Agencija za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine, ulica Kralja Petra I Karađorđevića 83A, Banja Luka, Bosna i Hercegovina

PRAKTIČNA PRAVILA PRUŽANJA USLUGE OVJERAVANJA OVJERIOCA IDDEEA (CPS)

Verzija 2.0

Vrijedi počev od 17.01.2024. godine

Identifikacioni broj	
Verzija	2.0
Predlaže:	PMA Ovjerioca IDDEEA

Verzija	Datum	Pripremio:	Kratak opis izmjena
1.0	2021-09-20	Službenik za bezbjednost	Početna verzija
2.0	2024-01-17	Službenik za bezbjednost	Verzija 2.0

Sadržaj:

1. UVODNI DIO

Agencija za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (u daljnjem tekstu: IDDEEA) je izgradila infrastrukturu javnih kriptografskih ključeva - *Public Key Infrastructure – PKI* i kao ovjerilac u smislu Zakona o elektronskom potpisu („Službeni glasnik BiH“, broj: 91/06) prisutna je kao ovjerilac koji pruža usluge izdavanja kvalificiranih i nekvalificiranih elektronskih potvrda, upravljanja životnim ciklusom elektronskih potvrda i izdavanje kvalificiranih elektronskih vremenskih žigova, pod imenom: Ovjerilac IDDEEA.

- Ovjerilac IDDEEA vrši izdavanje kvalificiranih elektronskih potvrda u skladu sa zakonskim propisima, općim aktima i uputstvima Ovjerioca IDDEEA koji reguliraju ovu oblast. Pravni okvir za obavljanje djelatnosti izdavanja kvalificiranih elektronskih potvrda Ovjerioca IDDEEA čine sljedeći zakoni i podzakonski akti:

- Zakon o elektronskom potpisu („Službeni glasnik BiH“, broj 91/06),
- Zakon o elektronskom dokumentu („Službeni glasnik BiH“, broj 58/14),
- Pravilnik o bližim uvjetima izdavanja kvalificiranih potvrda („Službeni glasnik BiH“,broj 14/17).

Opća pravila funkcioniranja Ovjerioca IDDEEA sadržana su u dokumentima:

- Politika ovjeravanja Ovjerioca Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (*Certification Policy - CP*) (u daljnjem tekstu Politika ovjeravanja),
- Praktična pravila pružanja usluge ovjeravanja Ovjerioca Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (*Certification Practices Statement - CPS*).

Praktična pravila pružanja usluge ovjeravanja Ovjerioca Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (u daljnjem tekstu: Praktična pravila), predstavljaju javni dokument koji definira proces pružanja usluge ovjeravanja i način njihovog korištenja pri izdavanju i upravljanju životnim ciklusom elektronskih potvrda i elektronskih pečata, operativne procedure u cilju ispunjenja postavljenih zahtjeva i način na koji Ovjerilac IDDEEA ispunjava tehničke, organizacione i proceduralne zahtjeve poslovanja koji su identificirani u Politici ovjeravanja, kao i upotrebu elektronske potvrde od strane korisnika.

Usluge povjerenja koje pruža Ovjerilac IDDEEA jesu obim ovog dokumenta. Ovaj dokument opisuje kompletan životni ciklus kvalificiranih i nekvalificiranih elektronskih potvrda izdanih na sigurnim kriptografskim uređajima ili u vidu softverskih potvrda od strane Ovjerioca IDDEEA. Politika ovjeravanja i Praktična pravila kao javni dokumenti objavljuju se na zvaničnoj *Web*stranici Ovjerioca IDDEEA.

Osim ovih dokumenata, korisnicima i svim zainteresiranim licima, na zvaničnoj *Web* stranici Ovjerioca IDDEEA dostupni su:

- Obrasci ugovora o izdavanju i korištenju kvalificiranih elektronskih potvrda,
- Obrasci zahtjeva za izdavanje i korištenje kvalificiranih elektronskih potvrda,
- Obrasci zahtjeva za promjenu statusa kvalificiranih elektronskih potvrda,
- Korisnička uputstva,
- Ostali akti vezani za rad Ovjerioca IDDEEA.

Ovjerilac IDDEEA utvrđuje i Posebna interna pravila rada Ovjerioca IDDEEA i zaštite sistema ovjeravanja (u daljnjem tekstu: Posebna pravila). Posebna pravila su interni dokumenti i predstavljaju poslovnu tajnu IDDEEA.

Kvalificirane i nekvalificirane elektronske potvrde i kvalificirani elektronski vremenski žigovi koje izdaje Ovjerilac IDDEEA su u skladu s eIDAS uredbom Evropske unije („Uredba broj 910/2014 Evropskog parlamenta i Vijeća o elektronskoj identifikaciji i uslugama povjerenja za elektronske transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ“) i odgovarajućim međunarodnim standardima i preporukama, kao i drugim standardima, dokumentima i preporukama, koje se odnose na izdavanje kvalificiranih elektronskih potvrda.

1.1 Pregled

Ovjerilac IDDEEA upravlja infrastrukturom javnog ključa za pružanje sljedećih kvalifikovanih usluga od povjerenja:

1) Izdavanje kvalifikovanih potvrda za elektronski potpis;
2) Izdavanje kvalifikovanih potvrda za udaljeni elektronski potpis;

Ovjerilac IDDEEA upravlja infrastrukturom javnog ključa za pružanje sljedećih usluga od povjerenja:

1) Izdavanje elektronskih potvrda za autentifikaciju korisnika koje se koriste za pouzdano utvrđivanje identiteta korisnika u različitim skupovima elektronskih usluga koje nudi IDDEEA, druge javne institucije kao i privatni sektor.

Ova Politika certifikacije je javni dokument koji predstavlja dio propisa koje definiše Ovjerilac IDDEEA koji se odnose na kvalifikovane usluge od povjerenja koje pruža Ovjerilac IDDEEA kao tijelo ovlašteno za pružanje usluga od povjerenja. Svrha ovog dokumenta je da pojasni tehničke, proceduralne i organizacione aktivnosti, kao i primjenu infrastrukture javnog ključa (PKI IDDEEA) i provedene procedure certifikacije koje pokazuju povjerljivost IDDEEA-e kao kvalifikovanog pružaoca usluga od povjerenja (TSP).

Ovaj dokument sadrži Politiku certifikacije IDDEEA-e. Dokument je izrađen u skladu sa okvirnim dokumentom IETF RFC 3647 “Internet X.509 Infrastruktura javnog ključa: Okvirna politika certifikacije i certifikacione prakse” koji sadrži okvir sa sveobuhvatnom listom tema koje treba da budu obrađene u politici certifikacije i/ili izjavi o praksi certifikacije. Sadržaj je usklađen sa:

- ETSI EN 319 401 Opšti uslovi politike za pružaoce usluga od povjerenja
- ETSI EN 319 411-1 Politika i bezbjednosni uslovi za pružaoce usluga povjerenja koji izdaju certifikate; Dio 1: Opšti uslovi
- ETSI EN 319 411-2 Politika i bezbjednosni uslovi za pružaoce usluga povjerenja koji izdaju certifikate; Dio 2: Uslovi koje moraju da ispune pružaoci usluga od povjerenja koji izdaju EU kvalifikovane sertifikate;
- ETSI EN 319 412-1 Profili certifikata; Dio 1: Pregled i zajednička struktura podataka

- ETSI EN 319 412-2 Profili certifikata; Dio 2: Profili sertifikata za fizička lica
- ETSI EN 319 412-3 Profili certifikata; Dio 3: Profili sertifikata za pravna lica
- ETSI EN 319 412-5 Profili certifikata; Dio 5: Profil kvalifikovanog elektronskog certifikata (QCStatement)
- ETSI TS 119 495 Uslovi karakteristični za sektor; Profili kvalifikovanog certifikata i Uslovi politike TSP-a u skladu sa Direktivom o platnim uslugama (EU) 2015/2366

Ovaj dokument opisuje javna pravila za kategorije kvalifikovanih i normalizovanih potvrda koji su navedeni u tabelama ispod.

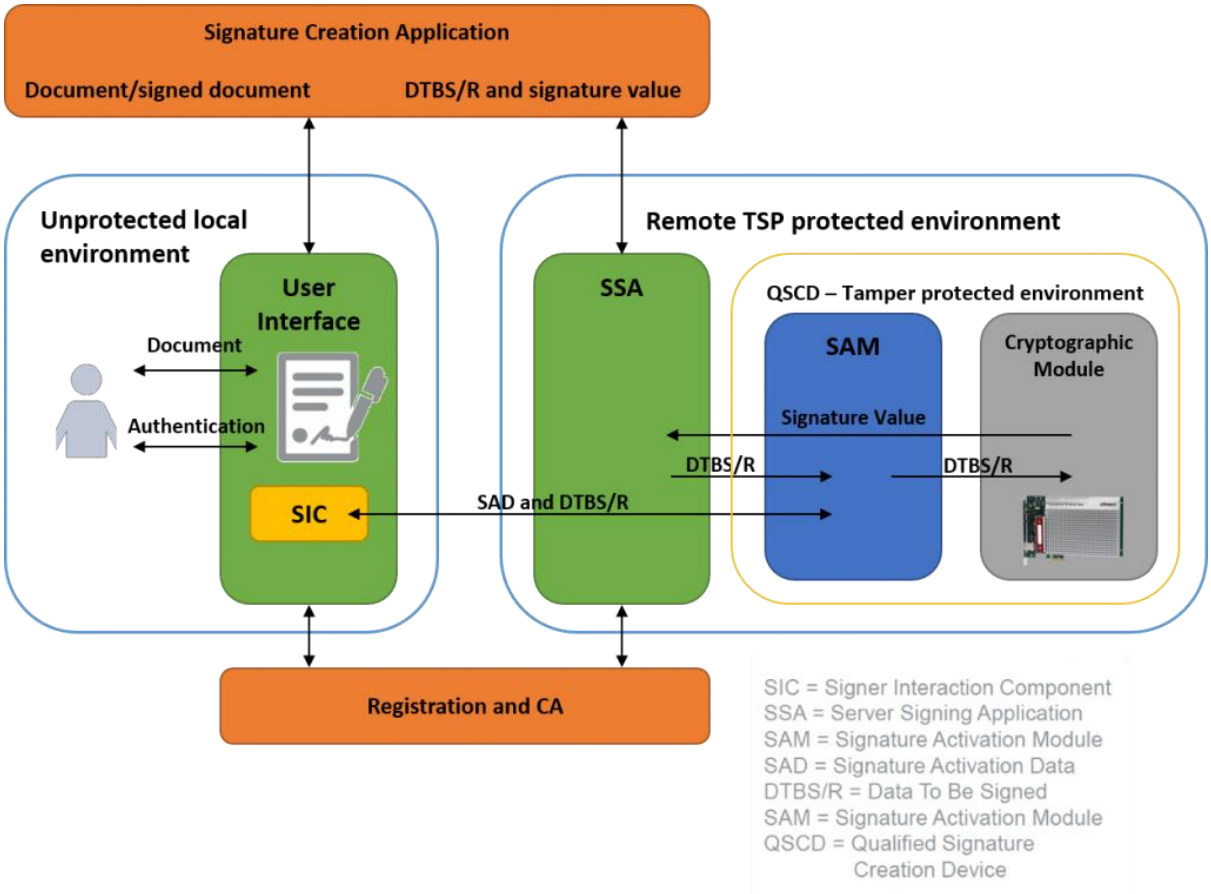
Tabela 1: Spisak kvalifikovanih certifikata

Kategorija certifikata	Opis
Elektronski certifikat za kvalifikovani e-potpis	Elektronski certifikat za kvalifikovani elektronski potpis izdat fizičkom licu gdje se privatni ključ i pripadajući certifikat nalaze na QSCD-u
Elektronski certifikat za kvalifikovani elektronski potpis za udaljeno potpisivanje	Elektronski certifikat za kvalifikovani elektronski potpis za udaljeno potpisivanje izdat fizičkom licu gdje se privatni ključ i pripadajući certfikat nalazi na serverskoj infrastrukturi Ovjerioca IDDEEA

Tabela 2: Spisak normalizovanih certifikata

Kategorija certifikata	Opis
Normalizovani elektronski certifikat – OCSP	Normalizovani OCSP

Na sljedećoj slici je prikazana arhitektura sistema za udaljeno elektronsko potpisivanje dokumenata.



Kao što se vidi sa prikazane arhitekture za udaljeno elektronsko potpisivanje, sistem se sastoji od više gradivnih blokova, od kojih se izdvajaju;

- Aplikacija za udaljeno elektronsko potpisivanje dokumenta sa korisničkim interfejsom integrisanim sa ključnim procesima autentifikacije korisnika, interakcijom sa serverskim komponentama za elektronsko potpisivanje, procesom registracije i izdavanja kvalifikovanih elektronskih potvrda.
- Serverski sistem za udaljeno elektronsko potpisivanje dokumenta, koje se sastoji od serverske aplikacije za udaljeno elektronsko potpisivanje i sigurnog serverskog repozitorija koji čuva certifikate i privatne ključeve korisnika u kripotovanom obliku koji mogu biti dektiptovani jedino PIN kodom koji ima korisnik aplikacije. Serverski sistem za udaljeno elektronsko potpisivanje dokumenta je povezan i sa CA tijelom koje vrši izdavanje kvalifikovanih potvrda za elektronsko potpisivanje.
- Korisnički certifikati za udaljeno elektronsko potpisivanje imaju istu strukturu, isto korijensko certifikaciono tijelo, isto potpisujuće certifikaciono tijelo kao i sve elemente u certifikatu kao i certifikati za za kvalifikovani e-potpis, a što se postiže zahvaljujući prikazanoj arhitekturi sistema.

1.2 Naziv dokumenta i identifikacija

Ovaj dokument predstavlja Politiku certifikacije IDDEEA-e, (u daljem tekstu Politika ili PS). Politika je objavljena na sljedećem URL-u:

- https://www.iddeea.gov.ba/PKI/CP i javno je dostupan.

Dokument pod nazivom Izjava o otkrivanju infrastrukture javnog ključa IDDEEA-e, sastavljen u skladu sa ETSI EN 319 411-1, Aneks A.1, u daljem tekstu PDS, objavljen je na sljedećim URL-ovima:

- https://www.iddeea.gov.ba/PKI/CP

Sljedeći identifikatori objekta (OIDs) se dodjeljuju kategorijama certifikata koji se izdaju u skladu sa ovom Politikom.

Kategorija certifikata	Identifikacija certifikacione politike
Elektronski certifikat za kvalifikovani e-potpis	0.4.0.194112.1.2
Elektronski certifikat za kvalifikovani elektronski potpis za udaljeno potpisivanje	0.4.0.194112.1.2
Normalizovani elektronski certifikat – OCSP	0.4.0.194112.1.2

Ovjerilac IDDEEA može izdati različite certifikate, koji moraju biti jasno označeni s posebnom politikom ili dodatnim identifikatorom objekta politike u ekstenziji X.509 *certificatePolicies*. Identifikator objekta ima prefiks 1.3.6.1.4.1.*18560*. Identifier i trebao bi biti jedinstven za ovaj prefiks.

1.3 Učesnici u infrastrukturi javnog ključa (PKI)

1.3.1. Certifikaciona tijela

Ovjerilac IDDEEA djeluje kao javni pružalac usluga od povjerenja (TSP) i izdaje certifikate javnog ključa fizičkim licima.

Ovjerilac IDDEEA djeluje kao centralno certifikaciono tijelo koje izdaje samopotpisane certifikate u procesu ceremonije generisanja korijenskog ključa i unakrsnog certifikata jednom hijerarhijski

podređenom certifikacionom tijelu (CA). Ovjerilac IDDEEA koristi jedno certifikaciono tijelo (CA za izdavanje certifikata) za izdavanje svih vrsta kvalifikovanih i normalizovanih certifikata krajnjim korisnicima.

Ovjerilac IDDEEA upravlja sljedećim certifikacionim tijelima:

Centralnim certifikacionim tijelom IDDEEA sa mandatom od 20. septembra 2021. do 20. septembra 2041. koje ima samopotpisni certifikat koji izdaje certifikacionim tijelima IDDEEA-e.

Certifikacionim tijelima Ovjerioca IDDEEA koja izdaju kvalifikovane certifikate krajnjeg identiteta sa mandatom od 29. septembra 2021. do 29. septembra 2031. koje potpisuje Centralno certifikaciono tijelo IDDEEA.

Sadržaj digitalnog certifikata “IDDEEA-RootCA-2021”:

Serijski broj	449FFCA0B7E0AFE2DC4C5D9754F945677B9028AC
Izdaje	IDDEEA
Subjekat	CN=IDDEEA-RootCA-2021, O=IDDEEA, emailAddress=eid@iddeea.gov.ba, L=Banja Luka, street=Kralja Petra I Karadjordjevica 83A, postalCode=78000, C=BA
Rok važenja: ne prije	20.09.2021
Rok važenja: ne poslije	20.09.2041
Javni ključ RSA	82:D0:61:16:28:EE:51:49:DF:40:C5:51:AA:DD:59:F8 66:B9:9D:1A:86:FB:7E:A8:37:33:54:B1:97:3C:72:26 C3:B8:B6:6C:0F:B0:35:CD:42:40:8A:87:22:DE:3A:90 5A:AA:29:52:AD:39:8E:C5:76:99:54:3B:3E:E1:00:12 DB:7E:0F:21:B1:31:EA:6B:87:5E:FC:B2:5B:AC:D7:FC F0:3C:BE:C3:BB:25:52:A5:C4:46:0B:94:8F:EF:C8:BE 25:4F:E2:F2:DC:69:60:F9:69:44:F7:2F:9A:01:2E:9E EE:88:A7:5D:7A:77:45:36:7F:70:ED:E9:A9:2C:2F:98 91:92:0B:FA:FB:B3:7F:62:C9:BA:EE:EE:60:60:26:65 66:FB:A6:7F:6A:F5:F7:2D:F6:39:50:68:68:EC:33:DD 4C:F8:35:42:92:57:0C:5E:8F:4A:DD:D4:83:2F:39:C3 D5:C7:68:CD:99:49:16:7F:1A:A8:F4:50:34:BF:5B:2C 10:C5:21:34:92:DF:35:AB:B6:4C:EF:32:12:EA:8B:AC CC:EE:71:06:1E:FF:46:53:DC:3B:32:F1:20:45:62:CC 50:39:DC:4F:14:7E:6D:2E:A1:D4:3A:82:45:61:4D:50 1B:91:06:35:C8:28:88:8B:26:FF:5C:40:DD:B5:42:08 C6:D8:AF:6D:02:B6:ED:EC:80:65:14:6F:AC:5D:E0:FB BC:B8:54:C3:F9:45:00:C4:F1:83:34:F8:2A:84:56:E8 DC:A3:37:FD:E2:1A:B9:9C:51:CC:37:20:BB:53:4D:64 37:BB:67:AD:85:D5:43:F7:80:60:C3:6E:F2:E5:51:5B B6:77:77:36:B0:03:45:33:06:2E:23:72:54:25:31:09 79:9C:05:4B:DF:D1:E2:E9:11:FE:2E:4D:93:B0:06:3D F0:84:02:56:D0:E7:FC:DE:11:6E:EE:F9:63:52:48:C6 68:6B:D4:76:E6:BB:A0:D5:96:A5:2B:DB:E7:58:99:16 47:37:90:13:1F:FF:F7:EA:9B:75:9A:7B:40:B2:FC:46 C7:5E:BA:96:C9:09:E9:74:FC:88:7E:B9:3E:73:2A:3D 2A:33:06:95:28:4B:68:86:78:D1:FF:32:CB:57:26:BE D3:C9:17:47:B8:26:A1:1C:03:77:C7:EE:57:FA:CE:E4 59:2E:BC:FD:43:AB:C1:56:8B:66:7D:28:58:A5:00:E8 B4:45:08:AB:25:5E:51:94:81:07:C2:67:8A:27:55:36 0E:D0:45:94:F5:17:1F:D2:52:E0:DA:38:78:99:AA:9A 79:7B:E3:04:B2:DF:6B:92:09:C2:A5:95:85:70:4F:8B
Algoritam potpisa	sha512WithRSAEncryption
Identifikator ključa	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
Identifikator ključa ovlaštenja	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
SHA-1 hash	A2:4E:6B:E6:78:98:AE:DD:5E:E9:5B:09:82:34:E5:80:48:37:E5:DD
SHA-256 hash	57:75:50:3D:A6:29:84:27:01:5B:33:79:6B:13:44:C2 D6:8E:C4:39:72:99:7B:6D:BB:83:DD:41:67:E3:CF:E5

