Opšta pravila pružanja usluga certifikacije

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

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

Opšta pravila pružanja usluga certifikacije

(CP – Certificate Policy)

OID: 1.3.6.1.4.26614.10.0.1

Трг Републике Српске 1, 78000 Бања Лука, Република Српска, БиХ
тел: +387 51 339 777 факс: +387 51 339 776 email: info@aidrs.org web: www.aidrs.org

Opšti podaci i verzije dokumenta

Referentni broj dokumenta	I - / 12
Puni naziv dokumenta	**Opšta pravila pružanja usluga certifikacije**
Skraćenica dokumenta	CP – Certificate Policy
Kod dokumenta	PKI-JU-RS-DOC-CP
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	**20**
Odgovorno lice	Srđan Rajčević, direktor
Autori	Milan Latinović, AIDRS Saša Vojnović, AIDRS Ljiljana Umićević, AIDRS 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)	**Opšta pravila pružanja usluga certifikacije je dokument koji opisuje opšta pravila koja 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 Version	Datum Date	Opis Description
1.0	30.08.2011.	Prvobitna javna verzija dokumenta
1.1	09.03.2012.	Dorađena verzija (lektorisanje, jasnije definisanje pojmova), bez strukturnih i logičkih promjena.
1.2.	16.12.2013.	Dorađena verzija, prilagođavanje CP-a za izdavanje certifikata APIF-u i privrednim sudovima prema zaključku Vlade RS.

Sadržaj

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.

Opšta pravila pružanja usluga certifikacije (eng. Certificate Policy – CP) je dokument koji opisuje opšta pravila po kojima posluje certifikaciono tijelo Agencije za informaciono društvo Republike Srpske (u daljem tekstu: AIDRSCA). Identifikaciona oznaka dokumenta (eng. Object Identifier – OID) je: **1.3.6.1.4.26614.10.0.1**

Sva opšta pravila opisana u CP-u urađena 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
- 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.

Učesnike PKI sistema čine AIDRSCA, korisnici usluga certifikacije i ostali učesnici u komunikaciji (u nastavku: treća lica).

Korisnici kvalifikovanih elektronskih certifikata AIDRSCA, posjeduju jedan par kriptografskih ključeva (javni i privatni ključ). Privatni kriptografski ključ koristi se za kvalifikovano elektronsko potpisivanje, a javni kriptografski ključ koristi se za verifikovanje kvalifikovanog elektronskog potpisa.

Kvalifikovani elektronski certifikati kreirani su po standardu X.509 v3. Kvalifikovani elektronski certifikati i pripadajući privatni kriptografski ključevi koriste se za:

- kvalifikovano elektronsko potpisivanje datoteka ili poruka; i
- autentifikaciju korisnika.

Kvalifikovani elektronski certifikati potvrđuju vezu između javnog kriptografskog ključa korisnika i identiteta korisnika koji je izvršio kvalifikovano potpisivanje elektronskog dokumenta.

Svaka upotreba kvalifikovanog elektronskog potpisa koja nije u skladu sa odredbama Zakona o elektronskom potpisu RS, podzakonskim aktima, opštim pravilima pružanja usluga certifikacije, praktičnim pravilima pružanja usluga certifikacije i drugim dokumentima koji regulišu ovu oblast, nije dozvoljena.

2. OBJAVLJIVANJE I LOKACIJA 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/. Registar opozvanih certifikata nalazi se na web adresi: http://cdp.aidrs.org/crl/ (adresa navedena u CDP svakog certifikata krajnjeg korisnika), a sekundarna lokacija registra opozvanih 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://cdp.aidrs.org/AIA/.

AIDRSCA objavljuje na svojoj zvaničnoj web strani sljedeće podatke:

- Zakon o elektronskom potpisu RS i podzakonske akte;
- dokument „Opšta pravila pružanja usluga certifikacije“;
- 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;
- obrazac ugovora o izdavanju certifikata zaposlenom;
- korisnička uputstva;
- certifikate AIDRS Root CA i AIDRS Issuing CA sa pridruženim hash vrijednostima;
- registre opozvanih certifikata; i
- druga akta i obavještenja.

3. IDENTIFIKACIJA I AUTENTIFIKACIJA

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.

