Politika sertifikacije
Agencije za identifikaciona dokumenta, evidenciju i razmjenu podataka BiH (IDDEEA)

Pravila o elektronskom potpisu koja je utvrdila IDDEEA kao ovlašćeno tijelo za pružanje usluga od povjerenja

Identifikacioni broj	
Verzija	1.0
Predlaže:	Generalni direktor

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

Contents

1. UVODNI DIO

1.1. Pregled

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

  1) Izdavanje kvalifikovanih sertifikata za elektronski potpis;

- Ova Politika sertifikacije je javni dokument koji predstavlja dio propisa koje definiše IDDEEA koji se odnose na kvalifikovane usluge od povjerenja koje pruža IDDEEA kao tijelo ovlašćeno 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 sertifikacije koje pokazuju povjerljivost IDDEEA-e kao kvalifikovanog pružaoca usluga od povjerenja (TSP).

  Ovaj dokument je usklađen sa zahtjevima Zakona o elektronskim dokumentima, elektronskoj identifikaciji i uslugama od povjerenja u Bosni i Hercegovini i podzakonskim aktima donesenim na osnovu navedenog zakona.

  Ovaj dokument sadrži Politiku sertifikacije IDDEEA-e. Dokument je izrađen u skladu sa okvirnim dokumentom IETF RFC 3647 “Internet X.509 Infrastruktura javnog ključa: Okvirna politika sertifikacije i sertifikacione prakse” koji sadrži okvir sa sveobuhvatnom listom tema koje treba da budu obrađene u politici sertifikacije i/ili izjavi o praksi sertifikacije. 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 sertifikate; Dio 1: Opšti uslovi
- ETSI EN 319 411-2 Politika i bezbjednosni uslovi za pružaoce usluga povjerenja koji izdaju sertifikate; Dio 2: Uslovi koje moraju da ispune pružaoci usluga od povjerenja koji izdaju EU kvalifikovane sertifikate;
- ETSI EN 319 412-1 Profili sertifikata; Dio 1: Pregled i zajednička struktura podataka
- ETSI EN 319 412-2 Profili sertifikata; Dio 2: Profili sertifikata za fizička lica
- ETSI EN 319 412-3 Profili sertifikata; Dio 3: Profili sertifikata za pravna lica
- ETSI EN 319 412-5 Profili sertifikata; Dio 5: Profil kvalifikovanog elektronskog sertifikata (QCStatement)
- ETSI TS 119 495 Uslovi karakteristični za sektor; Profili kvalifikovanog sertifikata 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 sertifikata koji su navedeni u tabelama ispod.

Tabela 1: Spisak kvalifikovanih sertifikata

Kategorija sertifikata	Opis
Kvalifikovani DS za kvalifikovani e-potpis	Kvalifikovani DS za kvalifikovani elektronski potpis izdat fizičkom licu gdje se privatni ključ i pripadajući sertifikat nalaze na QSCD-u

Tabela 2: Spisak normalizovanih sertifikata

Kategorija sertifikata	Opis
Normalizovani DS – OCSP	Normalizovani OCSP

1.2. Naziv dokumenta i identifikacija

- Ovaj dokument predstavlja Politiku sertifikacije 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 sertifikata koji se izdaju u skladu sa ovom Politikom.

Kategorija sertifikata	Identifikacija sertifikacione politike
Kvalifikovani DS za kvalifikovani elektronski potpis	0.4.0.194112.1.2
Normalizovani DS - OCSP	0.4.0.194112.1.2

- IDDEEA može izdati različite sertifikate, 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. Sertifikaciona tijela

- IDDEEA CA djeluje kao javni pružalac usluga od povjerenja (TSP) i izdaje sertifikate javnog ključa fizičkim i pravnim licima.
- IDDEEA CA djeluje kao centralno sertifikaciono tijelo koje izdaje samopotpisane sertifikate u procesu ceremonije generisanja korijenskog ključa i unakrsnog sertifikata jednom hijerarhijski podređenom sertifikacionom tijelu (CA). IDDEEA koristi jedno sertifikaciono tijelo (CA za izdavanje sertifikata) za izdavanje svih vrsta kvalifikovanih i normalizovanih sertifikata krajnjim korisnicima.
- IDDEEA CA upravlja sljedećim sertifikacionim tijelima:
    - Centralnim sertifikacionim tijelom IDDEEA sa mandatom od 20. septembra 2021. do 20. septembra 2041. koje ima samopotpisni sertifikat koji izdaje sertifikacionim tijelima IDDEEA-e.
    - Sertifikacionim tijelima IDDEEA-e koja izdaju kvalifikovane sertifikate krajnjeg identiteta sa mandatom od 29. septembra 2021. do 29. septembra 2031. koje potpisuje Centralno sertifikaciono tijelo IDDEEA.
- Sadržaj digitalnog sertifikata “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 sertifikat sertifikacionog tijela za izdavanje sertifikata 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

- IDDEEA CA je kao pružalac usluga od povjerenja dužna provoditi mjere i postupke kojima se osigurava upravljanje sertifikatima, u skladu sa važećim propisima u Bosni i Hercegovini i internim pravilima pružaoca usluga sertifikovanja. IDDEEA CA 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 sertifikacije IDDEEA CA;
- izradu i održavanje javnih dokumenata IDDEEA CA (Ugovor sa krajnjim korisnicima, itd.)
- predaju Politike sertifikacije IDDEEA CA nadležnom upravnom organu na odobrenje;
- registraciju i akreditovanje IDDEEA CA;
- angažovanje osoblja u tijelima za operativne poslove i registraciju (OA i RA);
- kontrolu i reviziju usklađenosti IDDEEA CA operacija i aktivnosti kako bi se osiguralo da TSP radi u skladu sa Politikom i relevantnim zakonodavstvom;
- kontrolu i odobravanje Politike sertifikacije (CP), ili Izjave o praksi sertifikacije (CPS dokument) spoljnjih unakrsno sertifikovanih tijela za sertifikaciju;
- rješavanje sporova između učesnika IDDEEA CA.

1.3.1.2. Operativno tijelo (OA)

Operativno tijelo IDDEEA CA 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 sertifikaciju;
- identifikaciju i autentikaciju pojedinaca ili lica koji se prijavljuju za sertifikat;
- odobravanje i odbijanje zahtjeva za izdavanje sertifikata;
- potpisivanje i izdavanje X.509 sertifikata koji korisnike obavezuje svojim javnim ključem, kao odgovor da je zahtjev za izdavanje sertifikata odobren;
- slanje X.509 seertifikata putem direktorija;
- pokretanje opoziva sertifikata, bilo na zahtjev korisnika ili na sopstvenu inicijativu subjekta;
- opoziv sertifikata, uključujući izdavanje i objavljivanje Spiska opozvanih sertifikata (CRL-ova) i održavanje servisa Protokola o elektronskoj provjeri sertifikata;
- 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 i LRA u okviru svoje nadležnosti;
- iniciraju opoziv sertifikata zaposlenih u TSP-u i RA.

1.3.2. Registraciona tijela IDDEEA CA (RA)

- Ministarstvo unutrašnjih poslova (MUP) je nadležni organ za izdavanje ličnih karata sa ugrađenim memorijskim elementom (e-OI/e-LK).
- Ministarstvo unutrašnjih poslova je registraciono tijelo (u daljem tekstu: pružalac usluga registracije ili RA) koje potvrđuje identitet i identifikacione podatke fizičkih lica, na osnovu čega IDDEEA CA izdaje, obnavlja, opoziva i suspenduje sertifikate.
- Ministarstvo unutrašnjih poslova nezavisno rukovodi svojim zaposlenim u policijskim upravama i policijskim stanicama (PU/PS) koje djeluju u svojstvu lokalnih registracionih tijela (LRA), a vrše registraciju osoba u skladu sa Zakonom o ličnim kartama državljana Bosne i Hercegovine.
- PU/PS poslovi su:
    - informisanje osoba o procesima registrovanja i izdavanja (e-OI/e-LK),
    - primanje zahtjeva za izdavanje, opoziv i suspenziju sertifikata (e-OI/e-LK),
    - utvrđivanje identiteta osoba i podnosilaca zahtjeva,
    - omogućavanje potpisivanja ugovora sa fizičkim licima,
    - izdavanje sertifikata (e-OI/e-LK).
- MUP i IDDEEA su sklopili sporazum kojim se MUP obavezuje da će obezbijediti provođenje bezbijednosnih propisa i procedura koji su opisani u ovom dokumentu, u odjeljku 5, naslovi 5.3 i 5.5.
- RA koristi dvije opšte kategorije registracionih tijela. Prva kategorija registracionih tijela (Lokalna registraciona tijela ili LRA) obuhvata registraciona tijela koja su nadležna za obavljanje verifikacije identiteta licem u lice i sakupljanje korisničkih podataka kako bi se obezbijedilo upisivanje korisnika i rutinska obnova sertifikata sa novim ključem. Druga kategorija registracionih tijela (primarno registraciono tijelo ili PRA) podrazumijeva službenike imenovane za kontrolu korisničkih podataka i odobravanje zahtjeva za registraciju.