Digitalni certifikat certifikacionog tijela za izdavanje certifikata IDDEEA-IssuingCA sa rokom važenja od 29. septembra 2021. do 29. septembra 2031." sadrži:

Serijski broj	27AF82049AC3D91AE8664A4A6FFFB991AE89B66C
Izdaje	IDDEEA
Subjekat	CN=IDDEEA-IssuingCA
Rok važenja: ne prije	29.09.2021
Rok važenja: ne poslije	29.09.2031
Javni ključ RSA	B0:DC:AF:AD:C5:1E:14:97:AC:A9:DA:77:C1:06:6A:61 D1:28:DA:45:78:93:B4:A6:70:8B:DE:82:37:EF:4B:61 7D:37:A8:C0:0E:A1:15:7E:D7:CB:9C:3D:43:7A:89:7C B6:FC:A5:93:12:CE:74:00:1B:5E:F7:C6:25:E8:C8:F0 DF:C9:D6:DF:EB:5C:B3:A2:A4:33:6C:54:D6:A4:EA:72 3D:D5:E2:38:F8:74:4C:B7:2F:4E:B4:92:13:3A:D5:07 50:34:57:BC:18:26:90:58:97:EA:BA:E1:17:DF:22:CA 3B:F3:2B:2C:5E:8D:77:93:BC:C8:75:3F:30:99:1C:87 D2:3A:36:80:6F:BC:D3:9D:D2:28:36:8E:84:51:DC:A1 80:FD:75:64:7E:D1:8E:E2:B0:9A:79:C6:36:9D:CB:3B 81:8D:90:E0:4C:D2:16:5F:F3:0A:4A:B9:39:04:B3:20 39:8B:DF:50:A5:22:64:54:27:C8:56:CC:C3:6E:5C:F0 D8:6D:2B:7B:09:13:FE:E9:6F:9A:16:29:3B:E4:A5:3B F2:74:68:39:88:4C:49:48:3A:35:A9:96:A6:D1:CC:22 B2:99:10:8F:05:C6:A3:A2:76:5A:DA:36:9E:7C:97:C2 4F:50:AA:A4:02:65:AA:34:53:56:0A:14:2A:A3:F4:BC 30:5E:E6:6A:71:71:1C:AF:E8:9B:2A:EB:5E:42:62:AD 39:2B:CA:C2:5F:02:7C:00:4F:D5:AE:F0:94:61:2D:B3 DF:D1:D1:50:96:3F:A9:63:2D:CC:B5:88:DD:FE:A3:AC 45:51:0E:76:D2:E7:E3:19:B0:EC:B3:06:DB:D9:FE:BD 2A:4C:5B:A9:77:AF:11:C1:1E:52:A8:3C:AD:BF:B5:86 9B:E5:B5:98:1D:94:CE:E2:7C:65:67:FF:D4:EF:51:0E 49:96:82:6B:FF:35:C6:08:8F:0E:7F:83:39:EE:15:2C 6A:A0:EF:3C:F9:88:1D:13:5C:22:EA:1F:A6:73:4C:41 B9:04:F5:B6:76:1F:46:A3:75:75:A6:D4:D6:31:54:0B 3D:C6:8C:67:A3:4B:0E:93:4B:81:9B:5B:86:3E:DB:57 76:F1:0A:B8:ED:75:E9:1C:95:1C:E4:45:15:09:93:E4 12:CD:91:D7:44:4A:9C:1E:AE:A1:4D:13:DB:70:F3:15 59:BA:56:EF:76:C4:21:41:3B:C5:D5:16:58:1D:57:04 71:6D:CB:97:46:A8:7A:9A:4F:7B:1E:E3:9A:C7:3C:60 0A:5D:FB:A4:E9:83:15:49:11:23:21:B1:B4:34:2A:68 DF:9F:6F:C6:16:8B:F0:E9:0F:E6:24:5A:7C:5C:50:DF
Algoritam potpisa	sha512WithRSAEncryption
Identifikator ključa	55:4D:EF:8B:87:48:55:BA:DD:AA:0E:41:D6:B6:CB:7D:77:1A:11:DA
Identifikator ključa ovlaštenja	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
SHA-1 hash	C2:A7:DF:30:66:40:D0:7E:D1:BF:E6:98:37:48:5E:32:E7:4A:60:5A
SHA-256 hash	71:27:C8:24:E2:47:5C:B8:A9:25:E0:53:83:91:41:6C 2D:F0:0B:B9:C1:B6:85:95:1D:98:F3:A1:D0:AD:CE:EF

Ovjerilac IDDEEA je kao pružalac usluga od povjerenja dužna provoditi mjere i postupke kojima se osigurava upravljanje certifikatima, u skladu sa važećim propisima u Bosni i Hercegovini i internim pravilima pružaoca usluga certifikovanja. Ovjerilac IDDEEA zapošljava osobe koje su odgovorne za:

- cjelokupni rad TSP-a (Tijela za upravljanje politikom u IDDEEA – IDDEEA PMA);
- osobe koje upravljaju i održavaju TSP infrastrukturu, privatne kriptografske ključeve CA, servere i softver (Tijelo za operativne poslove – OA); i
- osobe koje su odgovorne za identifikaciju korisnika (Tijelo za registraciju – RA) i koordinaciju sa spoljnim RA.

Kada je potrebno, ova pravila politike prave razliku između različitih korisnika i uloga onih koji pristupaju funkcijama TSP-a. Kada ova razlika nije potrebna, termin TSP se koristi za označavanje ukupnog TSP entiteta, uključujući softver i njegove operacije.

1.3.1.1 Tijelo za upravljanje politikom (PMA)

IDDEEA PMA je odgovorna za:

- izradu i održavanje Politike certifikacije Ovjerioca IDDEEA;
- izradu i održavanje javnih dokumenata Ovjerioca IDDEEA (Ugovor sa krajnjim korisnicima, itd.)
- izradu Politike certifikacije Ovjerioca IDDEEA i upućivanje na odobrenje;
- registraciju i akreditovanje Ovjerioca IDDEEA;
- angažovanje osoblja u tijelima za operativne poslove i registraciju (OA i RA);
- kontrolu i reviziju usklađenosti Ovjerioca IDDEEA operacija i aktivnosti kako bi se osiguralo da TSP radi u skladu sa Politikom i relevantnim zakonodavstvom;
- kontrolu i odobravanje Politike certifikacije (CP), ili Izjave o praksi certifikacije (CPS dokument) spoljnjih unakrsno certifikovanih tijela za certifikaciju;
- rješavanje sporova između učesnika Ovjerioca IDDEEA.

1.3.1.2 Operativno tijelo (OA)

Operativno tijelo Ovjerioca IDDEEA nadležno je za:

- generisanje TSP para ključeva, bezbjedno upravljanje privatnim tsp ključevima, i distribuciju javnih TSP ključeva;
- uspostavljanje okruženja i procedure za podnošenje zahtjeva za certifikaciju;
- identifikaciju i autentikaciju pojedinaca ili lica koji se prijavljuju za certifikat;
- odobravanje i odbijanje zahtjeva za izdavanje certifikata;
- potpisivanje i izdavanje X.509 certifikata koji korisnike obavezuje svojim javnim ključem, kao odgovor da je zahtjev za izdavanje certifikata odobren;
- slanje X.509 certifikata putem direktorija;
- pokretanje opoziva certifikata, bilo na zahtjev korisnika ili na sopstvenu inicijativu Ovjerioca IDDEEA;
- opoziv certifikata, uključujući izdavanje i objavljivanje Spiska opozvanih certifikata (CRL-ova) i održavanje servisa Protokola o elektronskoj provjeri certifikata;
- upravljanje TSP-om u skladu sa zakonima u Bosni i Hercegovini i ovom Politikom;
- odobravanje i angažovanje osoba kako bi se popunile radne pozicije za PKI službenike;
- kontrolu i reviziju poslova RA u okviru svoje nadležnosti;
- iniciranje opoziva certifikata zaposlenih u TSP-u i RA.

1.3.2 Registraciona tijela Ovjerioca IDDEEA (RA)

Registraciono tijelo (u daljem tekstu: RA) obavlja sljedeće zadatke za Ovjerioca IDDEEA:

- Provjeru identiteta fizičkih lica i ostalih relevantnih podataka za upravljanje certifikatima;
- Primanje obrazaca zahtjeva za izdavanje certifikata,
- Izdavanja neophodne dokumentacije za korisnike ili za buduće korisnike,
- Prenosa obrazaca zahtjeva, zahtjeva i ostalih informacija na siguran način Ovjeriocu IDDEEA.

TSP Ovjerioca IDDEEA može ovlastiti druge institucije kao i organizacije iz poslovnog i javnog sektora, pored svojih RA, da obavljaju zadatke koji pripadaju RA ili druge aktivnosti za koje im TSP Ovjerioca IDDEEA da ovlaštenje. Ovjerioc IDDEEA ugovorom obavezuje te institucije ili organizacije na ispunjavanje strogih sigurnosnih uslova u skladu sa mjerodavnim zakonodavstvom, evropskim uredbama i međunarodnim, evropskim i domaćim standardima, preporukama i pravilima, CPS-om i internim pravilima Ovjerioca IDDEEA.

Ovjerioc IDDEEA ima geografski raširene RA čime se budućim subjektima omogućava laka registracija. Informacije o lokacijama RA su dostupne na internet stranici TSP-a Ovjerioca IDDEEA.

1.3.3 Korisnici

Lice je fizičko lice kome se izdaje e-OI/e-LK, koje dobiva certifikat na ličnoj karti ili certifikat za udaljeno potpisivanje i potpisuje Ugovor sa IDDEEA-om o pružanju usluga certifikacije u skladu s relevantnim zakonima. Lice je direktno odgovorno za postupanje u skladu sa Uslovima certifikacionih usluga.

Lice je i ono lice koje je navedeno u certifikatu i potpisnik koji kreira elektronski potpis i koristi certifikat u njegovo/njeno ime.

Korisnik je lice, uključujući i fizičko lice (pojedince), koje koristi usluge.

Korisnik je lice koje je identifikovano u certifikatu kao nosilac privatnog ključa koji je povezan sa javnim ključem datim u certifikatu.

Korisnik je lice koje snosi krajnju odgovornost za korištenje privatnog ključa koji je povezan sa certifikatom javnog ključa, dok je subjekat osoba čija je autentikacija izvršena pomoću privatnog ključa.

1.3.4 Treće strane

Treća lica su osobe koje se oslanjaju na izdate certifikate i ostale usluge Ovjerioca IDDEEA, a koje mogu biti fizička ili pravna lica.

Treća lica moraju pratiti upute Ovjerioca IDDEEA i uvijek moraju provjeriti validnost certifikata (opoziv), svrhu korištenja certifikata, period validnosti certifikata (rok trajanja), itd. Obaveze i odgovornosti trećih lica su detaljnije obrađene u Odjeljcima 4.5.2 i 9.6.4

Treća lica ne moraju obavezno biti korisnici certifikata Ovjerioca IDDEEA ili digitalnih certifikata drugih pružalaca usluga povjerenja.

Prije nego što se oslone na informacije koje su date u certifikatu, treće strane se uvijek moraju pozvati na Ovjerioca IDDEEA CRL ili OCSP kako bi se potvrdila validnost sertifikata koji su dobili.

1.3..5 Ostali učesnici

Nije primjenjivo.

1.4 Upotreba certifikata

Ovjerilac IDDEEA upravlja (izdaje, provjerava, opoziva, obnavlja, pohranjuje, objavljuje) kvalifikovane certifikate za elektronske potpise. Certifikati su namijenjeni fizičkim licima.

1.4.1 Prihvatljivo korištenje certifikata

Certifikati za elektronske potpise se namijenjeni za potpisivanje unilateralnih ili uzajamnih komunikacija između korisnika certifikata i za korištenje u raznim aplikacijama i u različite svrhe koje se susreću na tržištu. Između ostalog, certifikati se mogu koristit za sljedeću namjenu:

- identifikacija korisnika,
- otkrivanje identiteta korisnika,
- potpisivanje dokumenta u elektronskoj formi,
- šifrovanje i dešifrovanje dokumenata u elektronskoj formi.

Elektronski potpis se može koristiti u sljedećim aplikacijama:

- elektronsko ili mobilno bankarstvo,
- aplikacije koje se koriste za eVladu ili mVladu (engleski: eGovernment ili mGovernment),
- aplikacije koje se koriste za eZdravlje ili mZdravlje (engleski: eHealth ili mHealth),
- elektronski potpisi ili mobilni obrasci,
- sigurna veza sa tijelima i organizacijama iz javnog sektora i sa ostalim fizičkim i pravnim licima,
- ostale aplikacije ili usluge u kojima se traži certifikat,
- kontrola pristupa.

Druge namjene na zahtjev korisnika i u skladu sa Zakonom o elektronskim dokumentima, Zakonom o elektronskom potpisu i drugim relevantnim zakonima u Bosni i Hercegovini.

Napomena: Ne čuvati kopiju privatnih ključeva za dešifrovanje korisnika za oporavak ključa. Odgovornost korisnika je da održava bezbjednu kopiju privatnih ključeva za dešifrovanje.

1.4.2 Zabrana korištenja certifikata

Svi certifikati koje izdaje Ovjerilac IDDEEA koriste se u skladu sa važećim zakonodavstvom Bosne i Hercegovine.

Zabranjena je upotreba certifikata, koji su izdati u skladu sa pravilima, koja je suprotna odredbama pravila ili uredbama koje su na snazi ili je izvan djelokruga dozvoljene upotrebe koja se navodi u prethodnom odjeljku.

Certifikati nisu namijenjeni za preprodaju.

1.5 Administriranje politike certifikacije

1.5.1 Administriranje dokumenta

Pravilima i CPS-om upravlja Ovjerilac IDDEEA koji djeluje u okviru Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine.

1.5.2 Kontakt osoba

Za pitanja koja su vezana za CPS i pravila, možete se obratiti ovlaštenim licima Ovjerioca IDDEEA koja možete dobiti na dolje navedenoj adresi;

Adresa:	Agencija za identifikaciona dokumenta evidenciju i razmjenu podataka Bosne i Hercegovine- IDDEEA; Kralja Petra I Karađorđevića 83A; Banja Luka
E-pošta:	eid@iddeea.gov.ba
Internet:	https://www.iddeea.gov.ba

1.5.3 Odgovorna osoba za utvrđivanje usklađenosti CPS-a sa pravilima

U skladu sa datim odgovornostima, ovlašteno osoblje Ovjerioca IDDEEA je odgovorno za usklađenost Ovjerioca IDDEEA sa CPS-om i pravilima.

1.5.4 Procedura odobravanja Izjave o certifikacionoj praksi

Certifikacionu politiku Ovjerioca IDDEEA izrađuje i održava IDDEEA PMA, a odobrava je direktor IDDEEA-e.

1.6 Definicije i skraćenice

Definicije:

Elektronski potpis je skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa drugim podacima u elektronskom obliku, a koristi ga potpisnik za potpisivanje.

Potpisnik je fizičko lice koje kreira elektronski potpis.

Informacioni sistem je sistem koji se koristi za prikupljanje, slanje, primanje, čuvanje ili drugu vrstu obrade elektronskih podataka.

Podaci za kreiranje potpisa su jedinstveni podaci koji se koriste u procesu izrade elektronskog potpisa, kao što su kodovi ili privatni kriptografski ključevi.

Sredstva za kreiranje potpisa su konfigurisani programi ili tehnička oprema koja se koristi za izradu elektronskog potpisa.

Sredstva za formiranje kvalifikovanog potpisa - QSCD su sredstva koja obezbjeđuju jedinstvene, bezbjedne i povjerljive podatke koji se odnose na elektronski potpis, sprečavaju mogućnost dobivanja podataka o elektronskom potpisu u razumnom roku i putem opravdanih sredstava od podataka za provjeru elektronskog potpisa, obezbjeđuju zaštitu od falsifikovanja elektronskog potpisa korištenjem trenutno dostupne tehnologije i omogućavaju potpisniku da bezbjedno zaštiti podatke u elektronskom potpisu od neovlaštenog pristupa.

Podaci za provjeru elektronskog potpisa su jedinstveni podaci koji se koriste za provjeru elektronskog potpisa, kao što su kodovi ili javni kriptografski ključevi.

Sredstva za provjeru elektronskog potpisa su konfigurisani softveri ili hardveri koji se koriste da bi potvrdili da je neki elektronski potpis validan.

Certifikat je certifikat u elektronskom obliku koji potvrđuje vezu između podataka za provjeru elektronskog potpisa i odgovarajućeg lica, subjekta certifikata i identiteta tog lica.

Kvalifikovani certifikat je certifikat koji sadrži ime i državu prebivališta, odnosno sjedište tijela, ime, odnosno pseudonim korisnika, odnosno pseudonim informacionog sistema koji nosi oznaku korisnika, podatke za verifikaciju elektronskog potpisa koji se odnose na podatke o elektronskom potpisu, početak i prestanak važenja certifikata, identifikacioni broj certifikata, napredni elektronski potpis organa i moguća ograničenja u korištenju certifikata.

Normalizovani certifikat je certifikat koji ima ista tehnička svojstva i nudi isti nivo povjerljivosti kao i kvalifikovani certifikat, ali bez pravnih ograničenja njegove namjene.

Napredni elektronski potpis je elektronski potpis koji ispunjava sljedeće zahtjeve:

a) na jedinstven način je povezan sa potpisnikom;

b) može identifikovati potpisnika;

c) formiran je korišćenjem podataka za formiranje elektronskog potpisa koji se koriste pod isključivom kontrolom potpisnika uz visok stepen povjerljivosti;

d) povezan je s podacima potpisanim tako da se svaka naredna promjena podataka može otkriti.

Kvlifikovani elektronski potpis je napredni elektronski potpis koji se kreira primjenom sredstva za kreiranje kvalifikovanog elektronskog potpisa, koji je zasnovan na kvalifikovanom certifikatu elektronskog potpisa.

