# Praktična pravila pružanja usluga certifikacije

Kod dokumenta: PKI-JU-RS-DOC-CPS

**AGENCIJA ZA INFORMACIONO DRUŠTVO REPUBLIKE SRPSKE**

16. decembar 2013.

АИДРС
Агенција за информационо друштво Републике Српске
AISRS
Agency for Information Society of Republic of Srpska

# Praktična pravila pružanja usluga certifikacije

(CPS – Certification Practice Statement)

OID: 1.3.6.1.4.26614.10.1.1

Трг Републике Српске 1, 78000 Бања Лука, Република Српска, БиХ
тел: +387 51 258 400 факс: +387 51 258 401 email: info@aidrs.org web: www.aidrs.org

## Opšti podaci i verzije dokumenta

| Referentni broj dokumenta | I - / 11 |
|---|---|
| **Puni naziv dokumenta** | **Praktična pravila pružanja usluga certifikacije** |
| **Skraćenica dokumenta** | CPS – Certification Practice Statement |
| **Kod dokumenta** | PKI-JU-RS-DOC-CPS |
| **Institucija** | Agencija za informaciono društvo Republike Srpske |
| **Sigurnost (nivo distribucije)** | Javni dokument, slobodna distribucija |
| **Datum kreiranja dokumenta** | septembar 2011. |
| **Datum posljednjeg ažuriranja dokumenta** | decembar 2013. |
| **Status i verzija** | Finalna verzija, v.1.2 |
| **Broj stranica** | **78** |
| **Odgovorno lice** | Srđan Rajčević, direktor |
| **Autori** | Milan Latinović, AIDRS<br>Saša Vojnović, AIDRS<br>Ljiljana Umićević, AIDRS<br>Stojan Radanović, AIDRS |
| **Dostavlja se** | Na uvid javnosti. |
| **Ključne riječi** | Infrastruktura javnih ključeva, elektronski certifikat, kvalifikovani elektronski certifikati, certifikaciono tijelo, Agencija za informaciono društvo Republike Srpske, certifikaciono tijelo Agencije za informaciono društvo Republike Srpske, praktična pravila rada, profili certifikata |
| **Apstrakt (za potrebe publikovanja)** | Praktična pravila pružanja usluga certifikacije je dokument koji opisuje postupke koje primjenjuje certifikaciono tijelo Agencije za informaciono društvo Republike Srpske (u daljem tekstu: AIDRSCA) prilikom procesa izdavanja kvalifikovanog elektronskog certifikata, upotrebe kvalifikovanog elektronskog certifikata od strane krajnjeg korisnika i opoziva kvalifikovanog elektronskog certifikata. |

| Verzija<br>Version | Datum<br>Date | Opis<br>Description |
|---|---|---|
| **1.0** | 28.09.2011. | Prihvatanje finalne verzije dokumenta |
| **1.1.** | 25.04.2012. | Dodatna lektorisanja i jasnije definisanje AD strukture. |
| **1.2.** | 16.12.2013. | Dorađena verzija, prilagođavanje CPS-a za izdavanje certifikata APIF-u i privrednim sudovima prema zaključku Vlade RS. |

## Sadržaj

**1. UVOD ..... 14**

1.1. Pregled ..... 14

1.2. Naziv i identifikacija dokumenta ..... 15

1.3. Učesnici PKI sistema ..... 17

1.3.1. AIDRSCA ..... 17

1.3.3. Korisnici ..... 18

1.3.4. Treća lica ..... 18

1.3.5. Ostali učesnici ..... 18

1.4. Upotreba certifikata ..... 18

1.4.1. Područje primjene ..... 18

1.4.2. Nedozvoljene primjene ..... 19

1.5. Politika administriranja dokumenta ..... 20

1.5.1. Organizacija upravljanja dokumentom ..... 20

1.5.2. Lica za kontakt ..... 20

1.5.3. Lica određena za usklađivanje dokumenta sa praksom izdavanja certifikata ..... 20

1.5.4. Procedura za odobrenje Praktičnih pravila ..... 20

1.6. Definicije i skraćenice ..... 21

1.6.1. Definicije ..... 21

1.6.2. Skraćenice ..... 23

**2. OBJAVLJIVANJE I LOKACIJA PODATAKA O CERTIFIKACIJI ..... 24**

2.1. Lokacija i objavljivanje podataka o certifikaciji ..... 24

2.2. Objavljivanje podataka o certifikaciji ..... 24

2.3. Učestalost objavljivanja podataka o certifikaciji ..... 25

2.4. Kontrola pristupa podacima o certifikaciji ..... 25

**3. IDENTIFIKACIJA I AUTENTIFIKACIJA ..... 26**

3.1. Konvencija imenovanja ..... 26
3.1.1. Vrste imena ..... 26
3.1.2. Nomenklatura imena ..... 26
3.1.3. Anonimnost ili pseudonimi korisnika ..... 26
3.1.4. Pravila za interpretaciju vrsta imena ..... 26
3.1.5. Jedinstvenost imena ..... 28
3.1.6. Priznavanje, autentifikacija i uloga zaštitnog znaka ..... 29
3.2. Inicijalna provjera identiteta ..... 29
3.2.1. Metoda dokazivanja posjeda privatnog ključa ..... 29
3.2.2. Identifikacija i autentifikacija identiteta organa ..... 29
3.2.3. Identifikacija i autentifikacija krajnjeg korisnika ..... 29
3.2.4. Podaci o korisniku koji se ne mogu provjeriti ..... 29
3.2.5. Kriteriji za međusobnu saradnju ..... 29
**4. PROCEDURE ŽIVOTNOG CIKLUSA CERTIFIKATA ..... 30**
4.1. Zahtjev za izdavanje certifikata ..... 30
4.1.1. Ko može da podnese zahtjev za izdavanje certifikata ..... 30
4.1.2. Proces podnošenja zahtjeva i obaveze ..... 30
4.2. Obrada zahtjeva za izdavanje certifikata (od strane CA) ..... 30
4.2.1. Sprovođenje funkcija identifikacije i autentifikacije ..... 30
4.2.2. Odobrenje ili odbijanje zahtjeva za izdavanje certifikata ..... 30
4.2.3. Vrijeme obrade zahtjeva za izdavanje certifikata ..... 30
4.3. Izdavanje certifikata ..... 31
4.3.1. Aktivnosti i postupci CA prilikom izdavanja certifikata ..... 31
4.3.2. Obavještavanje o izdavanju certifikata ..... 31
4.4. Preuzimanje certifikata ..... 31
4.4.1. Akcija kojom korisnik povrđuje da je preuzeo certifikat ..... 31

4.4.2. Objavljivanje certifikata ..... 31
4.4.3. Obavještavanje trećih lica o izdavanju certifikata ..... 32
4.5. Korišćenje para kriptografskih ključeva i certifikata ..... 32
4.5.1. Upotreba privatnog ključa i certifikata sa strane korisnika ..... 32
4.5.2. Upotreba javnog ključa i certifikata sa strane trećih lica ..... 32
4.6. Obnova certifikata bez promjene javnog ključa ..... 32
4.7. Obnova certifikata sa promjenom javnog ključa ..... 33
Pod obnovom certifikata sa promjenom javnom ključa podrazumjeva se ponovno izdavanje kvalifikovanog elektronskog certifikata u skladu sa opisanim procedurama ..... 33
4.8. Promjena podataka u certifikatu ..... 33
4.8.1. Okolnosti za izmjenu podataka u certifikatu ..... 33
4.8.2. Ko može da zahtjeva promjenu podataka u certifikatu ..... 33
4.8.3. Proces obrade zahtjeva za promjenu podataka u certifikatu ..... 33
4.8.4. Obavještavanje korisnika o izdavanju certifikata sa promjenjenim podacima ..... 33
4.8.5. Akcija kojom korisnik povrđuje da je preuzeo certifikat sa promjenjenim podacima ..... 34
4.8.6. Objava certifikata sa promjenjenim podacima ..... 34
4.8.7. Obavještavanje trećih lica o izdavanju certifikata sa promjenjenim podacima ..... 34
4.9. Opoziv i suspenzija certifikata ..... 34
4.9.1. Okolnosti za opoziv ..... 34
4.9.2. Ko može da zahtjeva opoziv certifikata ..... 35
4.9.3. Procedure za opoziv certifikata ..... 35
4.9.4. Vrijeme za podnošenje zahtjeva za opoziv certifikata ..... 35
4.9.5. Vrijeme u kojem CA mora izvršiti obradu zahtjeva za opoziv ..... 35
4.9.6. Provjera opozvanosti certifikata od strane trećih lica ..... 35
4.9.7. Učestalost objavljivanja CRL ..... 35
4.9.8. Maksimalno dozvoljeno zakašnjenje kod objave CRL liste ..... 36
4.9.9. Online provjera statusa certifikata (OCSP) ..... 36

4.9.10. Online provjera statusa certifikata od strane trećih lica ..... 36
4.9.11. Drugi oblici provjere statusa certifikata ..... 36
4.9.12. Posebni zahtjevi u slučaju kompromitovanja ključa ..... 36
4.9.13. Okolnosti za suspenziju korisničkog certifikata ..... 36
4.9.14. Ko može zahtjevati suspenziju korisničkog certifikata ..... 36
4.9.15. Proces obrade zahtjeva za suspenziju korisničkog certifikata ..... 36
4.9.16. Period trajanja suspenzije korisničkog certifikata ..... 37
4.10. Usluge o statusu certifikata ..... 37
4.10.1. Operacione karakteristike ..... 37
4.10.2. Dostupnost servisa ..... 37
4.10.3. Dodatne karakteristike ..... 37
4.11. Prekid ugovora sa naručiocem ..... 37
4.12.* Deponovanje i obnova privatnog ključa korisnika ..... 37
**5. FIZIČKA KONTROLA, OPERATIVNA KONTROLA I UPRAVLJANJE RESURSIMA ..... 38**
5.1. Fizička kontrola ..... 38
5.2. Kontrola procedura ..... 39
5.2.1. Povjerljive uloge osoblja certifikacionog tijela ..... 39
5.2.2. Broj osoba potrebnih za odredjene operativne procedure ..... 40
5.2.3. Identifikacija i autentifikacija ovlašćenih lica za svaku ulogu ..... 40
5.2.4.Povjerljive uloge koje zahtjevaju razgraničenje ovlašćenja ..... 41
5.3. Upravljanje ljudskim resursima ..... 41
5.3.1. Kvalifikacije, iskustvo i dozvola za rad sa zaštićenim podacima ..... 41
5.3.2.Procedure provjere biografije ..... 41
5.3.3. Obuka osoblja ..... 42
5.3.4. Učestalost obuke osoblja ..... 42
5.3.5. Učestalost i redosljed rotacije poslova zaposlenog osoblja ..... 42

5.3.6. Sankcije za neautorizovane aktivnosti zaposlenog osoblja ..... 42
5.3.7. Zahtjevi za spoljne saradnike ..... 42
5.3.8. Dokumentacija za potrebe stalno zaposlenog osoblja ..... 43
5.4. Procedure upravljanja revizijskih dnevnika ..... 43
5.4.1. Vrste događaja koji se evidentiraju ..... 43
5.4.2. Učestalost procesiranja revizijskih dnevnika ..... 43
5.4.3. Period čuvanja revizijskih dnevnika ..... 43
5.4.4. Zaštita revizijskih dnevnika ..... 43
5.4.5. Kreiranje rezervne kopije revizijskih dnevnika ..... 44
5.4.6. Sistem prikupljanja revizijskih dnevnika ..... 44
5.4.7. Obavještavanje lica koje je izazvalo događaj ..... 45
5.4.8. Procjena ugroženosti sistema ..... 45
5.5. Arhiviranje podataka ..... 45
5.5.1. Vrste podataka koji se arhiviraju ..... 45
5.5.2. Vrijeme čuvanje arhiviranih podataka ..... 46
5.5.3. Zaštita arhiviranih podataka ..... 46
5.5.4. Kreiranje rezervne kopije arhiviranih podataka ..... 46
5.5.5. Zahtjevi za vremenskim žigom arhiviranih podataka ..... 46
5.5.6. Sistem arhiviranja podataka ..... 46
5.5.7. Procedure za akviziciju i verifikovanje podataka iz arhive ..... 46
5.6. Obnova ključeva CA ..... 46
5.7. Kompromitovanje i oporavak sistema poslije kompromitiranja ili nepredvidjenih akcija ..... 47
5.7.1. Procedure rada u incidentnim situacijama prilikom kompromitovanja sistema ..... 47
5.7.2. Greške u radu sistema, programske opreme ili oštećenje podataka ..... 47
5.7.3. Kompromitovanje privatnog ključa CA ..... 48
5.7.4. Nastavak rada poslije prirodne katastrofe ili neke druge ..... 48

5.8. Prestanak rada CA ili RA ..... 48
**6. TEHNIČKO BEZBJEDNOSNE KONTROLE ..... 49**
6.1. Generisanje ključeva i instalacija ..... 49
6.1.1. Generisanje para ključeva ..... 49
6.1.2. Dostavljanje korisniku privatnog ključa ..... 49
6.1.3. Dostavljanje javnog ključa korisnika davaocu usluge certifikovanja ..... 49
6.1.4. Dostavljanje javnog ključa davaoca usluge certifikovanja trećim licima ..... 49
6.1.5. Dužina ključeva ..... 49
6.1.6. Generisanje parametara javnih ključeva ..... 50
6.1.7. Namjena upotrebe ključeva (X.509 keyUsage) ..... 50
6.2. Zaštita privatnog ključa i kontrole kriptografskih modula ..... 51
6.2.1. Standardi i kontrole kriptografskih modula ..... 51
6.2.2. M od N kontrola privatnog ključa ..... 51
6.2.3. Deponovanje privatnog ključa ..... 51
6.2.4. Kopija privatnog ključa ..... 51
6.2.5. Arhiviranje privatnog ključa ..... 51
6.2.6. Prenos privatnog ključa u kriptografski modul ..... 51
6.2.7. Čuvanje kriptografskih ključeva na kriptografskom modulu ..... 52
6.2.8. Način aktiviranja privatnog ključa ..... 52
6.2.9. Način deaktiviranja privatnog ključa ..... 52
6.2.10. Način uništavanja privatnog ključa ..... 52
6.2.11. Nivo sigurnosti kriptografskih modula ..... 52
6.3. Ostali aspekti upravljanja parom ključeva ..... 52
6.3.1. Arhiviranje javnog ključa ..... 52
6.3.2. Rok važnosti certifikata i period upotrebe para ključeva ..... 53
6.4. Aktivacioni podaci ..... 53

6.4.1. Generisanje i instalacija aktivacionih podataka ..... 53
6.4.2. Zaštita aktivacionih podataka ..... 53
6.4.3. Ostali aspekti aktivacionih podataka ..... 53
6.5. Bezbjednosni zahtjevi za računare ..... 53
6.5.1. Specifični računarski tehničko-bezbjedonosni zahtjevi ..... 53
6.5.2. Nivo zaštite računara ..... 54
6.6. Tehnički nadzor tokom upotrebe sistema ..... 54
6.6.1. Nadzor razvoja sistema ..... 54
6.6.2. Upravljanje bezbjednošću ..... 54
6.6.3. Nadzor bezbjednosti tokom upotrebe sistema ..... 54
6.7. Nadzor bezbjednosti računarske mreže ..... 54
6.8. Vremenski pečat (eng.*Time-stamping*) ..... 54
**7. CERTIFIKAT, CRL, I OCSP PROFILI CERTIFICATE, CRL, AND OCSP PROFILES ..... 55**
7.1. Profil certifikata ..... 55
7.1.1. Broj (brojevi) verzija (eng.Version number(s)) ..... 55
7.1.2. Ekstenzije certifikata (eng. *Certificate extensions*) ..... 56
7.1.3. Identifikatori algoritamskih objekata ..... 57
7.1.4. Oblik imena ..... 57
7.1.5. Ograničenja za ime ..... 57
7.1.6. Identifikator objekta za politiku certifikovanja ..... 58
7.1.7. Korišćenje Politike ograničenja ekstenzija ..... 58
7.1.8. Sintaksa i semantika za kvalifikatore politike ..... 58
7.1.9. Procesiranje semantike za kritične ekstenzije Politike Certifikovanja ..... 58
7.2. CRL profil ..... 58
7.2.1. CRL verzija ..... 58
7.2.2. CRL i CRL entry ekstenzije ..... 59