1.3.3. Korisnici

- Lice je fizičko lice kome se izdaje e-OI/e-LK, koje dobiva sertifikat na ličnoj karti i potpisuje sporazum sa IDDEEA-om o pružanju usluga sertifikacije u skladu sa Zakonom o ličnoj karti državljana Bosne i Hercegovine. Lice je direktno odgovorno za postupanje u skladu sa Uslovima sertifikacionih usluga.

- Lice je i ono lice koje je navedeno u sertifikatu i potpisnik koji kreira elektronski potpis i koristi sertifikat u njegovo/njeno ime.
- Korisnik je lice, uključujući i fizičko lice (pojedince), koje koristi usluge.
- Subjekat je lice koje je identifikovano u sertifikatu kao nosilac privatnog ključa koji je povezan sa javnim ključem datim u sertifikatu.
- Korisnik je lice koje snosi krajnju odgovornost za korištenje privatnog ključa koji je povezan sa sertifikatom javnog ključa, dok je subjekat osoba čija je autentikacija izvršena pomoću privatnog ključa.

1.3.4. Treće strane

- Treće strane su entiteti, uključujući i fizička lica (osobe), koje koriste sertifikat i/ili elektronski potpis koji se može provjeriti u odnosu na javni ključ naveden u sertifikatu subjekta;
- Prije nego što se oslone na informacije koje su date u sertifikatu, treće strane se uvijek moraju pozvati na IDDEEA CA CRL ili OCSP kako bi se potvrdila validnost sertifikata koji su dobili.

1.3.5. Ostali učesnici

- Nije primjenjivo.

1.4. Upotreba sertifikata

1.4.1. Prihvatljivo korišćenje sertifikata

IDDEEA CA sertifikati mogu se koristiti za:

- Aplikacije koje zahtijevaju korišćenje kvalifikovanog sertifikata u skladu sa Zakonom o elektronskim dokumentima, elektronskoj identifikaciji i uslugama od povjerenja Bosne i Hercegovine;
- Verifikaciju elektronski potpisanih dokumenata;
- Verifikaciju elektronski izdatih dokumenata za pravna lica;
- Identifikovanje nosioca sertifikata;
- Bezbjednu komunikaciju e-poštom;
- Šifrovanje i dešifrovanje dokumenata u elektronskom obliku;

  Napomena: Ne čuvati kopiju privatnih ključeva za dešifrovanje korisnika za oporavak ključa. Odgovornost korisnika je da održava bezbjednu kopiju privatnih ključeva za dešifrovanje.
- Druge namjene na zahtjev korisnika i u skladu sa Zakonom o elektronskim dokumentima, elektronskoj identifikaciji i uslugama od povjerenja i drugim relevantnim zakonima u Bosni i Hercegovini.

1.4.2. Zabrana korišćenje sertifikata

- Svi sertifikati koje izdaje IDDEEA CA koriste se u skladu sa važećim zakonodavstvom Bosne i Hercegovine.

1.5. Administriranje politike sertifikacije

1.5.1. Administriranje dokumenta

- Sertifikacionom politikom IDDEEA rukovodi sama IDDEEA.

1.5.2. Kontakt osoba

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. Osoba koja određuje pogodnost Izjave o sertifikacionoj praksi

- Nije primjenjivo.

1.5.4. Procedura odobravanja Izjave o sertifikacionoj praksi

- Sertifikacionu politiku IDDEEA CA izrađuje i održava IDDEEA PMA, a odobrava je generalni direktor.

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 korišćenjem trenutno dostupne tehnologije i omogućavaju potpisniku da bezbjedno zaštiti podatke u elektronskom potpisu od neovlašćenog 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.

Sertifikat je sertifikat u elektronskom obliku koji potvrđuje vezu između podataka za provjeru elektronskog potpisa i odgovarajućeg lica, subjekta sertifikata i identiteta tog lica.

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

Normalizovani sertifikat je sertifikat koji ima ista tehnička svojstva i nudi isti nivo povjerljivosti kao i kvalifikovani sertifikat, 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 sertifikatu elektronskog potpisa.

Sertifikaciono tijelo je svako fizičko ili pravno lice koje izdaje sertifikate ili pruža druge usluge koje su povezane sa sertifikatima, odnosno sa elektronskim potpisom.

Subjekat je svako fizičko ili pravno lice koje je identifikovano u sertifikatu kao zakupac privatnog ključa koji se odnosi na javni ključ koji je uključen u sertifikat.

Ugovarač/aplikant je lice koje podnosi zahtjev za izdavanje sertifikata od sertifikacionog tijela u ime jednog ili više subjekata. Ugovarač/aplikant može biti i subjekat, kada se sertifikat izdaje pojedincu za lično korištenje.

Treća strana je lice koje ima opravdano povjerenje u sertifikat.

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

Sertifikat javnog ključa za šifrovanje je sertifikat koji sadrži javni ključ za šifrovanje.

Ključ za provjeru javnog potpisa Pogledati Par ključeva za šifrovanje.

- **Sertifikat ključa za provjeru javnog potpisa** je sertifikat 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	Sertifikaciono tijelo (Certificate Authority)
CN	Ime i prezime (Common Name - Name X.500)
CPS	Izjava o praksi sertifikacije (Certification Practice Statement)
CRL	Spisak opozvanih sertifikata (Certificate Revocation List)
DC	Digitalni sertifikat (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)
LRA	Lokalno registraciono tijelo (Local Registration Authority)
PRA	Primarno registraciono tijelo (Primary 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 sertifikatima (PKIX-Certificate Management Protocols), opisani u RFC 4510
X.509	Standardi sertifikata 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 PUBLIKOVANJE I REPOZITORIJE

2.1. Repozitoriji

- IDDEEA CA objavljuje informacije vezane za sertifikacione usluge u repozitorijima na sljedećim adresama:

Javni veb-sajt: https://www.iddeea.gov.ba/PKI/CPS

2.2. Objavljivanje informacija o sertifikatima

IDDEEA CA objavljuje:

- Spisak opozvanih sertifikata (CRL)
- Status sertifikata putem Protokola za elektronsku provjeru sertifikata
- Sertifikate sertifikacionih tijela (CA)
- Politiku sertifikata i Izjavu o dostavi PKI
- Spisak registracionih tijela
- Korisnička uputstva
- IDDEEA CA obavještava i oglašava o ostalim uslugama sertifikacije koje se odnose na javno informisanje.

2.3. Vrijeme i učestalost objavljivanja

- Sertifikati se objavljuju odmah po izdavanju, kao što je navedeno u odjeljku 4.4. Spiskovi opozvanih sertifikata 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 neovlašćenih izmjena.

3. IDENTIFIKACIJA I AUTENTIKACIJA KORISNIKA

3.1.1. Vrste imena

- Polje sa imenom subjekta u sertifikatima koje je izdalo sertifikaciono 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 sertifikatu i u sertifikatima 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 sertifikatima.

3.1.2. Imena treba da budu smislena

- Skup DN karakteristika subjekta sertifikata jedinstveno identifikuje svakog vlasnika sertifikata 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

- Ne može se primijeniti.

3.1.4. Pravila za tumačenje različitih oblika imena

- Polje sa imenom subjekta 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 IDDEEA CA su kao što je navedeno u odjeljku **Error! Reference source not found.**.
- X.500 *Jedinstveno ime* (Subjekat) u sertifikatima koje izdaje IDDEEA CA 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=)	Ime i prezime nosioca sertifikata za fizička lica 1.6
Serijski broj (serialnumber=)	Jedinstveni serijski broj

3.1.5. Jedinstvenost imena

- IDDEEA CA u subjektu sertifikata 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

- IDDEEA CA će se strogo pridržavati pravila za dodjeljivanje imena datih u skladu sa odjeljcima Tipovi imena i Smislena imena. Korisnicima je zabranjeno da traže ona imena lica, koja bi izazvala kršenje intelektualnih i imovinskih prava drugih korisnika.