Certifikaciono tijelo je svako fizičko ili pravno lice koje izdaje Certifikate ili pruža druge usluge koje su povezane sa Certifikatima, odnosno sa elektronskim potpisom.

Korisnik je svako fizičko ili pravno lice koje je identifikovano u certifikatu kao zakupac privatnog ključa koji se odnosi na javni ključ koji je uključen u certifikat.

Ugovarač/aplikant je lice koje podnosi zahtjev za izdavanje certifikata od certifikacionog tijela u ime jednog ili više korisnika. Ugovarač/aplikant može biti i korisnik, kada se certifikat izdaje pojedincu za lično korištenje.

Treća strana je lice koje ima opravdano povjerenje u certifikat.

Korisnički nalog računara je korisnički nalog koji označava skup karakteristika koje omogućavaju pristup računarskom sistemu određenoj osobi. Svaki korisnički nalog je jedinstven za svaki računarski sistem, što se realizuje pomoću internih funkcija računarskog sistema. Osnova za pristup korisničkom nalogu je par korisničkog imena i lozinke. Korisničko ime je niz alfanumeričkih znakova koji se sastoji od identifikacionog imena korisnika u datom računarskom sistemu. Takvo identifikaciono ime mora biti jedinstveno na nivou računarskog sistema. Lozinka je takođe niz alfanumeričkih znakova, koji je poznat isključivo vlasniku korisničkog računa. Korisnička lozinka za one računarske sisteme koji zahtevaju visok nivo bezbjednosti može se dopuniti ili zamijeniti čip karticom.

Par ključeva za šifrovanje je par simetričnih ključeva koji se sastoje od javnog ključa za šifrovanje i pomoćnog privatnog ključa za dešifrovanje. Naziva se još i povjerljivi par ključeva.

Privatni ključ za dešifrovanje. Pogledati Par ključeva za šifrovanje.

Privatni ključ za potpisivanje. Pogledati Par ključeva za šifrovanje

Javni ključ za šifrovanje. Pogledati Par ključeva za šifrovanje

Certifikat javnog ključa za šifrovanje je Certifikat koji sadrži javni ključ za šifrovanje.

Ključ za provjeru javnog potpisa Pogledati Par ključeva za šifrovanje.

Certifikat ključa za provjeru javnog potpisa je certifikat koji sadrži javni ključ za potpis.

Par ključeva za potpis je par asimetričnih ključeva koji se sastoje od privatnog ključa za potpis i pomoćnog javnog ključa za provjeru potpisa.

QSCD (Smart kartica/token) je sredstvo za izradu kvalifikovanog elektronskog potpisa ili pečata u obliku smart kartice/tokena na kojem se privatni ključevi mogu čuvati.

HSM (Hardverski sigurnosni modul) je fizički uređaj za bezbjedno čuvanje digitalnih ključeva.

Pružalac usluga povjerenja je fizičko ili pravno lice koje pruža jednu ili više usluga od povjerenja, bilo kao kvalifikovani ili nekvalifikovani pružalac usluga od povjerenja.

Kvalifikovani pružalac usluga od povjerenja je pružalac usluga od povjerenja koji pruža jednu ili više kvalifikovanih usluga od povjerenja i kome nadzorni organ dodjeljuje status kvalifikovanog pružaoca usluga.

Skraćenice:

Spisak skraćenica, koje se koriste u ovom dokumentu i u Politici dat je u sljedećoj tabeli:

Skraćenica	**Objašnjenje**
ARL	Lista opoziva ovlaštenja (Authority Revocation List)
CA	Certifikaciono tijelo (Certificate Authority)
CN	Ime i prezime (Common Name - Name X.500)
CPS	Izjava o praksi certifikacije (Certification Practice Statement)
CRL	Spisak opozvanih certifikata (Certificate Revocation List)
DC	Digitalni certifikat (Digital Certificate)
DN	Jedinstveno ime (Distinguished Name X.500)
EAL	Nivo procijenjene sigurnosti (Evaluation Assurance Level)
EKU	Produžena upotreba ključa (Extended Key Usage)
RA	Registraciono tijelo (Registration Authority)
PMA	Primarni upravni organ (Primary Management Authority)
OA	Operativno tijelo (Operation Authority)
FIPS 140-1	Federalni standardi za obradu informacija http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf
PKCS #10	Standardi kriptografije javnog ključa (Public-Key Cryptography Standard #10)
PKI	Infrastruktura javnog ključa (Public Key Infrastructure)
PKIX	PKI zasnovan na X.509 (X.509 based PKI)
PKIX-CMP	PKIX Protokoli za upravljanje certifikatima (PKIX-Certificate Management Protocols), opisani u RFC 4510
X.509	Standardi certifikata opisani u RFC 5280
QSCD	Sredstva za provjeru kvalifikovanog elektronskog potpisa, smart kartica/token (Qualified Signature Creation Device) Sredstvo za formiranje kvalifikovanog ili naprednog elektronskog potpisa i kvalifikovanog ili naprednog pečata u skladu sa zahtjevima eIDAS
TSP	Pružalac usluga od povjerenja (Trust Service Provider)

2 ODGOVORNOST ZA OBJAVLJIVANJE I REPOZITORIJE

2.1 Repozitoriji

Ovjerilac IDDEEA objavljuje informacije vezane za certifikacione usluge u repozitorijima na sljedećim adresama: https://www.iddeea.gov.ba/PKI/CPS

Ovjerilac IDDEEA dostupnim će učiniti sve što ima veze sa njegovim poslovanjem, obavještenja subjektima i trećim licima kao i ostale relevantne dokumente.

Dokumenti dostupni za javnost su:

- Pravila o certifikatima (CP),
- Izjave o korištenju certifikata TSP-a (CPS)
- Obrasci izjave za zahtjev za certifikat, zahtjevi za opoziv, i ostale usluge koje su predmet ugovora sa TSP-om,
- Upute za sigurno korištenje digitalnih certifikata,
- Informacije o važećim uredbama i standardima u vezi sa poslovanjem TSP-a, i
- Ostale informacije vezane za poslovanje Ovjerioca IDDEEA.

Dokumenti koji čine povjerljivi dio interih pravila Ovjerioca IDDEEA nisu dostupni javnosti.

2.2 Objavljivanje informacija o certifikaciji

Ovjerilac IDDEEA objavljuje:

- Spisak opozvanih sertifikata (CRL)
- Status certifikata putem Protokola za elektronsku provjeru certifikata
- Certifikate certifikacionih tijela (CA)
- Politiku certifikata i Izjavu o dostavi PKI
- Spisak registracionih tijela
- Korisnička uputstva

IDDEEA CA obavještava i oglašava o ostalim uslugama certifikacije koje se odnose na javno informisanje.

2.3 Vrijeme i učestalost objavljivanja

Certifikati se objavljuju odmah po izdavanju, kao što je navedeno u odjeljku 4.4. Spiskovi opozvanih certifikata se objavljuju odmah nakon izdavanja, kako je navedeno u odjeljku 4.9.7. Sve informacije se objavljuju odmah nakon što se izmijene ili postanu dostupne TSP-u.

2.4 Kontrole pristupa repozitorijumima

Sve javne informacije su dostupne u dokumentu koji je samo za čitanje bez ograničenja. Repozitoriji su dodatno zaštićeni od neovlaštenih izmjena.

3 IDENTIFIKACIJA I AUTENTIKACIJA KORISNIKA

3.1.1. Vrste imena

Polje sa imenom korisnika u certifikatima koje je izdalo certifikaciono tijelo IDDEEA-e sadrži autentikovano ime korisnika kako je definisano u tabeli u dijelu 3.1.4 Pravila za tumačenje različitih oblika imena. Polje sa imenom subjekta u CA certifikatu i u certifikatima izdatim korisnicima je u obliku X.501 Distinguished Name (DN). Jedinstveno ime je kodirano kao Printable String ili UTF8String i mora biti navedeno u svim izdatim certifikatima.

3.1.2 Potreba za kreiranjem imena sa značenjem

Skup DN karakteristika korisnika certifikata jedinstveno identifikuje svakog vlasnika certifikata i ima značajne vrijednosti. Serijski broj se navodi radi razlikovanja onih imena za koja bi polje subjekta inače bilo identično.

3.1.3 Anonimnost ili pseudonimnost korisnika

Upotreba anonimnih imena ili pseudonima nije dozvoljena.

3.1.4 Pravila za tumačenje različitih oblika imena

Uz odgovarajuću kombinaciju slova, TSP će se pobrinuti za korištenje drugih nepredviđenih znakova.

Polje sa imenom korisnika je definisano kao X.501 type Name (x.500 Distinguished Name), u skladu sa RFC 5280.

Polje „Subjekat" i polje „Izdavalac" u CA sertifikatima za Ovjerioca IDDEEA su kao što je navedeno u odjeljku 1.3.1

X.500 *Jedinstveno ime* (Subjekat) u certifikatima koje izdaje Ovjerilac IDDEEA ima sljedeći oblik za:

Fizičko lice:

Komponenta jedinstvenog imena	Vrijednost
Country (C =)	BA
(O =) Za fizička lica na koja se odnosi	IDDEEA
organizationIdentifier Za fizička lica	IDDEEA
Ime	Ime
Prezime	Prezime
Common Name (CN=)	Broj lične karte korisnika certifikata
Serijski broj (serialnumber=)	Jedinstveni serijski broj

3.1.5 Jedinstvenost imena

Ovjerilac IDDEEA u subjektu certifikata dodijeljuje kombinaciju karakteristika *jedinstvenog imena*, kako je definisano u odjeljku 3.1.2 i odjeljku 3.1.4, da bi se osigurala nedvosmislenost i jedinstvenost imena.

3.1.6 Prepoznavanje, autentikacija i uloga zaštitnih znakova

Korisnici su obavezni koristiti svoje prave identitete i ne smiju se prijavljivati pod lažnim imenima ili pseudonimima. Također korisnik ne može biti anoniman.

Ovjerilac IDDEEA će odbiti svaki zahtjev za anonimnošću ili korištenjem pseudonima.

3.2 Inicijalna provjera identiteta

Identitet budućeg korisnika prilikom prvog izdavanja certifikata provjerava se u Ovjeriocu IDDEEA RA. Ovjerilac IDDEEA prije izdavanja certifikata provjerava podatke budućeg korisnika u odgovarajućim registrima.

3.2.1 Metod za dokazivanje posjedovanja privatnog ključa

Demonstracija postojanja privatnog ključa koji pripada javnom ključu u certifikatu osigurava se sigurnim procedurama prije i prilikom prihvatanja certifikata i standardom PKCS # 10.

3.2.2 Autentikacija identiteta pojedinca

Za svakog pojedinca (fizičko lice), koje želi da postane korisnik Ovjerioca IDDEEA, obavlja se provjera identiteta licem u lice. Lice koje je odgovorno za poslove registracije identifikuje fizičko lice koje podnosi zahtjev za certifikat ili uslugu pregledajući njegovu važeću ličnu kartu ili pasoš u prisustvu tog lica.

Ovjerilac IDDEEA vodi evidenciju o sredstvima kojima je potvrđen identitet lica.

3.2.3 Neprovjerene informacije o korisniku

Ovjerilac IDDEEA ne provjerava tačnost i e-maila i telefonskog broja korisnika.

3.2.4 Kriteriji za međuoperaciju

Ovjerilac IDDEEA nije obavezan da ugovara ili garantuje za druge pružaoce usluga povjerenja čak i ako drugi TSP ima status kvalifikovanog TSP-a ili TSP-a kvalifikovanih digitalnih certifikata.

Procedure i prakse svih unakrsno sertifikovanih CA-ova moraju biti jednake procedurama i praksama Ovjerioca IDDEEA koje su definisane u ovoj Politici certifikacije. Ovjerioc IDDEEA definiše detaljnije uslove zavisno od slučaja do slučaja.

3.3 Identifikacija i autentikacija zahtjeva za obnavljanje ključeva

3.3.1 Identifikacija i autentikacija prilikom rutinske obnove ključeva

Rutinska obnova ključeva vrši se onda kada istekne rok važenja certifikata ili privatnog ključa.

Identitet korisnika u ponovnom izdavanju certifikata se provjerava:

- u RA Ovjerioca IDDEEA,
- na osnovu već izdatog validnog digitalnog certifikata koji je izdao TSP, gdje Ovjerioc IDDEEA provjerava podatke o fizičkom licu u relevantnim registrima.

3.3.2 Identifikacija i autentikacija prilikom obnove ključa nakon opoziva

Autentikacija korisnika koji podnose zahtjev za obnovu ključeva obavljena je kako je navedeno u odjeljku 3.2.2 Autentikacija identiteta pojedinca.

3.4 Identifikacija i autentikacija prilikom podnošenja zahtjeva za opoziv

Zahtjev za opoziv certifikata podnosi korisnik:

- lično u RA, gdje ovlaštena lica verifikuju identitet podnosioca zahtjeva,
- elektronskim putem, ali zahtjev za opoziv mora biti digitalno potpisan sa kvalifikovanim certifikatom, čime se pokazuje identitet podnosioca zahtjeva.

Ako vlasnik potvrde preko telefona ili elektronske pošte zahtjeva poništenje potvrde, ponuđač usluge povjerenja Ovjerilac IDDEEA odredi suspenziju potvrde. Tek na osnovu pismenog zahtjeva za poništenje potvrde se stvarno izvede prekid potvrde.

Detaljna procedura za opoziv: odjeljak 4.9.3.

4 OPERATIVNI ZAHTJEVI U VEZI ŽIVOTNOG CIKLUSA CERTIFIKATA

4.1 Zahtjev za dobijanje certifikata

4.1.1 Ko može predati zahtjev za dobijanje certifikata

Certifikacioni zahtjev za javni certifikat može podnijeti svaka osoba (fizičko lice) koja ispunjava uslove navedene u Zahtjevu za registraciju digitalnog certifikata, Politici certifikacije Ovjerioca IDDEEA i pratećim ugovorima između TSP-a i krajnjeg korisnika.

Budući predmet certifikata su fizička lica.

Za dobijanje certifikata, moraju biti ispunjeni sljedeći uslovi:

- popunjen i lično dostavljen obrazac prijave za certifikat i ugovor u RA,
- identifikacijski uslovi,
- važeća lična karta državljana BiH ili postupak izdavanja/zamjene lične karte državljana BiH u slučaju podnošenja zahtjeva za kvalifikovani elektronski potpis na ličnoj karti.

Zahtjev za izdavanje i korištenje certifikata sadrži i podatke o adresi prebivališta, e mail adresi i/ili kontakt broju telefona na osnovu kojih Ovjerilac IDDEEA može da stupi u kontakt s korisnikom certifikata.

4.1.2 Proces dostavljanja zahtjeva za registraciju certifikata i odgovornosti

Certifikat se izdaje na temelju valjano ispunjenog i potpisanog obrasca prijave za certifikat od strane budućeg korisnika certifikata (fizičko lice). Fizičko lice podnosi obrazac prijave za certifikat RA-u Ovjerioca IDDEEA. Obrazac prijave za certifikat se može dobiti u RA-u Ovjerioca IDDEEA i na web stranici Ovjerioca IDDEEA.

Budući korisnik certifikata podnosi obrazac prijave za certifikat u pisanom obliku.

Prije izdavanja obrasca prijave za certifikat, Ovjerilac IDDEEA obavještava budućeg korisnika o pravilima, CPS-u i o poslovanju Ovjerioca IDDEEA.

Ovjerilac IDDEEA izdaje certifikate samo nakon potvrde identiteta korisnika i uspješnog završetka procesa registracije. Glavni koraci procesa upisa certifikata su:

- Korisnik predaje potpisan zahtjev za registraciju digitalnog certifikata i prilaže važeći identifikacioni dokument.
- Korisnik je saglasan sa Politikom certifikacije Ovjerioca IDDEEA i svojim obavezama po potpisivanju Ugovora sa krajnjim korisnikom.

Zahtjev za registraciju digitalnog certifikata odobrava registraciono tijelo Ovjerioca IDDEEA.

Registraciono tijelo podnosi zahtjev za registraciju digitalnog certifikata putem odgovarajuće aplikacije za registraciju ili direktno u operativnom tijelu Ovjerioca IDDEEA.

Operativno tijelo Ovjerioca IDDEEA kreira korisnika sa odgovarajućim profilom certifikata i generiše aktivacione kodove koji se sastoje od registracionog broja i autorizacionog koda. Ako se zahtjev šalje putem aplikacije, generisanje koda je automatsko ili ručno.

Oba aktivaciona koda se uručuju krajnjem korisniku kada certifikate priprema Ovjerilac IDDEEA na smart kartici/tokenu.

Ukoliko ključeve i sertifikate pripremi TSP na smart kartici/tokenu, PIN se može dostaviti na sljedeće načine:

- putem e-pošte i/ili SMS-om;
- preuzima ih lično korisnik u RA
- ili se šalje na registrovanu adresu putem pošte.

Aktivacioni i registracioni kodovi za kvalifikovane certifikate dostavljaju se nosiocu certifikata na jedan od sljedećih načina:

- Lično u RA
- Registracioni broj se šalje korisniku na e-mail adresu koja je navedena u zahtjevu za registraciju digitalnog certifikata,
- Registracioni broj se šalje na broj telefona naveden u obrascu zahtjeva za registraciju digitalnog certifikata putem SMS-a,

Korisnik upotrebljava aktivacioni kod korištenjem korisničke aplikacije (web ili klijentska aplikacija) koju je obezbijedio Ovjerilac IDDEEA. Spisak podržanih aplikacija objavljen je zajedno sa korisničkim uputstvom na web-sajtu Ovjerioca IDDEEA koji je naveden u odjeljku 2.1 Repozitoriji.

4.2 Obrada zahtjeva za dobivanje certifikata

4.2.1 Obavljanje funkcija identifikacije i potvrde autentičnosti

Ovlašteno lice iz RA potvrđuje identitet korisnika koji ima važeći identifikacijski dokument (lična karta ili pasoš) sa slikom prilikom posjete RA-u.

Ovlaštena lica moraju obavezno provjeriti identitet budućeg korisnika ili svih podataka koji se navode na obrascu prijave za certifikat i koji su dostupni u zvaničnoj evidenciji ili drugim službenih važećim dokumentima.

RA provjerava popunjene obrasce prijave za certifikate i preuzimaju originalnu dokumentaciju koju na siguran način prenosu operativnom tijelu Ovjerioca IDDEEA.

Ovjerilac IDDEEA obavlja funkcije identifikacije i autentikacije na način definisan u odjeljku 3.2.2 Autentikacija identiteta pojedinca.

4.2.2 Odobravanje ili odbijanje zahtjeva za certifikat

Zahtjev za registraciju odnosno dobijanje certifikata kod Ovjerioca IDDEEA biće odobren samo ukoliko su ispunjeni svi navedeni uslovi:

- Uspješno završena registracija za izdavanje digitalnog certifikata uz uspješnu identifikaciju i autentikaciju u skladu sa odjeljkom 3.2;
- Dostavljena identifikaciona dokumentacija je uspješno verifikovana;
- Korisnik je potpisao odgovarajući ugovor sa Ovjeriocem IDDEEA.

U slučaju da bilo koji od navedenih kriterija nije ispunjen, ili postoji osnovana sumnja da podnosilac zahtjeva krši odredbe ovog dokumenta, Ugovora sa krajnjim korisnikom ili važećeg zakonodavstva, službenik za registraciju Ovjerioca IDDEEA odbija zahtjev za certifikaciju. IDDEEA zadržava pravo da odbije bilo koji zahtjev za certifikaciju bez navođenja razloga za odbijanje.

