prikladnosti i usklađenosti dokumentacije s Uredbom (EU) br. 910/2014 [1] te obvezujućim nacionalnim, europskim ili međunarodnim normama i
- c) nadzor nad provedbom sigurnosnih zahtjeva koji su propisni ovim dokumentom.

9.6.2. Obveze i odgovornosti CA

Certifikacijsko tijelo je odgovorno za:

- a) osiguranje provedbe Uredbe (EU) br. 910/2014 [1] te primjenu upravnih i upravljačkih postupaka u skladu s obvezujućim nacionalnim, europskim ili međunarodnim normama,
- b) osiguranje provedbe usluga generiranja certifikata, upravljanja opozivom certifikata, provjere statusa certifikata kao i usluga informiranja u skladu s ovim dokumentom,
- c) pravovremenu obradu zahtjeva temeljem cjelovitih, točnih i provjerenih podataka dobivenih od RA,
- d) osiguranje osoblja koje posjeduje potrebno stručno znanje, pouzdanost, iskustvo i kvalifikacije dostatne za provedbu poslovnih aktivnosti i ispunjenje zahtjeva koji su utvrđeni ovim dokumentom,
- e) osiguranje dostatnih financijskih sredstva potrebnih za pružanje usluga certificiranja u skladu sa zahtjevima koji su utvrđeni ovim dokumentom,
- f) primjenu organizacijskih, provedbenih i fizičkih mjera zaštite CA sustava i podataka u skladu s ovim dokumentom,
- g) bilježenje i dugoročno arhiviranje svih bitnih informacija u vezi s podacima koje izdaje i prima CA i AKD mPotpis servis, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge,
- h) zakonitu obradu osobnih podataka u skladu s odredbama Zakona o provedbi Opće uredbe o zaštiti podataka [4] i vezanih pod-zakonskih akata odnosno Uredbe (EU) br. 2016/679 [3] i
- i) osiguranje ISO/IEC 9001 [48] i ISO/IEC 27001 [46] certifikata kao dokaza kvalitete i sigurnosti pružanje usluga certificiranja.

9.6.3. Obveze i odgovornosti RA

Registracijsko tijelo je odgovorno za:

- a) prikupljanje i provjeru podataka o identitetima fizičkih i pravnih osoba u skladu s ovim dokumentom,
- b) zaprimanje zahtjeva osoba uključujući zahtjeve za izdavanje certifikata, zahtjeve za opoziv i suspenziju certifikata kao i zahtjeve za deblokadu i uručivanje QSCD,
- c) izravnu provjeru i nedvojbeno utvrđivanje identiteta fizičkih osoba neposrednom identifikacijom u fizičkoj prisutnosti osobe prilikom zaprimanja zahtjeva, kao i prilikom uručivanja QSCD,
- d) prosljeđivanje cjelovitih, točnih i provjerenih podataka o fizičkim i pravnim osobama te o njihovim zahtjevima na daljnju obradu proizvođaču odnosno CA,
- e) osiguranje da poslove registracije provode isključivo pouzdani i savjesni službenici RA/LRA čiji je identitet nedvojbeno utvrđen i koji su adekvatno educirani prije nego što su im dodijeljena ovlaštenja,
- f) primjenu odgovarajućih fizičkih, organizacijsko-upravljačkih i provedbenih mjera zaštite informacijskog sustava RA i podataka,
- g) bilježenje i dugoročno arhiviranje podataka i dokumentacije prikupljene u postupku registracije i svih bitnih informacije u vezi s podacima koje izdaje i prima RA, a posebno za potrebe predlaganja dokaza u sudskim postupcima i u svrhu osiguravanja kontinuiteta usluge, najmanje 10 godina od prestanka važenja pripadajućeg certifikata i
- h) provedbu zakonite obrade i zaštite osobnih podataka u skladu s odredbama Zakona o provedbi Opće uredbe o zaštiti podataka [4] i vezanih pod-zakonskih akata odnosno Uredbe (EU) br. 2016/679 [3].
- i) Uklanjanje ograničenja pristupa uslugama osobama sa invaliditetom, gdje je moguće.
- j) Ostale odgovornosti propisane u CPS pojedinog CA, [54] i [55].