U kvalifikovanim certifikatima koje izdaje AIDRSCA imena korisnika su predstavljena kao jedinstvena (eng. distinguished name - DN) i vjerodostojno interpretiraju ime i prezime korisnika.

AIDRSCA je usvojilo nomenklaturu po kojoj garantuje jedinstvenost imena u svom domenu (tj. u svojoj direktorijskoj strukturi).

Kvalifikovani elektronski certifikat se može izdati samo fizičkom licu, u skladu sa Zakonom o elektronskom potpisu. Fizičko lice ima pravo da u ime pravnog lica koristi kvalifikovani elektronski certifikat, ukoliko ga za to ovlasti pravno lice.

U slučajevima kada fizičko lice koristi certifikat u ime pravnog lica, certifikaciono tijelo AIDRS će u sklopu certifikata fizičkog lica uvrstiti informaciju koja označava naziv pravnog lica u ime kojeg fizičko lice koristi kvalifikovani certifikat.

Certifikaciono tijelo AIDRS garantuje jedinstvenost imena u svom domenu, uvođenjem strukture korisničkog imena detaljno opisane u dokumentu Praktična pravila pružanja usluga certifikacije (u nastavku: CPS).

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 dužan predočiti identifikacioni dokument kojim se pouzdano može utvrditi identitet osobe.

4. PROCEDURE ŽIVOTNOG CIKLUSA CERTIFIKATA

AIDRSCA izdaje certifikate samo za potrebe organa republičke uprave RS, APIF-a i okružnih privrednih sudova u RS (u daljem tekstu: naručilac).

Zahtjev za izdavanje certifikata može da podnese zaposlenik naručioca (u daljem tekstu: krajnji korisnik), ako je ispunjen uslov da postoji zaključen Ugovor o pružanju usluga certifikacije između AIDRSCA i naručioca.

Krajnji korisnik podnosi zahtjev samostalno, putem naručioca.

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.

Izdavanje kvalifikovanog elektronskog certifikata, vrši se na sljedeći način:

- krajnji korisnik podnosi zahtjev za izdavanje kvalifikovanog elektronskog certifikata putem naručioca koji garantuje za identitet krajnjeg korisnika;
- prihvatanje zahtjeva od strane RA;
- kreiranje korisničkog naloga unutar CA aplikacije;
- vrši se personalizacija SSCD modula (kreiranje korisničkog para ključeva, vizuelna personalizacija, PIN protekcija);
- Dostavljanje personalizovanog SSCD modula i kovertiranog PIN-a ka RA; i
- Lično preuzimanje SSCD modula i kovertiranog PIN-a od strane krajnjeg korisnika, prilikom potpisivanja Ugovora između AIDRSCA i krajnjeg korisnika.

Potpisivanjem Ugovora smatra se da krajnji korisnik potvrđuje da je preuzeo certifikat.

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

Treća lica koriste javni ključ i kvalifikovani elektronski certifikat za verifikovanje kvalifikovanog elektronskog potpisa, u skladu sa Zakonom o elektronskom potpisu, podzakonskim aktima, opštim i praktičnim pravilima pružanja usluga certifikacije.

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

AIDRSCA ne dozvoljava obnovu kvalifikovanog elektronskog certifikata bez promjene javnog ključa. Pod obnovom kvalifikovanog elektronskog certifikata podrazumjeva se izdavanje novog kvalifikovanog elektronskog certifikata.

Okolnosti pod kojima se vrši obnova certifikata su:

- opoziv certifikata, nakon čega naručilac traži obnovu certifikata;
- neposredno pred istek perioda važenja (30 dana) certifikata ili privatnog ključa; i
- nakon isteka perioda važenja certifikata ili privatnog ključa.

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

Treća lica se ne obavještavaju o izdavanju kvalifikovanih elektronskih certifikata.

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

Okolnosti pod kojima krajnji korisnik / naručilac 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.

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

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

- kod kojih je došlo do raskida ugovora između naručioca i AIDRS
- 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.

Opoziv certifikata može zahtjevati:

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

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

Obrada zahtjeva za opoziv certifikata biće izvršena najkasnije do kraja narednog radnog dana od momenta podnošenja zahtjeva za opoziv certifikata.

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

Svaki opoziv certifikata rezultuje objavljivanjem nove CRL liste.