4.2.3 Vrijeme potrebno za obradu zahtjeva za certifikaciju

Obrazac zahtjeva za certifikaciju i identifikacioni dokument se provjeravaju i obrađuju u prisustvu podnosioca zahtjeva u prostorijama registracionog tijela Ovjerioca IDDEEA.

Podneseni zahtjev se dalje obrađuje u roku od 30 dana u slučaju izdavanja digitalnog certifikata na ličnoj karti državljana Bosne i Hercegovine, a u slučaju izdavnja digitalnih certifikata za elektronski potpis za udaljeno potpisivanje u roku od najviše 10 dana.

4.3 Izdavanje certifikata

4.3.1 Aktivnosti TSP-a tokom izdavanja certifikata

Sistem za izdavanje certifikata Ovjerioca IDDEEA po prijemu zahtjeva za izdavanje certifikata:

- Provjerava valjanost unesenih podataka prilikom procesa registracije;
- Provjera valjanosti unesenih podataka se vrši automatski ili ručno
- Izdaje traženi certifikat, ukoliko je ispunjeno sve prethodno navedeno

Postupak i proces za izdavanje certifikata zavisi od vrste certifikata:

4.3.1.1 Digitalni kvalifikovani certifikati na ličnoj karti državljana Bosne i Hercegovine;

Proces izdavanja za certifikate i za dva para ključeva sastoji se od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebnim podsistemima:

- pred-predstavljanje QSCD-a (generisanje ključeva na kartici, postavljanje lozinke za osiguranje certifikata)
- dobijanje obrasca zahtjeva za izdavanje certifikata,
- pregled obrasca zahtjeva za izdavanje certifikata,
- priprema certifikata,
- kreiranje QSCD-a (izdavanje i pohranjivanje certifikata, ispis podataka o subjektu)
- distribucija certifikata i privatne lozinke (PIN koda) i obavještenja subjektu.

Digitalni certifikat za QSCD i PIN dostavlja se RA-u i preuzima je lično korisnik ili se šalju korisniku e-poštom i/ili SMS-om na registrovanu e-adresu i/ili registrovani broj telefona.

4.3.1.2 Kvalifikovani digitalni certifikati za elektronsko potpisivanje na daljinu

Proces izdavanja za certifikate i za jedan par ključeva se sastoji od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebnim podsistemima:

- pregled obrasca zahtjeva za izdavanje certifikata,
- priprema certifikata, registracije i aktivacijskog koda,
- slanje registracije i aktivacijskog koda i obavještenja korisniku,
- generisanje ključeva na sigurnoj pohrani i izdavanje certifikata.

Registracijski kod se korisniku šalje putem dva odvojena kanala, jedan putem e-pošte, a drugi putem drugog sigurnog kanala (siguran web portal kojem se može pristupiti kvalifikovanim certifikatom, preporučenom poštom ili putem posebne web stranice na kojoj se imaoc identificira posebnim kodom primljenim putem SMS-a i drugim podacima koji su mu poznati (npr. Jedinstveni matični broj korisnika, broj važeće lične karte ili slično)). Iznimno, jedan od gore navedenih kodova može korisniku predati i ovlaštena osoba Ovjerioca IDDEEA RA lično.

Procedure su osmišljene na način da ih ne može provoditi samostalno jedna osoba.

Ovjerilac IDDEEA može ovlastiti provjerene vanjske izvođače za određene poslove (npr. ispis podataka o vlasniku, printanje PIN-a, isporuku itd.) na temelju pisanog ugovora, što redovito prati i za koje je odgovoran kao da obavlja same zadatke.

4.3.2 Obavještavanje korisnika o izdavanju certifikata

Aplikacija Ovjerioca IDDEEA će odmah uručiti certifikat podnosiocu zahtjeva, tako da nema potrebe za dodatnim obavještavanjem.

Za certifikate koji se izdaju putem smart kartice/tokena, ključ i certifikate priprema TSP na smart kartici/tokenu, korisnik se obavještava tokom procesa dostavljanja.

4.4 Prihvatanje certifikata

4.4.1 Postupak kojim se prihvata certifikat

Postupak prihvatanja certifikata zavisi od vrste certifikata:

U slučaju digitalnog kvalifikovanog certifikata na ličnoj karti državljana Bosne i Hercegovine, prihvatanje certifikata se ne primjenjuje jer budući korisnik prima certifikat putem QSCD-a, a PIN se dostavlja se RA-u i preuzima ga lično korisnik ili se šalju korisniku e-poštom i/ili SMS-om na registrovanu e-adresu i/ili registrovani broj telefona. Vidi odjeljak 4.3.1.

Za certifikate koji se ne izdaju na smart kartici/tokenu nosilac certifikata dobija pristup platformi za udaljeno elektronsko potpisivanje kroz odgovarajuću web aplikaciju Ovjerioca, na način da nakon uspješno završenog online procesa registracije (koristeći dobijeni registracijski broj podnošenjem zahtjeva u RA tijelu) aktiviraju vlastiti certifikat za udaljeno elektronsko potpisivanje.

U slučaju kvalifikovanih digitalnih certifikata za elektronsko potpisivanje na daljinu nije obavezno da certifikat bude prihvaćen, nego samo aktiviran budući da ga povjerenik Ovjerioca IDDEEA sigurno pohranjuje prema ovlaštenju korisnika. Korisniku se dostavljaju samo kodovi za pristup sigurnom certifikatu, vidi odjeljak 4.3.1.

Uputstvo za zanavaljnje certifikata može se pronaći na web-sajtu Ovjerioca IDDEEA https://www.iddeea.gov.ba.

Uputstvo za korištenje kvalifikovanog certifikata za elektronsko potpisivanje na daljinu biće dostavljeno korisniku putem e-pošte u postupku registracije. Sama uputstva su podložna promjenama u skladu sa aktuelnim promjenama u okviru PKI i nisu sastavni dio ove Politike.

Korisnik certifikata mora odmah po primitku certifikata provjeriti podatke u certifikatu i odmah obavijestiti Ovjerioca IDDEEA u slučaju potencijalnih grešaka ili problema.

4.4.2 Obavještavanje drugih lica o izdavanju certifikata koje izdaje TSP

Ovjerilac IDDEEA ne obavještava treće strane o izdavanju pojedinačnih certifikata. RA može doći u posjed informacija u vezi izdatih certifikata za koje je prihvaćen obrazac prijave za izdavanje certifikata.

4.5 Korištenje para ključeva i certifikata

4.5.1 Korištenje korisničkog privatnog ključa i Certifikata

Korisnik ili budući korisnik certifikata imaju obavezu:

- upoznavanja i djelovanja u skladu sa pravilima prije izdavanja certifikata,
- poštovanja pravila i ostalih važećih odredbi,
- da provjere informacije na certifikatu nakon primanja certifikata ili aktivacije certifikata i u slučaju postojanja potencijalnih grešaka ili problem o tome odmah obavijeste Ovjerioca IDDEEA ili zatraže opoziv certifikata
- praćenja i poštovanja svih obavještenja koja izda Ovjerioc IDDEEA,
- da u skladu sa obavještenjima ažuriraju potrebni softver radi osiguranja sigurnog rada sa certifikatima,
- odmah obavijestiti Ovjerioca IDDEEA o svim promjenama koje su vezane za certifikate,
- zatražiti opoziv certifikata u slučaju kompromitovanog privatnog ključa što može utjecati na pouzdanost korištenja, ili u slučaju rizika od zloupotrebe,
- zatražiti opoziv certifikata u slučaju gubitka ili krađe mobilnog uređaja, kredencijala, ili u slučaju rizika od zloupotrebe,

Koristiti certifikat u svrhu koja se navodi u certifikatu (vidi odjeljak 7.1) i na način određen pravilima Ovjerioca IDDEEA.

Korisnik ili budući korisnik certifikata također ima sljedeće obaveze, u smislu zaštite privatnog ključa:

- pažljivo štititi podatke za upis ili aktivaciju certifikata od neovlaštenih lica,
- čuvati privatni ključ i certifikat na način i na uređajima za sigurnu pohranu privatnih ključeva u skladu sa obavještenjima i preporukama Ovjerioca IDDEEA,
- čuvati privatni ključ i sve ostale povjerljive informacije pod prikladnim šiframa u skladu sa preporukama Ovjerioca IDDEEA ili osigurati zaštitu pod kojom je pristup dat samo korisniku,
- pažljivo čuvati šifre za zaštitu ili pristup privatnom ključu,
- poduzeti korake u skladu sa obavještenjima Ovjerioca IDDEEA nakon isteka ili opoziva certifikata.

Ovjerilac IDDEEA izdaje certifikate koji podržavaju nekoliko korištenja ključa. Ta podrška je obezbijeđena uključivanjem odgovarajućih ekstenzija za korištenje ključa.

Korisnici će koristiti certifikate u skladu s ekstenzijama certifikata keyUsage i extKeyUsage X.509 i u svrhe definisane u odjeljku 1.4.1. Odgovarajuća upotreba certifikata. Po isteku važenja certifikata ili opozivu certifikata, prateći privatni ključ se više ne može koristiti.

4.5.2 Korištenje javnog ključa i certifikata treće strane

Treća strana će ograničiti korištenje javnih ključeva koji se nalaze u potvrdama koje je izdala Ovjerilac IDDEEA za odgovarajuću upotrebu kako je navedeno u dijelu 1.4.1 Prihvatljivo korištenje certifikata. Treća strana je odgovorna i da:

- obezbijedi da certifikat ne bude opozvan elektronskim pristupom bilo kojem i svim važećim Spiskovima opozvanih certifikata (CRL spisak) ili Protokolu OCSP.
- odmah obavijesti TSP o svakoj sumnji ili poznatoj zloupotrebi bilo kog certifikata koji je TSP izdao.
- bude svjesna ograničenja certifikata i odgovornosti TSP-a kao što je detaljno navedeno u ovoj Politici.

Treća strana koja se oslanja na certifikat mora:

- rukovati sa i koristiti certifikate u skladu sa pravilima i ostalim važećim odredbama,
- pažljivo ispitati sve rizike i odgovornosti koji se odnose na korištenje certifikata i utvrditi pravila za korištenje,
- informisati Ovjerioca IDDEEA u slučaju da otkriju da su privatni ključevi korisnika certifikata kompromitovani na način koji može utjecati na pouzdanost korištenja ili u slučaju postojanja rizika od zloupotrebe, ili ako su podaci koji se navode u certifikatu promijenjeni,
- koristiti certifikat samo za svrhe koje se navode u certifikatu (vidi odjeljak 6.1.1) i na način koji je utvrđen pravilima,
- tokom certifikata osigurati da se certifikat ne nalazi u registru opozvanih certifikata,
- tokom korištenja certifikata potvrditi da je digitalni potpis kreiran tokom perioda validnosti i u skladu sa prikladnom svrhom certifikata,
- tokom korištenja certifikata potvrditi potpis Ovjerioca IDDEEA, koji je objavljen u ovom dokumentu CPS kao i na web stranici Ovjerioca IDDEEA.
- poštovati ostale propise u slučaju potpisivanja dodatnih ugovora o korištenju certifikata sa Ovjeriocem IDDEEA.

Za provjeru validnosti potpisa/pečata ili drugih kriptografskih operacija, treća strana mora koristiti softver i hardver kojima se mogu na siguran način provjeriti gore navedeni zahtjevi za sigurno korištenje certifikata.

4.6 Obnavljanje certifikata (bez generisanja novog ključa)

Obnavljanje certifikata je proces u kojem TSP izdaje novi certifikat za istog korisnika. Ovjerilac IDDEEA ne dozvoljava niti obezbjeđuje obnavljanje certifikata.

4.6.1 Uslovi za obnavljanje certifikata

Nije primjenjivo, kao što je navedeno u odjeljku 4.6. Obnavljanje certifikata (bez generisanja novog ključa).

4.6.2 Ko može tražiti obnavljanje zahtjeva

Nije primjenjivo, kao što je navedeno u odjeljku 4.6. Obnavljanje certifikata (bez generisanja novog ključa).

4.6.3 Obrada zahtjeva za obnavljanje certifikacionog ključa

Nije primjenjivo, kao što je navedeno u odjeljku 4.6. Obnavljanje certifikata (bez generisanja novog ključa).

4.6.4 Obavještavanje korisnika o novom izdavanju certifikata

Nije primjenjivo, kao što je navedeno u odjeljku 4.6. Obnavljanje certifikata (bez generisanja novog ključa).

4.6.5 Postupak koji predstavlja prihvatanje certifikata sa obnovljenim ključem

Nije primjenjivo, kao što je navedeno u odjeljku 4.6. Obnavljanje certifikata (bez generisanja novog ključa).

4.6.6 Objavljivanje obnovljenog certifikata koje obavlja TSP

Nije primjenjivo, kao što je navedeno u odjeljku 4.6. Obnavljanje certifikata (bez generisanja novog ključa).

4.6.7 Obavještavanje drugih lica o izdavanju certifikata koje obavlja TSP

Nije primjenjivo, kao što je navedeno u odjeljku 4.6. Obnavljanje certifikata (bez generisanja novog ključa).

4.7 Obnavljanje certifikata generisanjem novog ključa (obnavljanje generisanjem novog para ključeva)

Obnavljanje certifikata generisanjem novog ključa je proces u kome TSP izdaje korisniku novi certifikat. Novi certifikat sadrži iste informacije o korisniku kao i stari certifikat i nove javne ključeve.

4.7.1 Uslovi za obnovu certifikata generisanjem novog ključa

Obnavljanje ključa certifikata obavlja se:

- po opozivu certifikata;
- po isteku roka važenja ili neposredno prije isteka roka važenja.

4.7.2 Ko može tražiti certifikaciju sa novim javnim ključem

Korisnik, nosilac certifikata koji je tražio prvobitno izdavanje certifikata može tražiti obnavljanje certifikata generisanjem novog ključa.

4.7.3 Obrada zahtjeva za obnavljanje certifikata generisanjem novog ključa

Obnavljanje certifikata generisanjem novog ključa vrši se:

- na isti način kao i prvobitno izdavanje certifikata,
- u slučaju da je lična karta korisnika važeća poslije isteka certifikata, neposredno pred istek certifikata Ovjerilac IDDEEA može omogućiti korisniku da obnovi certifikat generisanjem novog para ključeva nakon eletronskog potpisivanja novog zahtjeva, korištenjem klijentske ili web aplikacije.

4.7.4 Obavještavanje korisnika o izdavanju novog certifikata

Kao što je navedeno u odjeljku 4.3.2 Obavještavanje korisnika o izdavanju certifikata koje obavlja TSP.

4.7.5 Postupak prihvatanja certifikata sa novim ključem

Kao što je navedeno u odjeljku 4.4.1 Postupak prihvatanja certifikata.

4.7.6 Objavljivanje certifikata sa novim ključem koje obavlja TSP

Kao što je navedeno u odjeljku 4.4.2 Objavljivanje certifikata koje obavlja TSP.

4.7.7 Obavještavanje drugih lica o izdavanju certifikata koje obavlja TSP

Kao što je navedeno u odjeljku 4.4.3 Obavještavanje drugih lica o izdavanju certifikata koje obavlja TSP.

4.8. Izmjena certifikata

Izmjena certifikata je procedura koja korisnicima olakšava podnošenje zahtjeva za izdavanje certifikata sa izmijenjenim podacima. Izmjena certifikata podrazumijeva obnavljanje ključeva certifikata i obrađuje se kao i prvobitni zahtjev.

4.8.1 Uslovi za izmjene certifikata

Korisnik može tražiti izmjene u certifikatu ukoliko se informacije o korisniku, kao što su ime ili e-adresa promijene.

4.8.2 Ko može tražiti izmjene certifikata

Izmjenu certifikata može tražiti korisnik koji je tražio prvobitno izdavanje certifikata.

4.8.3 Obrada zahtjeva za izmjenu certifikata

Zahtjevi za izmjenu certifikata obrađuju se na isti način kao i prvobitni zahtjevi za izdavanje certifikata.

4.8.4 Obavještavanje korisnika o izdavanju novog certifikata

Kao što je navedeno u odjeljku 4.3.2 Obavještavanje korisnika o izdavanju certifikata koje obavlja TSP.

4.8.5 Postupak prihvatanja izmijenjenog certifikata

Kao što je navedeno u odjeljku 4.4.1. Postupak prihvatanja certifikata. Objavljivanje izmijenjenog certifikata obavlja Ovjerilac IDDEEA.

4.8.6 Objavljivanje izmijenjenog certifikata koje obavlja TSP

Kao što je navedeno u odjeljku 4.4.2. Objavljivanje certifikata koje obavlja TSP.

4.8.7 Obavještavanje drugih lica o izdavanju certifikata koje obavlja TSP

Kao što je navedeno u odjeljku 4.4.3. Obavještavanje drugih lica o izdavanju certifikata koje obavlja TSP.

4.9 Opoziv i suspenzija certifikata

4.9.1 Uslovi za opoziv

Opoziv certifikata se može tražiti:

- ako to zahtijeva korisnik ili nosilac certifikata;
- ako TSP potvrdi da je nosilac certifikata preminuo ili je izgubio sposobnost za poslovanje ili ako su se okolnosti koje su u značajnoj mjeri uticale na validnost certifikata promijenile;
- ukoliko je poznato ili se sumnja da je netačna bilo koja informacija koja se nalazi u certifikatu;
- ukoliko je privatni ključ koji je povezan sa certifikatom kompromitovan ili se sumnja da je kompromitovan;
- kada je bilo koji aktivacioni podatak, kao što su lozinka ili PIN koji se koriste za zaštitu privatnog ključa, kompromitovan ili se sumnja da je kompromitovan;
- ukoliko TSP utvrdi da certifikat nije propisno izdat u skladu sa Politikom certifikacije Ovjerioca IDDEEA;
- kada korisnik ili nosilac certifikata prekrši odredbe Politike certifikacije Ovjerioca IDDEEA ili važeći zakon (neispunjavanje obaveza korisnika);
- iz bilo kog drugog razloga navedenog u Zakonu o elektronskiom potpisu;
- ako Tijelo za upravljanje politikom Ovjerioca IDDEEA smatra da je to neophodno.

4.9.2 Ko može tražiti opoziv

Opoziv certifikata može tražiti:

- ovlašteno lice Ovjerioca IDDEEA,
- korisnik,
- nadležni sud, organ za prekršaje ili upravna jedinica.

4.9.3 Procedura za podnošenje zahtjeva za opoziv

Nosilac certifikata može tražiti opoziv certifikata na sljedeći način:

- lično tokom radnog vremena u RA,
- elektronskim putem dvadeset i četiri (24) sata dnevno, u svim danima u godini, u slučaju mogućnosti zloupotrebe ili nepouzdanosti certifikata, a inače u službenom radnom vremenu državnih organa.

Ako se zahtjev za opoziv podnosi:

- Lično, potrebno je popuniti odgovarajući zahtjev za opoziv certifikata i dostaviti ga RA;
- elektronski, korisnik mora poslati elektronsku poruku Ovjeriocu IDDEEA sa zahtjevom za opoziv, koji mora biti digitalno potpisan sa pouzdanim certifikatom u svrhu njegove validacije.
- ako je korisnik zatražio opoziv certifikata putem telefona, e-maila ili faksa, Ovjerilac IDDEEA će obustaviti certifikat. Na osnovu pisanog zahtjeva za opoziv certifikata, izvršit će se stvarni opoziv certifikata.