9.6.4. Obveze i odgovornosti osoba

Osoba je odgovorna:

- a) da u postupku identifikacije predoči vjerodostojne dokaze kojima potvrđuje svoj identitet,
- b) da u postupku registracije dostavi točne i istinite podatke,
- c) da pregleda i provjeri da su podaci u certifikatu ispravni,
- d) da isključivo osoba koja je navedena u certifikatu ili ovlašteni predstavnik autora pečata koristiti privatni ključ koji odgovara javnom ključu u certifikatu,
- e) da certifikat u trenutku njegovog korištenja nije istekao i da nije opozvan,
- f) da certifikat koristi samo za legalne i autorizirane svrhe te u skladu s njihovom namjenom,
- g) da odgovorno koristi i čuva QSCD koji mu je u posjedu ili dvofaktorsko sredstvo elektroničke identifikacije za pristup AKD mPotpis servisu, privatne ključeve, aktivacijske podatke i registracijske kodove te da poduzima odgovarajuće mjere zaštite od neovlaštenog pristupa i uporabe,
- h) da odmah zatraži opoziv ili suspenziju certifikata ako je došlo do promjene osobnih identifikacijskih podataka u certifikatu (imena fizičke ili pravne osobe, prestanka povezanosti između fizičke osobe i organizacije, ili razloga navedenih u točki 4.9) ili ako sumnja u gubitak, krađu, zlouporabu ili neautorizirano korištenje privatnog ključa i

- i) da zatraži opoziv certifikata ako ne postoji osnova po kojoj je izdan certifikat ili ako je utvrđena bilo kakva okolnost zbog koje se certifikat više ne bi trebao koristiti.

9.6.5. Obveze i odgovornosti pouzdajućih strana

Pouzdajuće strane su odgovorne:

- a) da se prije korištenja usluga informiraju o CP, CPS i PDS, a posebno o svojim odgovornostima i obvezama te prihvatljivom načinu korištenja usluga certificiranja,
- b) da samostalno procijene i utvrde prikladnost korištenja certifikata za odgovarajuću namjenu,
- c) da prije ostvarivanja povjerenja u certifikat utvrde da certifikat nije istekao i da nije opozvan, a prema podacima koji su navedeni u certifikatu,
- d) da provjeru valjanosti certifikata vrše koristeći autorizirani izvor i pouzdanu opremu,
- e) da provjere status certifikata osobe i svih certifikata na certifikacijskoj stazi prema postupcima koji su navedeni u IETF RFC 5280 [39] i IETF RFC 3739 [38].

9.6.6. Obveze i odgovornosti ostalih sudionika

Proizvođač je odgovoran za:

- a) pripremu podataka i proizvodnju QSCD temeljem zahtjeva i nepromijenjenih podataka dobivenih od RA,
- b) generiranje parova ključeva i aktivacijskih podataka, pribavljanje certifikata od podređenog CA te njihovo unošenje u QSCD,
- c) generiranje podataka za aktivaciju QSCD i registraciju na portal te izrada sigurnosnih omotnica kada je primjenjivo,
- d) primjenu odgovarajućih fizičkih, organizacijsko-upravljačkih i provedbenih mjera zaštite informacijskog sustava proizvođača i podataka u skladu s ovim dokumentom,
- e) zakonitu obradu i zaštitu osobnih podataka u skladu s odredbama Zakona o provedbi Opće uredbe o zaštiti podataka [4] i vezanih pod-zakonskih akata odnosno Uredbe (EU) br. 2016/679 [3],
- f) osiguranje ISO/IEC 9001 [48], ISO/IEC 27001 [46] i ISO/IEC 14298 [45] certifikata kao dokaza kvalitete upravljanja poslovanjem i proizvodnjom zaštićenog tiska te sigurnošću informacijskih sustava i
- g) osiguranje QSCD koje zadovoljava zahtjeve EAL 4+ prema ISO/IEC 15408 [44] te da demonstrira sukladnost s obrascima zaštite iz serije EN 419 211 [26], [27], [28], [29], [30] i [31].