- IDDEEA CA ulaže opravdane napore da riješi sporove koji mogu nastati oko dodjele imena, npr. TSP može kontaktirati sa podnosiocem zahtjeva i usaglasiti da polje ime i prezime (CN) koji se odnosi na subjekat treba izmijeniti, kako bi se jedinstveno ime (DN) razlikovalo od već postojećeg jedinstvenog imena (DN).

- IDDEEA CA, može prema svom nahođenju, odbiti, promijeniti, ponovo izdati ili opozvati sertifikate u vezi sa bilo kojim jedinstvenim imenom (DN).

3.2. Inicijalna provjera identiteta

3.2.1. Metod za dokazivanje posjedovanja privatnog ključa

- Dokaz o posjedovanju privatnog ključa korisnika dostavlja se putem bezbjedne razmjene između TSP zahtjeva i PKI zahtjeva kljienata korišćenjem protokola o upravljanju sertifikatima u skladu sa standardom PKCS#10 Certification Request Syntax Standard.

- Kada TSP generiše privatne ključeve i sertifikate, kartica sa ključevima i PIN se šalju subjektu koji je podnio zahtjev za izdavanje sertifikata, i na taj način se obezbjeđuje da korisnici dobiju privatne ključeve.

3.2.2. Autentikacija identiteta pojedinca

- Za svakog pojedinca (fizičko lice), koje želi da postane korisnik IDDEEA CA, obavljaće se provjera identiteta licem u lice. Lice koje je odgovorno za poslove registracije identifikuje fizičko lice koje podnosi zahtjev za sertifikat ili uslugu pregledajući njegovu važeću ličnu kartu ili pasoš.

- IDDEEA CA vodi evidenciju o sredstvima kojima je potvrđen identitet lica.

3.2.3. Neprovjerene informacije o korisniku

Nije primjenjivo.

3.2.4. Kriteriji za međuoperaciju

- Procedure i prakse svih unakrsno sertifikovanih CA-ova moraju biti jednake procedurama i praksama IDDEEA CA koje su definisane u ovoj Politici sertifikacije. IDDEEA CA 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 sertifikata ili privatnog ključa.

- Autentikacija korisnika koji podnose zahtjev za obnovu sertifikata obavljena je kako je navedeno u odjeljku 3.2.2 Autentikacija identiteta i odjeljku 3.2.3 Autentikacija identiteta pojedinca.

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 i odjeljku 3.2.3 Autentikacija identiteta pojedinca.

3.4. Identifikacija i autentikacija prilikom podnošenja zahtjeva za opoziv

- Zahtjev za opoziv korisnik ili nosilac sertifikata može podnijeti pozivom na kontakt telefon TSP-a i identifikacijom sa PIN-om/lozinkom definisanom tokom procesa registracije, lično u prostorijama registracionog tijela, ili digitalno potpisanim zahtjevom, koji se potpisuje privatnim ključem potpisa lica koje traži opoziv;

- Autentikacija ovlašćenih lica TSP-a koja traže opoziv putem elektronske komunikacije obavlja se na osnovu digitalnog potpisa, čak i onda kada se sumnja da je korišćeni privatni ključ za potpisivanje kompromitovan.
- U suprotnom, autentikacija ovlašćenih lica obavlja se na osnovu informacija sadržanih u dosjeu korisnika ili kako je navedeno u odjeljku 3.2.2 Autentikacija identiteta pojedinca.

4. OPERATIVNI ZAHTJEVI U VEZI ŽIVOTNOG CIKLUSA SERTIFIKATA

4.1. Zahtjev za dobijanje sertifikata

4.1.1. Ko može predati zahtjev za dobijanje sertifikata

- Sertifikacioni zahtjev za javni sertifikat može podnijeti:
- Svaka osoba (fizičko lice) koja ispunjava uslove navedene u Zahtjevu za registraciju digitalnog sertifikata, Politici sertifikacije IDDEEA CA i pratećim ugovorima između TSP-a i krajnjeg korisnika.

4.1.2. Proces dostavljanja zahtjeva za registraciju sertifikata i odgovornosti

- IDDEEA CA izdaje sertifikate samo nakon potvrde identiteta korisnika i uspješnog završetka procesa registracije. Glavni koraci procesa upisa sertifikata su:
  - Korisnik predaje potpisan zahtjev za registraciju digitalnog sertifikata i prilaže važeći identifikacioni dokument.
  - Korisnik je saglasan sa Politikom sertifikacije IDDEEA CA i svojim obavezama po potpisivanju Ugovora sa krajnjim korisnikom.
  - Zahtjev za registraciju digitalnog sertifikata odobrava registraciono tijelo IDDEEA CA.
  - Registraciono tijelo podnosi zahtjev za registraciju digitalnog sertifikata putem odgovarajuće aplikacije za registraciju ili direktno u IDDEEA OA.
  - IDDEEA OA kreira korisnika sa odgovarajućim profilom sertifikata 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 su potrebna krajnjem korisniku da zatraži sertifikat od CA ili TCP RA kada ključeve ili sertifikate priprema IDDEEA na smart kartici/tokenu.

Ukoliko ključeve i sertifikate pripremi TSP na smart kartici/tokenu, PIN i PUK se šalju korisniku e-poštom i/ili SMS-om; dostavlja se RA-u u zapečaćenoj koverti i preuzima je lično korisnik ili se šalje na registrovanu e-adresu.

- Aktivacioni kodovi za upis sertifikata šalju se nosiocu sertifikata:
  - Registracioni broj se šalje korisniku na e-adresu koja je navedena u zahtjevu za registraciju digitalnog sertifikata.
  - Registracioni broj se šalje e-poštom pretplatniku na e-adresu navedenu u obrascu zahtjeva za registraciju digitalnog sertifikata putem SMS-a
  - Korisnik upotrebljava aktivacioni kod korištenjem korisničke aplikacije koju je obezbijedila IDDEEA CA ili putem internet pretraživača. Spisak podržanih klijentskih aplikacija i internet pretraživača objavljen je zajedno sa korisničkim uputstvom na veb-sajtu IDDEEA CA koji je naveden u odjeljku 2.1 Repozitoriji.

4.2. Obrada zahtjeva za dobivanje sertifikata

4.2.1. Obavljanje funkcija identifikacije i autentikacije

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

4.2.2. Odobravanje ili odbijanje zahtjeva za sertifikaciju

- Zahtjev za registraciju sertifikata kod IDDEEA CA biće odobren samo ukoliko su ispunjeni svi navedeni uslovi:
  - Korisnik podnosi zahtjev za registraciju digitalnog sertifikata uz uspješnu identifikaciju i autentikaciju u skladu sa odjeljkom 3.2;
  - Korisnik je ovlašćen na odgovarajući način, ukoliko djeluje u nečije ime (pravnog lica);

- Obrazac digitalnog sertifikata, dostavljena identifikaciona dokumentacija i ovlašćenja su uspješno verifikovani;
- Korisnik je potpisao odgovarajući ugovor sa IDDEEA CA.

- 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 IDDEEA CA odbija zahtjev za sertifikaciju. IDDEEA zadržava pravo da odbije bilo koji zahtjev za sertifikaciju bez navođenja razloga za odbijanje.

4.2.3. Vrijeme potrebno za obradu zahtjeva za sertifikaciju

- Obrazac zahtjeva za sertifikaciju i identifikacioni dokument se provjeravaju i obrađuju u prisustvu podnosioca zahtjeva u prostorijama registracionog tijela IDDEEA CA.
- Podneseni zahtjev se dalje obrađuje u roku od 30 dana.

4.3. Izdavanje sertifikata

4.3.1. Aktivnosti TSP-a tokom izdavanja sertifikata

- sistem za izdavanje sertifikata IDDEEA CA po prijemu zahtjeva za sertifikaciju (PKCS#10):
- provjerava valjanost aktivacijskih kodova koji se nalaze u primljenim podacima;
- provjerava da li korisnik posjeduje privatni ključ povezan sa javnim ključem koji se šalje na sertifikaciju, kao što je predviđeno u odjeljku 3.2.1 Metod za dokazivanje posjedovanja privatnog ključa;
- provjerava da li sertifikat zahtijeva usklađenost sa tehničkom specifikacijom PKCS#10;
- izdaje traženi sertifikat, ukoliko je ispunjeno sve prethodno navedeno.

4.3.2. Obavještavanje korisnika o izdavanju sertifikata

- Aplikacija IDDEEA CA će odmah uručiti sertifikat podnosiocu zahtjeva, tako da nema potrebe za dodatnim obavještavanjem.
- Za sertifikate koji se izdaju putem smart kartice/tokena, ključ i sertifikate priprema TSP na smart kartici/tokenu, korisnik se obavještava tokom procesa dostavljanja.