Korisnik uvijek mora biti obaviješten o datumu, vremenu i razlozima opoziva.

Sudovi, organi za prekršaje i upravne jedinice, koji mogu tražiti opoziv, to čine u skladu sa zakonima i službenim postupcima (krivični postupak, parnični postupak, opšti upravni postupak i drugi).

Odredbe koje se odnose na opoziv se razumno primjenjuju na postupke koji se odnose na regenerisanje pristupnih kodova za kvalifikovane certifikate i kodove za registraciju i aktivaciju elektronskih certifikata za sigurni potpis putem udaljenog pristupa.

Zahtjev za opoziv certifikata naveden je u odjeljku 3.4 Identifikacija i autentikacija zahtjeva za opoziv.

Opoziv zbog izmjene podataka u samom certifikatu

1. Zahtjev za opoziv:

Korisnik šalje zahtjev registracionom tijelu Ovjerioca IDDEEA lično ili putem e-pošte. Važećim zahtjevom se smatra onaj zahtjev koji je potpisan pomoću ključa koji je izdao Ovjerilac IDDEEA.

Korisnik se identifikuje (lično) i podnosi zahtjev (obrazac) za opoziv certifikata.

Registraciono tijelo Ovjerioca IDDEEA provjerava i odobrava opoziv.

2. Registraciono tijelo Ovjerioca IDDEEA pokreće opoziv certifikata kroz aplikaciju, navodeći razloge za opoziv ili šalje zahtjev za opoziv operativnom tijelu Ovjerioca IDDEEA da izvrši opoziv navodeći i razloge opoziva.

3. Za izdavanje novih ključeva, korisnici se autentikuju kako je navedeno u odjeljku 3.2.2. Autentikacija identiteta.

Opoziv zbog kompromitovanog privatnog ključa

1. Zahtjev za opoziv:

Korisnik šalje zahtjev registracionom tijelu Ovjerioca IDDEEA putem e-pošte ili lično.

Telefonskim pozivom, kada osoba mora znati tajnu riječ/lozinku/PIN koji je unesen u obrazac zahtjeva za registraciju digitalnog certifikata.

Korisnik se identifikuje (lično) i podnosi zahtjev (obrazac) za opoziv certifikata.

Registraciono tijelo Ovjerioca IDDEEA provjerava i odobrava opoziv.

2. Registraciono tijelo Ovjerioca IDDEEA pokreće opoziv certifikata kroz aplikaciju tako što uoči kompromitujući status ili šalje zahtjev za opoziv operativnom tijelu Ovjerioca IDDEEA da izvrši opoziv uočavajući kompromitujući status.

3. U slučaju zahtjeva za izdavanje novih ključeva, autentikacija korisnika se obavlja kao što je navedeno u odjeljku 3.2.2 Autentikacija identiteta pojedinca.

Opoziv certifikata zbog neispunjavanja obaveza korisnika

Ukoliko korisnik ne ispuni svoje obaveze i dužnosti u skladu sa ovom politikom i ugovorom zaključenim sa IDDEEA-om njen/njegov certifikat će biti opozvan, pri čemu:

- RA provjerava status digitalnog potpisa korisnika kod TSP-a;
- Zaposleni u operativnom tijelu Ovjerioca IDDEEA vrše opoziv certifikata navodeći razloge za to.

4.9.4 Odloženi opoziv certifikata

Korisnik koji je saznao za okolnosti koje zahtijevaju opoziv certifikata dužan je da zatraži opoziv u najkraćem mogućem roku, bez nepotrebnog odlaganja.

Ovjerilac IDDEEA može izvršiti opoziv certifikata zbog nepoštovanja obaveza korisnika odmah nakon isteka roka u kojem je korisnik trebao da ispuni svoje obaveze.

4.9.5 Rok u kojem Ovjerilac IDDEEA mora završiti obradu zahtjeva za opoziv

Ovjerilac IDDEEA nakon prihvatanja valjanog zahtjeva za opoziv:

- najkasnije u roku od četiri (4) sata, opoziva certifikat ako je opoziv podnesen zbog rizika od zloupotrebe ili nepouzdanosti itd.,
- u suprotnom, opoziva ga prvog radnog dana nakon prijema zahtjeva za opoziv,

Nakon opoziva, takav certifikat se odmah (u roku od najviše 5 sekundi) dodaje u registar opozvanih certifikata.

U drugim slučajevima opoziva certifikata, rok za opoziv certifikata ne bi trebalo da bude duži od 24 sata od prijema zahtjeva.

4.9.6 Zahtjev za provjeru opoziva za treće strane

Treće strane provjeravaju CRL spisak Ovjerioca IDDEEA ili Protokol OCSP prije korištenja svakog certifikata koji je izdao Ovjerioc IDDEEA. Ukoliko se ne može izvršiti valjana provjera opoziva, zbog kvara sistema ili gubitka servisa, ne treba prihvatiti nijedan certifikat Ovjerioca IDDEEA.

Treća strana provjerava odgovor sa CRL spiska ili Protokola OCSP tako što provjerava svoj elektronski potpis sa povezanim TSP certifikatom i da li je istekao.

4.9.7 Učestalost objavljivanja spiska opozvanih certifikata (ako je primjenjivo)

Ovjerioc IDDEEA redovno svakih 24 sata objavljuje novi spisak opozvanih certifikata. Rok važenja spiska opozvanih certifikata je do 48 sati. Ovjerioc IDDEEA ažurira spiskove opozvanih certifikata odmah ili čim je to moguće nakon što se obradi važeći zahtjev za opoziv certifikata. Maksimalan vremenski period između konačnog potvrđivanja opoziva certifikata, ili njegove suspenzije, do stvarne izmjene informacije o statusu certifikata koja je dostupna trećim stranama može biti do 60 minuta.

4.9.8 Maksimalno kašnjenje spiska opozvanih certifikata (ako je primjenjivo)

Nije određeno. (Pogledati odjeljak 4.9.7)

4.9.9 Dostupnost elektronskog opoziva/provjere statusa

TSP pruža OCSP uslugu. Lokacija usluge je naznačena ekstenzijom authorityInfoAccess koja se nalazi na svakom certifikatu.

4.9.10 Uslovi za elektronsku provjeru opoziva

Korisnici i treće strane su obavezni provjeravati status elektronskih certifikata na osnovu dotupnog registra opozvanih certifikata Ovjerioca IDDEEA.

4.9.11 Ostali načini oglašavanja opoziva

Nije primjenjivo.

4.9.12 Posebni uslovi vezani za kompromitovanje ključa

Nikakvi posebni uslovi se ne traže u slučaju kompromitovanja ključa nosioca certifikata.

4.9.13 Suspenzija certifikata

Ako korisnik certifikata traži opoziv putem telefona ili elektronskim putem, potvrda se privremeno obustavlja do prijema originalnog pisanog zahtjeva.

Ako korisnik certifikata, treće lice ili drugo lice, sud, organ za prekršaje, upravna jedinica, srodne vlasti ili sam TSP izraze sumnju da je certifikat u suprotnosti sa politikom ili važećim propisima, certifikat će biti privremeno suspendovan do konačne odluke.

Suspenzija certifikata se može tražiti u slučaju da nosilac certifikata izostaje duži vremenski period, npr. porodiljsko odsustvo. Ovjerioc IDDEEA može suspendovati certifikat nosioca certifikata za vrijeme obrade zahtjeva za opoziv certifikata.

Suspendovani certifikati se objavljuju na Spisku opozvanih certifikata (CRL) za vrijeme suspenzije.

4.9.14 Ko može tražiti suspenziju

Vidi odjeljak 4.9.13.

4.9.15 Procedura za podnošenje zahtjeva za suspenziju

Kao što je opisano u odjeljku 4.9.3 Procedure za podnošenje zahtjeva za suspenziju.

4.9.16 Ograničenje perioda suspenzije

Period suspenzije nije ograničen.

4.10 Servisi provjere statusa certifikata

4.10.1 Operativne karakteristike

Status certifikata se objavljuje korištenjem X.509 Spiska opozvanih certifikata (CRL) putem OCSP protokola.

CRL spisak se objavljuje kroz LDAP direktorij i web-sajt. Tačne lokacije (LDAP i http URLs) se objavljuju korištenjem ekstenzije X.509 CRL Distribution Points.

Dostupnost OCSP usluge je naznačena kao URL u certifikatu.

CRL profil i servisni protokol OCSP opisani su u odjeljcima 7.2. i 7.3.

4.10.2 Dostupnost usluga

Status certifikata Ovjerioca IDDEEA dostupan je 24 sata dnevno, 7 dana u sedmici, sa maksimalnim godišnjim neplaniranim zastojima od sedam (7) dana godišnje.

4.10.3 Opcione karakteristike

Nije primjenjivo.

4.11 Prestanak važenja certifikata

Certifikat prestaje da važi po isteku roka važenja ili nakon opoziva certifikata. Ovjerilac IDDEEA čuva dokumentaciju i podatke iz certifikata najmanje deset (10) godina po isteku ili opozivu certifikata.

4.12 Deponovanje i oporavak ključeva

Ovjerilac IDDEEA ne podržava deponovanje i oporavak ključeva.

4.12.1 Politika i praksa deponovanja i oporavka ključeva

Nije primjenjivo.

4.12.2 Politika i praksa enkapsulacije i oporavka sesijskog ključa

Nije primjenjivo.

5. UPRAVNE, OPERATIVNE I FIZIČKE BEZBJEDNOSNE KONTROLE

5.1 Fizičke kontrole

5.1.1 Lokacija objekta i konstrukcija

Tehnička sredstva Ovjerioca IDDEEA (mrežni računarski sistemi, terminali za nosioce i IT resursi) se nalaze u namjenskim prostorijama sa stalnim nadzorom u bezbjednoj zgradi (objektu).

Sistemske komponente i rad operativni dio Ovjerioca IDDEEA se nalaze unutar fizički zaštićenog okruženja kako bi se spriječila neovlaštena upotreba, pristup ili otkrivanje osjetljivih informacija. Kontroe fizičke bezbjednosti se provode u skladu sa važećim najboljim praksama fizičke bezbjednosti.

Zaštitne mjere podrazumijevaju:

- Pristup je ograničen samo za zaposlene u Ovjeriocu IDDEEA;
- Svi ostali pristupi su pod pratnjom i svaki pristup se evidentira;
- Zaposleni na održavanju i servisu su pod video nadzorom tokom svojih posjeta;
- Sigurne elektronske brave i pristupni sistem;

Nadgledanje 24 sata,7 dana u nedelji i video nadzor iz centra za video nadzor u zgradi.

5.1.2 Fizički pristup

Samo ovlašteni zaposleni u Ovjeriocu IDDEEA, u skladu sa njihovim dužnostima, imaju pristup određenim dijelovima infrastrukture Ovjerioca IDDEEA. Svaki pristup prostorijama Ovjerioca IDDEEA se elektronski zavodi i unosi u elektronski dnevnik pristupa prostorijama.

5.1.3 Električno napajanje i klimatizacija

IT centar Ovjerioca IDDEEA je opremljen sa klimatizacijom koja reguliše toplotu, vlagu a sve kritične komponente su povezane na neprekidno električno napajanje (UPS).

5.1.4 Opasnost od poplave

Unutar prostorija Ovjerioca IDDEEA nema vodovodnih instalacija. Poduzete su sve tehničke mjere za zaštitu od vodovodnih instalacija u okruženju.

5.1.5 Prevencija i zaštita od požara

Prostorije Ovjerioca IDDEEA su zaštićene sistemom za rano otkrivanje požara, automatskim požarnim alarmom i sistemom za gašenje.

5.1.6 Čuvanje medija

Svi računarski mediji koji sadrže podatke Ovjerioca IDDEEA, uključujući medij sa sigurnosnom kopijom podataka, čuvaju se u vatrootpornim ormarima, od kojih se jedan nalazi unutar Ovjerioca IDDEEA, a drugi na udaljenoj bezbjednoj lokaciji.

5.1.7 Odlaganje otpada

Papirna dokumenta i elektronski mediji se uništavaju prije odlaganja na način koji osigurava da se informacije ne mogu reprodukovati. TSP zadržava sve hardverske komponente koje se ne mogu servisirati radi njihovog sigurnog odlaganja.

5.1.8 Rezervne kopije na drugoj lokaciji

Ovjerioc IDDEEA čuva medije podataka na udaljenoj bezbjednoj lokaciji. Mediji se čuvaju na udaljenoj bezbjednoj lokaciji zaštićenoj od vanjskih uticaja i sa kontrolisanim pristupom, koji ima visok nivo zaštite, odnosno princip bankarskog sefa. Pristup sefu je ograničen na dvije ovlaštene osobe.

5.2 Proceduralne kontrole

5.2.1 Povjerljive uloge

Zavisno od njihove uloge, zaposleni u Ovjeriocu IDDEEA mogu imati nalog na host računaru TSP-a, TSP aplikaciji ili na oboje.TSP aplikacija koju koristi Ovjerioc IDDEEA implementira određeni broj povjerljivih uloga koje su dodjeljene zaposlenima TSP-a u skladu sa njihovim nadležnostima. Korisničkim pravima naloga operativnog sistema na TSP host računaru se ograničava pristup zaposlenima Ovjerioca IDDEEA samo na ono što im je potrebno kako bi izvršavali svoje zadatke.

- Raspored TSP uloga je:

Odgovorni zaposlenici	Nivo pristupa u operativnom sistemu	Nivo pristupa u TSP aplikaciji
CA Glavni korisnik	Da	Da
CA Službenik za bezbjednost	Ne	Da
CA Administrator	Ne	Da
Administrator direktorija	Ne	Ne
Službenici za registraciju	Ne	Da
Službenici u registracionom tijelu	Ne	Ne
Pravni savjetnik	Ne	Ne

Različiti nivoi fizičke zaštite i kontrole pristupa sistemima na osnovu uloga u TSP aplikaciji i korisničkih prava u sistemu se koriste za razdvajanje dužnosti.

Povjerljive uloge su

Uloga	Dužnosti
CA Glavni korisnik	• Odobrava početnu TSP aplikaciju i konfiguraciju hardverskog bezbjednosnog modula (HSM) i njihovo održavanje • Pokreće i zaustavlja usluge TSP aplikacije • Određuje prve PKI službenike za bezbjednost • Obnavlja nalog PKI službenicima za bezbjednost kada zaborave šifru • Obnovlja TSP administrativne usluge u slučaju da se ošteti profil • Pokreće proces zamjene HSM-a • Obnovlja smart kartice operatora HSM-a • Obnovlja i ponovo šifra TSP bazu podataka
CA Službenik za bezbjednost	• Upravlja korisničkim nalozima drugih PKI službenika za bezbjednost i PKI administratora • Upravlja korisničkim nalozima • Upravalja oporavkom ključeva za korisnike • Obrađuje revizijske zapise • Postavlja i mijenja bezbjednosnu politiku TSP aplikacije • Upravlja profilima TSP aplikacijskih sertifikata • Vršiti unakrsno sertifikovanje sa vanjskim sertifikovanim tijelima • Priprema izvještaje
CA Administrator	• Upravlja korisničkim nalozima • Upravlja certifikatima • Priprema izvještaje

Administrator direktorija	• Dodaje i briše korisnike u direktoriju • Podešava imenik
Službenici za registraciju	• Pogledati odjeljak 1.3.2
Službenici u registracionom tijelu	• Pogledati odjeljak 1.3.2

5.2.2 Broj osoba koje se zahtjevaju po svakom zadatku

Dvije (2) osobe sa odgovarajućim povjerljivim ulogama su potrebne za izvršavanje sljedećih zadataka:

- Opozivanje TSP ključa
- Pripremanje politika ključa i sertifikacije
- Kreiranje korisničkih naloga sa ulogom CA službenika za bezbjednost ili CA administratora
- Ažuriranje privatnog ključa Ovjerioca IDDEEA
- Resetovanje šifre na nalozima CA glavnih korisnika
- Unakrsno certifikovanje sa vanjskim CA

Jedna osoba može izvršavati sve ostale zadatke. Sve aktivnosti koje izvršavaju nosioci povjerljivih TSP uloga se zapisuju i pregledaju.

5.2.3 Identifikacija i autentikacija za svaku ulogu

- Zaposleni u PKI sa povjerljivom PST ulogom podliježu bezbjednosnoj provjeri prije nego što budu imenovani da rade kao članovi operativnog tijela Ovjerioca IDDEEA.
- Operativno tijelo Ovjerioca IDDEEA će se provjeriti u skladu sa pravilima navedenim u ovoj Politici prije nego što im se dodijeli bilo koja od sljedećih privilegija:
- Dodavanje unosa na odgovarajuću pristupnu listu za ulazak u zaštićene prostorije Ovjerioca IDDEEA (bezbjednosna i operativna zona)
- Dobijanje potrebnog sertifikata za izvršavanje dodjeljene povjerljive uloge
- Dobijanje korisničkog naloga u operativnom sistemu
- Dobijanje smart kartice / tokena
- Korisnički nalozi operativnog sistema i aplikacije, kao i certifikati su kreirani pojedinačno za svaku odgovornu osobu .

Zabranjena je svakodnevna upotreba naloga ili certifikata među zaposlenima Ovjerioca IDDEEA. Zaposleni su ograničeni na aktivnosti ovlaštene za datu ulogu kroz kontrolu postavljenu aplikacijom, operativnim sistemom i procedurama Ovjerioca IDDEEA.

Zaposleni u Ovjeriocu IDDEEA koriste samo smart kartice/tokene kako bi ispunili dužnosti koje su im dodijeljene u okviru njihovih uloga.

5.2.4 Uloge koje zahtijevaju razdvajanje dužnosti

Administrator operativnog sistema ima potrebna prava da instalira, konfiguriše i održava hardver i softver TSP host računara.

Prilikom dodjele korisničkih uloga i prava fizičkog pristupa strogo se poštuje princip podjele dužnosti, tako da jedna osoba ne može koristiti kriptografske materijale za izvršavanje bezbjednosno osjetljivih operacija, ali je uvijek potrebno osigurati prisustvo najmanje dvije osobe.

5.3 Kadrovske kontrole

Odgovorne osobe u Ovjeriocu IDDEEA su zaposlene na neodređen period, angažovane na osnovu ugovora koji utvrđuje njihove radne obaveze. Oni trebaju biti adekvatno kvalifikovani za izvršavanje svojih radnih obaveza.

Zaposleni u Registracionom tijelu (RA) su zaposleni na neodređen period. Oni trebaju biti adekvatno kvalifikovani za izvršavanje svojih radnih obaveza.

Zaposleni u Ovjeriocu IDDEEA i RA su ugovorom vezani da ne objavljuju niti otkrivaju povjerljive informacije vezane za bezbjednost Ovjerioca IDDEEA ili informacije o korisnicima.

U skladu sa ugovorom, korisnici su upoznati sa bezbjednosnim odredbama koje trebaju primjenjivati kako bi zaštitili svoje računare i uređaje za enkripciju, kao i sa ovom politikom po kojoj su im izdati certifikati.