Odgovornosti dobavljača koji isporučuju opremu ili sudjeluju u provedbi usluga povezanih sa PKI definirane su ugovorima.

9.7. Odricanje od odgovornosti

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

AKD ne daje jamstvo za:

- a) štete koje su prouzročene neprijemnom upotrebom certifikata,

- b) štete prouzročene lažnom ili nemarnom uporabom QSCD u posjedu, privatnih ključeva, aktivacijskih podataka, 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 sa svojim obvezama.

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

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

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

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

9.8. Ograničenja odgovornosti

Ukupna financijska odgovornost za transakcije obavljene na temelju pouzdanja 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.

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

Primjenjuju se slijedeća pravila:

Identifikator	Financijski limit
1	do 8 000,00 HRK
2	do 80 000,00 HRK
3	do 400 000,00 HRK

9.9. Naknada štete

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

Fizička i pravna osoba odgovara oštećenoj strani ako:

- a) stekne certifikat temeljem lažnih podataka u zahtjevu za izdavanje certifikata ili
- b) djeluje ili se predstavlja u ime druge fizičke osobe.

Pouzdajuća strana odgovara oštećenoj strani ako:

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

Pružatelj usluga povjerenja je odgovoran ako je ta odgovornost jasno uspostavljena ugovorom, općim pravilima, pravilnicima, uvjetima pružanja usluga certificiranja ili hrvatskom zakonskom regulativom.

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

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

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

9.10.2. Prestanak važenja

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

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

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

9.10.3. Posljedice prestanka važenja i nastavak djelovanja

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

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

9.11. Pojedinačne obavijesti i komunikacija sa sudionicima

Informiranje osoba i pouzdajućih strana se provodi putem portala.

Komunikacija s AKD se provodi pisanim putem ili elektroničkom poštom korištenjem kontaktnih podataka koji su navedeni pod 1.5.2.

9.12. Izmjene i dopune

9.12.1. Postupak izmjena i dopuna

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

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

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

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

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

9.12.2. Način obavještanja i period

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

O pojavi novije inačice dokumenta sudionici se neće obavještavati.

Prihvaćeni prijedlozi sudionika će se uvrstiti u novo izdanje dokumenta.

9.12.3. Okolnosti pod kojima se mora mijenjati OID

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

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

9.13. Postupak rješavanja sporova

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

9.14. Važeći propisi

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

9.15. Usklađenost s važećim propisima

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

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

9.16. Ostale odredbe

9.16.1. Sporazum

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

9.16.2. Prijenos odgovornosti

Nije primjenjivo.

9.16.3. Nevaljanost pojedine odredbe

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

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

9.16.4. Ovrha

Nije primjenjivo.

9.16.5. Viša sila

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

9.17. Ostale odredbe

Nije primjenjivo.