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 rada servisa, informacija o vremenu i planiranom periodu prekida servisa biće objavljena na javnoj web strani certifikacionog tijela kao što je definisano u sekciji 2. Objavljivanje i lokacija podataka o certifikaciji.

Razlozi za raskid ugovora sa naručiocem mogu biti:

- eksplicitni zahtjev naručioca za raskid 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.

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

5. FIZIČKA KONTROLA, OPERATIVNA KONTROLA I UPRAVLJANJE RESURSIMA

Najvažnija oprema AIDRSCA se nalazi u zaštićenoj prostoriji, lociranoj u zgradi Vlade RS. Kontrola fizičkog pristupa AIDRSCA je implementirana u skladu sa Zakonom o elektronskom potpisu i podzakonskim aktima, i to na sljedeći način:

- pristup bez pratnje ograničen je na zaposlene AIDRSCA koji su ovlašteni za pristup zaštićenoj prostoriji;
- pristup sa pratnjom ovlaštenog lica se zahtjeva za sva lica osim za zaposlene u AIDRSCA koji su ovlašteni za pristup bez pratnje;
- pristup se može sprovoditi isključivo uz prisustvo najmanje dva ovlašćena lica koja imaju pravo pristupa;
- pristup zbog održavanja sistema mora biti unaprijed najavljen osim u slučaju hitne intervencije; i
- svaki pristup zaštićenoj prostoriji evidentira se unutar elektronske evidencije.

AIDRSCA koristi kontrolu fizičkog pristupa putem elektronske brave sa bezkontaktnom karticom. Sve prostorije AIDRSCA su nadgledane 24 sata / 7 dana nedeljno.

AIDRSCA je opremljeno:

- sistemom za neprekidni izvor napajanja električnom energijom i stabilizaciju napona za računarsku i telekomunikacionu opremu, koji je povezan sa agregatom; i
- nezavisnim sistemom za klimatizaciju koji omogućava kontrolu temperature i vlažnosti vazduha unutar prostorija AIDRSCA.

Bezbjedna prostorija Vlade RS udaljena je od riječnih i drugih vodenih tokova i preduzete su sve tehničke mjere zaštite od eventualnih poplava od vodovodnih instalacija u okruženju.

Bezbjedna prostorija Vlade RS obezbjeđena je sa sistemom rane detekcije i dojave požara.

Svi mediji na kojima se nalaze podaci AIDRSCA, uključujući rezervne kopije sistema, smješteni su u sefu otpornom na vatru. Sekundarne kopije nalaze se u udaljenom sefu.

Svi materijali za koje se tokom poslovnih procesa zaključi da su nepotrebni u daljem radu, a da ih ne treba arhivirati prvo se uništavaju, a nakon toga se odlažu na otpad.

Rezervnu lokaciju za pohranjivanje podataka predstavlja eksterni hard disk.

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.

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.

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.

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, Član 23., Član 24.

Zaposleni u AIDRSCA se obavezuju na držanje u potpunoj tajnosti povjerljivih podataka, 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 nije obučena da radi poslove unutar AIDRSCA, ali na taj način da ta osoba ne obavlja ključne aktivnosti unutar sistema, dok ne prođe adekvatnu obuku za ove poslove.

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.

Zaposleni u AIDRSCA obavljaju svoje aktivnosti na osnovu propisane dokumentacije sa detaljnim opisom procedura kojih su obavezni da se pridržavaju.

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.

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.

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.

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.

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

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 prestaje 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

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, višestruka autentifikacija ovlašćenog 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.

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

Korisnički SSCD modul može biti preuzet i od strane ovlaštene osobe.

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.

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.

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.

Sve operacije za generisanje AIDRSCA kriptografskih ključeva i potpisivanja certifikata vrše se na 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.

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

AIDRSCA ne dozvoljava deponovanje svog privatnog ključa.

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

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.

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. Rezervna kopija privatnog ključa AIDRSCA za potpisivanje se čuva za potrebe oporavka sistema na drugoj sigurnoj lokaciji u bezbjednom sefu.

Privatni ključevi korisnika za potpisivanje se generišu u kriptografskom modulu pametne kartice i nikad se ne pojavljuju izvan SSCD modula.

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.

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

najboljim praksama.

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

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

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

AIDRSCA sprovodi sva testiranja prije implementacije u kontrolisanom okruženju.