5.3.1 Kvalifikacije, iskustvo i sigurnosne provjere

Prakse zapošljavanja u Ovjerioca IDDEEA podrazumijevaju razmatranje kvalifikacijskih zahtjeva za svaku poziciju, prethodne dužnosti potencijalnih kandidata i broj godina iskustva na sličnim pozicijama.

5.3.2 Procedure provjere biografije

TSP prati provjere zaposlenih i politiku navedenu u odjeljku 6.1.2 Provjera zaposlenih i ISO/IEC 27001 zahtjevi.

5.3.3 Zahtjevi za obuke

Ovjerioc IDDEEA obezbjeđuje obuke za svoje zaposlene.

Za odgovorne osobe u Ovjeriocu IDDEEA, pod obukama se podrazumijevaju procedure za zaštitu sistema i podataka, specifične obuke za njihove uloge i dužnosti, obuke za korištenje aplikacije Ovjerioca IDDEEA i obuke za preuzimanje procedura za oporavak od katastrofa i procedura kontinuiranog poslovanja.

Za zaposlene u registracionom tijelu, pod obukama se podrazumijevaju procedure za zaštitu sistema i podataka i specifične obuke za njihove uloge i dužnosti.

5.3.4 Frekvencija i zahtjevi za ponovnu obuku

Obuke za zaposlene u Ovjeriocu IDDEEA se organizuju u skladu sa realnim potrebama i tehnološkim izmjenama.

5.3.5 Frekvencija i redoslijed rotacije poslova

Rotacija poslova se ne primjenjuje.

5.3.6 Kazne za neovlaštene radnje

U slučaju sumnje da je izvršena neovlaštena aktivnost ili je neovlaštenu aktivnost zaista izvršila osoba koja obavlja poslove vezane za rad Ovjerioca IDDEEA ili Registracionog tijela, Ovjerioc IDDEEA će mu onemogućiti dalji pristup tehničkim uređajima (hardver i softver).

Ovjerioca IDDEEA će oduzeti ili opozvati sve certifikate izdate toj osobi.

Neovlaštene aktivnosti se prijavljuju nadležnim državnim organima i institucijama, u skladu sa važećim zakonskim, podzakonskim i internim aktima.

5.3.7 Uslovi za spoljne saradnike

Ovjerioc IDDEEA nema praksu zapošljavanja spoljnih saradnika za osjetljive poslove. Ali ako su takvi saradnici angažovani, provode se odgovarajuće provjere. Svi izvršioci moraju potpisati ugovor o neotkrivanju podataka u skladu sa internim procedurama u Ovjeriocu IDDEEA.

5.3.8 Dokumentacija koja se dostavlja zaposlenima

Odgovorne osobe u Ovjeriocu IDDEEA imaju pristup TSP dokumentaciji, uključujući hardver, softver, priručnike za TSP aplikaciju, operativne procedure, bezbjednosne i protivpožarne procedure, procedure kontrole pristupa i ovu Politiku.

5.4 Procedure revizijskih zapisa (audit)

5.4.1 Tipovi zabilježenih događaja

Ovjerioc IDDEEA redovno provjerava i evidentira sve što značajno utječe na:

- sigurnost infrastrukture,
- rad svih sigurnosnih sistema i
- da li je došlo do upada ili pokušaja upada neovlaštenih lica u opremu ili podatke.

Detaljne informacije u vezi navedenog se utvrđuju u skladu sa Uredbom za interna pravila Ovjeriocu IDDEEA.

5.4.2 Frekvencija procesiranja zapisa

Ovjerioc IDDEEA na dnevnoj osnovi provodi sigurnosne provjere svoje infrastrukture i evidencije.

5.4.3 Period čuvanja revizijskih zapisa

U skladu sa važećim propisima, revizijski zapisi se čuvaju najmanje 10 godina. .

5.4.4 Zaštita revizijskih zapisa

Pristup glavnom (host) računarskom sistemu koji sadrži datoteke revizijskih zapisa dozvoljen je samo ovlaštenim licima, uz kombinaciju fizičkih kontrola i kontrola računarske bezbjednosti. Računarski sistem, rezervna kopija revizijskih zapisa i fizički revizijski zapisi čuvaju se u zoni visoke bezbjednosti kod Operativnog tijela Ovjerioca IDDEEA, koja je opremljena fizičkim kontrolama i kontrolama okruženja kako je definisano u odjeljku 5.1 Fizičke kontrole.

Unosi revizijskih zapisa koje generiše TSP host operativni sistem su pojedinačno vremenski označeni. Operativni sistem štiti integritet svojih datoteka revizijskih zapisa koristeći funkcionalnost operativnog sistema.

Unosi revizijskih zapisa koje generiše TSP aplikacija su pojedinačno vremenski označeni. TSP aplikacija štiti integritet svojih datoteka revizijskih zapisa korištenjem enkripcije javnog ključa i verifikacije svakog unosa pri preuzimanju.

5.4.5 Procedure rezervnih kopija (Backup) revizijskih zapisa

Rezervne kopije datoteka revizijskih zapisa se vrši svaki dan kao dio redovnog backup-a host sistema Ovjerioca IDDEEA.

Detalji se utvrđuju u internim pravilima Ovjerioca IDDEEA.

5.4.6 Sistem prikupljanja revizija (interne ili eksterne)

Sistem sakupljanja revizija Ovjerioca IDDEEA je kombinacija automatskih i manuelnih procesa koje izvodi TSP host operativni sistem, TSP aplikacija, i zaposleni u Ovjeriocu IDDEEA, kao što se navodi u tebeli:

Zapisani događaji	Sistem prikupljanja	Subjekt koji zapisuje
Pokretanje i gašenje TSP aplikacije	Automatsko	TSP host operativni sistem
Pokretanje i gašenje TSP host operativni sistem	Automatsko	TSP host operativni sistem

Zapisani događaji	Sistem prikupljanja	Subjekt koji zapisuje
Uspješni i neuspjeli pokušaji kreiranja, modifikacije, uklanjanja, onemogućavanja, omogućavanja i oporavka korisnika	Automatsko	TSP application
Uspješni i neuspjeli pokušaji kreiranja, modifikacije, uklanjanja, onemogućavanja, omogućavanja i oporavka naloga TSP host operativnog sistema	Automatsko	TSP host operativni sistem
Uspješni i neuspjeli pokušaji kreiranja, modifikacije, uklanjanja, onemogućavanja, omogućavanja i oporavka naloga TSP aplikacije	Automatsko	TSP aplikacija
Uspješni i neuspjeli pokušaji logovanja na TSP aplikaciju	Automatsko	TSP aplikacija
Uspješni i neuspjeli pokušaji logovanja na host računar	Automatsko	TSP host operativni sistem
Neovlašteni pokušaji pristupa sistemskim datotekama	Automatsko	TSP host operativni sistem
Neovlašteni pokušaji pristupa PKI mreži	Automatsko	Ruteri i TSP host operativni sistem
Uspješni i neuspjeli pokušaji generisanja, ažuriranja i oporavka ključeva	Automatsko	TSP aplikacija
Uspješni i neuspjeli pokušaji kreiranja, ažuriranja, obustave, opoziva i oporavka sertifikata	Automatsko	TSP aplikacija
Promjene politika kreiranja sertifikata (npr. period važenja)	Automatsko	TSP aplikacija
Uspješni i neuspjeli pokušaji TSP-a da se poveže, pročita i upiše u direktorij	Automatsko	TSP aplikacija
Značajne promjene imena	Automatsko	TSP aplikacija
TSP backup baze podataka i oporavak	Automatsko	TSP aplikacija i TSP host operativni sistem
Backup, oporavak i brisanje revizijskih zapisa	Automatsko	TSP host operativni sistem and TSP zaposlenici
Fizički pristup prostorijama TSP-a	Manuelno	TSP zaposlenici
Promjene konfiguracije sistema	Manuelno	TSP zaposlenici
Ažuriranje softvera i hardvera	Manuelno	TSP zaposlenici
Planirano i neplanirano održavanje sistema i sajta	Manuelno	TSP zaposlenici
Neslaganja I prilagođavanja	Manuelno	TSP zaposlenici
Kadrovske promjene	Manuelno	TSP zaposlenici
Uništavanje određenih informacija	Manuelno	TSP zaposlenici

5.4.7 Obavještavanje subjekta koji je prouzrokovao događaj

Nije neophodno obavijestiti subjekat koji je uzročnik događaja.

5.4.8 Ocjena ranjivosti sistema

Ovjerilac IDDEEA realizuje ocjenu ranjivosti sistema kao dio procedure obrade revizijskih zapisa.

5.5 Arhiviranje zapisa

5.5.1 Tipovi arhiviranih zapisa

IDDEEA CA čuva sljedeće zapise:

- Informacije o revizijama navedenim u odjeljku 5.4 Procedure revizijskih zapisa

- dnevnici,

- evidencija,

- svi dokazi o provedenoj identifikaciji korisnika,

- svi obrasci zahtjeva,

- certifikati i lista opozvanih certifikata,

- pravila,

- CPS,

- Objave i obavještenja iz TSP Ovjerioca IDDEEA i

Ostali dokumenti u skladu sa važećim uredbama.

5.5.2 Period čuvanja arhive

U skladu sa relevantnim zakonima, arhiva se čuva najmanje 10 godina.

5.5.3 Zaštita arhive

Pristup podacima iz arhive Ovjerioca IDDEEA je dozvoljen samo zaposlenima u TSP-u na principu nužnog znanja.

5.5.3 Procedure rezervnih kopija arhive

Arhivirani podaci se čuvaju na namjenskom arhivskom mediju ili kao kopija na papiru. Arhivirani podaci se sigurno pohranjuju.

Arhivski materijal se u skladu s važećim propisima, standardima i preporukama navedenim u internim pravilima Ovjerioca IDDEEA.

5.5.4 Zahtjevi za vremensku oznaku zapisa

Arhivski zapisi su vremenski označeni u trenutku njihovog kreiranja, koristeći vrijeme sistema na kojem je događaj snimljen.

Svi sistemi su sinhronizovani sa vremena koji se može pratiti prema UTC.

5.5.5 Sistem prikupljanja arhiva (interni ili eksterni)

Ovjerioc IDDEEA koristi internu rezervnu kopiju i arhivski sistem u IDDEEA.

5.5.6 Procedure za dobijanje i verifikaciju informacija iz arhive

Pristup čuvanim podacima je dozvoljen samo predstavnicima Ovjerioca IDDEEA koji imaju pristup informacijama ili u skladu sa važećim zakonom.

5.6 Zamjena ključeva

Zamjena ključa privatnog ključa TSP-a će se izvršiti blagovremeno prije isteka TSP certifikata. Prilikom promjene ključa privatnog ključa TSP-a, novi TSP javni ključ će biti dostupan vlasnicima certifikata preko TSP javnog repozitorija.

5.7 Kompromitacija i oporavak u slučaju katastrofe

5.7.1 Procedure za postupanje u incidentnim i kompromitujućim situacijama

Ovjerilac IDDEEA sprovodi proceduru usklađenu sa ISO/IEC 27001 za postupanje u slučaju bezbjednosnog incidenta i kvara.

5.7.2 Računarski resursi, softver i/ili podaci koji su oštećeni

Ovjerioc IDDEEA je donio plan za nepredviđene situacije i oporavak od katastrofe, a koji se odnosi na oporavak operacija nakon oštećenja računskih resursa, softvera i podataka.

5.7.3 Procedure koje se sprovode kod kompromitacije privatnog ključa korisnika

U slučaju kompromitacije TSP privatnog ključa za potpisivanje, TSP će opozvati i ponovo izdati sve certifikate Ovjerioca IDDEEA koji se trenutno koriste.

5.7.4 Upravljanje kapacitetom poslovanja nakon katastrofe

Nakon prirodne ili druge vrste katastrofe, rad TSP operacija i IT centra će biti ponovo uspostavljen na nezavisnoj lokaciji za oporavak od katastrofe koristeći rezervne podatke. Ovjerioc IDDEEA će preduzeti sve razumne mjere za ponovno uspostavljanje usluga u najkraćem mogućem roku, ali ne dužem od pet (5) radnih dana.

5.8 Završetak rada TSP ili RA

U slučaju da Ovjerilac IDDEEA dobrovoljno prekine svoje aktivnosti, TSP će:

- Obavjestiti Ured za nadzor i akreditaciju ovjerilaca i sve aktuelne korisnike najmanje devedeset (90) dana prije namjere prestanka rada;
- U dogovoru sa Uredom za nadzor i akreditaciju ovjerilaca prebaciti svoje aktivnosti na drugog pružaoca usluga povjerenja ili opozvati sve važeće certifikate na dan ili nakon isteka otkaznog roka;
- U slučaju da prebacivanje usluga drugom pružaocu usluga nije moguće, Ovjerilac IDDEEA će dostaviti svu dokumentaciju, podatke i opremu Ministarstvu transporta i komunikacija Bosne i Hercegovine u skladu sa Zakonom o elektronskom potpisu;
- Obezbijediti da se sva dokumentacija i arhiva prebaci na drugog pružaoca usluga povjerenja ili na Ministarstvo transporta i komunikacija Bosne i Hercegovine ili da se čuva najmanje deset (10) godina od posljednjeg dana rada;
- Obezbijediti dostupnost i pristup relevantnim spiskovima opozvanih certifikata i OSCP-u u periodu od 6 mjeseci nakon opoziva svih certifikata.

Prije prestanka pružanja usluga, Ovjerilac IDDEEA će uništiti privatne ključeve CA, uključujući i rezervne kopije ili ih povući iz upotrebe, na način da se privatni ključevi ne mogu ponovo preuzeti.

Na web-sajtu IDDEEA-e izdati obavijest o prekidu pružanja usluga.

6 TEHNIČKE BEZBJEDNOSNE KONTROLE TSP-A

6.1 Generisanje i instalacija para ključeva

6.1.1 Generisanje para ključeva

Ovjerilac IDDEEA par ključeva za potpis se kreira na hardverski bezbjednosnoom modulu (HSM) tokom početne procedure generisanja ključa TSP-a i zaštićen je master ključem. U toku generisanja para kriptografskih ključeva CA koristi se višestruka autentifikacija ovlaštenih osoba i zaštita koja vrijedi za prostorije Ovjerioca IDDEEA.

Par ključeva za potpis nosioca certifikata TSP-a se uvijek generiše putem PKI korisničke aplikacije ili na QSCD uređaju (smart kartica/token).

Privatni ključevi koji se koriste za kvalifikovani elektronski potpis ili kvalifikovani elektronski pečat se generišu u hardverskom tokenu koji je u skladu sa QSCD specifikacijom. Privatni ključevi koji se koriste za druge tipove certifikata se generišu u softverskom kripto tokenu kod korisnika ili na hardverskom tokenu (uređaj za kreiranje potpisa).

Ključevi korisnika se generišu u zavisnosti od vrste certifikata u skladu sa tabelom nastavku.

Vrsta certifikata	Ključ	Generisanje ključeva
Korijenski i posrednički certifikati Ovjerioca IDDEEA	Par ključeva	u hardverskom sigurnosnom modulu TSP-a
Certifikat na smart kartici/ličnoj karti	Dva para ključeva	na QSCD u sigurnom okruženju TSP-a Ovjerioca IDDEEA
Certifikat za elektronski potpis za potpisivanje na daljinu	Par ključeva	u hardverskom sigurnosnom modulu TSP-a

6.1.2 Isporuka privatnog ključa korisniku

TSP generiše privatne ključeve na QSCD uređaju i dostavlja korisniku.

Privatne ključeve za druge Certifikate (koji se ne izdaju na QSCD uređaju) generiše sam korisnik na svojoj PKI aplikacij tako da se ne dostavljaju nosiocu certifikata.

6.1.3 Dostava javnog ključa do izdavaoca certifikata

Javni ključevi TSP-a se dostavljaju do TSP aplikacije u PKCS#10 formatu. PKCS#10 zahtjev mora biti potpisan privatnim ključem koji odgovara javnom ključu sadržanom u PKCS#10 zahtjevu.

6.1.4 Dostava javnog ključa TSP-a trećim stranama

TSP dostavlja javne ključeve za verifikaciju potpisa Ovjerioca IDDEEA korisnicima u obliku X.509 sertifikata, kao dio procedure upisa.

Javni ključ Ovjerioca IDDEEA je dostupan u formi certifikata na sljedećim lokacijama:

- U javnom LDAP direktoriju;

- Na web-sajtu.

Certifikat TSP-a se takođe može dobiti kontaktiranjem Ovjerioca IDDEEA (pogledati odjeljak 1.5.2 Kontakt osoba).

U svakom slučaju, subjekat koji koristi certifikate Ovjerioca IDDEEA mora provjeriti autentičnost i integritet certifikata TSP-a.

6.1.5 Dužine ključeva

TSP generiše svoje asimetrične ključeve za potpis sa dužinom najmanje 3072bita RSA.

Nosilac certifikata generiše svoje asimetrične private ključeve za potpis sa dužinom najmanje 2048 bita RSA.

6.1.6 Generisanje javnih ključeva i provjera kvaliteta

Ovjerilac IDDEEA trenutno ne izdaje DSA (algoritam digitalnog potpisa) ključeve.

6.1.7 Namjene ekstenzije "Key usage" (definisano u X.509 v3 polju upotrebe ključa)

- Ovjerilac IDDEEA koristi polja ekstenzije key usage u certifikatima za označavanje namjene javnih ključeva u certifikatima, kao što je definisano u RFC 5280 "Internet X.509 Certifikat infrastructure javnog ključa i u profilima spiska opozvanih certifikata".

- Pored te ekstenzije, IDDEEA CA takođe koristi proširenu namjenu ključa (extKeyUsage) za dodatno označavanje namjene ili ograničavanja upotrebe javnih ključeva u certifikatima kao što je definisano RFC 5280 "Internet X.509 Certifikat infrastrukture javnog ključa i u profilima spiska opozvanih certifikata":

- serverAuth: TLS WWW server authentication
- clientAuth: TLS WWW client authentication
- codesigning: Signing of downloadable executable code
- email Protection: E-mail protection
- timestamping: Binding the hash of an object to a time
- EKU Ossining: Signing OCSP responses

Za certifikate za potpisivanje i spisak opozvanih certifikata TSP koriste se samo privatni kriptografski ključevi CA.

Kriptografski ključevi i certifikati odgovornih osoba u Ovjeriocu IDDEEA se koriste samo za rad sa tehničkim sredstvima u vlasništvu Ovjerioca IDDEEA (hardver i softver).

Preostali certifikati Ovjerioca IDDEEA se mogu koristiti za namjene polja KeyUsage, kao što je prikazano u dole navedenoj tabeli.

Upotreba ključa se navodi u certifikatima koje izdaje Ovjerilac IDDEEA u poljima ekstenzija keyUsage i extKeyUsage, zavisno od vrste certifikata i vrste javnog ključa u certifikatu, kao što je prikazano u dole navedenoj tabeli.