PRILOG 1: Definicije

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

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

33. "Opća pravila pružanja usluga certificiranja (CP)": imenovani skup pravila koja ukazuju na prikladnost certifikata za određenu zajednicu i/ili skupinu sa zajedničkim sigurnosnim zahtjevima;
34. "Lista opozvanih certifikata CRL": potpisana lista s nizom certifikata koje izdavatelj više ne smatra valjanim;
35. "Certifikacijsko tijelo (CA)": tijelo kojem vjeruje jedan ili više korisnika, a koje kreira i dodjeljuje certificate;
- Napomena 1: CA može biti:
- 1) pružatelj usluga povjerenja koji kreira i dodjeljuje javni ključ certifikata; ili
 - 2) usluga tehničkog generiranja certifikata koju koristi pružatelj usluga certificiranja da kreira i dodjeljuje javni ključ certifikata.
36. "Pravilnik o postupcima certificiranja (CPS)": izjava o praksi koju primjenjuju radnici certifikacijskog tijela u upravljanju postupkom izdavanja, opoziva, obnove ili izdavanja certifikata s novim parom ključeva;
37. "koordinirano svjetsko vrijeme (UTC)": vremenska skala koja je definirana u preporuci ITU-R TF.460-6 [53];
38. „digitalni potpis“: podaci koji se dodaju podatkovnom skupu ili kriptografska transformacija podatkovnog skupa koja omogućuje njegovom primatelju dokazivanje izvornosti i cjelovitosti podatkovnog skupa te koja podatkovni skup štiti od krivotvorenja, npr. od strane primatelja;
39. "zona visoke sigurnost": specifična fizička lokacija gdje se čuva privatni ključ krovnog CA;
40. "Registracijsko tijelo (RA)": tijelo koje je prvenstveno odgovorno za identifikaciju i autentikaciju subjekta certifikata
- Napomena 1: RA pomaže u postupku podnošenja zahtjeva za izdavanje i opoziv certifikata;
41. "službenik RA": radnik odgovoran za provjeru informacija i pripremu podataka koja se nužno provodi pri izdavanju certifikata i odobrenje zahtjeva za izdavanje certifikata;
42. "službenik za opoziv": radnik odgovoran za provedbu zahtjeva za promjenu statusa certifikata;
43. "krovno certifikacijsko tijelo (krovni CA)": certifikacijsko tijelo koje na najvišem nivou djeluju u sklopu hijerarhijske strukture i koje potpisuje certifikat podređenim CA;
44. "siguran kriptografski uređaj": uređaj koji čuva privatni ključ korisnika, štiti taj ključ od kompromitacije i provodi operacije potpisivanja ili dešifriranja u ime korisnika;
45. „sigurna zona“: zona (fizička ili logička) zaštićena fizičkim i logičkim kontrolama tako da na odgovarajući način štiti povjerljivost, izvornost i dostupnost sustava pružatelja usluga povjerenja;
46. "subjekt": osoba identificirana u certifikatu kao vlasnik privatnog ključa koji odgovara javnom ključu u certifikatu;
47. Osobe naručitelji (engl. Applicant ili Subscriber) su fizičke ili pravne osobe koje su podnijeli zahtjev za izdavanje certifikata, te su ujedno i vlasnici certifikata;
48. Osobe subjekti certificiranja (engl. Subject); fizičke osobe čije je ime, prezime navedeno u subjektu certifikata u poljima Common name i(li) givenName i surname, odnosno osobni identifikacijski broj sadržan u polju serialNumber;

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

PRILOG 2: Kratice

AKD	AKD d.o.o.
AKDCA	Certifikacijsko tijelo AKD
HRIDCA	Certifikacijsko tijelo za izdavanje certifikata osobama za potrebe elektroničke osobne iskaznice građana Republike Hrvatske
KIDCA	Certifikacijsko tijelo za izdavanje kvalificiranih certifikata fizičkim i pravnim osobama i organizacijama u komercijalne svrhe
PKI	Public Key Infrastructure
eOI	Elektronička osobna iskaznica građana RH
TSP	Trust Service Provider
TW4S	Trustworthy System Supporting Server Signing
CP	Certificate Policy
CPS	Certificate Practice Statement
TSP/PS	Time-stamp Policy/Practice Statement
TSA	Time-Stamping Authority
EUSCP	EU SSASC Policy
SSASC	Server Signing Application Service Component
SSASC PS	SSASC Practice Statement
AKD mPotpis	AKD SSASC
SCP	SSASC Policy
SSASP	Server Signing Application Service Provider
QCP	Qualified Certificate Policy
PMA	Policy Management Authority
CA	Certificate Authority
RA	Registration Authority
OID	Object Identifier - Identifikacijska oznaka
SCD/ SCDev	Signature Creation Device
SSCD	Secure Signature Creation Device
QSCD	Qualified Electronic Signature Creation Device
RQSCD	Remote Qualified Electronic Signature Creation Device
IdP	Identity Provider
AKD IdP	AKD Identity Provider
SAML	Security Assertion Markup Language
SMS-OTP	One Time Password sent over Short Message Service
SCD	Signature Creation Data
DTBS	Data to be Signed