4.4. Prihvatanje sertifikata

4.4.1. Postupak kojim se prihvata sertifikat

- Procedura upisivanja sertifikata zavisi od vrste sertifikata:
- Smart kartica/token se dostavlja u zatvorenoj koverti korisniku lično ili preporučenom poštom na adresu korisnika ako se radi o fizičkom licu; dok se za pravna lica dostavlja na adresu pravnog lica ili se lično preuzima;
- Sertifikate koji se ne izdaju na smart kartici/tokenu nosilac sertifikata unosi kroz aplikaciju internet pretraživača.
- Za sertifikate koji se ne izdaju na smart kartici/tokenu:
- Uputstvo za unos sertifikata može se pronaći na veb-sajtu IDDEEA CA https://www.iddeea.gov.ba/PKI/CPS. Korisnik će, takođe, dobiti uputstvo putem e-pošte kada dobije registracioni broj. Sama uputstva su podložna promjenama u skladu sa aktuelnim promjenama u okviru PKI i nisu sastavni dio ove Politike. Za uspješan upis sertifikata relevantna su posljednja objavljena uputstva.
- Korisnik može upisati sertifikat samo sa važećim aktivacionim podacima: registracionim brojem i autorizacionim kodom. Vijek trajanja podataka za aktivaciju je ograničen na 30 dana. Po isteku aktivacionih podataka, potrebno je ponoviti postupak registracije.

- U slučaju neuspješnog procesa upisa, nosilac sertifikata prijavljuje problem RA (vidi kontakt informacije za RA u odjeljku 1.5.2 Kontakt osoba).

- Podnosilac zahtjeva dobiva sve sertifikate tokom elektronskog procesa upisa sertifikata ili na smart kartici/tokenu. Nije potrebna dodatna potvrda o prihvatanju sertifikata.

4.4.2. Obavještavanje drugih lica o izdavanju sertifikata koje izdaje TSP

- IDDEEA CA ne obavještava druga lica.

4.5. Korišćenje para ključeva i sertifikata

4.5.1. Korišćenje korisničkog privatnog ključa i sertifikata

- IDDEEA CA izdaje sertifikate koji podržavaju nekoliko korišćenja ključa. Ta podrška je obezbijeđena uključivanjem odgovarajućih ekstenzija za korišćenje ključa.

- Korisnici će koristiti sertifikate u skladu s ekstenzijama sertifikata keyUsage i extKeyUsage X.509 i u svrhe definisane u odjeljku 1.4.1. Odgovarajuća upotreba sertifikata. Korisnici moraju čuvati svoj privatni ključ na sigurnom i preduzeti mjere predostrožnosti kako bi spriječili kompromitovanje ključa i neovlašćeno korišćenje.

- Po isteku važenja sertifikata ili opozivu sertifikata, prateći privatni ključ se više ne može koristiti.

4.5.2. Korišćenje javnog ključa i sertifikata treće strane

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

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

4.6. Obnavljanje sertifikata (bez generisanja novog ključa)

- Obnavljanje sertifikata je proces u kojem TSP izdaje novi sertifikat za istog korisnika. IDDEEA CA ne dozvoljava niti obezbjeđuje obnavljanje sertifikata.

4.6.1. Uslovi za obnavljanje sertifikata

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

4.6.2. Ko može tražiti obnavljanje zahtjeva

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

4.6.3. Obrada zahtjeva za obnavljanje sertifikacionog ključa

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

4.6.4. Obavještavanje korisnika o novom izdavanju sertifikata

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

4.6.5. Postupak koji predstavlja prihvatanje sertifikata sa obnovljenim ključem

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

4.6.6. Objavljivanje obnovljenog sertifikata koje obavlja TSP

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

4.6.7. Obavještavanje drugih lica o izdavanju sertifikata koje obavlja TSP

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

4.7. Obnavljanje sertifikata generisanjem novog ključa (obnavljanje generisanjem novog para ključeva)

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

4.7.1. Uslovi za obnovu sertifikata generisanjem novog ključa

Obnavljanje ključa sertifikata obavlja se:

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

4.7.2. Ko može tražiti sertifikaciju sa novim javnim ključem

Korisnik, nosilac sertifikata ili ovlašćeni predstavnik koji je tražio prvobitno izdavanje sertifikata može tražiti obnavljanje sertifikata generisanjem novog ključa.

4.7.3. Obrada zahtjeva za obnavljanje sertifikata generisanjem novog ključa

Obnavljanje sertifikata generisanjem novog ključa vrši se na isti način kao i prvobitno izdavanje sertifikata.

4.7.4. Obavještavanje korisnika o izdavanju novog sertifikata

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

4.7.5. Postupak prihvatanja sertifikata sa novim ključem

- Kao što je navedeno u odjeljku 4.4.1 Postupak prihvatanja sertifikata.

4.7.6. Objavljivanje sertifikata sa novim ključem koje obavlja TSP

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

4.7.7. Obavještavanje drugih lica o izdavanju sertifikata koje obavlja TSP

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

4.8. Izmjene sertifikata

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

4.8.1. Uslovi za izmjene sertifikata

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

4.8.2. Ko može tražiti izmjene sertifikata

- Izmjenu sertifikata može tražiti korisnik, nosilac sertifikata ili subjekat koji je tražio prvobitno izdavanje sertifikata.

4.8.3. Obrada zahtjeva za izmjenu sertifikata

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

4.8.4. Obavještavanje korisnika o izdavanju novog sertifikata

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

4.8.5. Postupak prihvatanja izmijenjenog sertifikata

- Kao što je navedeno u odjeljku 4.4.1. Postupak prihvatanja sertifikata. Objavljivanje izmijenjenog sertifikata obavlja CA.

4.8.6. Objavljivanje izmijenjenog sertifikata koje obavlja TSP

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

4.8.7. Obavještavanje drugih lica o izdavanju sertifikata koje obavlja TSP

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

4.9. Opoziv i suspenzija sertifikata

4.9.1. Uslovi za opoziv

Opoziv sertifikata se može tražiti:

- ako to zahtijeva korisnik ili nosilac sertifikata;
- ako TSP potvrdi da je nosilac sertifikata preminuo ili je izgubio sposobnost za poslovanje ili ako pravno lice prestane da postoji ili ako su se okolnosti koje su u značajnoj mjeri uticale na validnost sertifikata promijenile;
- ukoliko je poznato ili se sumnja da je netačna bilo koja informacija koja se nalazi u sertifikatu;
- ukoliko je privatni ključ koji je povezan sa sertifikatom 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 sertifikat nije propisno izdat u skladu sa Politikom sertifikacije IDDEEA CA;
- kada korisnik ili nosilac sertifikata prekrši odredbe Politike sertifikacije IDDEEA CA ili važeći zakon (neispunjavanje obaveza korisnika);
- iz bilo kog drugog razloga navedenog u Zakonu o elektronskim dokumentima, elektronskoj identifikaciji i uslugama od povjerenja.
- ako Tijelo za upravljanje politikom IDDEEA CA smatra da je to neophodno.

4.9.2. Ko može tražiti opoziv

Opoziv sertifikata može tražiti:

- Korisnik (npr. pravno lice) ili subjekat (nosilac sertifikata);
- Ovlašćeni predstavnik koji je podnio zahtjev za izdavanje sertifikata;
- IDDEEA CA;
- Nadležni sud.

4.9.3. Procedura za podnošenje zahtjeva za opoziv

Nosilac sertifikata može tražiti opoziv sertifikata na sljedeći način:

- Putem elektronski potpisanog zahtjeva za opoziv poslatog e-poštom;
- Ličnim kontaktiranjem sa kancelarijom registracionog tijela IDDEEA CA; ili
- Telefonskim pozivom, kada osoba mora znati tajnu riječ/lozinku/PIN koji/a je unesen/a u obrazac zahtjeva za registraciju digitalnog sertifikata;

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

Opoziv zbog izmjene podataka u samom sertifikatu

1. Zahtjev za opoziv:

   - Korisnik šalje zahtjev registracionom tijelu IDDEEA CA lično ili putem e-pošte. Važećim zahtjevom se smatra onaj zahtjev koji je potpisan pomoću ključa koji je izdala IDDEEA CA.
   - Korisnik se identifikuje (lično) i podnosi zahtjev (obrazac) za opoziv sertifikata.
   - Registraciono tijelo IDDEEA CA provjerava i odobrava opoziv.

2. Registraciono tijelo IDDEEA CA pokreće opoziv sertifikata kroz aplikaciju, navodeći razloge za opoziv ili šalju zahtjev za opoziv operativnom tijelu IDDEEA CA 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 i odjeljku 3.2.3 Autentikacija identiteta pojedinca.