7.3. OCSP profil ..... 59
**8. REVIZIJA, USAGLAŠENOSTI I DRUGE PROCJENE ..... 60**
8.1. Učestalost ili okolnosti kada se vrše revizije ..... 60
8.2. Identitet/kvalifikacije revizora ..... 60
8.3. Revizorov odnos prema ocjenjivanom subjektu ..... 60
8.4. Oblasti koje pokriva revizija ..... 60
8.5. Aktivnosti koje se preduzimaju u slučaju nedostatka ..... 60
8.6. Objavljivanje rezultata ..... 60
**9. OSTALE POSLOVNE I PRAVNE STVARI ..... 61**
9.1. Cijene ..... 61
9.1.1. Cijene usluga AIDRSCA ..... 61
9.1.2. Nadoknada za pristup certifikatu ..... 61
9.1.3. Nadoknada za opoziv ili pristup statusu informacija ..... 61
9.1.4. Nadoknade za ostale servise ..... 61
9.1.5. Politika refundiranja ..... 61
9.2. Finansijska odgovornost ..... 61
9.2.1. Osiguranja ili garancije davaoca usluge certifikacije ..... 61
9.2.2. Ostala sredstva ..... 61
9.2.3. Osiguranja ili garancije korisnika ..... 62
9.3. Povjerljivost poslovnih informacija ..... 62
9.3.1. Obim povjerljivih informacija ..... 62
9.3.2. Informacije koje ne ulaze u obim povjerljivih informacija ..... 62
9.3.3. Odgovornost za zaštitu povjerljivih informacija ..... 62
9.4. Povjerljivost ličnih podataka ..... 62
9.4.1. Plan povjerljivosti ..... 62
9.4.2. Informacija koja se tretira privatnom ..... 62
9.4.3. Informacija koja se ne smatra privatnom ..... 62

9.4.4. Odgovornost za zaštitu ličnih podataka ..... 63
9.4.5. Obavještenje i davanje saglasnosti za korišćenje ličnih podataka ..... 63
9.4.6. Otkrivanje informacije u skladu sa sudskim ili administrativnim procesom ..... 63
9.4.7. Ostale okolnosti kada se mogu otkrivati informacije ..... 63
9.5. Prava na intelektualnu svojinu ..... 63
9.6. Obaveze i odgovornosti ..... 63
9.6.1. Obaveze AIDRSCA ..... 63
9.6.2. Obaveze RA ..... 64
9.6.3. Odgovornosti i obaveze krajnjeg korisnika ..... 64
9.6.4. Odgovornosti i obaveze trećih lica ..... 65
9.6.5. Odgovornosti i garancije ostalih učesnika ..... 65
9.7. Izuzeća od odgovornosti ..... 65
9.8. Ograničenja finansijske odgovornosti ..... 66
9.9. Obeštećenja ..... 66
9.10. Stupanje na snagu i period važenja ..... 66
9.10.1. Stupanje na snagu ..... 66
9.10.2. Period važenja ..... 66
9.10.3. Efekti prekida važenja ..... 66
9.11. Individualno obavještavanje i komunikacija sa učesnicima ..... 66
9.12. Izmjene ..... 67
9.12.1. Procedura za izmjenu ..... 67
9.12.2. Mehanizmi obaveštavanja i vremenski periodi ..... 67
9.12.3. Okolnosti pod kojima se OID mora izmijeniti ..... 67
9.13. Rješavanja u slučaju spora ..... 67
9.14. Primjena zakona ..... 67
9.15. Usaglašenost sa primjenljivim zakonom ..... 67
9.16. Ostale odredbe ..... 68

9.16.1. Cjelokupni ugovor ..... 68
9.16.2. Prenos prava ..... 68
9.16.3. Klauzula o valjanosti ..... 68
9.16.4. Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava) ..... 68
9.16.5. Viša sila ..... 68
9.17. Napomene ..... 68

# 1. UVOD

Na osnovu člana 20. stav 2. Zakona o elektronskom potpisu Republike Srpske („Službeni glasnik Republike Srpske“, broj 59/08) i čl. 2 i 43 stav 2. Zakona o Vladi Republike Srpske („Službeni glasnik Republike Srpske“, br. 118/08), Vlada Republike Srpske je donijela „Uredbu o nosiocu poslova elektronske certifikacije u republičkim organima uprave“ kojom je **Agencija za informaciono društvo Republike Srpske** (u daljem tekstu: AIDRS) imenovana nosiocem poslova elektronske certifikacije u republičkoj upravi **Republike Srpske** (u daljem tekstu: RS). U svrhu ispunjavanja navedene uredbe AIDRS je izgradila infrastrukturu javnih kriptografskih ključeva (eng. Public Key Infrastructure – PKI) i na području RS prisutna je kao certifikaciono tijelo koje pruža usluge certifikacije organima republičke uprave RS.

Na osnovu zaključka Vlade RS **broj 04/1-012-2-2550/13** od **30.11.2013.** Agencija za informaciono društvo je zadužena da izdaje certifikate učesnicima u postupku registracije poslovnih subjekata i to:

- Agenciji za posredničke, informatičke i finansijske usluge Republike Srpske (APIF), i
- Okružnim privrednim sudovima u Republici Srpskoj.

**Praktična pravila pružanja usluga certifikacije** (eng. Certificate Practice Statement – CPS) je dokument koji opisuje postupke koje primjenjuje certifikaciono tijelo Agencije za informaciono društvo Republike Srpske (u daljem tekstu: AIDRSCA) prilikom procesa izdavanja kvalifikovanog elektronskog certifikata, upotrebe kvalifikovanog elektronskog certifikata od strane krajnjeg korisnika i opoziva kvalifikovanog elektronskog certifikata. Dakle, ovaj dokument opisuje kompletan životni ciklus kvalifikovanog elektronskog certifikata izdatog od strane AIDRSCA i upravljanje infrastrukturom AIDRSCA.

## 1.1. Pregled

CPS definiše prava i obaveze svih učesnika PKI sistema, u skladu sa 1.3., a kreiran je skladu sa RFC 3647 [1]. Sva pravila i procedure opisane u CPS-u urađene su u skladu sa propisima:

- Zakon o elektronskom potpisu RS - “Službeni glasnik Republike Srpske", br. 59/08, 68/13
- Pravilnik o mjerama zaštite elektronskog potpisa i kvalifikovanog elektronskog potpisa, najnižem iznosu obaveznog osiguranja i primjeni organizacionih i tehničkih mjera zaštite certifikata - “Službeni glasnik Republike Srpske", br. 88/09, 127/11

[1] RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“, novembar 2003.

- Pravilnik o tehničkim pravilima za osiguranje povezanosti evidencija izdatih i opozvanih certifikata certifikacionih tijela u Republici Srpskoj - "Službeni glasnik Republike Srpske", br. 127/11
- Pravilnik o sadržaju i načinu vođenja registra certifikacionih tijela za izdavanje kvalifikovanih elektronskih certifikata - "Službeni glasnik Republike Srpske", br. 127/11
- Pravilnik o evidenciji certifikacionih tijela - "Službeni glasnik Republike Srpske", br. 88/09, 127/11

AIDRSCA koristi u svojoj infrastrukturi za izdavanje kvalifikovanih elektronskih certifikata hijerarhiju više CA servera. Infrastruktura AIDRSCA je sastavljena od dva certifikaciona tijela:

- **AIDRS Root CA server**, kao Root certifikaciono tijelo, samopotpisani krovni CA; i
- **AIDRS Issuing CA server**, kao podređeno certifikaciono tijelo za izdavanje certifikata, potpisan od strane AIDRS Root CA.

AIDRS Root CA server radi kao Root certifikaciono tijelo na osnovu certifikata izdatog samom sebi u toku procesa generisanja privatnog kriptografskog ključa aplikacije certifikacionog tijela. AIDRSCA Root server izdaje certifikat podređenom certifikacionom tijelu koje je dio infrastrukture AIDRSCA.

AIDRS Issuing CA server izdaje kvalifikovane elektronske certifikate krajnjim korisnicima certifikata.

## 1.2. Naziv i identifikacija dokumenta

Ovaj dokument nosi naziv „Praktična pravila pružanja usluga" kao što je naznačeno na početnoj strani dokumenta.

Identifikaciona oznaka dokumenta (eng. Object Identifier – OID) je: **1.3.6.1.4.26614.10.1.1**

Identifikacione oznake politika certifikacije, certifikata koje izdaje AIDRSCA, prikazane su u tabeli 1.2.1.

| AIDRS profil certifikata | OID |
|---|---|
| **Profil AIDRSCA certifikata kranjeg korisnika** | **1.3.6.1.4.1.26614.10.1.1.1** |
| **Profil AIDRSCA testnog certifikata** | **1.3.6.1.4.1.26614.10.1.1.2** |

**Tabela 1.2.1** – OID politika certifikacije AIDRSCA certifikata

U tabeli 1.2.2 je dat prikaz generisanja OID-ova za AIDRSCA kao i objašnjenje njihovog značenja.

<table>
<tr><th colspan="2">OID[2]</th><th>Objašnjenje</th></tr>
<tr><td colspan="2">1.3.6.1.4.1.26614.</td><td>Jedinstveni identifikacioni broj koji je dodjeljen Vladi Republike Srpske od strane IANA</td></tr>
<tr><td colspan="2">1.3.6.1.4.1.26614.10.</td><td>Jedinstveni identifikacioni broj dodjeljen AIDRS odnosno AIDRSCA od strane Vlade Republike Srpske</td></tr>
<tr><td rowspan="2">1.3.6.1.4.1.26614.10.X</td><td>X=0</td><td>Jedinstveni identifikacioni broj dodjeljen od strane AIDRSCA za dokument Opšta pravila pružanja usluga certifikacije</td></tr>
<tr><td>X=1</td><td>Jedinstveni identifikacioni broj dodjeljen od strane AIDRSCA za dokument Praktična pravila pružanja usluga certifikacije</td></tr>
<tr><td>1.3.6.1.4.1.26614.10.X.Y<br><br>Y – verzija dokumenta</td><td colspan="2">Jedinstveni identifikacioni broj dodijeljen od strane AIDRSCA za zvaničnu dokumentaciju pri čemu se koriste sljedeća značenja:<br><br>• X – vrsta dokumenta koji se koristi<br>(primjer za slučaj AIDRSCA:<br>X=0 -> Dokument „Opšta pravila pružanja usluga certifikacije“;<br>X=1 -> Dokument „Praktična pravila pružanja usluga certifikacije“<br><br>• Y – aktuelna verzija dokumenta koja je u zvaničnoj upotrebi</td></tr>
<tr><td rowspan="2">1.3.6.1.4.1.26614.10.X.Y.Z<br><br>Z – oznaka politike certifikacije certifikata</td><td>Z=1</td><td>Jedinstveni identifikacioni broj dodijeljen od strane AIDRSCA za politiku certifikacije kvalifikovanih certifikata</td></tr>
<tr><td>Z=2</td><td>Jedinstveni identifikacioni broj dodijeljen od strane AIDRSCA za politiku certifikacije testnih certifikata</td></tr>
</table>

**Tabela 1.2.2** – Objašnjenje procesa generisanja OID-ova i njihovog značenja unutar AIDRSCA

[2] Kada govorimo o OID-u politika certifikacije certifikata, Y predstavlja verziju CPS-a od koje je politika certifikacije certifikata uvedena. Dakle, sve ranije verzije CPS-a ne prepoznaju navedenu politiku certifikacije certifikata.

## 1.3. Učesnici PKI sistema

Učesnike PKI sistema čine AIDRSCA, korisnici usluga certifikacije (naručioci i krajnji korisnici) i treća lica.

### 1.3.1. AIDRSCA

AIDRSCA sastoji se od:

- PMA (eng. Policy Management Authority);
- CA (eng. Certification Authority); i
- RA (eng. Registration Authority).

#### *1.3.1.1. PMA*

Tijelo u okviru AIDRSCA odgovorno za administriranje, razmatranje, usvajanje i sprovođenje odluka koje se odnose na AIDRSCA. Obavlja nadzor nad radom CA, RA i ostalih učesnika u AIDRSCA poslovnim procesima.

#### *1.3.1.2. CA*

Tijelo u okviru AIDRSCA imenovano od strane PMA, zaduženo za kreiranje, potpisivanje i izdavanje certifikata, upravljanje životnim vijekom certifikata završno sa opozivom certifikata. CA radi u skladu sa CPS dokumentom, pri čemu su poslovni procesi načelno opisani u CPS, a detaljno propisani internim pravilnicima AIDRSCA.

AIDRCA obuhvata dva CA:

- **AIDRS Root CA**, samopotpisani krovni CA; i
- **AIDRS Issuing CA**, podređeni CA, potpisan od strane AIDRS Root CA.

#### *1.3.1.3. RA*

Tijelo u okviru AIDRSCA imenovano od strane PMA, zaduženo za identifikaciju korisnika i obradu korisničkih zahtjeva. Obrađene zahtjeve RA dostavlja CA koje kreira korisničke certifikate. RA je zaduženo za distribuciju korisničkih certifikata i komunikaciju sa korisnicima. Identifikacija i obrada zahtjeva od strane RA radi se u skladu sa Zakonom o elektronskom potpisu i podzakonskim aktima.

### 1.3.3. Korisnici

Korisnici usluga AIDRSCA su organi republičke uprave RS i zaposleni u organima republičke uprave RS, Agencija za posredničke, informatičke i finansijske usluge (APIF) i zaposleni u APIF-u i okružni privredni sudovi i zaposleni u okružnim privrednim sudovima. U svrhu jasnijeg definisanja korisnika i njihovih uloga u PKI sistemu uvodi se sljedeća terminologija:

- **Naručilac** - organ koji se obraća AIDRSCA za pružanje usluga certifikacije;
- **Odgovorna osoba** – lice koje predstavlja naručioca;
- **Krajnji korisnik** – lice zaposleno kod naručioca, kojem se dodjeljuje certifikat u svrhu obavljanja poslova za naručioca.

### 1.3.4. Treća lica

Treća lica su lica koja se pouzdaju u kvalifikovane elektronske certifikate izdate od AIDRSCA. Treća lica su obavezna provjeriti status certifikata u registru opozvanih certifikata (eng. Certificate Revocation List – CRL), pri čemu je CA odgovorno za redovno ažuriranje CRL.

Treća lica ni pod kojim uslovom ne treba da se oslanjaju na CRL nakon isteka roka važenja. Svako oslanjanje i pouzdavanje u CRL nakon isteka roka važenja, treća lica rade na svoju odgovornost.

### 1.3.5. Ostali učesnici

Ostali učesnici su sva lica, koja na bilo koji način učestvuju u radu AIDRSCA.

## 1.4. Upotreba certifikata

### 1.4.1. Područje primjene

AIDRSCA izdaje četiri vrste certifikata, od kojih svaka ima posebnu namjenu i područje primjene.

#### *1.4.1.1. Područje primjene AIDRS Root CA certifikata*

Ovaj certifikat je samopotpisani certifikat, a njegov privatni kriptografski ključ se koristi za:

- potpisivanje certifikata podređenih certifikacionih tijela; i
- potpisivanje CRL liste koju izdaje AIDRSA Root CA.

#### *1.4.1.2. Područje primjene AIDRS Issuing CA certifikata*

Ovaj certifikat je certifikat podređenog certifikacionog tijela koje izdaje kvalifikovane elektronske certifikate krajnjim korisnicima. Privatni kriptografski ključ AIDRS Issuing CA certifikata se koristi za:

- potpisivanje certifikata krajnjih korisnika, koje izdaje AIDRS Issuing CA; i
- potpisivanje CRL lista koje izdaje AIDRS Issuing CA.

#### *1.4.1.3. Područje primjene AIDRSCA kvalifikovanog certifikata krajnjeg korisnika*

AIDRS kvalifikovani certifikati za krajnje korisnike imaju identifikacionu oznaku politike certifikacije: 1.3.6.1.4.1.26614.10.1.1.1. i obavezno su kreirani na SSCD (eng. Secured Signature Creation Device) modulu, pri čemu se privatni kriptografski ključ nalazi na SSCD modulu i ne može se eksportovati.

Ovi certifikati i pripadajući privatni kriptografski ključevi se koriste za:

- generisanje kvalifikovanog elektronskog potpisa; i
- autentifikaciju, tj. identifikaciju korisnika certifikata.

#### *1.4.1.4. Područje primjene AIDRSCA testnog certifikata krajnjeg korisnika*

AIDRS testni certifikati za krajnje korisnike imaju identifikacionu oznaku politike certifikacije: 1.3.6.1.4.1.26614.10.1.1.2. i nisu obavezno kreirani na SSCD modulu.