Vrsta sertifikata	Upotreba u polju "keyUsage"
CAs (Root CA, ORGANIZATION)	keyCertSign, cRLSign
Elektronski certifikat za kvalifikovani elektronski potpis	digitalSignature, nonrepudiation, keyEncipherment
Normalizovani DS – OCSP	digitalSignature extKeyUsage: OCSPSigning

6.2 Zaštita privatnog ključa i kontrola kriptografskog hardverskog modula

6.2.1 Standardi i kontrole kriptografskog modula

Generisanje svih TSP-ovih ključeva za digitalno potisivanje i aktivnosti vezane za potpisivanje certifikata se vrše u okviru kriptografskog hardverskog modula koja ispunjava standard FIPS 140-2 Nivo 3. Sve druge kriptografske aktivnosti se vrše u kriptografskom modulu koji ispunjava standard FIPS 140-2 Nivo 3.

Privatni ključevi koje se koriste za kvalifikovani digitalni potpis i kvalifikovani digitalni pečat se generišu i koriste u kriptografskom hardverskom modulu certifikovanom u skladu sa QSCD specifikacijama.

Privatni ključevi nosioca certifikata oslanjaju se na fizičke i logičke kontrole koje štite računarski sistem nosioca certifikata. Odgovornost nosioca certifikata je da osigura da se privatni ključ čuva u okruženju sa dovoljnim nivoom fizičke zaštite. Međutim, preporučuje se da nosilac certifikata ima QSCD ocjenu koja zadovoljava najmanje standard FIPS 140-2 nivo 2 ili drugi standard verifikovan na jednak nivo bezbjednosti.

6.2.2 Kontrola privatnih ključeva od strane više osoba (n od m)

Kao što je definisano u odjeljku 5.2.2 Broj osoba koje se zahtjevaju po svakom zadatku.

6.2.3 Deponovanje privatnog ključa kod trećih lica

Ovjerilac IDDEEA ne podržava deponovanje privatnog ključa kod trećih lica.

6.2.4 Sigurnosne kopije privatnog ključa

U skladu sa važećim propisima i CPS-om, sigurnosna kopija privatnog ključa Ovjerioca IDDEEA navedena je u internim pravilima Ovjerioca IDDEEA.

6.2.5 Arhiviranje privatnog ključa

Privatni ključevi se ne arhiviraju.

6.2.6 Prenos privatnih ključeva sa i na kriptografski modul

Privatni ključevi za potpisivanje Ovjerioca IDDEEA se generišu u hardverski bezbjednom modulu (HSM). Prenos privatnih ključeva TSP-a na ili sa HSM-a se oganičava samo za svrhe kreiranja sigurnosnih kopija ili oporavka. Privatni ključevi TSP-a su zaštićeni enkripcijom kada se prenose sa jednog na drugi HSM, tako da privatni ključ za potpisivanje TSP-a nikada nije bez zaštite ukoliko je izvan HSM-a.

Ključevi koji se čuvaju u QSCD uređaju (smart kartice/tokeni) se ne prenose.

6.2.7 Čuvanje privatnog ključa u kriptografskom modulu

Privatni ključ za potpisivanje Ovjerioca IDDEEA se koristi samo u hardverski bezbjednom modulu. Privatni ključ za potpisivanje CA se čuva na kopiranom tokenu hardverski bezbjednog modula za svrhe sigurnosnih kopija i oporavka.

6.2.8 Postupak aktivacije privatnog ključa

Privatni kriptografski ključ za potpisivanje Ovjerioca IDDEEA se aktivira nakon pokretanja aplikacije certifikacionog tijela. Za aktivaciju je potrebna smart kartica ili token za pristup kriptografskom hardverskom modulu kao i korisnička šifra sa ulogom CA Master korisnika.

Korisnički privatni kriptografski ključevi koji su generasni na QSCD uređaju se aktiviraju nakon uspješne autentifikacije PIN brojem.

6.2.9 Postupak deaktiviranja privatnog ključa

Kriptografski ključ za potpisivanje Ovjerioca IDDEEA se deaktivira prekidom rada aplikacije TSP.

Korisničke aplikacije deaktiviraju privatni kriptografski ključ kada se korisnik izloguje iz sistema, tj. aplikacije.

6.2.10 Postupak uništavanja privatnog ključa

Privatni ključevi TSP se brišu kada certifikat TSP-a prestane da važi, na način da se briše privatni ključ na HSM-u i brisanjem rezervih kopija u rezervnem HSM.

Servisni ključevi koji se čuvaju na smart kartici se brišu uništavanjem kartice.

Korisničke aplikacije moraju izbrisati privatne kriptografske ključeve iz operativne memorije prije nego što ih ponovno dodijele. Takođe moraju izbrisati cijeli prostor na disku koji se koristi za privatne kriptografske ključeve prije nego što se taj prostor dodijeli operativnom sistemu.

6.2.11 Ocjenjivanje kriptograskog modula

Pogledati odjeljak 6.2.1 Standardi i kontrole kriptografskog modula.

6.3 Drugi aspekti upravljanja parom ključeva

6.3.1 Arhiviranje javnog ključa

Ovjerilac IDDEEA arhivira javne ključeve CA i korisničke javne ključeve kao što je definisano u odjeljku 5.5.4 Procedure rezervnih kopija arhive.

6.3.2 Periodi validnosti certifikata i parova ključeva

Period važenja javnih i privatnih kriptografskih ključeva u cerifikatima koje izdaje Ovjerilac IDDEEA je:

- Root javni verifikacijski ključ i certifikat TSP-a: 20 godina.
- Root privatni ključ za potpisivanje TSP-a: 20 godina.
- Javni verifikacijski ključ i certifikat izdavaoca TSP-a: 10 godina.
- Privatni ključ izdavaoca TSP-a: 10 godina.
- Javni verifikacijski ključ i certifikat korisnika: do 10 godina.
- Privatni ključ korisnika: do 10 godina.
- OCSP javni verifikacijski ključ i certifikat: do 3 godine.
- OCSP privatni ključ za potpisivanje: do 3 godine.

Ovjerilac IDDEEA može prilagoditi period važenja nekih kriptografskih ključeva korisnika na osnovu posebnih zahtjeva i zahtjeva javne nabavke u skladu sa propisima i vrstom certifikata.

6.4 Aktivacioni podaci

6.4.1 Generisanje i instalacija aktivacionih podataka

Referentne brojeve i autorizacione kodove generiše TSP aplikacija i čuvaju se šifrovani u bazi podataka TSP-a do isporuke korisnicima. Brojevi i kodovi su jedinstveni i generišu se na nepredvidiv način.

TSP generiše PIN kod za ključ koji je generisan na uređaju QSCD šalje se odnosno uručuje korisniku kao dio procedure definisane u odjeljku 4.1.2. Proces dostavljanja zahtjeva za registraciju certifikata i odgovornosti

Registracijski i aktivacijski kod za kvalifikovani elektronski certifikat za udaljeno potpisivanje se kreira sigurno od strane Ovjerioca IDDEEA. Registracijski i aktivacijski kod se korisniku prenosi putem dva odvojena kanala, jedan putem e-pošte, a drugi putem drugog sigurnog kanala (sigurni web portal kojem se može pristupiti kvalifikovanim certifikatom, SMS-om ili drugog sličnog sigurnog kanala). Izuzetno, ovlaštena osoba Ovjerioca IDDEEA RA može lično korisniku predati neki od gore navedenih kodova. Kodovi su namijenjeni samo za aktiviranje pristupa cloud certifikatu, tokom kojeg korisnik postavlja svoj lični kod (PIN kod).

6.4.2 Zaštita aktivacionih podataka

Aktivacioni kodovi se generišu bezbjedno u TSP aplikaciji i čuvaju se šifrovani u bazi podataka TSP-a.

6.4.3 Drugi aspekti koji se odnose na aktivacione podatke

Nije navedeno.

6.5 Bezbjednosne kontrole računara

6.5.1 Specifični tehnički zahtjevi za bezbjednost računara

Ovjerilac IDDEEA vrši niz tehničkih bezbjednosnih kontrola na računarima, koje provode host operativni sistem TSP-a i TSP aplikacija, uključujući:

- Kontrolu pristupa TSP uslugama;
- Strogo razdvajanje dužnosti i uloga operativnim licima u TSP;
- Korištenje smart kartica za čuvanje profila CA službenika za bezbjednost i administratora za certifikate;
- Šifrovane sesije između aplikacije TSP-a i korisničkih aplikacija korisnika;
- Šifrovanje osjetljivih podataka u bazi podataka TSP-a;
- Arhiviranje istorije certifikata i revizijskih podataka TSP-a i korisnika;
- Reviziju događaja koji se odnose na bezbjednost;
- Mehanizme oporavka za ključeve i TSP aplikaciju.

6.5.2 Ocjenjivanje bezbjednosti računara

Host operativni sistemi TSP-a su komercijalni gotovi proizvodi.

6.6 Životni ciklus i bezbjednosne kontrole

6.6.1 Kontrole razvoja sistema

Sve aplikacije i proizvodi koje koristi Ovjerilac IDDEEA su proizvodi sa odgovarajućim standardima iz ove oblasti.

6.6.2 Provjere upravljanja bezbjednošću

Ovjerilac IDDEEA sprovodi procedure upravljanja problemima, promjenama i konfiguracijom za sve PKI softverske i hardverske komponente u skladu sa zahtjevima ISO/IEC 27001.

6.6.3 Provjera bezbjednosti životnog ciklusa

TSP testira sve softvere i procedure u kontrolisanom okruženju.

6.7 Kontrole mrežne bezbjednosti

Računarska mreža Ovjerioca IDDEEA sastoji se od povezanih mrežnih segmenata, gdje su smješteni serveri i operativne stanice. Ti segmenti su međusobno povezani zaštitnim zidovima (firewalls). Računarska mreža Ovjerioca IDDEEA povezana je na Internet preko nekoliko nivoa zaštite (firewalls). Bezbjednosna pravila tih zaštitnih zidova dozvoljavaju promet samo za protokole koji su neophodni za pristup uslugama Ovjerioca IDDEEA.

6.8 Vremenski pečat

Datum i vrijeme se dodaju u sve revizijske zapise na nivou sistema i aplikacije. Sistemsko vrijeme je sinhronizovano s više vanjskih referenci koje se mogu pratiti prema UTC. Za sinhronizaciju se koristi NTP protokol.

7 PROFILI CERTIFIKATA, CRL SPISKA I OCSP

7.1 Profili certifikata

7.1.1. Broj verzije certifikata

Ovjerilac IDDEEA izdaje certifikate u X.509v3 formatu i u skladu sa RFC 5280, EN 319 412-2, EN 319 412-3 i EN 319 412-5. Sljedeća osnovna polja X.509 se koriste:

Ekstenzija X.509	Opis
Potpis	TSP potpis za autentifikaciju certifikata
Izdavalac	TSP naziv
Period važenja	Datum aktivacije i isteka važenja certifikata
Subjekat	Prepoznatljivo ime korisnika
Informacije o javnom ključu korisnika	Algoritam ID, ključ
Verzija	Verzija certifikata X.509, verzija 3 (2)
Serijski broj	Jedinstveni serijski broj certifikata

7.1.2 Ekstenzije certifikata

Sljedeća polja osnovne ekstenzije X.509 se koriste

Ekstenzija X.509	Opis
Potpis	TSP potpis za autentifikaciju certifikata
Izdavalac	TSP naziv
Period važenja	Datum aktivacije i isteka važenja certifikata
Subjekat	Određeno ime korisnika
Informacije o javnom ključu korisnika	Algoritam ID, ključ
Verzija	Verzija Certifikata X.509, verzija 3 (2)
Serijski broj	Jedinstveni serijski broj certifikata

Certifikati TSP-a sadrže sljedeće kritične ekstenzije:

Ekstenzija X.509	Opis
keyUsage	keyCertSign, cRLSign
basicConstraints	CA=TRUE, pathLenConstraint

Korisnički i certifikati usluga mogu sadržavati sljedeće ekstenzije:

Ekstenzija X.509		Opis
authorityKeyIdentifier		Hash ključa izdavaoca
subjectKeyIdentifier		Hash ključa nosioca
keyUsage		Kao što je definisano u odjeljku 6.1.7 Namjena ekstenzije "keyUsage" Ekstenzije su uvijek označene kao kritične.
extendedKeyUsage		Kao što je definisano u odjeljku 6.1.7 Namjena ekstenzije "keyUsage"
privateKeyUsagePeriod		Kao što je definisano u odjeljku 6.3.2. Periodi važenja certifikata i parova ključeva
certificatePolicies:		Politika certifikacije OID = OID kao što je definisano u 1.2 Naziv dokumenta i identifikacija
	CertPolicyID	
	CPS URI	
CRLDistributionPoints		CRL lokacije

subjectAlternativeName	Alternativno ime korisnika
basicConstraints	CA=false
Authority Information Access	accessMethod=caIssuers; and accessMethod=OCSP
qcStatement	According to ETSI EN 319 412-5

7.1.3 Ekstenzije privatnih certifikata

X.509	OID
Key Usage: digitalSignature,nonRepudiation,keyEncipherment	2.5.29.15
extendedKeyUsage: Document Signing,	1.3.6.1.4.1.311.10.3.12
extendedKeyUsage: PDF Signing	1.2.840.113583.1.1.5

7.1.4 Identifikator objekta (OID) algoritama

Algoritam	Identifikacioni broj
RSA	1.2.840.113549.1.1.1
SHA512 with RSA	1.2.840.113549.1.1.13

7.1.5 Oblici naziva

U sve certifikate koje izdaje Ovjerilac IDDEEA se upisuje puno prepoznatljivo ime certifikacionog tijela i subjekta certifikata u polja ime izdavaoca odnosno ime korisnika. Kodiranje tih imena se vrši u UTF8 string ili PrintableString formatu.

7.1.6 Ograničenja imena

Nije primjenjivo.

7.1.7 Identifikator objekta politike certifikacije

Svi certifikati koje izdaje TSP sadrže OID politike certifikacije po kojoj se izdaje certifikat. OID za svaki certifikat je definisan u odjeljku 1.2 Naziv dokumenta i identifikacija.

7.1.8 Upotreba "Policy Constraints" ekstenzija

Nije primjenjivo.

7.1.9 Sintaksa i semantika kvalifikatora politike

Kvalifikatori politike se koriste u skladu sa RFC5280.

7.1.10 Semantika procesiranja kritične ekstenzije "Certificate Policies"

Korisničke aplikacije PKI-a moraju obraditi ekstenziju certifikata kao kritičnu u skladu sa RFC 5280.

7.2 Profil spiska opozvanih certifikata

7.2.1 Broj verzije certifikata

TSP izdaje spiskove opozvanih certifikata u X.509 v2 formatu koristeći niz distribucionih tačaka u okviru LDAP direktorija i http web servera.

Sljedeća osnovna polja ekstenzije X.509 se koriste:

Ekstenzija X.509	Opis
Verzija	Set to v2
Potpis	Algoritam identifikatora koji se koristi za potpisivanje spiska

	opozvanih certifikata
Izdavalac	Određeno ime CA
thisUpdate	Datum izdavanja spiska opozvanih certifikata
nextUpdate	Datum narednog izdavanja spiska opozvanih certifikata
revokedCertificate	Serijski brojevi opozvanih certifikata

7.2.2 CRL i CRL "entry" ekstenzije

Ekstenzija X.509	Opis
CRLNumber	Redni broj spiska opozvanih certifikata
authorityKeyIdentifier	"Hash" ključa izdavaoca
reasonCode	TSP može sadržavati vrijednosti u skladu sa RFC5280
invalidityDate	Popunjava TSP aplikacija kako je operater odredio
expiredCertsOnCRL	Spisak opozvanih certifikata koji sadrži ovu ekstenziju uključuje informacije o statusu opoziva za certifikate koji su već istekli.

7.3 OCSP profil

Profil OCSP koji se koristi definisan je u RFC 6960.

7.3.1 Broj verzije certifikata

Verzija OSCP v1 u skladu sa RFC 6960 se koristi.

7.3.2 Ekstenzije OCSP

Ekstenzije OCSP zahtjeva su:

Ekstenzija	Opis
nonce	Vrijednost "nonce" povezuje zahtjev i odgovor kako bi se spriječili napadi ponavljanja. Vrijednost će biti u skladu sa RFC6280

Ekstenzije OCSP odgovora su :

Ekstenzija	Opis
nonce	Ista vrijednost kao u zahtjevu ukoliko se traži tako u zahtjevu.
ArchiveCutoff	Vremenski period koji OCSP čuva informacije o opozivu nakon isteka certifikata.

8 REVIZIJA USKLAĐENOSTI I DRUGA OCJENJIVANJA

8.1 Učestalost ili uslovi ocjenjivanja

Revizija usklađenosti Ovjerioca IDDEEA se vrši u skladu sa Zakonom o elektronskom potpisu i drugim važećim zakonskim propisima Bosne i Hercegovine.

Ovjerilac IDDEEA sprovodi obavezne interne revizije najmanje jednom godišnje.

8.2 Identitet/kvalifikacije procjenjivača (interna i eksterna revizija)

Službenik za internu reviziju ima odgovarajuće tehnološko i pravno znanje.

Revizor vanjske revizije mora imati odgovarajuća tehnološka i pravna znanja.

8.3 Odnos revizora s predmetom revizije

Interni ili eksterni revizor ne obavljaju poslove koji se odnose ili koji su vezani za upravljanje certifikatima.

8.4 Teme koje su obuhvaćene revizijom

Interna revizija utvrđuje da li:

Politika dovoljno ispunjava tehničke, proceduralne i organizacione aktivnosti TSP-a, u skladu sa uslovima Zakona o elektronskom potpisu i drugim važećim propisima Bosne i Hercegovine.

Sistem TSP-a je usklađen i sa tehničkim, proceduralnim i organizacionim praksama i politikama.

8.5 Aktivnosti preduzete kao rezultat utvrđenih nedostataka

Ovjerilac IDDEEA će preduzeti odgovarajuće aktivnosti za rješavanje svih nedostataka ili neusklađenosti identifikovanih kao rezultat revizije unutar dogovorenog vremenskog okvira koji zavisi od ozbiljnosti uključenog rizika.

8.6 Saopštavanje rezultata

Informacije o reviziji koje se odnose na usklađenost Ovjerilac IDDEEA sa relevantnim zakonima smatraju se izuzetno osjetljivim i ne smiju se otkriti nikome niti iz bilo kojeg razloga, osim za potrebe revizije ili u slučajevima nametnutim zakonom.

9 DRUGI POSLOVNI I PRAVNI ASPEKTI

9.1 Naknade

9.1.1 Naknade za izdavanje ili obnovu certifikata

Ovjerilac IDDEEA može da naplaćuje izdavanje elektronske potvrde na osnovu posebnih odluka Vijeća ministara Bosne i Hercegovine koje će u slučaju donošenja biti objavljene na Web stranici Ovjerioca IDDEEA.

9.1.2 Naknade za pristup certifikatu

Pogledati odjeljak 9.1.1 Naknade za izdavanje ili obnovu certifikata.

9.1.3 Naknade za opoziv i pristup informacijama o statusu certifikata

Pogledati odjeljak 9.1.1 Naknade za izdavanje ili obnovu certifikata.

9.1.4 Naknade za ostale usluge

Pogledati odjeljak 9.1.1 Naknade za izdavanje ili obnovu certifikata.

9.1.5 Povrat naknade

Podnosioci zahtjeva za certifikate mogu besplatno otkazati zahtjev za certifikat prije izdavanja aktivacionih kodova.