Opoziv zbog kompromitovanog privatnog ključa

1. Zahtjev za opoziv:

   - Korisnik šalje zahtjev registracionom tijelu IDDEEA CA putem e-pošte ili lično.
   - Telefonskim pozivom, kada osoba mora znati tajnu riječ/lozinku/PIN koji je unesen u obrazac zahtjeva za registraciju digitalnog sertifikata.
   - Korisnik se identifikuje (lično) i podnosi zahtjev (obrazac) za opoziv sertifikata.
   - Primarno registraciono tijelo IDDEEA CA provjerava i odobrava opoziv.

2. Primarno registraciono tijelo IDDEEA CA pokreće opoziv sertifikata kroz aplikaciju tako što uoči kompromitujući status ili šalje zahtjev za opoziv operativnom tijelu IDDEEA CA 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 sertifikata 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 sertifikat će biti opozvan, pri čemu:

1. RA provjerava status digitalnog potpisa korisnika kod TSP-a
2. Zaposleni u operativnom tijelu IDDEEA CA vrše opoziv sertifikata navodeći razloge za to.

4.9.4. Odloženi opoziv sertifikata

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

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

4.9.5. Rok u kojem CA mora završiti obradu zahtjeva za opoziv

- U drugim slučajevima opoziva sertifikata, rok za opoziv sertifikata 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 IDDEEA CA ili Protokol OCSP prije korišćenja svakog sertifikata koji je izdala IDDEEA CA. Ukoliko se ne može izvršiti valjana provjera opoziva, zbog kvara sistema ili gubitka servisa, ne treba prihvatiti nijedan IDDEEA CA sertifikat.

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

4.9.7. Učestalost objavljivanja spiska opozvanih sertifikata (ako je primjenjivo)

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

4.9.8. Maksimalno kašnjenje spiska opozvanih sertifikata (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 sertifikatu.

4.9.10. Uslovi za elektronsku provjeru opoziva

- Pogledati odjeljak 4.9.6.

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 sertifikata.

4.9.13. Suspenzija sertifikata

- Suspenzija sertifikata se može tražiti u slučaju da nosilac sertifikata izostaje duži vremenski period, npr. porodiljsko odsustvo. IDDEEA CA može suspendovati sertifikat nosioca sertifikata za vrijeme obrade zahtjeva za opoziv sertifikata.

- Suspendovani sertifikati se objavljuju na Spisku opozvanih sertifikata (CRL) za vrijeme suspenzije.

4.9.14. Ko može tražiti suspenziju

- Suspenziju sertifikata može tražiti:
- Korisnik ili subjekat (nosilac sertifikata)
- Ovlašćeni predstavnik koji je tražio izdavanje sertifikata
- Registraciono tijelo IDDEEA CA (RA)
- Službenici IDDEEA CA.

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 sertifikata

4.10.1. Operativne karakteristike

- Status sertifikata se objavljuje korišćenjem X.509 Spiska opozvanih sertifikata (CRL) putem OCSP protokola.
- CRL spisak se objavljuje kroz LDAP direktorij i veb-sajt. Tačne lokacije (LDAP i http URLs) se objavljuju korišćenjem ekstenzije X.509 CRL Distribution Points.
- Dostupnost OCSP usluge je naznačena kao URL u sertifikatu.
- CRL profil i servisni protokol OCSP opisani su u odjeljcima 7.2. i 7.3.

4.10.2. Dostupnost usluga

- Status sertifikata IDDEEA CA dostupan je 24 časa 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 sertifikata

- Sertifikat prestaje da važi po isteku roka važenja ili nakon opoziva sertifikata. IDDEEA CA čuva dokumentaciju i podatke iz sertifikata najmanje deset (10) godina po isteku ili opozivu sertifikata.

4.12. Deponovanje i oporavak ključeva

- IDDEEA CA 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 BEZBIJEDNOSNE KONTROLE

5.1. Fizičke kontrole

5.1.1. Lokacija objekta i konstrukcija

- Tehnička sredstva IDDEEA CA (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 IDDEEA CA 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 IDDEEA CA;
- 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 od strane čuvara na licu mesta, i video nadzor iz centra za video nadzor u zgradi.

5.1.2. Fizički pristup

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

5.1.3. Električno napajanje i klimatizacija

- IT centar 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 IDDEEA CA nema vodovodnih instalacija. Poduzete su sve tehničke mjere za zaštitu od vodovodnih instalacija u okruženju.

5.1.5. Prevencija i zaštita od požara

- Prostorije IDDEEA CA 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 IDDEEA CA, uključujući medij sa sigurnosnom kopijom podataka, čuvaju se u vatrootpornim ormarima, od kojih se jedan nalazi unutar IDDEEA CA, 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

- IDDEEA CA 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, IDDEEA CA zaposleni mogu imati nalog na host računaru TSP-a, TSP aplikaciji ili na oboje.TSP aplikacija koju koristi IDDEEA CA 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 IDDEEA CA 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	• Odobravati početnu TSP aplikaciju i konfiguraciju hardverskog bezbjednosnog modula (HSM) i njihovo održavanje • Pokretati i zaustavljati usluge TSP aplikacije • Određivati prve PKI službenike za bezbjednost • Obnovitii nalog PKI službenicima za bezbjednost kada zaborave šifru • Obnoviti TSP administrativne usluge u slučaju da se ošteti profil • Pokrenuti proces zamjene HSM-a • Obnoviti smart kartice operatora HSM-a • Obnoviti i ponovo šifrovati TSP bazu podataka
CA Službenik za bezbjednost	• Upravljati korisničkim nalozima drugih PKI službenika za bezbjednost i PKI administratora • Upravljati korisničkim nalozima • Upravaljati oporavkom ključeva za korisnike • Obrađivati revizijske zapise • Postavljati i mijenjati bezbjednosnu politiku TSP aplikacije • Upravljati profilima TSP aplikacijskih sertifikata • Vršiti unakrsno sertifikovanje sa vanjskim sertifikovanim tijelima • Pripremati izvještaje
CA Administrator	• Upravljati korisničkim nalozima • Upravljati sertifikatima • Pripremati izvještaje

Administrator direktorija	• Dodavati i brisati korisnike u direktoriju • Podešavati 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 IDDEEA CA privatnog ključa
- Resetovanje šifre na nalozima CA glavnih korisnika
- Unakrsno sertifikovanje 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 IDDEEA CA.
- Operativno tijelo IDDEEA CA 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 IDDEEA CA (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 sertifikati su kreirani pojedinačno za svaku odgovornu osobu
- Zabranjena je svakodnevna upotreba naloga ili sertifikata među zaposlenima IDDEEA CA. Zaposleni su ograničeni na aktivnosti ovlaštene za datu ulogu kroz kontrolu postavljenu aplikacijom, operativnim sistemom i procedurama IDDEEA CA.
- Zaposleni u IDDEEA CA 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 IDDEEA CA su zaposlene na neodređen ili određen 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 ili određen period. Oni trebaju biti adekvatno kvalifikovani za izvršavanje svojih radnih obaveza.
- Zaposleni u IDDEEA CA i RA su ugovorom vezani da ne objavljuju niti otkrivaju povjerljive informacije vezane za bezbjednost IDDEEA CA 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 sertifikati.

5.3.1. Kvalifikacije, iskustvo i sigurnosne provjere

- Prakse zapošljavanja u IDDEEA CA 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

- IDDEEA CA obezbjeđuje obuke za svoje zaposlene.
- Za odgovorne osobe u IDDEEA CA, pod obukama se podrazumijevaju procedure za zaštitu sistema i podataka, specifične obuke za njihove uloge i dužnosti, obuke za korištenje aplikacije IDDEEA CA 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 IDDEEA CA 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 IDDEEA CA ili Registracionog tijela, IDDEEA CA će mu onemogućiti dalji pristup tehničkim uređajima (hardver i softver).
- IDDEEA CA će oduzeti ili opozvati sve sertifikate 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

- IDDEEA CA 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 IDDEEA CA.

5.3.8. Dokumentacija koja se dostavlja zaposlenima

- Odgovorne osobe u IDDEEA CA 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

- U IDDEEA CA se sljedeći događaji zapisuju automatski ili ručno za potrebe revizije:

  - Događaji vezani za korisničke ključeve i sertifikate: registracija, izdavanje, opoziv, suspenzija;

  - Događaji vezani za TSP ključeve;

  - Događaji vezani za administraciju, čuvanje podataka i javni direktorij;

  - Događaji operativnih sistema i hardverske opreme;

  - Događaji koji se odnose na fizički pristup TSP-u.