SAD	Signature Activation Data
SAP	Signature Activation Protocol
SIC	Signer's Interaction Component
SSA	Server Signing Application
SCA	Signature Creation Application
SCAL	Sole Control Assurance Level
SAM	Signature Activation Module
2FA	Two-Factor Authentication
PBKDF	Password Based Key Derivation Function
NIAS	Nacionalni identifikacijski i autentikacijski sustav
CRL	Certificate Revocation List
CARL	Certification Authority Revocation List
LDAP	Lightweight Directory Access Protocol
OCSP	On-line Certificate Status Protocol
HTTP	Hypertext Transfer Protocol
UTC	Coordinated Universal Time
RSA	Rivest, Shamir and Adleman algorithm
AES	Advanced Encryption Standard
HSM	Hardware security module
FIPS	Federal Information Processing Standard
x.509v3	Public Key Infrastructure Standard
PIN	Personal Identification Number
PUK	Personal Unblocking Code
EAL	Evaluation Assurance Level
IDS	Intrusion Detection System
EULA	End User Licence Agreement
PDS	Policy Disclosure Statement
PTC	Publicly-Trusted Certificate
TSU	Time-Stamping Unit

PRILOG 3: Reference

EU i nacionalni akti:

- [1] Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ.
- [2] Zakon o provedbi Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnje tržištu i stavljanju izvan snage Direktive 1999/93/EZ (NN 62/17).
- [3] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ.
- [4] Zakon o provedbi opće Uredbe o zaštiti podataka (NN 42/2018).
- [5] Provedbena odluka komisije (EU) 2015/1502 od 8. rujna 2015. o utvrđivanju minimalnih tehničkih specifikacija i postupaka za razine osiguranja identiteta koje se pripisuju sredstvima elektroničke identifikacije u skladu s člankom 8. stavkom 3. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.
- [6] Provedbena odluka komisije (EU) 2016/650 od 25. travnja 2016. o utvrđivanju normi za ocjenu sigurnosti kvalificiranih sredstava za izradu potpisa i pečata u skladu s člankom 30. stavkom 3. i člankom 39. stavkom 2. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.
- [7] Provedbena odluka komisije (EU) 2015/296 od 24. veljače 2015. o utvrđivanju postupovnih aranžmana za suradnju među državama članicama u području elektroničke identifikacije u skladu s člankom 12. stavkom 7. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.
- [8] Provedbena odluka komisije (EU) 2015/1501 od 8. rujna 2015. o okviru za interoperabilnost u skladu s člankom 12. stavkom 8. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu.
- [9] Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93.
- [10] Zakon o tajnosti podataka (NN 79/2007, 86/2012).
- [11] Zakon o pravu na pristup informacijama (NN 25/2013, 85/2015).
- [12] Zakon o obveznim odnosima (NN 35/2005, 41/2008, 125/2011, 78/2015, 29/2018).
- [13] Zakon o osobnoj iskaznici (NN 62/2015, 144/2020).

Normizacijski dokumenti:

- [14] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- [15] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".
- [16] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- [17] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2; Requirements for trust service providers issuing EU qualified certificates".
- [18] ETSI EN 319 412-1: „Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures“.
- [19] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".
- [20] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".
- [21] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".
- [22] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- [23] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
- [24] ETSI TS 119 431-1: „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev“.
- [25] ETSI TS 119 431-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".
- [26] CEN EN 419 211-1: "Protection profiles for secure signature creation device - Part 1: Overview".
- [27] CEN EN 419 211-2: "Protection profiles for secure signature creation device - Part 2: Device with key generation".
- [28] CEN EN 419 211-3: "Protection profiles for secure signature creation device - Part 3: Device with key import".
- [29] CEN EN 419 211-4: "Protection profiles for secure signature creation device - Part 4: Extension for device with key generation and trusted communication with certificate generation application".
- [30] CEN EN 419 211-5: "Protection profiles for secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application".
- [31] CEN EN 419 211-6: "Protection profiles for secure signature creation device - Part 6: Extension for device with key import and trusted communication with signature creation application".