9.2 Finansijska odgovornost

9.2.1 Pokrivanje osiguranja

Ovjerilac IDDEEA je dužan da osigura najniži iznos osiguranja od odgovornosti za moguću štetu nastalu vršenjem usluga izdavanja kvalificirane elektronske potvrde u skladu sa važećim propisima, tako da:

Osigurana suma na koju mora biti ugovoreno osiguranje po jednom štetnom događaju ne može iznositi manje od 50.000,00 KM, podrazumijevajući pri tom kao štetni događaj pojedinačnu štetu nastalu upotrebom jedne kvalificirane elektronske potvrde u jednom aktu u pravnom prometu;

Ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti Ovjerioca kumulativno na godišnjem nivou, po svim štetnim događajima, ne može biti niža od 1.500.000,00 KM.

9.2.2 Ostala sredstva

Nema odredbi.

9.2.3 Osiguranje ili garancije za krajnje korisnike

Korisnici i treće strane su isključivo odgovorni da obezbijede adekvatno osiguranje ili pokriće garancije u odnosu na upotrebu ili uslugu njihovog certifikata.

9.3 Zaštita ličnih podataka

Svi lični podaci dostavljeni Ovjeriocu IDDEEA ili njegovim ovlaštenim predstavnicima čuvaju se u skladu sa zahtjevima propisanim Zakonom o zaštiti ličnih podataka u Bosni i Hercegovini. Objavljivanje navedenih informacija treba biti samo u skladu sa Zakonom o zaštiti ličnih podataka, Politikom zaštite ličnih podataka Ovjerilac IDDEEA ili u skladu sa drugim važećim propisom.

9.3.1 Opseg povjerljivih informacija

Sve informacije koje prikuplja, generiše, prenosi ili čuva Ovjerilac IDDEEA smatraju se povjerljivim, osim informacija navedenih u odjeljku 9.3.2, koje se smatraju nepovjerljivim.

9.3.2 Informacije koje nisu u opsegu poverljivih informacija

Informacije koje se objavljuju kao dio certifikata Ovjerioca IDDEEA, spiska opozvanih certifikata, Politike certifikacije i druge informacije objavljene u javnom repozitoriju CA se ne smatraju povjerljivim informacijama.

9.3.3 Odgovornost za zaštitu poverljivih informacija

Ovjerilac IDDEEA je odgovoran za zaštitu povjerljivih informacija u skladu sa Politikom zaštite ličnih podataka Ovjerioca IDDEEA i Zakonom o zaštiti ličnih podataka i drugom važećim propisima.

9.4 Privatnost ličnih informacija

9.4.1 Plan privatnosti

Kao što je navedeno u odjeljku 9.3 i 9.4.

9.4.2 Opseg privatnih informacija

Sve informacije vezane za nosioca certifikata ili korisnika, a koje nisu objavljene u certifikatu koji izdaje Ovjerilac IDDEEA, spisku opozvanih certifikata ili javnom LDAP direktoriju se smatraju povjerljivim.

9.4.3 Informacije koje se ne smatraju privatnim

Sve informacije koje su sadržane u certifikatu koji izdaje Ovjerilac IDDEEA, spisku opozvanih certifikata ili javnom LDAP direktoriju se ne smatraju povjerljivim.

9.4.4 Odgovornost za zaštitu povjerljivih informacija

Kao što je navedeno u odjeljku 9.3.3.

9.4.5 Obavještenje i saglasnost za upotrebu privatnih informacija

Ovjerilac IDDEEA će koristiti privatne informacije samo za potrebe za koje je korisnik dao saglasnost u procesu registracije.

9.4.6 Otkrivanje informacija u skladu sa pravnim i administrativnim procesima

Ovjerilac IDDEEA će otkriti povjerljive informacije samo predstavnicima institucija nadležnim za primjenu zakona u skladu sa važećim propisima.

9.4.7 Druge okolnosti za otkrivanje informacija

Ovjerilac IDDEEA će otkriti privatne informacije samo u okolnostima utvrđenim Politikom zaštite ličnih podataka Ovjerioca IDDEEA, Zakonom o zaštiti ličnih podataka u Bosni i Hercegovini i drugim relevantnim zakonima, na zahtjev suda ili drugog nadležnog organa, a pod uslovom da zahtjev ima pravni osnov.

9.5 Prava intelektualnog vlasništva

Nije primjenjivo.

9.6 Obaveze i odgovornosti

9.6.1 Obaveze i odgovornosti TSP-a

Ovjerilac IDDEEA će izdavati certifikate, provoditi ostale procedure upravljanja certifikatima i upravljati infrastrukturom CA u skladu sa Politikom certifikacije i važećim zakonima. TSP je odgovoran za usklađivanje sa procedurama navedenim u ovoj politici, čak i kada funkcionalnost TSP-a preuzima RA ili druga ovlaštena tijela.

Ovjerilac IDDEEA je dužan:

- postupati u skladu sa svojim internim pravilima i drugim važećim propisima,
- postupati u skladu sa međunarodnim preporukama,
- objaviti sve relevantne dokumente koji određuju njegovo poslovanje (politike, obrasce zahtjeva za izdavanje certifikata, zahtjevi za opoziv, cjenovnici, upute za sigurno korištenje kvalifikovanih digitalnih certifikata, itd.)
- objaviti na svojoj internet stranici sve informacije o promjenama u aktivnosti TSP-a, koje na bilo koji način utječu na subjekte certifikata i treća lica,
- osigurati rad usluga obavještavanja u skladu sa odredbama Ovjerioca IDDEEA i drugim važećim propisima,
- pridržavati se odredbi koje se odnose na sigurnu obradu ličnih i povjerljivih informacija o TSP-u, subjektima certifikata ili trećim stranama,
- opozvati certifikat i objaviti ga na CRL-u nakon otkrivanja razloga prema ovom CPS-u ili drugim, važećim propisima,
- izdati kvalifikovane digitalne certifikate u skladu s ovim CPS-om i drugim propisima i preporukama,
- Izdavanje Politike sertifikacije,
- osigurati ispravnost podataka o izdatim certifikatima,
- osigurati ispravno objavljivanje CRL-a,
- osigurati jedinstvenost prepoznatljivih imena,
- osigurati odgovarajuću fizičku sigurnost prostorija i pristup prostorijama TSP-a,
- profesionalno osigurati neprekidan rad i maksimalnu dostupnost usluge,
- profesionalno osigurati maksimalnu dostupnost usluga,
- profesionalno upravljati kontinuiranim radom svih ostalih pratećih usluga,
- na najbolji način otkloniti bilo kakve probleme u najkraćem mogućem roku,
- upravljati optimizacijom korištenog hardvera i softvera,
- informisati korisnike o važnim pitanjima i
- ispuniti sve ostale zahtjeve u skladu sa ovom politikom,

Ovjerilac IDDEEA osigurava maksimalnu dostupnost svojih usluga, svaki dan u godini, osim u sljedećim slučajevima:

- planirane i unaprijed najavljene tehničke ili servisne intervencije na infrastrukturi,
- neplanirane tehničke ili servisne intervencije na infrastrukturi kao rezultat nepredviđenih kvarova,
- tehničke ili servisne intervencije zbog kvara infrastrukture izvan nadležnosti Ovjerioca IDDEEA i nedostupnost kao rezultat više sile ili vanrednih događaja.

Ovjerilac IDDEEA će najaviti održavanje ili modernizaciju infrastrukture najmanje tri (3) dana prije početka aktivnosti.

Ovjerilac IDDEEA je isključivo odgovoran za sve informacije u ovom dokumentu i za implementaciju svih odredbi u ovom CPS-u.

Ostale obaveze TSP-a Ovjerioca IDDEEA se mogu odrediti mogućim uzajamnim sporazumom sa trećom stranom.

9.6.2 Odgovornosti i obaveze registracionog tijela (RA)

RA je dužan:

- provjeriti identitet korisnika ili budućih korisnika,
- primiti obrazac zahtjeva za izdavanje certifikata za usluge Ovjerioca IDDEEA,
- provjeriti obrazac zahtjeva za izdavanje certifikata,
- izdati neophodnu dokumentaciju korisnicima ili budućim korisnicima,
- poslati obrasce i druge informacije na siguran način Ovjeriocu IDDEEA.

RA snosi odgovornost za implementaciju svih odredbi, pravila i drugih uslova CPS-a dogovorenih sa Ovjeriocem IDDEEA.

9.6.3 Korisničke odgovornosti i obaveze

Korisnik preuzima punu odgovornost za upotrebu privatnog ključa povezanog sa javnim ključem u certifikatu pri čemu je vlasnik fizičko lice identifikovano privatnim ključem.

Prije izdavanja ključeva i certifikata, odnosno prilikom podnošenja zahtjeva za certifikat, korisnici zaključuju ugovor sa Ovjeriocem IDDEEA, uzimajući u obzir pravila i uslove korištenja.

Korisnici su odgovorni da:

- Tačno navedu svoj identitet i sve ostale elemente u Zahtjevu za izdavanje kvalifikovanih potvrda;
- Čuvaju podatke i sredstva za izradu kvalifikovanih elektronskih potpisa od neovlaštene upotrebe;
- Odmah obavijeste Ovjerioca IDDEEA o gubitku sredstava, otkrivanju podataka ili neovlaštenoj upotrebi podataka i sredstava za izradu kvalifikovanih elektronskih potpisa;
- Obavijeste Ovjerioca IDDEEA o promjeni informacija na osnovu kojih je izdata kvalifikovana potvrda;
- Koriste potvrde u skladu sa ovim Pravilima.

Prihvatanjem certifikata koji izdaje Ovjerioc IDDEEA, korisnik treba da:

- čuva u tajnosti svoj privatni ključ za potpisivanje;
- čuva u tajnosti svoju šifru;
- odmah obavijesti CA o svim netačnostima ili promjenama u informacijama sadržanim u certifikatu;
- isključivo koristi svoj certifikat u zakonite svrhe i ovlaštene svrhe detaljno opisane u odjeljku 1.4 Upotreba certifikata;
- odmah obavijesti CA o sumnjivoj ili otkrivenoj kompromitaciji privatnog ključa;
- odmah obavijesti Ovjerioca IDDEEA o svakoj sumnji ili poznatoj zloupotrebi bilo kojeg certifikata izdanog od strane CA.

9.6.4 Obaveze i odgovornosti trećih strana

Za provjeru validnosti certifikata koji dobijaju, treća lica se uvijek moraju prvo pozvati na Ovjerioca IDDEEA spisak opozvanih sertifikata.

Treća strana,kojoj je povjeren certifikat koji izdaje Ovjerioc IDDEEA je dužna da:

- Ograniči validnost certifikata samo u svrhu definisanu u ovom dokumentu;
- Provjeri validnost certifikata;
- Pročita ovaj dokument i nauči dužnosti, odgovornosi i ograničenja TSP-a;

- Zatraži opoziv certifikata ako:
  - Ima saznanja da je privatni ključ kompromitovan tako da utiče na pravilnu upotrebu,
  - Postoji opasnost od zloupotrebe,
  - Postoje promjene u podacima navedenim u certifikatu.

Prije preuzimanja certifikata, odgovornosti trećih strana su:

- Upoznati sa ograničenjima certifikata i odgovornostima TSP-a kao što je detaljno opisano u ovoj Politici;
- ograničiti oslanjanje na certifikate koje izdaje TSP na odgovarajuću upotrebu kao što je detaljno opisano u odjeljku 1.4 Upotreba certifikata;
- obezbijediti da certifikat nije opozvan pristupom važećim, bilo kojim i svim, primjenjivim spiskovima opozvanih certifikata (CRL) ili OCSP;
- odmah obavijestiti Ovjerioca IDDEEA o svakoj sumnji ili poznatoj zloupotrebi bilo kojeg certifikata izdatog od strane TSP-a.

9.6.5 Odgovornosti i obaveze drugih učesnika

Svi drugi učesnici su obavezni da koriste certifikate i djeluju u skladu da ovom Politikom i važećim propisima.

9.7 Nepriznavanje garancija

Osim garancija navedenih u ovoj Politici certifikacije i srodnim ugovorima, i u najvećoj mjeri dozvoljenoj zakonom, Ovjerilac IDDEEA isključuje bilo koje druge moguće garancije, uslove ili izjave (izričite, podrazumijevane, usmene ili pismene), uključujući bilo koju garanciju mogućnosti za prodaju ili prikladnosti za određenu upotrebu. TSP posebno isključuje:

- svaku odgovornost za moguću štetu koja može nastati od trenutka kada TSP primi važeći zahtjev za opoziv, do trenutka objavljivanja informacija o opozivu na spisku opozvanih certifikata-u u skladu sa odeljkom 4.9.6;
- svaku garanciju u pogledu tačnosti ili pouzdanosti bilo koje informacije sadržane u certifikatima koju ne daje Ovjerioc IDDEEA;
- odgovornost za predstavljanje informacija sadržanih u certifikatu;
- svaku garanciju u pogledu ovlaštenja ili statusa bilo koje osobe koja koristi certifikat Ovjerioca IDDEEA
- svaku odgovornost vezano za pitanja koje su van vlastite kontrole, uključujući dostupnost ili rad Interneta, ili telekomunikacione ili druge infrastrukture ili sistema RA, uključujući hardver i softver;
- svaku odgovornost za štetu kao rezultat više sile kao što je detaljno opisano u odjeljku 9.16.5 Viša sila.

9.8 Ograničenja odgovornosti

Ovjerioc IDDEEA odriče se odgovornosti bilo koje vrste za bilo kakvu vrstu naknade, štete ili druge zahtjeve ili obaveze bilo koje vrste po osnovu odštetnog prava, ugovora ili bilo kojeg drugog razloga u vezi s bilo kojom uslugom povezanom s izdavanjem, korištenjem ili oslanjanjem na certifikat izdat od Ovjerioca IDDEEA.

9.9 Naknada štete

Svaka strana snosi isključivu odgovornost za obeštećenje Ovjerioca IDDEEA ili drugih strana za gubitke ili štetu koji su rezultat lažne upotrebe certifikata ili nepostupanja u skladu sa ovom Politikom certifikata i važećim zakonima.

9.10 Trajanje i prestanak važenja

9.10.1 Trajanje

Politika certifikacije Ovjerioca IDDEEA i drugih dokumenata postaju važeća potvrdom od strane nadležnih tijela u Ovjeriocu IDDEEA, i objavljivanja na web-sajtu Ovjerioca IDDEEA kao što je definisano u odjeljku 2.1. Repozitoriji

9.10.2 Prestanak važenja

Prestanak važenja Politike certifikacije Ovjerioca IDDEEA nije vremenski određeno. Trenutna verzija prestaje da važi kada se objavi nova verzija.

9.10.3 Posljedice prestanka važenja i nastavak djelovanja

Nakon prestanka važenja ove Politike certifikacije, kao rezultat objavljivanja nove verzije, certifikat će se koristiti u skladu sa onom verzijom Politike certifikacije koja je bila važeća na dan izdavanja certifikata. U slučaju da se okolnosti promijene u mjeri u kojoj to nije moguće, Ovjerioc IDDEEA će obavijestiti korisnike kako je definisano u odjeljku 9.12.2 Mehanizam i period obavještavanja i treće strane putem web-sajta definisano u odjeljku 2.1 Repozitoriji.

9.11 Pojedinačna obavještenja i komunikacija sa učesnicima

Ovjerioc IDDEEA distribuiše trenutnu verziju ove Politike certifikacije i trenutnu verziju svih drugih javnih dokumenata putem svoje internet stranice definisane u odjeljku 2.1 Repozitoriji.

Takođe pogledati 9.12.2 Mehanizam i period obaveštavanja.

9.12 Izmjene i dopune

9.12.1 Postupak izmjena i dopuna

Zaposleni u Ovjeriocu IDDEEA i drugi subjekti mogu poslati svoje komentare direktno Tijelu za upravljanje politikom u pisanoj formi, putem e-pošte ili na adrese navedene u odjeljku 1.5.2 Kontakt osoba.

9.12.2 Mehanizam i period obaveštavanja

Ovjerioc IDDEEA može odlučiti da li će obavijestiti korisnike i treće strane u slučaju izmjena sa malim ili bez uticaja. Ovjerioc IDDEEA odlučuje da li izmjene imaju uticaj na korisnike i treće strane prema vlastitom nahođenju.

Sve promjene Politike certifikacije će biti objavljene kao što je opisano u odjeljku 2. ODGOVORNOSTI OBJAVLJIVANJA I REPOZITORIJA. Ovjerioc IDDEEA će obavijestiti korisnike o promjenama koje utiču na korisnike ili treće strane putem e-pošte.

9.12.3 Okolnosti pod kojima se mora mijenjati identifikator objekta OID

OID Politike certifikacije će se izmijeniti u slučaju kada izmjene utiču na korisnike ili treće strane.

9.13 Postupak rješavanja sporova

Svi sporovi vezani za poslovanje sa certifikatima upućuju se pisanim putem Ovjeriocu IDDEEA na adresu definisanu u odjeljku 1.5.2 Kontakt osoba. Ako je moguće, spor treba riješiti sporazumom. Spor koji se ne riješi pregovorima rješava nadležni sud.

9.14 Važeći propisi

Ova Politika certifikacije i odnos između TSP-a, RA, korisnici, subjekti (nosioci certifikata) i druge treće strane podliježu i tumače se u skladu sa zakonima Bosne i Hercegovine.

9.15 Usklađenost sa važećim propisima

Dokumenti i rad Ovjerioca IDDEEA usklađeni su sa važećim zakonodavstvom u Bosni i Hercegovini, koje primarno uključuje;

- Zakon o zaštiti ličnih podataka u Bosni Hercegovini,
- Zakon o elektronskim dokumentima, elektronskom potpisu Bosne i Hercegovine i podzakonski akte usvojene na osnovu pomenutog Zakona.
- Drugi relevantne propise.

9.16 Ostale odredbe

9.16.1 Kompletan ugovor

Politika certifikacije Ovjerioca IDDEEA i ugovor Ovjerioca IDDEEA sa krajnjim korisnikom navode sve relevantne odredbe o odnosu između Ovjerioca IDDEEA i nosilaca Ovjerioca IDDEEA javnih certifikata.

9.16.2 Dodjeljivanje

Korisnicima i nosiocima certifikata nije dozvoljeno da ustupaju prava i obaveze koje proizilaze iz ovog ugovora ni u cjelini ni djelimično trećoj strani po bilo kom osnovu.

9.16.3 Slučajevi neprimjenjivosti odredbi (razdvojenost)

Neprimjenjivost jednog ili više dijelova ovog dokumenta, neće uticati na primjenjivost ostalih odredbi, pod uslovom da to ne utiče na materijalne odredbe (pouzdanost certifikata i korištenje certifikata).

9.16.4 Izvršenje (advokatske naknade i odricanje od prava)

Nije primjenjivo

9.16.5 Viša sila

Viša sila označava hitne i nepredvidive situacije poput prirodnih katastrofa, terorizma, nestanka struje ili telekomunikacija, požara, nepredvidivih incidenata kao što su virusi ili blokada usluga zbog hakerskih napada, vladinih mjera i narušavanja jačine kriptografskih algoritama.

Ovjerioc IDDEEA ili druge strane neće biti odgovorne za bilo kakvu štetu uzrokovanu događajima više sile.

9.17 Ostale odredbe

Nije primjenjivo.

Direktor IDDEEA

Broj: 15-02-07-5-807/2023
Datum: 17.01.2024.

Prof.dr. Almir Badnjević