- Većina elektronskih zapisa sadrži datum i vrijeme svakog događaja i identitet subjekta koji ga je generisao. Svi unosi u evidencije fizičke provjere identifikovani su datumom i vremenom.

- Zapisi se prikupljaju i slažu u IDDEEA CA Operativnom tijelu.

5.4.2. Frekvencija procesiranja zapisa

- Zapisi se provjeravaju na dnevnom nivou.

- Revizija podrazumijeva:

  - Prikupljanje svih zapisa od zadnje obrade zapisa,

  - Pregled unosa revizijskih zapisa,

  - Pregled prikupljenih zapisa.

Potrebno je analizirati i objaviti sve relevantne događaje u cilju rješavanja ili ograničavanja eskalacije problema.
Sve zapise kojima je istekao rok trajanja treba premjestiti, očistiti ili uništiti.

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, kertridži sa rezervnom kopijom revizijskih zapisa i fizički revizijski zapisi čuvaju se u zoni visoke bezbjednosti IDDEEA CA Operativnog tijela, 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 IDDEEA CA host sistema.
- Rezervne kopije se čuvaju u vatrootpornom ormaru u IDDEEA CA Operativnog tijela.
- Rezervne kopije koje sadrže konsolidovanu kopiju datoteka revizijskih zapisa se šalju u sigurno skladište van lokacije u svrhe skladištenja i arhiviranja van lokacije.

5.4.6. Sistem prikupljanja revizija (interne ili eksterne)

- Sistem sakupljanja revizija IDDEEA CA je kombinacija automatskih i manuelnih procesa koje izvodi TSP host operativni sistem, TSP aplikacija, i zaposleni u IDDEEA CA, 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
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

- Subjekat koji je prouzrokovao određeni revizijski događaj se ne obavještava.

5.4.8. Ocjena ranjivosti sistema

- IDDEEA CA 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
  - Ugovori korisnika i sve forme koje pripadaju zahtjevu
  - Sertifikati, status opoziva sertifikata
  - Neslaganje i prilagođavanje i korespondencija

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 IDDEEA CA je dozvoljen samo zaposlenima u TSP-u na principu nužnog znanja.

5.5.4. Procedure rezervnih kopija arhive

- Arhivirani podaci se čuvaju na namjenskom arhivskom mediju ili kao kopija na papiru. Najmanje jednom mjesečno se premeštaju na bezbjedno mjesto na udaljenu lokaciju predviđenu za njihovo skladištenje.
- Arhivski materijal se skladišti van lokacije u bezbjednom objektu gde su fizičke i bezbjednosne kontrole iste onima koje se primjenjuju na primarnoj lokaciji TSP-a

5.5.5. 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.

5.5.6. Sistem prikupljanja arhiva (interni ili eksterni)

- IDDEEA CA koristi internu rezervnu kopiju i arhivski sistem u IDDEEA CA.

5.5.7. Procedure za dobijanje i verifikaciju informacija iz arhive

- Pristup sačuvanim podacima je dozvoljen samo predstavnicima IDDEEA CA koji moraju da znaju informacije ili u skladu sa važećim zakonom.

5.6. Zamjena ključeva

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

5.7. Kompromitacija i oporavak u slučaju katastrofe

5.7.1. Procedure za postupanje u incidentnim i kompromitujućim situacijama

- IDDEEA CA 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

- IDDEEA CA je donijelo 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 sertifikate IDDEEA-CA 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. IDDEEA CA 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 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 sertifikate na dan ili nakon isteka otkaznog roka;
- U slučaju da prebacivanje usluga drugom pružaocu usluga nije moguće, IDDEEA CA će dostaviti svu dokumentaciju, podatke i opremu Ministarstvu transporta i komunikacija Bosne i Hercegovine u skladu sa Zakonom o digitalnom 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 sertifikata i OSCP-u u periodu od 6 mjeseci nakon opoziva svih sertifikata.
- Prije prestanka pružanja usluga, 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.
- Obavijestiti na web-sajtu IDDEEA-e o prekidu pružanja usluga.

6. TEHNIČKE BEZBJEDNOSNE KONTROLE TSP-A

6.1. Generisanje i instalacija para ključeva

6.1.1. Generisanje para ključeva

- IDDEEA CA 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 IDDEEA CA.

- Par ključeva za potpis nosioca sertifikata 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 sertifikata se generišu u softverskom kripto tokenu kod korisnika ili na hardverskom tokenu (uređaj za kreiranje potpisa).

6.1.2. Isporuka privatnog ključa korisniku

- TSP generiše privatne ključeve na QSCD uređaju i dostavlja korisniku.

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

6.1.3. Dostava javnog ključa do izdavaoca sertifikata

- 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 IDDEEA CA korisnicima u obliku X.509 sertifikata, kao dio procedure upisa.

- Javni ključ IDDEEA CA je dostupan u formi sertifikata na sljedećim lokacijama:

  - U javnom LDAP direktoriju;

  - Na web-sajtu.

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

- U svakom slučaju, subjekat koji koristi sertifikate IDDEEA CA mora provjeriti autentičnost i integritet sertifikata TSP-a.

6.1.5. Dužine ključeva

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

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

6.1.6. Generisanje javnih ključeva i provjera kvaliteta

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

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

- IDDEEA CA koristi polja ekstenzije key usage u sertifikatima za označavanje namjene javnih ključeva u sertifikatima, kao što je definisano u RFC 5280 “Internet X.509 Sertifikat infrastructure javnog ključa i u profilima spiska opozvanih sertifikata”.

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

  - 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 sertifikate za potpisivanje i spisak opozvanih sertifikata TSP koriste se samo privatni kriptografski ključevi CA.

- Kriptografski ključevi i sertifikati odgovornih osoba u IDDEEA CA se koriste samo za rad sa tehničkim sredstvima u vlasništvu IDDEEA CA (hardver i softver).

- Preostali sertifikati IDDEEA CA se mogu koristiti za namjene polja KeyUsage, kao što je prikazano u dole navedenoj tabeli.

- Upotreba ključa se navodi u sertifikatima koje izdaje IDDEEA CA u poljima ekstenzija keyUsage i extKeyUsage, zavisno od vrste sertifikata i vrste javnog ključa u sertifikatu, kao što je prikazano u dole navedenoj tabeli.

Vrsta sertifikata	Upotreba u polju “keyUsage”
CAs (Root CA, ORGANIZATION)	keyCertSign, cRLSign
Kvalifikovani digitalni potpis 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 sertifikata 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 hardverkom modulu sertifikovanom u skladu sa QSCD specifikacijama.

- Privatni ključevi nosioca sertifikata oslanjaju se na fizičke i logičke kontrole koje štite računarski sistem nosioca sertifikata. Odgovornost nosioca sertifikata je da osigura da se privatni ključ čuva u okruženju sa dovoljnim nivoom fizičke zaštite. Međutim, preporučuje se da nosilac sertifikata 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

- IDDEEA CA ne podržava deponovanje privatnog ključa kod trećih lica.

6.2.4. Sigurnosne kopije privatnog ključa

- TSP zadržava kopiju privatnog ključa CA.
- Kopije korisničkih privatnih ključeva TSP-a se ne čuvaju u IDDEEA CA.

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 IDDEEA CA-a 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 IDDEEA CA 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 IDDEEA CA-a se aktivira nakon pokretanja aplikacije sertifikacionog 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 IDDEEA CA-a 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 sertifikat 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

- IDDEEA CA 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 sertifikata i parova ključeva

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

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

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

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 sertifikata i odgovornosti

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

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

- Kontrola 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 sertifikate;

- Šifrovane sesije između aplikacije TSP-a i korisničkih aplikacija korisnika;

- Šifrovanje osjetljivih podataka u bazi podataka TSP-a;

- Arhiva istorije sertifikata i revizijskih podataka TSP-a i korisnika;
- Revizija događaja koji se odnose na bezbjednost;
- Mehanizmi 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 IDDEEA CA su komercijalni gotovi proizvodi.

6.6.2. Provjere upravljanja bezbjednošću

- IDDEEA CA 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 IDDEEA CA sastoji se od povezanih mrežnih segmenata, gdje su smješteni serveri i operativne stanice. Ti segmenti su međusobno povezani zaštitnim zidovima (firewalls). Računarska mreža IDDEEA CA 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 IDDEEA CA.