Ovi certifikati i pripadajući kriptografski ključevi se izdaju isključivo zaposlenima u AIDRSCA i koriste se isključivo u testne svrhe.

- Mogu da se koriste za generisanje elektronskog potpisa u svrhu testiranja;
- Ne mogu da se koriste za generisanje kvalifikovanog elektronskog potpisa; i
- Ne mogu da se koriste za validnu autentifikaciju tj. identifikaciju korisnika, ali se mogu koristiti za simulaciju scenarija autentifikacije u svrhe testiranja i razvoja web servisa.

### 1.4.2. Nedozvoljene primjene

Upotreba kvalifikovanog elektronskog certifikata se vrši u skladu sa Zakonom o elektronskom potpisu RS i podzakonskim aktima. Svaka druga upotreba kvalifikovanog elektronskog certifikata koja nije u saglasnosti sa gore navedenim propisima i ovim dokumentom nije dozvoljena.

## 1.5. Politika administriranja dokumenta

### 1.5.1. Organizacija upravljanja dokumentom

Dokument „Praktična pravila pružanja usluga certifikacije“ kreiran je i ažuriran od strane AIDRSCA:

JAVNA USTANOVA „AGENCIJA ZA INFORMACIONO DRUŠTVO REPUBLIKE SRPSKE“

TRG REPUBLIKE SRPSKE 1

78000 BANJALUKA

Telefon: + 387 51 339 777

Faks: + 387 51 339 776

Elektronska pošta: info@aidrs.org , ca@aidrs.org

Web stranica AIDRS : http://www.aidrs.org

Web stranice AIDRSCA: http://ca.aidrs.org

Tekuća verzija dokumenta može se preuzeti sa web strane: http://ca.aidrs.org/dokumentacija

### 1.5.2. Lica za kontakt

Lica za kontakt su svi zaposleni u okviru AIDRSCA koji su ovlašćeni za pružanje informacija u vezi ovog dokumenta, poslovnih procesa AIDRSCA, kao i komunikacije sa korisnikom. Kontakt informacije rukovodioca i ostalih zaposlenih AIDRSCA, mogu se preuzeti sa web strane: http://ca.aidrs.org

### 1.5.3. Lica određena za usklađivanje dokumenta sa praksom izdavanja certifikata

Sve promjene poslovnih procesa AIDRSCA koje utiču na korisnike certifikata uzrokuju usklađivanje sa ovim dokumentom, za što je zadužen PMA.

### 1.5.4. Procedura za odobrenje Praktičnih pravila

U nastavku, opisana je procedura kojoj se pristupa u slučaju ažuriranja, korekcija ili kreiranja nove verzije dokumenta „Praktična pravila pružanja usluga“.

- CA kreira novu verziju CPS-a u skladu sa izmjenama u poslovnim procesima AIDRSCA;
- CA podnosi novu verziju CPS-a prema PMA na validaciju i odobravanje; i

- PMA odobrava novi CPS ili ga vraća CA na dodatne korekcije.

## 1.6. Definicije i skraćenice

### 1.6.1. Definicije

U tabeli 1.6.1.1 je dat prikaz i objašnjenje pojedinih izraza koji se koriste u ovom dokumentu.

| Definicija | Značenje definicije[3] |
|---|---|
| **Certifikaciono tijelo** | Pravno ili fizičko lice koje izdaje elektronske certifikate ili daje druge usluge koje su u vezi sa elektronskim potpisima |
| **Kvalifikovani elektronski certifikat** | Elektronski certifikat koji ispunjava uslove iz člana 11. Zakona o elektronskom potpisu i koji izdaje certifikaciono tijelo, a koje ispunjava uslove iz člana 17. ovog zakona |
| **Kvalifikovani elektronski potpis** | Potpis koji kojim se pouzdano garantuje identitet potpisnika i koji ispunjava uslove iz člana 4. Zakona o elektronskom potpisu |
| **Potpisnik** | Lice koje posjeduje sredstvo za izradu elektronskog potpisa, a koje djeluje u svoje ime ili u ime fizičkog ili pravnog lica |
| **Elektronski zapis** | Cjelovit skup podataka koji su elektronski generisani, poslani, primljeni ili sačuvani na elektronskom, magnetnom, optičkom ili drugom mediju. Sadržaj elektronskog zapisa uključuje sve oblike pisanog i drugog teksta, podatke, slike i crteže, karte, zvuk, muziku, govor i računarske baze podataka |
| **Elektronski potpis** | Skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku i koji služe za identifikaciju potpisnika i autentičnost potpisanog elektronskog dokumenta |
| **Podaci za izradu elektronskog potpisa** | Jedinstevni podaci, kao što su kodovi ili privatni kriptografski ključevi koje potpisnik koristi za izradu elektronskog potpisa |
| **Sredstvo za izradu elektronskog potpisa** | Odgovarajuća računarska oprema ili računarski program koji potpisnik koristi pri izradi elektronskog potpisa |

[3] Zakon o elektronskom potpisu RS - “Službeni glasnik Republike Srpske", br. 59/08

| Definicija | Značenje definicije[3] |
|---|---|
| **Sredstvo za izradu kvalifikovanog elektronskog potpisa** | Sredstvo za izradu potpisa koje ispunjava uslove iz člana 9. Zakona o elektronskom potpisu |
| **Podaci za verifikovanje elektronskog potpisa** | Podaci, kao što su kodovi ili javni kriptografski ključevi koji se koriste radi verifikovanja (ovjere) elektronskog potpisa |
| **Sredstvo za verifikovanje elektronskog potpisa** | Odgovarajuća računarska oprema ili računarski program koji se koristi za primjenu podataka za verifikovanje potpisa |
| **Elektronski certifikat** | Potvrda u elektronskom obliku koja povezuje podatke za verifikovanje elektronskog potpisa sa nekim licem i potvrđuje identitet tog lica |
| **Sredstvo za elektronski potpis** | Računarska oprema ili računarski program ili njihovi relevantni dijelovi koji su namijenjeni certifikacionom tijelu u vezi sa elektronskim potpisima ili su namijenjeni za primjenu prilikom izrade ili verifikovanja elektronskih potpisa |
| **Identifikacioni dokument** | Lična karta ili pasoš |
| **Krajnji korisnik** | Lice zaposleno kod naručioca, kojem se dodjeljuje certifikat u svrhu obavljanja poslova za naručioca. |
| **Naručilac** | Organ koji se obraća AIDRSCA za pružanje usluga certifikacije |
| **Odgovorna osoba** | Lice koje predstavlja naručioca (ministar / direktor) |
| **Ovlaštena osoba** | Lice koje je ovlašteno od strane odgovorne osobe da komunicira sa AIDRSCA u ime naručioca |
| **Web strana AIDRSCA** | Odnosi se na zvaničnu prezentaciju AIDRSCA |
| **Web adresa AIDRSCA** | Odnosi se na bilo koju adresu u sklopu zvanične prezentacije AIDRSCA, koja može biti namjenjena za korisnički pristup ili pristup od strane klijentskog softvera. |
| **arhiva CA** | Sva elektronska i papirna arhiva CA |
| **arhiva RA** | Sva elektronska i papirna arhiva RA |

**Tabela 1.6.1.1** – Definicije izraza koji se koriste u dokumentu

### 1.6.2. Skraćenice

U tabeli 1.6.2.1 je dat prikaz skraćenica koje se koriste u ovom dokumentu kao i njihovo značenje.

| Skraćenica | Značenje skraćenice |
|---|---|
| **AIDRS** | Agencija za informaciono društvo Republike Srpske |
| **AIDRSCA** | Certifikaciono tijelo Agencije za informaciono društvo Republike Srpske |
| **CA** | eng. Certifiticate Authority – Certifikaciono tijelo |
| **CPS** | eng. Certificate Practice Statement – Praktična pravila pružanja usluga certifikacije |
| **CRL** | eng. Certificate Revocation List – Registar opozvanih certifikata |
| **OID** | eng. Object Identifier – Jedinstveni identifikacioni broj objekta na mreži |
| **PKI** | eng. Public Key Infrastructure – Infrasturktura javnih ključeva |
| **PMA** | eng. Policy Management Authority – Tijelo za menadžment politika CA |
| **RA** | eng. Registration Authority – Registraciono tijelo |
| **RFC** | eng. Request for comments |
| **RS** | Republika Srpska |
| **CDP** | eng. CRL Distribution Points – Direktorij opozvanih certifikata |
| **SSCD** | eng. Secured Signature Creation Device - sigurnosni kriptografski modul, odnosno modul na kojem se nalazi par kriptografskih ključeva krajnjeg korisnika zaštićeni PIN kodom |
| **PEN** | eng.Private Enterprise Numbers – jedinstveni identifikacioni broj organizacije |
| **IANA** | eng. Internet Assigned Number Authority – međunarodno priznato tijelo za dodjelu OID-ova |
| **DN** | eng. Distinguished Name – Jedinstveno ime |

**Tabela 1.6.2.1** – Skraćenice koje se koriste u ovom dokumentu

# 2. OBJAVLJIVANJE I LOKACIJA PODATAKA O CERTIFIKACIJI

## 2.1. Lokacija i objavljivanje podataka o certifikaciji

AIDRS objavljuje podatke i svu dokumentaciju koja se odnosi na izdavanje kvalifikovanih elektronskih certifikata na web strani: http://ca.aidrs.org koja je javno dostupna, zajedno sa navedenim podacima i dokumentacijom.

Sva javna dokumentacija AIDRSCA nalazi se na web adresi: http://ca.aidrs.org/dokumentacija. Registar povučenih certifikata nalazi se na web adresi: http://cdp.aidrs.org/crl (adresa navedena u CDP svakog certifikata krajnjeg korisnika), a sekundarna lokacija registra povučenih certifikata nalazi se na web adresi: http://cdp2.aidrs.org/crl (adresa navedena u CDP svakog certifikata krajnjeg korisnika).

Certifikati AIDRS Root CA i AIDRS Issuing CA mogu se preuzeti sa web adrese: http://ca.aidrs.org/aia.

## 2.2. Objavljivanje podataka o certifikaciji

AIDRSCA objavljuje na svojoj zvaničnoj web strani sljedeće podatke:

- Zakon o elektronskom potpisu RS i podzakonske akte;
- dokument „Praktična pravila pružanja usluga certifikacije“;
- obrazac zahtjeva za korišćenje usluga certifikacionog tijela Agencije za informaciono društvo Republike Srpske;
- obrazac zahtjeva za izdavanje kvalifikovanog elektronskog certifikata;
- obrazac zahtjeva za promjenu statusa kvalifikovanog elektronskog certifikata;
- obrazac ugovora o obavljanju usluga certifikacije;
- korisnička uputstva;
- certifikate AIDRS Root CA i AIDRS Issuing CA sa pridruženim hash vrijednostima;
- registre opozvanih certifikata; i
- druga akta i obavještenja.

## 2.3. Učestalost objavljivanja podataka o certifikaciji

AIDRSCA ažurira objavljene podatke sljedećom dinamikom:

- podaci o opozvanim certifikatima objavljuju se dinamikom opisanom u sekciji 4.9.7. Učestalost objavljivanja CRL;
- promjene na postojećim dokumentima objavljuju se u najkraćem intervalu poslije nastale promjene; i
- dodatni dokumenti objavljuju se u najkraćem roku po odobravanju.

## 2.4. Kontrola pristupa podacima o certifikaciji

Svi podaci koji se nalaze unutar javnog repozitorija javno su dostupni korisnicima za čitanje i preuzimanje. AIDRSCA je uspostavilo javni repozitorij podataka na način koji obezbjeđuje adekvatnu zaštitu od neovlaštene promjene podataka i brisanja istih.

# 3. IDENTIFIKACIJA I AUTENTIFIKACIJA

## 3.1. Konvencija imenovanja

### 3.1.1. Vrste imena

U kvalifikovanim certifikatima koje izdaje AIDRSCA imena korisnika su predstavljena kao jedinstvena (eng. distinguished name - DN) u obliku *X.509 v3* i vjerodostojno interpretiraju ime i prezime korisnika koristeći tip podataka UTF-8 String.

Znakovi koje nije dozvoljeno koristiti u imenima korisnika su: " (navodnici), ? (upitnik), \ (*obrnuta kosa crta*), # (taraba), $ (dolar), % (procenat), = (jednako), + (plus), |(uspravna crta), ; (tačka zarez), < (manje), > (veće) i , (zarez).

### 3.1.2. Nomenklatura imena

AIDRSCA je usvojilo nomenklaturu po kojoj garantuje jedinstvenost imena u svom domenu (tj. u svojoj direktorijskoj strukturi). Sadržaj svakog polja imena mora imati vezu sa korisnikovim autentičnim imenom. Za korisnika, jedinstvenost korisničkog imena obezbjeđena je kombinacijom imena i prezimena korisnika i njegovog jedinstvenog matičnog broja, kao što je navedeno u sekciji 3.1.5. Jedinstvenost imena.

### 3.1.3. Anonimnost ili pseudonimi korisnika

Korisnici ne mogu da budu anonimni niti mogu da koriste isključivo pseudonime. Upotreba pseudonima je moguća jedino u okvirima koji su propisani Zakonom o elektronskom potpisu, Član 11. stav 2) tačka v.

AIDRSCA odbija svaki zahtjev unutar kog korisnik želi da bude anoniman ili želi da koristi isključivo pseudonim.

### 3.1.4. Pravila za interpretaciju vrsta imena

Unutar AIDRSCA, razlikujemo 3 vrste imena:

- imena certifikacionih tijela; i
- imena krajnjih korisnika usluga certifikacije.

### *3.1.4.1. Imena certifikacionih tijela*

Struktura imena AIDRS Root CA prikazana je u tabeli 3.1.4.1.1., a struktura imena AIDRS Issuing CA prikazana je u tabeli 3.1.4.1.2.

| Komponenta imena | Vrijednost |
|---|---|
| **DC** | ba |
| **DC** | rs |
| **DC** | aidrs |
| **CN** | configuration |
| **CN** | services |
| **CN** | Public Key Services |
| **CN** | AIA |
| **CN** - ime CA servera | AIDRS Root CA |

**Tabela 3.1.4.1.1.** - Struktura imena AIDRS Root CA

| Komponenta imena | Vrijednost |
|---|---|
| **DC** | ba |
| **DC** | rs |
| **DC** | aidrs |
| **CN** | configuration |
| **CN** | services |
| **CN** | Public Key Services |
| **CN** | AIA |
| **CN** - ime CA servera | AIDRS Issuing CA |

**Tabela 3.1.4.1.2. -** Struktura imena AIDRS Issuing CA

### *3.1.4.2. Imena krajnjih korisnika usluga certifikacije*

Struktura imena krajnjih korisnika usluga certifikacije prikazana je u tabeli 3.1.4.3.1.

| Komponenta imena | Vrijednost |
|---|---|
| **DC** | ba |
| **DC** | rs |
| **DC** | aidrs |
| **DC** | ca |
| **OU** | [naziv kategorije naručioca] |
| **OU** | [naziv organa] |
| **CN** | [ime korisnika][4] |

**Tabela 3.1.4.2.1.** - Struktura imena krajnjeg korisnika usluga certifikacije

### 3.1.5. Jedinstvenost imena

Certifikaciono tijelo AIDRS garantuje jedinstvenost imena u svom domenu.

Jedinstvenost imena garantuje se na sljedeći način:

- **Pun naziv organa:** naziv institucije _ JIB; i
- **Puno ime korisnika:** ime korisnika _ prezime korisnika _ serijski broj [5]_ tip certifikata
    - tip certifikata = KVC – Kvalifikovani elektronski certifikat krajnjeg korisnika
    - tip certifikata = TEC – Testni elektronski certifikat krajnjeg korisnika

Napomena: ''_'' predstavlja vizuelnu reprezentaciju praznog polja, odnosno znaka ''space''.

[4] Struktura imena krajnjih korisnika razlikuje se po zadnja dva OU parametra I CN parametru. Prvi OU predstavlja naziv kategorije naručioca, a sljedeći OU predstavlja naziv organa unutar kog je korisnik zaposlen, a CN predstavlja lično ime korisnika u skladu sa 3.1.2.

[5] Serijski broj predstavlja jedinstvenu oznaku za svaki certifikat.

### 3.1.6. Priznavanje, autentifikacija i uloga zaštitnog znaka

Imena kojima bi se kršila intelektualna ili autorska prava drugih nisu dozvoljena. AIDRSCA nije obavezno da verifikuje da li je korišćenje takvih imena zakonito. Naručilac, odnosno korisnik koji se identifikuje je dužni dostaviti identifikacioni dokument kojim se pouzdano može utvrditi identitet osobe.