- [32] CEN TS 419 261:2015: "Security Requirements for Trustworthy Systems Managing certificates and time-stamps".
- [33] CEN EN 419 241-1: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements".
- [34] CEN EN 419 241-2: "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing".
- [35] CEN 419 221-5: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services".
- [36] IETF RFC 6960: „X.509 Internet Public Key Infrastructure On-line Certificate Status Protocol – OCSP (2013)“.
- [37] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".
- [38] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".
- [39] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“.
- [40] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
- [41] IETF RFC 5019 (2007): „The Lightweight On-line Certificate Status Protocol (OCSP) Profile for High-Volume Environments“.
- [42] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".
- [43] FIPS PUB 186-4: „Digital Signature Standard (DSS)“.
- [44] ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".
- [45] ISO/IEC 14298: "Graphic technology - Management of security printing processes".
- [46] ISO/IEC 27001:2013: " Information technology — Security techniques — Information security management systems — Requirements“.
- [47] ISO/IEC 27002:2013: „Information Technology – Security Techniques – Code of practice for information security controls“.
- [48] ISO/IEC 9001:2015: "Quality management systems - Requirements".
- [49] ISO/IEC 27005:2011: "Information technology - Security techniques - Information security risk management".
- [50] ITU-T X.509 Recommendation: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".
- [51] ITU-T X.520 Recommendation: "Information technology - Open Systems Interconnection - The Directory: Selected attribute types".
- [52] ITU-T X.501 Recommendation: „Information technology – Open Systems Interconnection – The Directory: Models“.
- [53] ITU-R TF.460-6 Recommendation: "Standard-frequency and time-signal emissions".

AKD dokumenti:

- [54] HRIDCA Pravilnik o postupcima certificiranja.
- [55] KIDCA Pravilnik o postupcima certificiranja.
- [56] AKD QTSA Pravila i postupci pružanja usluga vremenskog žiga.

Prilog 4: Povijest promjena dokumenta

Izdanje	Datum	Obrazloženje izmjene
1.3	08.06.2015.	Prvo objavljeno izdanje dokumenta
2.0	15.05.2017.	Usklađivanje s Provedbenim odlukama EU iz i novim ETSI normama.
2.1	12.12.2017.	Ispravci i manje promjene u dokumentu. Usklađivanja s Zakonom o provedbi Uredbe eIDAS [2]. Nadopune pojedinih točki zbog uspostave AKD QTSA servisa.
2.2	04.07.2018.	Ispravci i manje promjene u dokumentu. Nadopuna pojedinih točaka dokumenta zbog izdavanja certifikata namijenjenih za izradu kvalificiranog elektroničkog pečata i certifikata namijenjenih za udaljeno potpisivanje. Usklađivanje s Zakonom o provedbi opće Uredbe o zaštiti podataka. Usvojena i odobrena verzija dokumenta.
2.3.	01.07.2019.	Ispravci uočenih grešaka u dokumentu. Ispravak i ažuriranje referenci u dokumentu. Nadopuna pojedinih točaka vezano za AKD mPotpis servis za udaljeno potpisivanje i udaljeno pečatiranje. Usvojena i odobrena verzija dokumenta. Vrijedi od 15.07.2019.
2.4	01.05.2020.	Ispravci uočenih grešaka u dokumentu. Pojašnjenje pohrane privatnih ključeva korisnika kod treće osobe. Usklađivanje s pravnom regulativom.
2.5	01.07.2021.	Usklađivanje s Izmjenama i dopunama Zakona o osobnoj iskaznici (NN 144/2020). Ispravci uočenih grešaka u dokumentu.