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 SERTIFIKATA,CRL SPISKA I OCSP

7.1. Profili sertifikata

7.1.1. Broj verzije sertifikata

- IDDEEA CA izdaje sertifikate 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 sertifikata
Izdavalac	TSP naziv
Period važenja	Datum aktivacije i isteka važenja sertifikata
Subjekat	Prepoznatljivo ime korisnika
Informacije o javnom ključu korisnika	Algoritam ID, ključ
Verzija	Verzija sertifikata X.509, verzija 3 (2)
Serijski broj	Jedinstveni serijski broj sertifikata

7.1.2. Ekstenzije sertifikata

- Sljedeća polja osnovne ekstenzije X.509 se koriste

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

- Sertifikati TSP-a sadrže sljedeće kritične ekstenzije:

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

- Korisnički i sertifikati 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 sertifikata i parova ključeva
certificatePolicies:		Politika sertifikacije 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

7.1.2.1. Ekstenzije privatnih sertifikata

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

7.1.3. 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

7.1.4. Oblici naziva

- U sve sertifikate koje izdaje IDDEEA CA se upisuje puno prepoznatljivo ime sertifikacionog tijela i subjekta sertifikata u polja ime izdavaoca odnosno ime korisnika. Kodiranje tih imena se vrši u UTF8 string ili PrintableString formatu.

7.1.5. Ograničenja imena

- Nije primjenjivo.

7.1.6. Identifikator objekta politike sertifikacije

- Svi sertifikati koje izdaje TSP sadrže OID politike sertifikacije po kojoj se izdaje sertifikat. OID za svaki sertifikat je definisan u odjeljku 1.2 Naziv dokumenta i identifikacija.

7.1.7. Upotreba "Policy Constraints" ekstenzija

- Nije primjenjivo.

7.1.8. Sintaksa i semantika kvalifikatora politike

- Kvalifikatori politike se koriste u skladu sa RFC5280.

7.1.9. Semantika procesiranja kritične ekstenzije "Certificate Policies"

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

7.2. Profil spiska opozvanih sertifikata

7.2.1. Broj verzije sertifikata

- TSP izdaje spiskove opozvanih sertifikata 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 sertifikata
Izdavalac	Određeno ime CA
thisUpdate	Datum izdavanja spiska opozvanih sertifikata
nextUpdate	Datum narednog izdavanja spiska opozvanih sertifikata
revokedCertificate	Serijski brojevi opozvanih sertifikata

7.2.2. CRL i CRL "entry" ekstenzije

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

7.3. OCSP profil

- Profil OCSP koji se koristi definisan je u RFC 6960.

7.3.1. Broj verzije sertifikata

- 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 sertifikata.

8. REVIZIJA USKLAĐENOSTI I DRUGA OCJENJIVANJA

8.1. Učestalost ili uslovi ocjenjivanja

- Reviziju usklađenosti IDDEEA CA sa relevantnim zakonima se vrši u skladu sa Zakonom o elektronskom potpisu i drugim važećim zakonskim propisima Bosne i Hercegovine.
- IDDEEA CA sprovodi obavezne interne revizije najmanje jednom godišnje.

8.2. Identitet/kvalifikacije procjenjivača (interna revizija)

- Interni revizor je zaposlen u IDDEEA CA, sa odgovarajućim informacionim znanjem i iskustvom u reviziji.
- Nezavisnog eksternog revizora angažuje nadležna nezavisna kompanija koja ispunjava odgovarajuće domaće i međunarodne standarde i pravila prakse.
- Interni i eksterni revizor treba da ispunjavaju sljedeće uslove:
- Značajno iskustvo u primjeni PKI i kriptografske tehnologije
- Iskustvo u radu sa aplikacijom TSP-a
- Iskustvo u obavljanju aktivnosti sertifikacije ili revizije sistema informacionih tehnologija

8.3. Odnos revizora s predmetom revizije

- Interni ili eksterni revizor ne smije biti u sukobu interesa, odnosno treba biti nezavisan od TSP-a.

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

- IDDEEA CA 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 IDDEEA CA 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 sertifikata

- IDDEEA CA će naplaćivati svoje usluge PKI sertifikacije. Cjenovnik će biti objavljen na web-sajtu TSP-a.

9.1.2. Naknade za pristup sertifikatu

- Pogledati odjeljak 9.1.1 Naknade za izdavanje ili obnovu sertifikata.

9.1.3. Naknade za opoziv i pristup informacijama o statusu sertifikata

- Pogledati odjeljak 9.1.1 Naknade za izdavanje ili obnovu sertifikata.

9.1.4. Naknade za ostale usluge

- Pogledati odjeljak 9.1.1 Naknade za izdavanje ili obnovu sertifikata.

9.1.5. Povrat naknade

- Podnosioci zahtjeva za sertifikate mogu besplatno otkazati zahtjev za sertifikat prije izdavanja aktivacionih kodova. Nikakve naknade neće biti vraćene nakon što se isporuče aktivacioni kodovi, izdaju sertifikate ili softver bude isporučen ili instaliran.

9.2. Finansijska odgovornost

9.2.1. Pokrivanje osiguranja

- IDDEEA CA ima osiguranje u okviru osiguranja opšte odgovornosti i odgovornosti za proizvode, uključujući pokriće čistog finansijskog gubitka, što je uobičajeno za osnovnu delatnost. Ograničenja pokrića su u skladu sa zakonodavstvom Bosne i Hercegovine.

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 sertifikata.

9.3. Zaštita ličnih podataka

- Svi lični podaci dostavljeni IDDEEA CA ili njenim ovlaštenim predstavnicima čuvaće se u skladu sa zahtjevima propisanim Zakonom o zaštiti ličnih podataka Bosne i Hercegovine. Objavljivanje navedenih informacija treba biti samo u skladu sa Zakonom o zaštiti ličnih podataka, Politikom zaštite ličnih podataka IDDEEA CA ili u skladu sa drugim važećim propisom.

9.3.1. Opseg povjerljivih informacija

- Sve informacije koje prikuplja, generiše, prenosi ili čuva IDDEEA CA 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 sertifikata IDDEEA CA, spiska opozvanih sertifikata, Politike sertifikacije i druge informacije objavljene u javnom repozitoriju CA se ne smatraju povjerljivim informacijama.

9.3.3. Odgovornost za zaštitu poverljivih informacija

- IDDEEA CA je odgovorna za zaštitu povjerljivih informacija u skladu sa Politikom zaštite ličnih podataka IDDEEA CA 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 sertifikata ili korisnika, a koje nisu objavljene u sertifikatu koji izdaje IDDEEA CA, spisku opozvanih sertifikata ili javnom LDAP direktoriju se smatraju povjerljivim.

9.4.3. Informacije koje se ne smatraju privatnim

- Sve informacije koje su sadržane u sertifikatu koji izdaje IDDEEA CA, spisku opozvanih sertifikata 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

- IDDEEA CA će koristiti private 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

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

9.4.7. Druge okolnosti za otkrivanje informacija

- IDDEEA CA će otkriti privatne informacije samo u okolnostima utvrđenim Politikom zaštite ličnih podataka IDDEEA CA, Zakonom o zaštiti ličnih podataka Bosne i Hercegovine i drugim relevantnim zakonima, na zahtjev suda ili drugog legitimnog 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

- IDDEEA CA će izdavati sertifikate, provoditi ostale procedure upravljanja sertifikatima i upravljati infrastrukturom CA u skladu sa Politikom sertifikacije i važećim zakonima. TSP je odgovoran za usklađivanje sa procedurama navedenim u ovoj politici, čak i kada funkcionalnost TSP-a preuzima RA ili podizvođači.