## 3.2. Inicijalna provjera identiteta

### 3.2.1. Metoda dokazivanja posjeda privatnog ključa

Privatni ključ korisnika kreira se na sigurnosnom kriptografskom modulu (eng. *Secure Signature Creation Device – SSCD*) u okviru kontrolisanog procesa na aplikaciji CA, nakon čega se SSCD modul preuzima lično od strane naručioca ili krajnjeg korisnika. Prilikom preuzimanja SSCD modula potvrđen je posjed privatnog ključa, a evidentiran kroz protokol RA.

### 3.2.2. Identifikacija i autentifikacija identiteta organa

Kvalifikovani elektronski certifikat se može izdati krajnjem korisniku čije ime je naznačeno u CN, odnosno krajnjem korisniku koji ima pravo da u ime organa, u kojem je zasposlen, koristi taj kvalifikovani elektronski certifikat. U procesu autentifikacije organa potrebno je utvrditi tačan identitet institucije i autorizovanje korišćenja njenog imena u skladu sa Zakonom kao i identitet odgovornog lica.

### 3.2.3. Identifikacija i autentifikacija krajnjeg korisnika

Identifikacija krajnjeg korisnika odvija se od strane RA tako što se krajnji korisnik lično identifikuje ispred RA predočavanjem važećeg identifikacionog dokumenta.

### 3.2.4. Podaci o korisniku koji se ne mogu provjeriti

Unutar podataka o korisniku koji se ne mogu provjeriti su:

- svi podaci koji se nalaze na korisničkom zahtjevu, a ne nalaze se na ličnoj karti ili pasošu; i
- adresa elektronske pošte (pri čemu se vrši provjera domena organa, ali ne i provjera same adrese elektronske pošte krajnjeg korisnika).

### 3.2.5. Kriteriji za međusobnu saradnju

Procedure i praksa povezanih certifikacionih tijela moraju biti materijalno ekvivalentni procedurama i praksi AIDRS CA, kao što je definisano u ovom CPS. PMA vrši procjenu procedura i praksi certifikacionog tijela sa kojim se želi uspostaviti međusobna saradnja, od slučaja do slučaja.

# 4. PROCEDURE ŽIVOTNOG CIKLUSA CERTIFIKATA

## 4.1. Zahtjev za izdavanje certifikata

### 4.1.1. Ko može da podnese zahtjev za izdavanje certifikata

Zahtjev za izdavanje certifikata može da podnese krajnji korisnik, ako je ispunjen uslov da postoji zaključen Ugovor o pružanju usluga certifikacije između AIDRSCA i naručioca.

### 4.1.2. Proces podnošenja zahtjeva i obaveze

Naručilac podnosi zahtjev u ime krajnjeg korisnika, na sljedeći način:

- Krajnji korisnik popunjava obrazac zahtjeva za izdavanje kvalifikovanog elektronskog certifikata i svojeručno ga potpisuje i predaje naručiocu;
- Naručilac službenim putem dostavlja korisnički zahtjev ka RA;
- RA vrši provjeru ispravnosti zahtjeva i prosljeđuje primljeni zahtjev ka CA;

## 4.2. Obrada zahtjeva za izdavanje certifikata (od strane CA)

### 4.2.1. Sprovođenje funkcija identifikacije i autentifikacije

Sve identifikacije i autentifikacije sprovodi RA.

### 4.2.2. Odobrenje ili odbijanje zahtjeva za izdavanje certifikata

Nakon što RA izvrši provjeru zahtjeva za izdavanje kvalifikovanog elektronskog certifikata i utvrdi da su ispunjeni svi uslovi, RA prosljeđuje taj zahtjev ka CA. CA utvrđuje da li je zahtjev stigao od RA, i nakon potvrde stupa u proces obrade zahtjeva, u roku propisanom u 4.2.3. Vrijeme obrade zahtjeva za izdavanje certifikata. Ukoliko zahtjev za izdavanje kvalifikovanog elektronskog certifikata bude odbijen od strane RA, ovaj zahtjev se ne prosljeđuje ka CA.

### 4.2.3. Vrijeme obrade zahtjeva za izdavanje certifikata

Obrada zahtjeva na strani RA vrši se na licu mjesta.

Obrada zahtjeva na strani CA vrši se u periodu ne dužem od 10 radnih dana.

## 4.3. Izdavanje certifikata

### 4.3.1. Aktivnosti i postupci CA prilikom izdavanja certifikata

Izdavanje kvalifikovanog elektronskog certifikata vrši ovlašteno osoblje CA na sledeći način:

- prihvatanje zahtjeva od strane RA;
- kreiranje korisničkog naloga unutar CA aplikacije;
- vrši se personalizacija SSCD modula:
    - kreiranje korisničkog para ključeva na SSCD modulu;
    - preuzimanje korisničkog certifikata od CA aplikacije i zapis na SSCD modul;
    - generisanje slučajnog PIN-a za upotrebu SSCD modula;
    - štampanje PIN-a na zatvorenu kovertu;
    - vizuelna personalizacija SSCD modula; i
- Dostavljanje personalizovanog SSCD modula i kovertiranog PIN-a ka RA.

### 4.3.2. Obavještavanje o izdavanju certifikata

RA šalje obavještenje krajnjem korisniku o izdavanju kvalifikovanog elektronskog certifikata na prethodno utvrđenu adresu elektronske pošte, koja je navedena u zahtjevu za izdavanje kvalifikovanog elektronskog certifikata ili krajnjem korisniku putem telefonskog poziva na prethodno naveden broj telefona.

## 4.4. Preuzimanje certifikata

### 4.4.1. Akcija kojom korisnik povrđuje da je preuzeo certifikat

Potpisivanjem Ugovora o izdavanju kvalifikovanog elektronskog certifikata, potvrđuje se da je krajnji korisnik preuzeo certifikat.

Krajnji korisnik ima pravo da u roku od 10 radnih dana od dana preuzimanja certifikata ukaže na netačnost podataka unutar certifikata. U slučaju kada krajnji korisnik u navedenom roku ne ukaže na netačnost podataka unutar certifikata, smatra se da su podaci unutar certifikata tačni.

### 4.4.2. Objavljivanje certifikata

Kvalifikovani elektronski certifikati krajnjih korisnika se javno ne objavljuju od strane AIDRSCA.

### 4.4.3. Obavještavanje trećih lica o izdavanju certifikata

Treća lica se ne obavještavaju o izdavanju kvalifikovanih elektronskih certifikata.

## 4.5. Korišćenje para kriptografskih ključeva i certifikata

### 4.5.1. Upotreba privatnog ključa i certifikata sa strane korisnika

Privatni kriptografski ključ korisnika koristi se za kreiranje kvalifikovanog elektronskog potpisa i autentifikaciju korisnika, a kvalifikovani elektronski certifikat koristi se za verifikovanje kvalifikovanog elektronskog potpisa.

**Krajnji korisnik je dužan:**

- koristiti privatni ključ i certifikat u skladu sa Zakonom o elektronskom potpisu i podzakonskim aktima;
- privatni ključ koristi za slučajeve definisane u 1.4.1. Područje primjene, a ne može ga koristiti za slučajeve definisane u 1.4.2. Nedozvoljene primjene;
- osigurati da privatni ključ i PIN SSCD modula ne budu kompromitovani; i
- obavezati se da neće koristiti privatni ključ nakon njegovog isteka ili opoziva certifikata.

### 4.5.2. Upotreba javnog ključa i certifikata sa strane trećih lica

Treća lica koriste javni ključ i kvalifikovani elektronski certifikat za verifikovanje kvalifikovanog elektronskog potpisa, u skladu sa Zakonom o elektronskom potpisu, podzakonskim aktima i sekcijama 1.4.1. Područje primjene i 1.4.2. Nedozvoljene primjene, ovog dokumenta.

Treća lica moraju biti svjesna svih ograničenja i upotrebe javnih ključeva i certifikata definisanih u ovom dokumentu.

Treće lice snosi odgovornost za provjeru statusa certifikata prilikom verifikovanja kvalifikovanog elektronskog potpisa, kao u 9.6.4. Odgovornosti i obaveze trećih lica.

## 4.6. Obnova certifikata bez promjene javnog ključa

AIDRSCA ne dozvoljava obnovu kvalifikovanog elektronskog certifikata bez promjene javnog ključa.

## 4.7. Obnova certifikata sa promjenom javnog ključa

Pod obnovom certifikata sa promjenom javnom ključa podrazumjeva se ponovno izdavanje kvalifikovanog elektronskog certifikata u skladu sa opisanim procedurama.

## 4.8. Promjena podataka u certifikatu

Promjena podataka u certifikatu rezultuje izdavanjem novog certifikata sa promjenjenim podacima i sa novim javnim ključem.

### 4.8.1. Okolnosti za izmjenu podataka u certifikatu

Okolnosti pod kojima korisnik može tražiti izmjenu podataka u certifikatu jesu:

- Bilo koja promjena obaveznih podataka propisanih zakonom, a koji se nalaze u certifikatu;
- Promjena adrese elektronske pošte koja je vezana za korisnika; i
- Promjena naziva direktorija usljed promjene naziva institucije ili promjene organizacione strukture direktorija.

### 4.8.2. Ko može da zahtjeva promjenu podataka u certifikatu

Promjenu podatka u kvalifikovanom elektronskom certifikatu može da zahtjeva naručilac usluge certifikacije ukoliko su ispunjeni uslovi iz 4.8.1. Okolnosti za izmjenu podataka u certifikatu, a na osnovu sopstvene procjene ili na osnovu zahtjeva primljenog od strane krajnjeg korisnika.

### 4.8.3. Proces obrade zahtjeva za promjenu podataka u certifikatu

Proces obrade zahtjeva za promjenu podataka u certifikatu se izvodi na isti način kao i proces obrade zahtjeva za izdavanje certifikata.

### 4.8.4. Obavještavanje korisnika o izdavanju certifikata sa promjenjenim podacima

Obavještavanje korisnika o izdavanju certifikata sa promjenjenim podacima sprovodi se na isti način kao i u sekciji 4.3.2. Obavještavanje o izdavanju certifikata.

### 4.8.5. Akcija kojom korisnik povrđuje da je preuzeo certifikat sa promjenjenim podacima

Akcija kojom korisnik povrđuje da je preuzeo certifikat sa promjenjenim podacima se sprovodi na isti način kao i u sekciji 4.4.1. Akcija kojom korisnik povrđuje da je preuzeo certifikat.

### 4.8.6. Objava certifikata sa promjenjenim podacima

Kvalifikovani elektronski certifikati krajnjih korisnika se ne objavljuju javno od strane AIDRSCA.

### 4.8.7. Obavještavanje trećih lica o izdavanju certifikata sa promjenjenim podacima

Treća lica se ne obavještavaju o izdavanju kvalifikovanih elektronskih certifikata.

## 4.9. Opoziv i suspenzija certifikata

AIDRSCA pruža usluge opoziva kvalifikovanih elektronskih certifikata, a ne pruža uslugu suspenzije kvalifikovanih elektronskih certifikata.

### 4.9.1. Okolnosti za opoziv

Certifikaciono tijelo obavezno je da prekine uslugu certifikacije, odnosno izvrši opoziv certifikata onim potpisnicima:

- kod kojih je došlo do raskida ugovora između naručioca i AIDRSCA u skladu sa sekcijom 4.11. Prekid ugovora sa naručiocem;
- koji su to izričito tražili;
- za koje se sumnja ili je utvrđena netačnost ili nepotpunost podataka u certifikatu;
- za koje je utvrđena netačnost ili nepotpunost podataka u evidenciji certifikata;
- za koje je primljena službena obavijest o smrti;
- za koje je primljena službena obavjest o gubitku poslovne sposobnosti;
- za koje se sumnja ili je utvrđena kompromitovanost privatnog ključa korisnika;
- za koje se sumnja ili je utvrđena kompromitovanost PIN koda SSCD modula; i
- za koje se sumnja ili je utvrđeno kršenje odredbi Zakona o elektronskom potpisu, podzakonskih akata i ovog dokumenta.

### 4.9.2. Ko može da zahtjeva opoziv certifikata

**Opoziv certifikata može zahtjevati:**

- naručilac certifikata na osnovu vlastite procjene ili na osnovu zahtjeva krajnjeg korisnika;
- AIDRSCA; i
- nadležni državni organ.

### 4.9.3. Procedure za opoziv certifikata

Procedure za opoziv certifikata su sljedeće:

- Naručilac certifikata može podnijeti zahtjev za opoziv certifikata direktno na RA;
- Krajnji korisnik certifikata može zahtjevati opoziv certifikata putem elektronske pošte potpisane kvalifikovanim potpisom korisnika certifikata koji se opoziva;
- Krajnji korisnik certifikata može zahtjevati opoziv svog certifikata na način kako je to definisano u sekciji 3.4. Identifikacija i autentifikacija zahtjeva za opozivom;

### 4.9.4. Vrijeme za podnošenje zahtjeva za opoziv certifikata

Podnošenje zahtjeva za opoziv certifikata treba izvršiti u najkraćem mogućem roku od trenutka nastanka bilo koje okolnosti za opoziv certifikata opisane u sekciji 4.9.1. Okolnosti za opoziv.

### 4.9.5. Vrijeme u kojem CA mora izvršiti obradu zahtjeva za opoziv

Obrada zahtjeva za opoziv certifikata biće izvršena najkasnije do kraja narednog radnog dana od momenta podnošenja zahtjeva za opoziv certifikata u skladu sa sekcijama 4.9.3. Procedure za opoziv certifikata i 4.9.4. Vrijeme za podnošenje zahtjeva za opoziv certifikata.

### 4.9.6. Provjera opozvanosti certifikata od strane trećih lica

Treća lica su dužna provjeriti CRL listu prije korišćenja bilo kojeg certifikata izdatog od strane AIDRSCA.

Ukoliko u datom trenutku nije moguće provjeriti status certifikata na CRL listi, ne preporučuje se prihvatanje certifikata čiji su statusi neprovjereni, u suprotnom treća lica snose svu odgovornost za prihvatanje takvog certifikata .

### 4.9.7. Učestalost objavljivanja CRL

Svaki opoziv certifikata rezultuje objavljivanjem nove CRL liste.

U slučaju da nema opoziva certifikata, životni vijek CRL liste može biti maksimalno:

- 180 dana, u slučaju AIDRS Root CA CRL liste; i
- 2 dana, u slučaju AIDRS Issuing CA CRL liste.

CA objavljuje novu CRL listu maksimalno 1 dan prije isteka stare CRL liste.

### 4.9.8. Maksimalno dozvoljeno zakašnjenje kod objave CRL liste

Maksimalno kašnjenje objave CRL liste u javnom repozitoriju jeste 1 sat. U slučaju nepredviđenih okolnosti koje rezultuju dužim kašnjenjem CRL liste certifikaciono tijelo će obavjestiti korisnike o razlogu kašnjenja i vremenskom intervalu unutar kog nije objavljena validna CRL lista.

### 4.9.9. Online provjera statusa certifikata (OCSP)

AIDRSCA ne pruža ovu uslugu.

### 4.9.10. Online provjera statusa certifikata od strane trećih lica

AIDRSCA ne pruža ovu uslugu.

### 4.9.11. Drugi oblici provjere statusa certifikata

AIDRSCA ne pruža ovu uslugu.

### 4.9.12. Posebni zahtjevi u slučaju kompromitovanja ključa

Ne postoje posebni zahtjevi u slučaju kompromitovanja ključa.

### 4.9.13. Okolnosti za suspenziju korisničkog certifikata

U skladu sa sekcijom 4.9. Opoziv i suspenzija certifikata, AIDRSCA ne pruža uslugu suspenzije korisničkog certifikata.

### 4.9.14. Ko može zahtjevati suspenziju korisničkog certifikata

AIDRSCA ne pruža uslugu suspenzije korisničkog certifikata.

### 4.9.15. Proces obrade zahtjeva za suspenziju korisničkog certifikata

AIDRSCA ne pruža uslugu suspenzije korisničkog certifikata.

### 4.9.16. Period trajanja suspenzije korisničkog certifikata

AIDRSCA ne pruža uslugu suspenzije korisničkog certifikata.

## 4.10. Usluge o statusu certifikata

### 4.10.1. Operacione karakteristike

CRL liste su kreirane u skladu sa X.509 v2 i preporukama RFC 3280 dokumenta. Lokacija CRL liste nalazi se unutar CDP ekstenzije korisničkog certifikata.