7. CERTIFIKATI, CRL LISTE I OCSP PROFILI

AIDRSCA izdaje kvalifikovane elektronske certifikate kreirane po standardu X.509 v3 , pri čemu je profil kvalifikovanog elektronskog certifikata u skladu sa Zakonom o elektronskom potpisu RS i podzakonskim aktima, tj. pravilnicima.

AIDRSCA izdaje registre opozvanih certifikata (eng. Certificate Revocation List – CRL) kreirane po standardu X.509 v2, pri čemu je profil registra opozvanih certifikata u skladu sa Zakonom o elektronskom potpisu RS i podzakonskim aktima, tj. pravilnicima.

AIDRSCA ne omogućava on-line provjeru statusa kvalifikovanog elektronskog certifikata (eng. OnLine Certificate Status Protocol – OCSP).

8. NADZOR, REVIZIJA, USAGLAŠENOSTI I DRUGE PROCJENE

Nadležni državni organ vrši nadzor nad radom AIDRSCA u skladu sa Zakonom o elektronskom potpisu, podzakonskim aktima i drugim pozitivnim zakonskim propisima.

Tijelo za upravljanje politikama certifikacije (eng. Policy Management Authority – PMA) nalazi se u sklopu AIDRSCA i odgovorno za organizovanje interne revizije i drugih procjena, kao i načina sprovođenja 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.

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.

Revizor će ocijeniti usklađenost između:

- ovog Pravilnika i Zakona o elektronskom potpisu i podzakonskih akata; i

- ovog Pravilnika i implementiranih AIDRSCA servisa i procedura.

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. Rezultati revizije se dostavljaju AIDRSCA PMA, a zaključak revizije će se objaviti javno na web strani AIDRSCA.

9. OSTALE POSLOVNE I PRAVNE STVARI

Krajni korisnici su zaposleni u organima republičke uprave i usluge certifikacije se ne naplaćuju.

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.

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.

Sve informacije koje se prikupljaju, generišu, prenose, i održavaju od strane AIDRSCA, smatraju se povjerljivim, osim informacija koje se objavljuju kao dio certifikata, CRL, CPS-a ili druge informacije koje se objavljuju u javnom registru certifikacionog tijela.

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

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 vlasnik je svih podataka, deficinija procesa, procedura i razultata nastalih u radu AIDRSCA.

AIDRSCA ima obavezu da izdaje certifikate, izvršava ostale procedure vezane za upravljanje certifikatima i upravlja infrastrukturom certifikacionog tijela u skladu sa ovim dokumentom, pravilnicima 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: [1]

- 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;
- da vodi tačnu i zaštićenu evidenciju nevažećih elektronskih certifikata koja mora biti javno dostupna;
- 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.

Prihvatanjem certifikata koji je izdalo AIDRSCA, korisnik se obavezuje u skladu sa Zakonom da: [2]

- Preduzme sve potrebne organizacione i tehničke mjere zaštite od gubitaka certifikata 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;
- 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 zatraži opoziv svog certifikata u svim slučajevima gubitka ili oštećenja sredstava ili podataka za izradu elektronskog potpisa;

[1] Zakon o elektronskom potpisu RS - “Službeni glasnik Republike Srpske", br. 59/08, član 29.

[2] Zakon o elektronskom potpisu RS - “Službeni glasnik Republike Srpske", br. 59/08, član 24.-28.

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

- budu upoznata sa ograničenjima upotrebe certifikata i odgovornosti AIDRSCA kako je detaljno opisano u ovom dokumentu, Praktičnim pravilima rada certifikacionog tijela, pravilnicima i važećim zakonima koji propisuju ovu oblast;
- ograniče oslanjanje na certifikate koje je izdalo AIDRSCA za odgovarajuće upotrebe kako je detaljno objašnjeno u praktičnim pravilima pružanja usluga certifikata, sekciji 1.4 Upotreba certifikata;
- provjere status certifikata na validnim listama opozvanih certifikata (CRLs) i da se na ovaj način 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.

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 republičkom organu uprave 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.

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.

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

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).

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.

CP stupa na snagu nakon njegovog usvajanja tj. odobrenja od strane AIDRSCA PMA. AIDRSCA distribuira aktuelnu verziju CP i tekuće verzije svih javnih dokumenata preko svoje web stranice.