- Ukratko, neeksluzivna lista obaveza IDDEEA CA je:
  - Izdavanje Politike sertifikacije
  - obezbijediti procedure korisnicima sertifikata za podnošenje zahtjeva za dobijanje sertifikata;

- Izdavanje ključeva i sertifikata u skladu da aktivnostima definisanim u ovoj Politici, bezbjedno upravljanje privatnim ključevima sertifikacionih tijela IDDEEA CA CA i distribucija javnih ključeva IDDEEA CA CA
- odobravanje ili odbijanje zahtjeva korisnika sertifikata;
- potpisivanje i izdavanje sertifikata u formatu X.509 sa javnim ključevima nosioca kao odgovor na odobrene zahtjeve za sertifikate;
- objavljivanje X.509 sertifikata u direktorijima;
- opoziv sertifikata, uključujući objavljivanje spiska opozvanih sertifikata;
- utvrđivanje identiteta korisnika aplikacije koji podnose zahtjev za izdavanje sertifikata, za obnovu sertifikata ili zahtjeve za novi sertifikat u slučaju opoziva sertifikata;
- obezbijediti da su osobe zadužene za registraciju odgovarajuće obučene i da djeluju u skladu sa pravilima koja se na njih primjenjuju u ovoj politici;
- osigurati da su krajnji korisnici upoznati i saglasni da prihvate odredbe i uslove za dobijanje ključeva i sertifikata;
- potvrditi rad u skladu sa aktivnostima opisanim u ovoj Politici putem periodičnih revizija poslovanja (najmanje svaka 24 mjeseca);
- zapošljavanje lica koja, pored opštih uslova za zapošljavanje, ispunjavaju i posebne uslove propisane Zakonom o elektronskom dokumentu, elektronskoj identifikaciji i povjerljivim uslugama
- osigurati da su informacije o korisniku i TSP-u koje su sadržane u sertifikatima tačne;
- dokazivanje identiteta podnosioca zahtjeva prije izdavanja sertifikata;
- obezbijediti tačnost i integritret informacija objavljenih u LDAP direktoriju ili drugom repozitoriju;
- omogućiti pristup on-line javnom direktoriju;
- izdavanje sertifikata odobrenim podnosiocima zahtjeva u skladu sa ovom Politikom sertifikacije;
- opoziv sertifikata koje je izdao CA, po prijemu valjanog zahtjeva za to, ili u skladu sa ovom Politikom sertifikacije;
- izdavanje i objavljivanje spiska opozvanih sertifikata (CRL);
- Održavanje OCSP usluge;
- Obezbijediti da su registraciona tijela upoznata sa odredbama koje se na njih odnose u ovoj Politici sertifikacije.

9.6.2. Odgovornosti i obaveze registracionog tijela (RA)

- RA je odgovorno za tačnost i potpunost informacija korisnika o odobrenim obrascima za prijavu. Detaljne obaveze RA su navedene u relevantnim odjeljcima ove Politike sertifikacije.

9.6.3. Korisničke odgovornosti i obaveze

- Korisnik preuzima punu odgovornost za upotrebu privatnog ključa povezanog sa javnim ključem u sertifikatu pri čemu je vlasnik fizičko lice identifikovano privatnim ključem.
- Kada se sertifikati izdaju licu za ličnu upotrebu, korisnik i vlasnik čine jedno te isto lice.
- Prije izdavanja ključeva i sertifikata, korisnici zaključuju ugovor sa IDDEEA CA, uzimajući u obzir pravila i uslove korištenja.
- Korisnici su odgovorni da:
  - Budu potpuno svjesni svojih dužnosti i odgovornosti kao što je navedeno u relevantnoj dokumentaciji koja je gore navedena, kao i pravila po kojima se sertifikati izdaju;
  - U roku od pet radnih dana od dana prijema pokrenu inicijalni kod koji im šalje IDDEEA CA – upotreba privatnih ključeva za predviđenu svrhu;
  - Kontrolišu pristup računaru, uređaju ili specijalnom hardverskom uređaju koji sadrži privatni ključ za koji su odgovorni;

- Čuvaju šifre koje se koriste za pristup privatnim ključevima;
- Hitno obavijeste IDDEEA CA o svakoj sumnji za kompromitaciju njihovog privatnog ključa.

- Prihvatanjem sertifikata koji izdaje IDDEEA CA, 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 sertifikatu;
  - isključivo koristi svoj sertifikat u zakonite svrhe i ovlaštene svrhe detaljno opisane u odjeljku 1.4 Upotreba sertifikata;
  - odmah obavijesti CA o sumnjivoj ili otkrivenoj kompromitaciji privatnog ključa;
  - odmah obavijesti IDDEEA CA o svakoj sumnji ili poznatoj zloupotrebi bilo kojeg sertifikata izdanog od strane CA.

9.6.4. Obaveze i odgovornosti trećih strana

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

- Treća strana,kojoj je povjeren sertifikat koji izdaje IDDEEA CA je dužna da:
  - Ograniči validnost sertifikata samo u svrhu definisanu u ovom dokumentu;
  - Provjeri validnost sertifikata;
  - Pročita ovaj document i nauči dužnosti, odgovornosi i ograničenja TSP-a;
  - Zatraži opoziv sertifikata ako:
    - Ima saznanja da je privatni ključ kompromitovan tako da utiče na pravilnu upotrebu,
    - Postoji opasnost od zloupotrebe,
    - Postoje promjene u podacima navedenim u sertifikatu.

- Prije preuzimanja sertifikata, odgovornosti trećih strana su:
  - Upoznati sa ograničenjima sertifikata i odgovornostima TSP-a kao što je detaljno opisano u ovoj Politici;
  - ograničiti oslanjanje na sertifikate koje izdaje TSP na odgovarajuću upotrebu kao što je detaljno opisano u odjeljku 1.4 Upotreba sertifikata;
  - obezbijediti da sertifikat nije opozvan pristupom važećim, bilo kojim i svim, primjenjivim spiskovima opozvanih sertifikata (CRL) ili OCSP;
  - odmah obavijestiti IDDEEA CA o svakoj sumnji ili poznatoj zloupotrebi bilo kojeg sertifikata izdatog od strane TSP-a.

9.6.5. Odgovornosti i obaveze drugih učesnika

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

9.7. Nepriznavanje garancija

- Osim garancija navedenih u ovoj Politici sertifikacije i srodnim ugovorima, i u najvećoj mjeri dozvoljenoj zakonom, IDDEEA CA 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 sertifikata-u u skladu sa odeljkom 4.9.6;

- svaku garanciju u pogledu tačnosti ili pouzdanosti bilo koje informacije sadržane u sertifikatima koju ne daje IDDEEA CA;
- odgovornost za predstavljanje informacija sadržanih u sertifikatu;
- svaku garanciju u pogledu ovlaštenja ili statusa bilo koje osobe koja koristi sertifikat IDDEEA CA
- 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

IDDEEA CA 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 sertifikat izdat od IDDEEA CA.

9.9. Naknada štete

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

9.10. Trajanje i prestanak važenja

9.10.1. Trajanje

- Politika sertifikacije IDDEEA CA i drugih dokumenata postaju važeća potvrdom od strane ORGANIZACIJE, i objavljivanja na web-sajtu IDDEEA CA kao što je definisano u odjeljku 2.1. Repozitoriji

9.10.2. Prestanak važenja

- Prestanak važenja Politike sertifikacije IDDEEA CA 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 sertifikacije, kao rezultat objavljivanja nove verzije, sertifikat će se koristiti u skladu sa onom verzijom Politike sertifikacije koja je bila važeća na dan izdavanja sertifikata. U slučaju da se okolnosti promijene u mjeri u kojoj to nije moguće, IDDEEA CA 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

- IDDEEA CA distribuiše trenutnu verziju ove Politike sertifikacije 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 IDDEEA CA 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

- IDDEEA CA može odlučiti da li će obavijestiti korisnike i treće strane u slučaju izmjena sa malim ili bez uticaja. IDDEEA CA odlučuje da li izmjene imaju uticaj na korisnike i treće strane prema vlastitom nahođenju.
- Sve promjene Politike sertifikacije će biti objavljene kao što je opisano u odjeljku 2. ODGOVORNOSTI OBJAVLJIVANJA I REPOZITORIJA. IDDEEA CA 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 sertifikacije će se izmijeniti u slučaju kada izmjene utiču na korisnike ili treće strane.

9.13. Postupak rješavanja sporova

- Svi sporovi vezani za poslovanje sa sertifikatima upućuju se pisanim putem IDDEEA CA 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 sertifikacije i odnos između TSP-a, RA, korisnici, subjekti (nosioci sertifikata) i druge treće strane podliježu i tumačiće se u skladu sa zakonima Bosne i Hercegovine.

9.15. Usklađenost sa važećim propisima

- Zakon o zaštiti ličnih podataka
- Zakon o elektronskim dokumentima, elektronskoj identifikaciji i povjerljivim uslugama i podzakonski akti usvojeni na osnovu pomenutog Zakona.
- Drugi relevantni propisi

9.16. Ostale odredbe

9.16.1. Kompletan ugovor

- Politika sertifikacije IDDEEA CA i ugovor IDDEEA CA sa krajnjim korisnikom navode sve relevantne odredbe o odnosu između IDDEEA CA i nosilaca IDDEEA CA javnih sertifikata.

9.16.2. Dodjeljivanje

- Korisnicima i nosiocima sertifikata 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 sertifikata i korišćenje sertifikata).

9.16.4. Izvršenje (advokatske naknade i odricanje od prava)

- Nije primjenjivo

9.16.5. Vlša 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.

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

9.17. Ostale odredbe

Nije primjenjivo