### 4.10.2. Dostupnost servisa

AIDRSCA garantuje dostupnost servisa za objavljivanje CRL lista 24 sata/7 dana nedeljno, uz maksimalne neplanirane prekide rada najviše dvanaest (12) dana u godini. U slučaju planiranih prekida servisa, informacija o vremenu i planiranom periodu prekida servisa biće objavljena na javnoj web strani kao što je definisano u sekciji 2. Objavljivanje i lokacija podataka o certifikaciji.

### 4.10.3. Dodatne karakteristike

Na CRL listama nema dodatnih karakteristika.

## 4.11. Prekid ugovora sa naručiocem

Razlozi za prekid ugovora sa naručiocem mogu biti:

- Eksplicitni zahtjev naručioca za prekid Ugovora o pružanju usluga certifikacije;
- U slučaju kada naručilac prestaje da postoji; i
- Ukoliko naručilac krši prava i obaveze definisane Zakonom o elektronskom potpisu, podzakonskih akata i ovog dokumenta.

Prekidom ugovora sa naručiocem automatski se prekida usluga pružanja certifikacije svim korisnicima koji su certifikate dobili po osnovu ovog ugovora i automatski se vrši opoziv svih certifikata ovog naručioca.

## 4.12.* Deponovanje i obnova privatnog ključa korisnika

Certifikaciono tijelo zabranjuje deponovanje i obnovu privatnog ključa korisnika za kvalifikovane elektronske certifikate.

# 5. FIZIČKA KONTROLA, OPERATIVNA KONTROLA I UPRAVLJANJE RESURSIMA

Ovo poglavlje opisuje fizičku kontrolu, operativnu kontrolu i procedure koje definišu način sprovođenja navedenih kontrola, upravljanje resursima certifikacionog tijela, zahtjeve za obuku zaposlenih, kao i za akviziciju dodatnih znanja angažovanjem spoljnih saradnika i obezbjeđivanjem adekvatne ekspertize. Takođe ovo poglavlje opisuje vođenje evidencija certifikacionog tijela, revizijskih dnevnika, kao i procedure arhiviranja.

## 5.1. Fizička kontrola

Pošto se oprema AIDRSCA nalazi u server sali, lociranoj u zgradi Vlade RS, sva pravila fizičke kontrole AIDRSCA tijela usklađena su sa postojećom infrastrukturom i praksama fizičke kontrole. Ove prakse se odnose na:

- Lokaciju i konstrukciju prostorije
- Kontrolu fizičkog pristupa
- Napajanje i klimatizaciju
- Zaštitu od poplave, vode
- Zaštitu od požara
- Čuvanje i smještanje podataka
- Uništavanje nepotrebnih materijala
- Pohranjivanje podatka na rezervnu lokaciju

## 5.2. Kontrola procedura

### 5.2.1. Povjerljive uloge osoblja certifikacionog tijela

AIDRSCA garantuje da sve poslove koji se obavljaju u okviru propisane djelatnosti obavljaju osobe od povjerenja sa tačno propisanim obavezama i ovlaštenjima. Rad ovih osoba je podložan stalnim provjerama.

Ovlašćena lica AIDRSCA mogu da imaju određene ulogu, odnosno da obavljaju poslove na:

- serverima AIDRSCA;
- HSM modulu;
- aplikaciji CA;
- aplikaciji RA; i
- firewall-ovima i radnoj stanici za administriranje firewall-a.

U tabeli 5.2.2.1 je dat pregled raspodjele dužnosti povjerljivih uloga osoblja AIDRSCA.

| Osoblje AIDRSCA | Nalog na operativnom sistemu | Nalog na aplikaciji CA | Nalog na aplikaciji RA |
|---|---|---|---|
| **HSM administrator**<br><br>**(HSM Security Officer)** | Serveri sa aplikacijom CA | Da | Ne |
| **Master User** | Serveri sa aplikacijom CA | Da | Ne |
| **Security Officer** | Serveri sa aplikacijom CA | Da | Ne |
| **Administrator** | Administratorska radna stanica sa aplikacijom CA | Da | Ne |
| **RA User** | Administratorska radna stanica sa aplikacijom RA | Ne | Da |
| **Help Desk** | Administratorska radna stanica sa aplikacijom | Ne | Da |

| | | | |
|---|---|---|---|
| | RA | | |
| **Auditor** | Serveri sa aplikacijom CA | Da | Ne |
| **M od N autentifikacija** | Ne posjeduju nalog na operativnom sistemu. Posjeduju pristupne HSM tokene. | Ne | Ne |

**Tabela 5.2.1.1** – Raspodjela dužnosti povjerljivih uloga osoblja AIDRSCA

### 5.2.2. Broj osoba potrebnih za odredjene operativne procedure

AIDRSCA ima implementiranu višestruku autorizaciju za ključne operativne poslove i to na način opisan u ovom poglavlju. Tabela 5.2.2.1 prikazuje procedure kao i vrstu autentifikacije za određene operativne procedure.

| Procedura | Vrsta autentifikacije |
|---|---|
| **Promjena lozinke Master User-a** | Potrebne dvije Master User autorizacije |
| **Kreiranje ili ažuriranje profila Security Officer-a** | Potrebne dvije Master User autorizacije |
| **Konfigurisanje profila certifikata CA** | Potrebne dvije Master User autorizacije |
| **Opoziv certifikata CA** | Potrebne dvije Master User autorizacije |
| **Registrovanje korisnika u aplikaciji CA** | Potrebne dvije Security Officer autorizacije |
| **Dodavanje krajnjih korisnika na Active Directory** | Potrebna jedna Administrator autorizacija |
| **Dodavanje krajnjih korisnika u Entrust bazu** | Potrebna jedna Administrator autorizacija |

**Tabela 5.2.2.1** – Procedure i vrste autentifikacije

### 5.2.3. Identifikacija i autentifikacija ovlašćenih lica za svaku ulogu

AIDRSCA vrši provjeru svojih zaposlenih, prije nego što im dodijeli određene privilegije koje mogu da budu:

- upis u odgovarajuću pristupnu listu za ulazak u zaštićene prostorije AIDRSCA;

- identifikaciona bezkontaktna kartica za ulazak u zaštićene prostorije AIDRSCA;
- nalog na operativnom sistemu servera i radnih stanica AIDRSCA;
- nalog na aplikaciji certifikacionog tijela i HSM smart kartica; i
- nalog na aplikaciji registracionog tijela i SSCD sa certifikatom.

### 5.2.4.Povjerljive uloge koje zahtjevaju razgraničenje ovlašćenja

Aktivnosti zaposlenih u AIDRSCA ograničene su putem ovlašćenja definisanih na nivou:

- operativnog sistema servera i radnih stanica, odnosno terminala koji se koriste za pristup udaljenoj lokaciji;
- aplikacije certifikacionog tijela; i
- aplikacije registracionog tijela.

## 5.3. Upravljanje ljudskim resursima

Ova oblast opisuje kvalifikacije zaposlenih u AIDRSCA, potrebno iskustvo, dozvolu za rad sa zaštićenim podacima, procedure provjere biografije zaposlenih, obuku zaposlenog osoblja kao i učestalost obuka, učestalost i redoslijed rotacije poslova zaposlenog osoblja, sankcije za neautorizovane aktivnosti zaposlenog osoblja, zahtjeve za spoljne saradnike te dokumentaciju za potrebe stalno zaposlenog osoblja.

### 5.3.1. Kvalifikacije, iskustvo i dozvola za rad sa zaštićenim podacima

Zaposleni u AIDRSCA moraju da zadovolje određene zahtjeve u skladu sa Pravilnikom o mjerama zaštite elektronskog potpisa i kvalifikovanog elektronskog potpisa, najnižem iznosu obaveznog osiguranja i primjeni organizacionih i tehničkih mjera zaštite certifikata.

Zaposleni u AIDRSCA dužni su da ne objavljuju odnosno da ne saopštavaju neovlašćenim licima povjerljive informacije vezane za bezbjednost AIDRSCA ili informacije o korisnicima kvalifikovanih elektronskih certifikata, te ne smiju da obavljaju poslove koji bi mogli da dovedu do sukoba interesa.

AIDRSCA može odlučiti da zaposli osobu koja nema potpune kvalifikacije za svoje radno mjesto, ali na taj način da ta osoba ne obavlja ključne aktivnosti unutar sistema, dok ne prođe adekvatnu obuku za ove poslove. Obuka zaposlenih definisana je u sekciji 5.3.3. Obuka osoblja.

### 5.3.2.Procedure provjere biografije

AIDRSCA vrši provjeru zaposlenih lica prema trenutno uspostavljenoj praksi u AIDRS u skladu sa zakonom i propisima iz ove oblasti.

### 5.3.3. Obuka osoblja

AIDRSCA obezbjeđuje obuku osoblja za stručna znanja u radu sa tehnologijom certifikacije za postupke zaštite računarske opreme i programa u sistemu certifikacionog tijela i certifikacije te obezbjeđuje trajno usavršavanje znanja i vještina potrebnih za rad u sistemu certifikacije, u skladu sa Zakonom o elektronskom potpisu i podzakonskim aktima.

Obuka zaposlenih u AIDRSCA obuhvata:

- upoznavanje sa infrastrukturom AIDRSCA;
- upoznavanje sa postupcima zaštite infrastrukture i podataka;
- osposobljavanje za provođenje procedure oporavka sistema poslije nastale štete;
- osposobljavanje za korišćenje aplikacije certifikacionog tijela, registracionog tijela, u skladu sa dodijeljenom ulogom; i
- osposobljavanje za kreiranje rezervnih kopija podataka.

AIDRS će obezbjediti sve potrebne obuke osoblja AIDRSCA u svrhu osiguravanja nesmetanog i kontinualnog rada AIDRSCA sistema.

### 5.3.4. Učestalost obuke osoblja

Osoblje AIDRSCA pohađa obuke kad su imenovani na funkciju i po potrebi, kada se vrše promjene tehničkih sredstava (hardvera i softvera) certifikacionog tijela i načina obavljanja poslovanja. Plan obrazovanja osoblja AIDRSCA se redovno revidira i prilagođava potrebama koje su uslovljene promjenama u okviru PKI sistema.

### 5.3.5. Učestalost i redosljed rotacije poslova zaposlenog osoblja

Certifikaciono tijelo AIDRSCA ne vrši rotaciju poslova zaposlenog osoblja.

### 5.3.6. Sankcije za neautorizovane aktivnosti zaposlenog osoblja

U slučaju neautorizovanih aktivnosti od strane zaposlenog osoblja u AIDRSCA onemogućava im se pristup kompletnom CA sistemu, nakon čega se vrši dalje sankcionisanje u skladu sa internim procedurama AIDRSCA, odobrenim od strane PMA.

### 5.3.7. Zahtjevi za spoljne saradnike

U slučaju da se dodijeli povjerljiva uloga za spoljnog saradnika za to lice važe isti uslovi kao za stalno zaposlena lica AIDRSCA kao što je definisano u sekciji 5.3.1. Kvalifikacije, iskustvo i dozvola za rad sa zaštićenim podacima.

### 5.3.8. Dokumentacija za potrebe stalno zaposlenog osoblja

Zaposlenima u AIDRSCA se daje odgovarajuća dokumentacija sa detaljnim opisom procedura kojih moraju da se pridržavaju.

## 5.4. Procedure upravljanja revizijskih dnevnika

Događaji koji se odnose na obavljanje poslovanja AIDRSCA zapisuju se u elektronske dnevnike (*audit log*) i evidencije koje se ručno vode, sa datumom i vremenom događanja. Ova oblast opisuje vrste događaja koji se evidentiraju, učestalost procesiranja kao i period čuvanja revizijskih dnevnika, te njihovu zaštitu, kreiranje i sistem prikupljanja revizijskih dnevnika.

### 5.4.1. Vrste događaja koji se evidentiraju

Događaji koji se evidentiraju su u vezi sa:

- fizičkim pristupom sistemu AIDRSCA;
- tehničkim sredstvima (hardver i softver) AIDRSCA;
- kriptografskim ključevima aplikacije AIDRSCA;
- korisničkim kriptografskim ključevima i kvalifikovanim elektronskim certifikatima: izdavanje, preuzimanje, opoziv, suspenzija, prekid suspenzije, deaktiviranje, arhiviranje i drugi;
- administracijom, kreiranjem rezervnih kopija, sigurnosnim pravilima i korišćenjem aplikacija AIDRSCA, registracionog tijela; i
- kadrovskim promjenama u okviru AIDRSCA.

### 5.4.2. Učestalost procesiranja revizijskih dnevnika

Procesiranje revizijskih dnevnika definisano je internim procedurama AIDRSCA.

### 5.4.3. Period čuvanja revizijskih dnevnika

Kopije elektronskih dnevnika i ručnih evidencija se čuvaju najmanje 10 godina.

### 5.4.4. Zaštita revizijskih dnevnika

Podaci za elektronske dnevnike se prikupljaju u bezbjednoj zoni. Pristup bezbjednoj zoni je dozvoljen samo ovlašćenim osobama, kako je to definisano internim procedurama za pristup. Za elektronske dnevnike operativnog sistema se upotrebljavaju zaštite koje omogućava sam operativni sistem. Elektronski dnevnici aplikacija certifikacionog tijela su zaštićeni tehnologijom kriptografije javnih kriptografskih ključeva.

### 5.4.5. Kreiranje rezervne kopije revizijskih dnevnika

Elektronski dnevnici se snimaju na odgovarajućim medijima u okviru redovne procedure izrade rezervnih kopija. Za kreiranje rezervnih kopija zaduženi su ovlašćeni administratori. Rezervne kopije elektronskih dnevnika se čuvaju na primarnoj lokaciji certifikacionog tijela i na drugoj udaljenoj lokaciji u zaštićenom prostoru. Na udaljenu lokaciju se rezervne kopije prenose jednom nedjeljno.

### 5.4.6. Sistem prikupljanja revizijskih dnevnika

S obzirom na navedene događaje koji se prikupljaju i arhiviranju, razlikuju se dva načina automatsko prikupljanje i ručno prikupljanje.

U tabeli 5.4.6.1 je dat prikaz događaja koji se arhiviraju te njihov način prikupljanja.

| Vrste događaja koji se evidentiraju | Način prikupljanja podataka vezano za događaj koji se evidentira | Lice koje prikuplja podatke ili sistem |
|---|---|---|
| **Kadrovske promjene u okviru AIDRSCA** | ručno | Zaposleni u AIDRSCA, odnosno odgovorna osoba |
| **Fizički pristup sistemu AIDRSCA** | ručno / automatski | Zaposleni u AIDRSCA / sistem za kontrolu pristupa |
| **Promjena hardvera** | ručno | Zaposleni u AIDRSCA |
| **Promjena softvera** | ručno / automatski | Zaposleni u AIDRSCA / zapis u softveru |
| **Događaji povezani sa aplikacijom CA** | automatski | Aplikacija CA |
| **Događaji povezani sa aplikacijom RA** | automatski | Aplikacija RA |
| **Kreiranje rezervnih kopija i obnova logova konfiguracije CA** | automatski | Operativni sistem, aplikacija CA |
| **Kreiranje rezervnih kopija i obnova baze korisnika kvalifikovanih elektronskih certifikata** | automatsko | Operativni sistem, aplikacija CA |
| **Događaji na računarskoj mreži** | automatsko | Operativni sistem |

| | | |
|---|---|---|
| **Događaji na operativnom sistemu** | automatsko | Operativni sistem |
| **Događaji na aplikaciji RA** | automatsko | Aplikacija RA |
| **Događaji povezani sa korisničkim kvalifikovanim elektronskim certifikatom** | automatsko | Aplikacija CA |

**Tabela 5.4.6.1** – Vrste i način prikupljanja podataka za arhivu

### 5.4.7. Obavještavanje lica koje je izazvalo događaj

O događaju se obavještava rukovodilac poslova AIDRSCA koji naknadno vrši obavještavanje drugih lica od interesa, u skladu sa internim procedurama.

### 5.4.8. Procjena ugroženosti sistema

Procjena ranjivosti sistema se vrši u sklopu svakodnevnih aktivnosti koje se sprovode na sistemu, analizama rizika, razmjenom iskustava sa certifikacionim tijelima iz okruženja i pregledom elektronskih dnevnika i ručnih evidencija.

## 5.5. Arhiviranje podataka

AIDRSCA ima obavezu arhiviranja podataka vezanih za sistem certifikacije. Ova oblast opisuje vrste podatka koje AIDRSCA arhivira, vrijeme čuvanja i zaštitu arhiviranih podataka, kreiranje rezervne kopije arhiviranih podataka, sistem arhiviranja podataka i procedure za akviziciju i verifikovanje podataka iz arhive.

### 5.5.1. Vrste podataka koji se arhiviraju

AIDRSCA arhivira sledeće podatke i dokumenta:

- elektronske dnevnike;
- ugovore i dokumetaciju korisnika;
- zahtjeve za izdavanje i korišćenje kvalifikovanog elektronskog certifikata;
- zahtjeve za promenu statusa kvalifikovanog elektronskog certifikata (opoziv, suspenzija, prekid suspenzije i drugo);
- kvalifikovane elektronske certifikate;
- podatke o statusu i opozivu certifikata; i

- interna akta AIDRSCA vezana za obavljanje delatnosti AIDRSCA.

### 5.5.2. Vrijeme čuvanje arhiviranih podataka

Podaci o potpisnicima, izdati certifikati, liste opozvanih certifikata kao i tehnički podaci nastali bilježenjem rada sistema certifikacije, moraju se čuvati najmanje 10 godina od datuma izdavanja na medijima koji osiguravaju trajnost zapisa od najmanje 20 godina.

### 5.5.3. Zaštita arhiviranih podataka

Arhivirani podaci se nalaze na backup serveru AIDRSCA i na eksternom disku. AIDRCA backup server zaštićen je procedurama kojima se štiti i sam AIDRSCA sistem u skladu sa sekcijama 5.1.Fizička kontrola i 5.2.Kontrola procedura, a eksterni disk nalazi se unutar sigurnog sefa izmještenog iz prostorija AIDRSCA.

### 5.5.4. Kreiranje rezervne kopije arhiviranih podataka

Rezervna kopija arhiviranih podataka nalazi se na eksternom disku opisanom u sekciji 5.5.3. Zaštita arhiviranih podataka.

### 5.5.5. Zahtjevi za vremenskim žigom arhiviranih podataka

Nije definisano.

### 5.5.6. Sistem arhiviranja podataka

AIDRSCA koristi i interni sistem arhiviranja podataka.

### 5.5.7. Procedure za akviziciju i verifikovanje podataka iz arhive

Definisano internim procedurama AIDRSCA.

## 5.6. Obnova ključeva CA

AIDRSCA poslije obnove svog ključa i certifikata, dostavlja svoj javni ključ na isti način kao i pri prvom generisanju.

Generisanje novih ključeva AIDRSCA, vrši se pet godina prije isteka roka važnosti postojećih ključeva.
Generisanje ključeva moguće je sprovesti i ranije, iz sledećih razloga:

- potrebno je promijeniti kriptografski algoritam kojim AIDRSCA potpisuje certifikate i registre opozvanih certifikata;
- potrebno je promijeniti dužinu ključeva CA;
- potrebno je promijeniti rok važnosti ključeva CA;
- potrebno je promijeniti hash algoritam CA, primjenom koga se izračunava hash vrijednost certifikata i registra opozvanih certifikata;
- potrebno je promijeniti sadržaj postojećih polja (ekstenzija) certifikata CA ili dodati nova polja (ekstenzije) certifikata CA; i
- privatni ključ CA je oštećen ili je kompromitovan.

## 5.7. Kompromitovanje i oporavak sistema poslije kompromitiranja ili nepredvidjenih akcija

U narednoj sekciji se opisuju procedure rada u incidentnim situacijama kompromitovanja sistema, greške u radu sistema, programske opreme, oštećenje podataka, kompromitovanje privatnog ključa CA, nastavak rada poslije prirodne katastrofe ili neke druge.

### 5.7.1. Procedure rada u incidentnim situacijama prilikom kompromitovanja sistema

U slučaju kompromitovanja ili sumnje u kompromitovanje privatnog kriptografskog ključa aplikacije CA sprovode se sledeće operacije:

- opoziv izdatih kvalifikovanih elektronskih certifikata korisnika;
- opoziv certifikata aplikacije CA; i
- objavljivanje opozvanih certifikata u registru opozvanih certifikata tj. na CRL listama.

### 5.7.2. Greške u radu sistema, programske opreme ili oštećenje podataka

Sve greške u radu sistema, programske opreme ili oštećenje podataka biće otklonjene u najkraćem intervalu od momenta njihovog registrovanja, u skladu sa procedurama AIDRSCA.

U slučaju štete nastale na tehničkim sredstvima ili podacima, pri čemu privatni kriptografski ključ aplikacije CA nije uništen ili oštećen, servisi aplikacije CA biće ponovo uspostavljeni u najkraćem mogućem roku.

U slučaju uništenja ili oštećenja privatnog kriptografskog ključa aplikacije CA, poslije otklanjanja uzroka uništenja ili oštećenja, sprovodi se postupak povratka (eng. restore) ključa sa kriptografskog modula za Backup ključeva.

### 5.7.3. Kompromitovanje privatnog ključa CA

Standardna procedura u slučaju kompromitovanja privatnog ključa je da CA napravi opoziv svog certifikata i opoziv svih certifikata krajnjih korisnika, nakon toga se generiše novi par ključeva i kreće proces izdavanja novih certifikata.

- AIDRSCA u slučaju kompromitovanja privatnog kriptografskog ključa aplikacije CA vrši sledeće:
  - opoziv izdatih kvalifikovanih elektronskih certifikata;
  - opoziv certifikata aplikacije CA;
  - objavu registra opozvanih certifikata; i
  - obavještavanje korisnika izdatih kvalifikovanih elektronskih certifikata.
- Nakon otklanjanja uzroka kompromitovanja, AIDRSCA vrši sledeće:
  - generisanje novih kriptografskih ključeva aplikacije CA; i
  - izdavanje novih kvalifikovanih elektronskih certifikata korisnicima.

### 5.7.4. Nastavak rada poslije prirodne katastrofe ili neke druge

Poslije prestanka katastrofe i otklanjanja njenog uzroka, AIDRSCA će u najkraćem mogućem roku da dovede sistem u produkciono stanje i nastavi sa radom.

## 5.8. Prestanak rada CA ili RA

AIDRSCA ima obavezu da zbog mogućeg stečaja ili potrebe, odnosno namjere prestanka poslovanja obavijesti o prekidu ugovora svakog potpisnika i Ministarstvo nauke i tehnologije (u daljem tekstu: Ministarstvo) najmanje tri mjeseca prije dana predviđenog za raskid ugovora.

Obaveza AIDRSCA je da osigura kod drugog certifikacionog tijela nastavak obavljanja usluga certifikacije za potpisnike kojima je izdalo certifikate, a ukoliko za to nema mogućnosti, dužno je da opozove sve izdate certifikate i o tome odmah obavijesti Ministarstvo.

Ako AIDRSCA prekida da obavlja usluge elektronske certifikacije ima obavezu da dostavi svu dokumentaciju u vezi sa obavljenim uslugama certifikacije drugom certifikacionom tjelu na koga prenosi obaveze obavljanja usluga certifikacije, odnosno Ministarstvu ako nema drugog certifikacionog tjela**.**

Ministarstvo mora odmah izvršiti opoziv svih elektronskih certifikata koje je izdalo AIDRSCA koje je iz bilo kojih razloga prekinulo obavljanje elektronske certifikacije, a nije osiguralo nastavak obavljanja kod drugog certifikacionog tijela i nije opozvalo izdane certifikate.

# 6. TEHNIČKO BEZBJEDNOSNE KONTROLE

## 6.1. Generisanje ključeva i instalacija

### 6.1.1. Generisanje para ključeva

Par kriptografskih ključeva AIDRSCA za potpisivanje je generisan prilikom instaliranja aplikacije certifikacionog tijela. U toku generisanja para kriptografskih ključeva za potpisivanje koristi se zaštita koja važi za prostorije AIDRSCA iz sekcije 5. FIZIČKA KONTROLA, OPERATIVNA KONTROLA I UPRAVLJANJE RESURSIMA, višestruka autentifikacija ovlašćenih osoblja CA i zaštita koju pruža hardverski kriptografski modul ( eng.*Hardware Security Module - HSM*).

Korisnikov par kriptografskih ključeva za potpisivanje i verifikovanje potpisa se generiše na SSCD modulu koji je sredstvo za formiranje kvalifikovanog elektronskog potpisa. Kriptografski ključ korisnika za potpisivanje se nikada ne smješta na hardverskoj ili softverskoj opremi AIDRSCA.

### 6.1.2. Dostavljanje korisniku privatnog ključa

Korisnički privatni ključ nalazi se na SSCD modulu i krajnji korisnik ga preuzima lično putem RA.

### 6.1.3. Dostavljanje javnog ključa korisnika davaocu usluge certifikovanja

Korisnički javni ključ se generiše na strani CA, zajedno sa privatnim ključem na SSCD modul i nema potrebe da korisnik dostavlja javni ključ certifikacionom tijelu AIDRSCA.

### 6.1.4. Dostavljanje javnog ključa davaoca usluge certifikovanja trećim licima

AIDRSCA predstavlja Certifikaciono tijelo koje se nalazi u sastavu Agencije za informaciono društvo Republike Srpske, i kao takvo je ovlašteno za izdavanje kvalifikovanih elektronskih certifikata.

Certifikat AIDRS Root CA za verifikaciju potpisa AIDRSCA se dostavlja zainteresovanim stranama u okviru AIDRSCA certifikata u X.509 obliku. Treća lica obavezna su da naprave minimalno provjeru identiteta AIDRS ROOT CA, da bi potvrdili validnost certifikacionog tijela AIDRSCA koje je izdalo certifikat drugim učesnicima u komunikaciji.

### 6.1.5. Dužina ključeva

Kriptografski ključevi koje AIDRSCA koristi za potpisivanje certifikata su RSA ključevi dužine **najmanje 4096** bita. Korisnički kriptografski ključevi moraju biti RSA ključevi **minimalne dužine 2048** bita.

### 6.1.6. Generisanje parametara javnih ključeva

AIDRSCA ne koristi DSA ključeve.

### 6.1.7. Namjena upotrebe ključeva (X.509 keyUsage)

Za potpisivanje certifikata i CRL liste upotrebljava se isključivo privatni kriptografski ključ aplikacije AIDRSCA i to na način da se AIDRS Root CA privatni ključ koristi za potpisivanje AIDRS Issuing CA certifikata, a AIDRS Issuing CA privatni ključ koristi se za potpisivanje korisničkih certifikata.

AIDRS Root CA certifikat ima postavljene *keyUsage* bitove za *keyCertSigning* i *CRLSigning.*

AIDRS Issuing CA certifikat ima postavljene *keyUsage* bitove za *keyCertSigning* i *CRLSigning.*

| Namjena certifikata | sadržaj polja Key Usage |
|---|---|
| **za potpisivanje kvalifikovanih elektronskih certifikata i CRL liste** | *keyCertSigning, CRLSigning* |

**Tabela 6.1.7.1** – Namjena upotrebe ključeva certifikata CA tijela

U kvalifikovanim certifikatima koje izdaje AIDRSCA za krajnje korisnike sadržaj polja keyUsage ima postavljene bite *digitalSignature* i *nonRepudiation* i ovi certifikati se izdaju sa OID oznakom **1.3.6.1.4.1.26614.10.1.1.1.**

| Namjena certifikata | sadržaj polja Key Usage |
|---|---|
| **kvalifikovani elektronski certifikat za kreiranje kvalifikovanog elektronskog potpisa i autentifikaciju** | Digital Signature, Non-Repudiation |

**Tabela 6.1.7.2** – Namjena upotrebe ključeva kvalifikovanih certifikata krajnjih korisnika

U testnim certifikatima koje izdaje AIDRSCA za krajnje korisnike sadržaj polja keyUsage ima postavljene bite *digitalSignature* i *nonRepudiation* i ovi certifikati se izdaju sa OID oznakom **1.3.6.1.4.1.26614.10.1.1.2.**

| Namjena certifikata | sadržaj polja Key Usage |
|---|---|
| **testni certifikat za potrebe testiranja** | Digital Signature, Non-Repudiation |

**Tabela 6.1.7.3** – Namjena upotrebe ključeva testnih certifikata krajnjih korisnika

## 6.2. Zaštita privatnog ključa i kontrole kriptografskih modula

### 6.2.1. Standardi i kontrole kriptografskih modula

Sve operacije za generisanje AIDRSCA kriptografskih ključeva i potpisivanja certifikata vrše se na hardverskom kriptografskom modulu (u daljem tekstu HSM) koji zadovoljava sigurnosne standarde nivoa FIPS 140-2 nivo 3 i EAL4+. Ostale kriptografske operacije na strani aplikacije certifikacionog tijela vrše se u kriptografskom modulu koji zadovoljava sigurnosne standarde nivoa FIPS 140-2 nivo 2.

Korisničke pametne kartice, odnosno SSCD, moraju ispunjavati minimalno zahtjeve propisane Zakonom o elektronskom potpisu RS i podzakonskim aktima.

### 6.2.2. M od N kontrola privatnog ključa

AIDRSCA koristi višestruku autorizaciju za potrebe pristupanja privatnom kriptografskom ključu aplikacije certifikacionog tijela. Višestruka autorizacija i procedure višestruke autorizacije opisane su internim pravilnicima AIDRSCA.

### 6.2.3. Deponovanje privatnog ključa

AIDRSCA ne dozvoljava deponovanje svog privatnog ključa.

AIDRSCA zabranjuje deponovanje i obnovu privatnog ključa korisnika za kvalifikovane elektronske certifikate.

### 6.2.4. Kopija privatnog ključa

Aplikacija AIDRSCA čuva kopiju svog privatnog ključa za potpisivanje certifikata.

Aplikacija AIDRSCA tijela radi rezervnu kopiju baze najmanje tri puta dnevno, pri čemu rezervna kopija baze ne sadrži kopiju privatnog ključa. Rezervna kopija baze aplikacije certifikacionog tijela se kopira na rezervne medije u okviru izrade redovne rezervne kopije sistema.

Korisnički kriptografski ključevi se ne čuvaju na strani AIDRSCA.

### 6.2.5. Arhiviranje privatnog ključa

Privatni ključevi AIDRS Root CA i AIDRS Issuing CA se ne arhiviranju nakon isteka njihovog roka važnosti.

### 6.2.6. Prenos privatnog ključa u kriptografski modul

Privatni ključ za potpisivanje AIDRSCA tijela se generiše unutar HSM modula. Privatni ključ za potpisivanje AIDRSCA nikad se ne pojavljuje izvan HSM modula u čitljivom obliku.

Privatni ključevi korisnika za potpisivanje se generišu u kriptografskom modulu pametne kartice i nikad se

ne pojavljuju izvan SSCD modula.

### 6.2.7. Čuvanje kriptografskih ključeva na kriptografskom modulu

Privatni ključ AIDRSCA za potpisivanje se koristi samo na HSM modulu. Rezervna kopija privatnog ključa AIDRSCA za potpisivanje se čuva za potrebe oporavka sistema na drugoj sigurnoj lokaciji u bezbjednom sefu.

### 6.2.8. Način aktiviranja privatnog ključa

Privatni kriptografski ključ aplikacije AIDRSCA za potpisivanje se aktivira poslije startovanja aplikacije certifikacionog tijela. Za aktiviranje je potrebna autentifikacija ovlaštenih lica zaposlenih u AIDRSCA koji su raspoređeni na odgovarajuće dužnosti. Ta autentifikacija se može odvijati putem lozinke ili PIN koda uz korištenje odgovarajućih tokena.

Korisnički privatni kriptografski ključevi se aktiviraju poslije uspješne autentifikacije korisnika sa PIN-om SSCD modula.

### 6.2.9. Način deaktiviranja privatnog ključa

Privatni kriptografski ključ aplikacije AIDRSCA za potpisivanje se deaktivira sa zaustavljanjem aplikacije certifikacionog tijela i deaktiviranjem HSM-a.

Korisnički privatni kriptografski ključ se deaktivira fizičkim odvajanjem SSCD modula od radne stanice ili istekom vremena korisničke sesije.

### 6.2.10. Način uništavanja privatnog ključa

Privatni ključ CA biće uništen poslije isteka njegovog životnog vijeka.

### 6.2.11. Nivo sigurnosti kriptografskih modula

Nivo sigurnosti kriptografskih modula AIDRSCA i korisničkih SSCD modula je definisan u 6.2.1. Standardi i kontrole kriptografskih modula.

## 6.3. Ostali aspekti upravljanja parom ključeva

### 6.3.1. Arhiviranje javnog ključa

Certifikaciono tijelo arhivira javni kriptografski ključ aplikacije certifikacionog tijela i javne korisničke ključeve na medije koji osiguravaju trajnost zapisa od najmanje 20 godina. U svrhu čuvanja zapisa moraju se izraditi i sigurnosne kopije koje moraju biti smještene na drugoj lokaciji, izdvojeno od sistema certifikacije, kao što je propisano *Pravilnikom o mjerama zaštite elektronskog potpisa i kvalifikovanog*

*elektronskog potpisa, najnižem iznosu obaveznog osiguranja i primjeni organizacionih i tehničkih mjera zaštite certifikata.*

### 6.3.2. Rok važnosti certifikata i period upotrebe para ključeva

Rok važnosti javnih i privatnih kriptografskih ključeva AIDRSCA je:

- CA ključevi:
  - Javni ključ Root CA za verifikovanje potpisa: 20 godina;
  - Privatni ključ Root CA za potpisivanje: 20 godina;
  - Javni ključ Issuing CA za verifikovanje potpisa: 20 godina (obnavlja se nakon 15 godina); i
  - Privatni ključ Issuing CA za potpisivanje: 20 godina (obnavlja se nakon 15 godina).
- Korisnički ključevi:
  - Korisnički javni ključ za verifikovanje potpisa: 5 godina; i
  - Korisnički privatni ključ za potpisivanje: 5 godina.

## 6.4. Aktivacioni podaci

### 6.4.1. Generisanje i instalacija aktivacionih podataka

Korisnici upotrebljavaju PIN kod SSCD modula za aktiviranje privatnih kriptografskih ključeva.

### 6.4.2. Zaštita aktivacionih podataka

Svaki korisnik kvalifikovanog elektronskog certifikata certifikata je odgovoran za čuvanje PIN koda svog SSCD modula.

### 6.4.3. Ostali aspekti aktivacionih podataka

Nije primjenljivo.

## 6.5. Bezbjednosni zahtjevi za računare

### 6.5.1. Specifični računarski tehničko-bezbjedonosni zahtjevi

AIDRSCA ima na računarima i aplikacijama implementirane tehničke bezbjednosne kontrole u skladu sa najboljim praksama.

### 6.5.2. Nivo zaštite računara

AIDRSCA koristi aplikaciju CA koja je ocjenjena sa nivoom sigurnosti EAL4+.

Operativni sistemi računara AIDRSCA i drugi proizvodi koji se koriste su komercijalni proizvodi.

## 6.6. Tehnički nadzor tokom upotrebe sistema

### 6.6.1. Nadzor razvoja sistema

Sve aplikacije i proizvodi koje koristi AIDRSCA su komercijalni proizvodi.

### 6.6.2. Upravljanje bezbjednošću

AIDRSCA ima uspostavljano upravljanje rizicima, promjenama, i konfiguracijama za hardverske i softverske komponente svog sistema, u skladu sa pozitivnim zakonskim propisima.

### 6.6.3. Nadzor bezbjednosti tokom upotrebe sistema

AIDRSCA sprovodi sva testiranja prije implementacije u kontrolisanom okruženju.

## 6.7. Nadzor bezbjednosti računarske mreže

Nadzor bezbjednosti računarske mreže vrši se pomoću firewall-a. Računarska mreža podjeljena je na više logičkih nivoa gdje se AIDRS Root CA i AIDRS Issuing CA nalaze na najzaštićenijem nivou, iza DMZ (eng.*Demilitarized Zone*).

## 6.8. Vremenski pečat (eng.*Time-stamping*)

Nije primjenljivo.

# 7. CERTIFIKAT, CRL, I OCSP PROFILI CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1. Profil certifikata

### 7.1.1. Broj (brojevi) verzija (eng.Version number(s))

AIDRSCA izdaje X.509 v3 certifikate u skladu sa RFC 3280.

Koriste se sledeća X.509 osnovna polja:

| X.509 ekstenzija | Opis |
|---|---|
| ***Version*** | Verzija X.509 certifikata |
| ***Serial number*** | Jedinstveni serijski broj certifikata |
| ***Signature algorithm*** | Kriptografski algoritam korišten za potpisivanje certifikata od strane aplikacije CA |
| ***Signature Hash algorithm*** | Hash algoritam aplikacije CA |
| ***Issuer*** | Domenska struktura imena CA tijela koje izdaje certifikate krajnjim korisnicima:<br>CN = AIDRS Issuing CA<br>CN = AIA<br>CN = Public Key Services<br>CN = Services<br>CN = Configuration<br>DC = aidrs<br>DC = rs<br>DC = ba |
| ***Valid from*** | Datum i vrijeme početka važenja izdatog certifikata |
| ***Valid to*** | Datum i vrijeme prestanka važenja izdatog certifikata |
| ***Subject*** | Jedinstveno ime krajnjeg korisnika certifikata |
| ***Public key*** | Javni kriptografski ključ krajnjeg korisnika certifikata, Naziv algoritma korištenog za kreiranje javnog ključa, kao i dužina javnog ključa u bitima |

**Tabela 7.1.1.1** – Osnovna polja X.509 certifikata

### 7.1.2. Ekstenzije certifikata (eng. *Certificate extensions*)

U tabeli 7.1.2.1 je dat prikaz X.509 ekstenzija koje se pojavljuju u kvalifikovanim elektronskim certifikatima koje izdaje AIDRSCA. Takođe, stavljena je napomena koje ekstenzije se moraju označiti kao kritične kako bi ih određene aplikacije obavezno procesuirale.

| X.509 ekstenzija | Kritična ekstenzija | Opis |
|---|---|---|
| ***Certificate Policy*** | | Identifikacija politike certifikacije, OID profila certifikata krajnjeg korisnika, web adresa na kojoj se nalazi ovaj dokument |
| ***Authority Information Access*** | | (OID: 1.3.6.1.5.5.7.48.2)<br>Pristup certifikatima CA tijela u svrhu verifikovanja statusa CA tijela |
| ***Subject Alternative Name*** | | Alternativno ime krajnjeg korisnika certifikata<br>(npr. adresa elektronske pošte krajnjeg korisnika) |
| ***CRL Distribution Point*** | | Lokacija na kojoj se nalaze registri opozvanih certifikata |
| ***Authority Key Identifier*** | | Identifikator javnog kriptografskog ključa CA tijela |
| ***Subject Key Identifier*** | | Identifikator javnog kriptografskog ključa krajnjeg korisnika certifikata |
| ***Entrust Vers Info*** | | (OID: 1.2.840.113533.7.65.0)<br>Verzija aplikacije CA tijela |
| ***Key Usage*** | x | Namjena javnog kriptografskog ključa CA tijela<br>***Key Usage* = Certificate Signing, Off-line CRL Signing** |
| | x | Namjena javnog kriptografskog ključa korisnika<br>***Key Usage* = Digital Signature, Non-Repudiation** |
| ***Basic Constraints*** | x | Oznaka koja pokazuje da li je certifikat CA tijela<br>**Subject Type=CA** |
| | x | Oznaka koja pokazuje da li je certifikat korisnički<br>**Subject Type=End Entity** |
| ***Qualified Certificate Statement*** | | Polje u kome se nalazi izjava da je izdati certifikat kvalifikovan prema Annex-u I i II direktive *1999/93/EC* Evropske unije i da je implementiran prema Zakonu o elektronskom potpisu RS |

**Tabela 7.1.2.1** - Ekstenzije certifikata

AIDRSCA koristi *custom* ekstenzije isključivo u kvalifikovanim elektronskim certifikatima za zaposlene u organima, koji se generišu sa OID-om 1.3.6.1.4.1.26614.10.1.1.1

*Custom* ekstenzije su neophodne kako bi se ispunili zahtjevi koji su propisani Zakonom o elektronskom potpisu, Član 11.

U tabeli 7.1.2.2 su prikazane *custom* ekstenzije koje AIDRSCA koristi u pomenutim certifikatima.

| X.509 *custom* ekstenzija | OID / Opis |
|---|---|
| ***JMB*** | 1.3.6.1.4.1.26614.10.1.1.1.1 / Jedinstveni matični broj krajnjeg korisnika, koristi se kao jedinstveni identifikator krajnjeg korisnika zajedno sa imenom i prezimenom |
| ***Ime oca ili majke*** | 1.3.6.1.4.1.26614.10.1.1.1.2 / Ime oca ili majke krajnjeg korisnka |
| ***Nadimak*** | 1.3.6.1.4.1.26614.10.1.1.1.3 / Nadimak krajnjeg korisnika |
| ***Datum rođenja*** | 1.3.6.1.4.1.26614.10.1.1.1.4 / Datum rođenja krajnjeg korisnika |
| ***Prebivalište*** | 1.3.6.1.4.1.26614.10.1.1.1.5 / Adresa prebivališta krajnjeg korisnika |

**Tabela 7.1.2.2** - *Custom* ekstenzije certifikata

### 7.1.3. Identifikatori algoritamskih objekata

U tabeli 7.1.3.1 je dat prikaz identifikacijskih oznaka za pojedine algoritme koji se koriste prilikom kreiranja kvalifikovanog elektronskog certifikata i kreiranja kvalifikovanog elektronskog potpisa.

| Algoritam | Identifikacijska oznaka - OID |
|---|---|
| ***RSA Encryption*** | 1.2.840.113549.1.1.1 |
| ***RSA with SHA-1 Signature*** | 1.2.840.113549.1.1.5 |
| ***SHA256 with RSA Encryption*** | 1.2.840.113549.1.1.11 |
| ***SHA 256*** | 2.16.840.1.101.3.4.2.1 |

**Tabela 7.1.3.1 –** Identifikatori algoritamskih objekata

### 7.1.4. Oblik imena

Certifikati izdati od strane AIDRSCA sadrže kompletno x.500 jedinstveno ime izdavača certifikata i vlasnika certifikata u sledećim poljima: *issuer name* (CA ime) i *subject name* (korisnikovo jedinstveno ime). Jedinstvena imena su tekstualna polja u X.501 UTF8 formatu.

### 7.1.5. Ograničenja za ime

AIDRSCA koristi *nameConstraints* ekstenziju samo u među-certifikatima (cross-certificates), ukoliko su u upotrebi.

### 7.1.6. Identifikator objekta za politiku certifikovanja

Svi certifikati izdati od strane AIDRSCA sadrže OID politike certifikovanja na osnovu koje je izdat certifikat. OID za svaku politiku certifikovanja definisan je u sekciji 1.2 Naziv dokumenta i identifikacioni podaci.

### 7.1.7. Korišćenje Politike ograničenja ekstenzija

AIDRSCA koristi *policyConstraints* ekstenziju samo u među-certifikatima (cross-certificates), ukoliko su u upotrebi.

### 7.1.8. Sintaksa i semantika za kvalifikatore politike

Ne koriste se

### 7.1.9. Procesiranje semantike za kritične ekstenzije Politike Certifikovanja

PKI klijentske aplikacije moraju procesuirati ekstenzije označene kao kritične (*eng.critical*) u saglasnosti sa RFC 3280.

## 7.2. CRL profil

### 7.2.1. CRL verzija

CA izdaje X.509 v2 format CRLs koristeći višestruke distribucijske tačke u okviru sopstvenog direktorijuma i http web servera. Web adresa CDP direktorija, odnosno CRL lista je navedena u sekciji 2.1. Lokacija i objavljivanje podataka o certifikaciji.

U tabeli 7.2.2.1 je dat prikaz osnovnih X.509 V2 polja sa opisom i vrijednošću navedenih polja.

| X.509 polje | Opis i vrijednost |
|---|---|
| ***Version*** | u skladu sa X.509 V2 |
| ***Signature*** | Algoritam za kreiranje potpisa, sha256RSA |
| ***Issuer*** | Domenska struktura imena CA tijela koje izdaje CRL listu:<br>CN = AIDRS Root CA ili CA = AIDRS Issuing CA<br>CN = AIA<br>CN = Public Key Services<br>CN = Services<br>CN = Configuration |

| | |
|---|---|
| | DC = aidrs<br>DC = rs<br>DC = ba |
| ***Effective date*** | Datum početka važenja aktuelne CRL liste |
| ***Next update*** | Datum prestanka važenja aktuelne CRL liste |
| ***Signature algorithm*** | Algoritam za kreiranje potpisa, sha256RSA |
| ***Signature hash algorithm*** | Algoritam za kreiranje hasha potpisa, sha256 |
| ***CRL Number*** | Serijski broj CRL liste |
| ***Authority Key Identifier*** | Identifikator javnog kriptografskog ključa AIDRSCA |

**Tabela 7.2.1.1** – Osnovna X.509 V2 polja

### 7.2.2. CRL i CRL entry ekstenzije

U tabeli 7.2.2.1 je dat prikaz CRL i CRL entry ekstenzija sa opisom i vrijednošću pojedinih ekstenzija.

| X.509 ekstenzija | Opis i vrijednost |
|---|---|
| ***CRL Number*** | Serijski broj CRL liste. Popunjava CA aplikacija. |
| ***CRL Reason Code*** | Razlog opoziva certifikata.<br>Popunjava CA aplikacija, a u skladu sa podešavanjima od strane operatora. Može da sadrži: (0) Unspecified (Nije specificirano), (1) Key compromise (Ključ je kompromitovan), (3) Affiliation change (Promjenu grupacije), (4) Superseded (Nadomještanje), (5) Cessation of operation (Prestanak rada), (6) Suspended (Suspendovan) |
| ***Revocation date*** | Popunjava CA aplikacija, a u skladu sa podešavanjima od strane operatora. |
| ***Invalidity Date*** | (OID: 2.5.29.24)<br>Datum kompromitovanja ili sumnje u kompromitovanje privatnog kriptografskog ključa, odnosno datum kad je kvalifikovani elektronski certifikat prestao da bude važeći. |

**Tabela 7.2.2.2** – X.509 V2 ekstenzije

## 7.3. OCSP profil

Nije podržano.

# 8. REVIZIJA, USAGLAŠENOSTI I DRUGE PROCJENE

## 8.1. Učestalost ili okolnosti kada se vrše revizije

Nadležni državni organ vrši reviziju rada AIDRSCA u skladu sa Zakonom o elektronskom potpisu, podzakonskim aktima i drugim pozitivnim zakonskim propisima. AIDRSCA PMA je tijelo odgovorno za organizovanje interne revizije i drugih procjena, kao i načina organizovanja iste. PMA će inicirati provjere jednom godišnje uz pomoć revizora, koji mogu biti interni ili eksterni. Ova se provjera može proširiti i na RA. Moguće je izvršiti i više od jedne interne revizije godišnje ukoliko je to zahtjevano od strane PMA ili je to posljedica nezadovoljavajućih rezultata prethodne revizije.

## 8.2. Identitet/kvalifikacije revizora

Odabrani revizor mora posjedovati odgovarajuce IT znanje i revizijsko iskustvo. Interni ili eksterni revizor mora ispunjavati sljedeće kriterijume: iskustvo u primjeni PKI i kriptografskih tehnologija; i iskustvo u sprovođenju aktivnosti izdavanja certifikata ili revizije sistema informacionih tehnologija.

## 8.3. Revizorov odnos prema ocjenjivanom subjektu

Interni ili eksterni revizor treba da je oslobođen od konflikta interesa i da je nezavisan od AIDRSCA.

## 8.4. Oblasti koje pokriva revizija

Revizor će ocijeniti usklađenost između ovog Pravilnika i Zakona o elektronskom potpisu i podzakonskih akata; i ovog Pravilnika i implementiranih AIDRSCA servisa i procedura.

## 8.5. Aktivnosti koje se preduzimaju u slučaju nedostatka

U cilju rješavanja bilo kakvih nedostataka ili identifikovanih neusklađenosti koje su rezultat revizije, AIDRSCA PMA će preduzeti odgovarajuće radnje unutar dogovorenog vremenskog okvira u zavisnosti od ozbiljnosti rizika.

## 8.6. Objavljivanje rezultata

Rezultati revizije se dostavljaju AIDRSCA PMA.

Zaključak revizije će se objaviti javno na web strani AIDRSCA u skladu sa 2.1. Lokacija i objavljivanje podataka o certifikaciji.

# 9. OSTALE POSLOVNE I PRAVNE STVARI

## 9.1. Cijene

### 9.1.1. Cijene usluga AIDRSCA

AIDRSCA ne naplaćuje usluge certifikacije krajnjim korisnicima.

### 9.1.2. Nadoknada za pristup certifikatu

Ne naplaćuje se, u skladu sa 9.1.1. Cijene usluga AIDRSCA **.**

### 9.1.3. Nadoknada za opoziv ili pristup statusu informacija

Ne naplaćuje se, u skladu sa 9.1.1. Cijene usluga AIDRSCA **.**

### 9.1.4. Nadoknade za ostale servise

Ne naplaćuje se, u skladu sa 9.1.1. Cijene usluga AIDRSCA **.**

### 9.1.5. Politika refundiranja

Troškovi se ne refundiraju, u skladu sa 9.1.1. Cijene usluga AIDRSCA**.**

## 9.2. Finansijska odgovornost

### 9.2.1. Osiguranja ili garancije davaoca usluge certifikacije

U skladu sa dokumentom *„Pravilnik o mjerama zaštite elektronskog potpisa i kvalifikovanog elektronskog potpisa, najnižem iznosu obaveznog osiguranja i primjeni organizacionih i tehničkih mjera zaštite certifikata - "Službeni glasnik Republike Srpske"*, član 50., stav 3., AIDRSCA nije dužno osigurati rizik od odgovornosti za štete koje nastanu obavljanjem usluga certifikacije.

### 9.2.2. Ostala sredstva

Nije primjenljivo.

### 9.2.3. Osiguranja ili garancije korisnika

Naručioci i treća strana od povjerenja isključivo su odgovorni da obezbjede adekvatno osiguranje ili garanciju pokrivenosti osiguranjem za korišćenje certifikata u okviru njihovih servisa ili aplikacija.

## 9.3. Povjerljivost poslovnih informacija

### 9.3.1. Obim povjerljivih informacija

Sve informacije koje se prikupljaju, generišu, prenose, i održavaju od strane AIDRSCA, smatraju se povjerljivim, osim informacija opisanih u sekciji 9.3.2. Informacije koje ne ulaze u obim povjerljivih informacija, koje se ne smatraju povjerljivim.

### 9.3.2. Informacije koje ne ulaze u obim povjerljivih informacija

Informacije koje se objavljuju kao dio certifikata, CRL, CPS-a ili druge informacije koje se objavljuju u javnom registru certifikacionog tijela, ne smatraju se povjerljivim.

### 9.3.3. Odgovornost za zaštitu povjerljivih informacija

AIDRSCA je odgovorno za zaštitu povjerljivih informacija u skladu sa Zakonom o zaštiti ličnih podataka i pozitivnim zakonodavstvom Republike Srpske.

## 9.4. Povjerljivost ličnih podataka

### 9.4.1. Plan povjerljivosti

Bilo koji lični podatak koji obezbeđuje AIDRSCA čuvaće se u skladu sa zahtjevima postavljenim u Zakonu o zaštiti ličnih podataka. Davanje gore navedenih informacija može se vršiti jedino u saglasnosti sa Zakonom o zaštiti ličnih podataka.

### 9.4.2. Informacija koja se tretira privatnom

Definisano u sekciji 9.3.1. Obim povjerljivih informacija

### 9.4.3. Informacija koja se ne smatra privatnom

Definisano u sekciji 9.3.2. Informacije koje ne ulaze u obim povjerljivih informacija

### 9.4.4. Odgovornost za zaštitu ličnih podataka

Kao što je definisano u sekciji 9.3.3. Odgovornost za zaštitu povjerljivih informacija

### 9.4.5. Obavještenje i davanje saglasnosti za korišćenje ličnih podataka

AIDRSCA će koristiti lične podatke isključivo u svrhe za koje je naručilac dao saglasnost u toku procesa registracije. Smatra se da je naručilac dao saglasnost potpisivanjem ugovora sa AIDRSCA.

### 9.4.6. Otkrivanje informacije u skladu sa sudskim ili administrativnim procesom

Lični podatak može jedino biti predat od strane AIDRSCA zakonom ovlašćenim službenicima u skladu sa važećim zakonodavstvom za tu oblast.

### 9.4.7. Ostale okolnosti kada se mogu otkrivati informacije

AIDRSCA će otkriti privatnu informaciju samo u slučajevima kada dobije pismenu saglasnost od naručioca i krajnjeg korisnika.

## 9.5. Prava na intelektualnu svojinu

AIDRSCA je vlasnik ovog dokumenta. Svako neovlašćeno korišćenje bilo kog dijela ovog dokumenta smatra se kršenjem autorskih prava vlasnika ovog dokumenta i podložno je zakonskim mjerama. AIDRS je vlasnik svih podataka, deficinija procesa, procedura i razultata nastalih u radu AIDRSCA.

## 9.6. Obaveze i odgovornosti

### 9.6.1. Obaveze AIDRSCA

AIDRSCA ima obavezu da izdaje certifikate, izvršava ostale procedure vezane za upravljanje certifikatima i upravlja infrastrukturom certifikacionog tijela u skladu sa ovim Pravilnikom i važećim zakonima iz te oblasti. AIDRSCA odgovara za usklađenost sa procedurama opisanim u ovom Pravilniku i važećim zakonima iz te oblasti, čak i u slučaju kada pojedinu funkciju certifikacionog tijela preuzmu pod-ugovarači.

Generalno, AIDRSCA ima obavezu:

- da osigura da svaki kvalifikovani elektronski certifikat sadrži sve potrebne podatke u skladu sa članom 11. Zakona o elektronskom potpisu;
- da provjeri identitet potpisnika za kojeg sprovodi usluge certifikacije;
- da osigura tačnost i cjelovitost podataka koje unosi u evidenciju izdanih certifikata;
- da u svaki certifikat unese osnovne podatke o svom indentitetu;
- da omogući svakom zainteresovanom licu uvid u identifikacione podatke certifikacionog tijela i uvid u dozvolu za izdavanje kvalifikovanih elektronskih certifikata;
- da vodi tačnu i zaštićenu evidenciju elektronskih certifikata koja mora biti javno dostupna;
- da vodi tačnu i zaštićenu evidenciju nevažećih elektronskih certifikata;
- da osigura vidljiv podatak o tačnom datumu i vremenu (sat i minuta) izdavanja, odnosno opoziva elektronskih certifikata u evidenciji izdanih elektronskih certifikata;
- da čuva sve podatke i dokumentaciju o izdatim elektronskih certifikatima najmanje deset godina, pri čemu podaci i prateća dokumentacija mogu biti i u elektronskom obliku; i
- da primjenjuje odredbe zakona i drugih propisa kojima je uređena zaštita ličnih podataka.

### 9.6.2. Obaveze RA

RA ima obavezu da obezbjedi tačnost i potpunost informacija koje provjeravaju njeni referenti. Detaljne obaveze RA definisane su u relevantnim odjeljcima ovog Pravilnika.

Za cjelokupan rad RA odgovoran je AIDRSCA.

### 9.6.3. Odgovornosti i obaveze krajnjeg korisnika

Prihvatanjem certifikata koji je izdalo AIDRSCA, korisnik se obavezuje u skladu sa Zakonom da:

- Preduzme sve potrebne organizacione i tehničke mjere zaštite od gubitaka i štete koje može uzrokovati drugim potpisnicima, certifikacionom tijelu ili trećim licima;
- Pažljivo koristi i čuva sredstva i podatke za izradu elektronskog potpisa, koristi sredstva i podatke za izradu elektronskog potpisa u skladu sa odredbama Zakona o elektronskom potpisu, te zaštiti i čuva sredstva i podatke za izradu elektronskog potpisa od neovlašćenog pristupa i upotrebe;
    - *čuva svoje privatne ključeve;*
    - *čuva svoju lozinku za zaštitu kriptografskih modula u kojem drži svoj privatni ključ;*
- Dostavi AIDRSCA sve potrebne podatke i informacije o promjenama koje utiču ili mogu uticati na tačnost elektronskog potpisa u roku od 2 dana od nastalih promjena;
    - *odmah obavijesti certifikaciono tijelo, o bilo kakvoj netačnosti ili promjenama u informacijama sadržanim u certifikatu;*

- Odmah zatraži opoziv svog certifikata u svim slučajevima gubitka ili oštećenja sredstava ili podataka za izradu elektronskog potpisa;
    - *odmah obavijesti certifikaciono tijelo, ako je kompromitovan privatni ključ povezan s certifikatom ili se sumnja da je bio kompromitovan; i*
    - *odmah obavijesti certifikaciono tijelo o bilo kojoj sumnjivoj ili poznatoj zloupotrebi bilo kojeg certifikata koji je izdat od strane AIDRSCA.*

### 9.6.4. Odgovornosti i obaveze trećih lica

Prije oslanjanja na AIDRSCA certifikat, obaveza trećih lica je da:

- Budu svjesna ograničenja certifikata i odgovornosti AIDRSCA kako je detaljno opisano u CPS;
- Ograniče oslanjanje na certifikate koje je izdalo AIDRSCA za odgovarajuće upotrebe kako je detaljno objašnjeno u sekciji 1.4 Upotreba certifikata;
- Se preko provjere statusa certifikata na validnim listama opozvanih certifikata (CRLs) uvjere da certifikat nije opozvan; i
- Odmah obavijeste AIDRSCA o bilo kojoj sumnjivoj ili poznatoj zloupotrebi bilo kojeg certifikata koji je izdat od strane AIDRSCA.

### 9.6.5. Odgovornosti i garancije ostalih učesnika

Ne primjenjuje se.

## 9.7. Izuzeća od odgovornosti

Osim odgovornosti navedenih u CPS i povezanim ugovorima, i onim što je do najvišeg stepena dozvoljeno zakonom, AIDRSCA isključuje sve druge moguće odgovornosti, uključujući bilo koje odgovornosti za mogućnost trgovine ili korišćenja za određenu upotrebu. AIDRSCA naročito isključuje:

- bilo koju odgovornost za štetu koja može da se pojavi od momenta kada AIDRSCA primi validan zahtjev za opoziv certifikata, do momenta objave informacije o opozivu istog na CRL;
- bilo kakvu odgovornost za tačnost ili pouzdanost bilo koje informacije sadržane u certifikatima koju nije provjerio RA ili AIDRSCA;
- odgovornost za prezentaciju informacija sadržanih u certifikatu;
- bilo kakvu garanciju ovlašćenja ili statusa bilo koje osobe koja koristi certifikat AIDRSCA, (AIDRSCA nije odgovoran za provjeru statusa da li je neko zaposlen u organu ili kakva je njegova funkcija u tom organu);
- bilo koju odgovornost za stvari van kontrole AIDRSCA uključujući raspoloživost ili rad Interneta, ili telekomunikacija ili drugih infrastruktura ili RA sistema, uključujući opremu i programe; i
- bilo koju odgovornost za štete koje su nastale kao rezultat događaja više sile kako je detaljno

opisano u sekciji 9.16.5. Viša sila.

## 9.8. Ograničenja finansijske odgovornosti

Kako je AIDRSCA u skladu sa Zakonom o elektronskom potpisu i podzakonskim aktima izuzet od obaveznog osiguranja za svoju djelatnost, ne snosi odgovornost nadoknade stete, u skladu sa sekcijom 9.2.1. Osiguranja ili garancije davaoca usluge certifikacije

## 9.9. Obeštećenja

Treće strane i korisnici za sebe snose isključivu odgovornost za nadoknađivanje štete drugim strankama za pretrpljene gubitke ili štetu koji su nastali kao rezultat neovlaštenog korišćenja certifikata ili nepostupanja u skladu sa Zakonom o elektronskom potpisu, podzakonskim aktima i CPS.

## 9.10. Stupanje na snagu i period važenja

### 9.10.1. Stupanje na snagu

CPS stupa na snagu nakon njegovog usvajanja tj. odobrenja od strane AIDRSCA PMA.

### 9.10.2. Period važenja

Važnost CPS nije vremenski ograničena. Trenutna verzija će biti na snazi do objavljivanja nove verzije.

### 9.10.3. Efekti prekida važenja

Nakon prestanka važenja CPS, kao rezultata objavljivanja nove verzije, certifikat će se koristiti u skladu sa onim CPS-om koji je bio validan na dan izdavanja certifikata.

U slučaju promjena okolnosti do nivoa kada ovo nije moguće, AIDRSCA će obavijestiti naručioce na način definisan u sekciji 9.12.2. Mehanizmi obaveštavanja i vremenski periodi preko javne web stranice definisane u sekciji 2.1. Lokacija i objavljivanje podataka o certifikaciji

U slučaju kada dolazi do promjene neke sekcije ovog dokumenta koja nema materijalne posljedice po korisnika, ostale sekcije dokumenta mogu ostati na snazi. Takođe, zavisno od promjena koje u tom slučaju pretrpi ovaj dokument PMA može inicirati kreiranje nove verzije ovog dokumenta.

## 9.11. Individualno obavještavanje i komunikacija sa učesnicima

AIDRSCA distribuira aktuelnu verziju CPS i tekuće verzije svih javnih dokumenata preko web stranice definisane u sekciji 2.1. Lokacija i objavljivanje podataka o certifikaciji.

## 9.12. Izmjene

### 9.12.1. Procedura za izmjenu

AIDRSCA osoblje može svoje primjedbe slati direktno AIDRSCA PMA u pisanom obliku ili elektronskom poštom, na adrese definisane u sekciji 1.5.2. Lica za kontakt.

### 9.12.2. Mehanizmi obaveštavanja i vremenski periodi

AIDRSCA PMA može odlučiti da ne obavještava naručioce i treća lica u slučaju izmjena sa malim ili nikakvim uticajem. AIDRSCA PMA u potpunosti odlučuje o tome da li izmjene imaju bilo kakav uticaj na naručioce i treća lica, na sopstvenu odgovornost.

Sve izmjene u CPS biće objavljene na na web stranici definisani u sekciji 2.1. Lokacija i objavljivanje podataka o certifikaciji.

AIDRSCA će obavijestiti korisnike o promjenama koje imaju materijalnog uticaja na njih, putem elektronske pošte i na javnoj web stranici definisanoj u sekciji 2.1. Lokacija i objavljivanje podataka o certifikaciji.

### 9.12.3. Okolnosti pod kojima se OID mora izmijeniti

OID CPS-a će biti promjenjen u slučaju kada promjene imaju materijalni uticaj na naručioce i treća lica, tj. nova verzija CPS rezultuje novim OID-om.

## 9.13. Rješavanja u slučaju spora

Sva sporenja u vezi certifikata izdatih od strane AIDRSCA se moraju dostaviti na adresu naznačenu u odjeljku 1.5.2. Lica za kontakt. Sporove treba, ako je moguće, rješavati pregovorima. Ukoliko se ne postigne razrješenje nesporazuma putem pregovora, rješenje će se potražiti kod nadležnog suda u Banjaluci.

## 9.14. Primjena zakona

CPS, kao i odnosi između AIDRSCA i RA, naručioca, korisnika certifikata i trećih lica predmet su i biće tumačene u skladu sa relevantnim zakonodavstvom.

## 9.15. Usaglašenost sa primjenljivim zakonom

Ovaj pravilnik usaglašen je sa:

- Zakonom o zaštiti ličnih podataka; i

- Zakonom o elektronskom potpisu i podzakonskim aktima.

## 9.16. Ostale odredbe

### 9.16.1. Cjelokupni ugovor

Ovaj CPS i ugovor sa naručiocem obuhvataju sve elemente koji definišu odnos između AIDRSCA i naručioca certifikata.

### 9.16.2. Prenos prava

Naručiocima certifikata nije dozvoljeno da prava i obaveze koji proističu iz ovog pravilnika i ugovora sa naručiocem u cjelosti ili parcijalno prenesu na treća lica po bilo kom osnovu.

### 9.16.3. Klauzula o valjanosti

Nevaljanost jednog ili više djelova ovog dokumenta, neće imati uticaj na valjanost ostalih odredbi, pod uslovom da nemaju uticaj na materijalne odredbe (povjerenje u certifikat i upotrebu certifikata).

### 9.16.4. Izvršenje (nadoknade za pravnog zastupnika i odricanje od prava)

Nema odredbi.

### 9.16.5. Viša sila

Višu silu predstavljaju vanredne okolnosti i nepredvidljive situacije kao što su prirodne katastrofe, terorizam, nedostatak napajanja ili prekid telekomunikacionih veza, požar, nepredvidljivi incidenti kao što su virusi ili napadi sa ciljem onemogućavanja servisa, vladine mjere, greške u kriptografskim alogaritmima i sl.

AIDRSCA ili druge stranke neće biti odgovorne za bilo kakvu štetu koja je nastala usljed događaja koji su rezultat više sile.

## 9.17. Napomene

Nema odredbi.