Na temelju člana 45. Statuta "JP BH POŠTA" d.o.o. Sarajevo, člana 26. Zakona o organizaciji organa uprave u Federaciji Bosne i Hercegovine (objavljenog u "Službenim novinama Federacije BiH" broj 35/05), Zakona o elektronskom potpisu (objavljenog u "Službenim novinama BiH" broj 91/06), te članka 5., stavka (3), pod tačke b) Pravilnika o bližim uvjetima za izdavanje kvalificiranih potvrda (objavljenog u "Službenim novinama BiH" broj 14/17), u skladu s Odlukom Vlade Federacije BiH broj 29/2014 od 09.01.2014. godine o privremenom rješenju arhitekture PKI infrastrukture na nivou Federacije BiH ("Službene novine Federacije BiH" broj 5/14), Uprava Društva donosi dokument na 258. sjednici održanoj dana 01.12.2023. godine.

PRAKTIČNA PRAVILA PRUŽANJA USLUGE OVJERAVANJA OVJERIOCA „JP BH POŠTA“ d.o.o. Sarajevo

Datum stupanja na snagu: 10.01.2025.
OID Dokumenta: 1.3.6.1.4.1.59867.10.1.2.1.1.

Informacije o dokumentu

Naziv dokumenta:	Praktična pravila pružanja usluge ovjeravanja Ovjerioca „JP BH POŠTA“ d.o.o. Sarajevo
OID dokumenta:	1.3.6.1.4.1.59867.10.1.2.1.1.
Tip dokumenta:	Pravilnik o postupcima certificiranja (*Certification Practice Statement*, CPS)

Istorija izmjena

Verzija	Datum	Razlog izmjene
1.0	30.11.2023	Inicijalna verzija
1.1	10.01.2025	Korigovanje štamparskih grešaka i jezično usklađivanje

Sadržaj

1. UVOD

„JP BH POŠTA“ d.o.o. Sarajevo (u nastavku teksta: JP BH POŠTA) je uspostavila infrastrukturu javnih kriptografskih ključeva - Public Key Infrastructure – PKI i djeluje kao ovjerilac u skladu s Zakonom o elektronskom potpisu („Službeni glasnik BiH“, broj: 91/06). Kao ovjerilac, JP BH POŠTA pruža usluge izdavanja kvalificiranih elektronskih potvrda i upravljanja njihovim životnim ciklusom, kao i izdavanja kvalificiranih elektronskih vremenskih žigova pod imenom: Ovjerilac JP BH POŠTA.

Ovjerilac JP BH POŠTA izdaje kvalificirane elektronske potvrde u skladu s relevantnim zakonima, općim aktima i smjernicama koje uređuju ovu oblast. Zakoni i podzakonski akti koji čine pravni okvir za izdavanje kvalificiranih elektronskih potvrda Ovjerioca JP BH POŠTA uključuju:

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

Opća pravila rada Ovjerioca JP BH POŠTA detaljno su opisana u dokumentima:

- Politika ovjeravanja Ovjerioca (Certification Policy - CP).
- Praktična pravila pružanja usluge ovjeravanja Ovjerioca (Certification Practices Statement - CPS).

Praktična pravila pružanja usluge ovjeravanja Ovjerioca, u daljem tekstu nazivana Praktična pravila, predstavljaju javni dokument koji precizira proces pružanja usluge ovjeravanja i način njihove primjene u izdavanju i upravljanju kvalificiranim elektronskim potvrdama i elektronskim vremenskim žigovima. Ova dokumentacija također obuhvata operativne procedure koje Ovjerilac JP BH POŠTA primjenjuje kako bi zadovoljio postavljene zahtjeve, uključujući tehničke, organizacijske i proceduralne zahtjeve navedene u Politici ovjeravanja, kao i način korištenja elektronskih potvrda i pečata od strane korisnika.

Ovaj dokument opisuje cijeli životni ciklus kvalificiranih elektronskih potvrda izdanih od strane Ovjerioca JP BH POŠTA. Politika ovjeravanja i Praktična pravila su javni dokumenti koji se objavljuju na službenoj web stranici Ovjerioca JP BH POŠTA.

Osim navedene dokumentacije, na službenoj web stranici Ovjerioca JP BH POŠTA dostupni su i sljedeći materijali za korisnike i zainteresirane strane:

- Zahtjev za korištenje usluga ovjerioca za izdavanje kvalificiranih elektronskih potvrda,
- Ugovor o pružanju usluga ovjerioca za izdavanje kvalificiranih elektronskih potvrda,
- Zahtjev za izdavanje i korištenje kvalificirane elektronske potvrde za fizička lica,
- Zahtjev za izdavanje i korištenje kvalificirane elektronske potvrde za fizička lica u pravnom licu
- Ugovor o izdavanju i korištenju kvalificirane elektronske potvrde za fizičko lice,
- Ugovor o izdavanju i korištenju kvalificirane elektronske potvrde za fizičko lice u pravnom licu,
- Zahtjev za promjenu statusa kvalificiranih elektronskih potvrda,
- Korisnička uputstva,
- Ostali dokumenti povezani s radom Ovjerioca JP BH POŠTA.

Ovjerilac JP BH POŠTA također donosi Posebna interna pravila rada i zaštite sistema ovjeravanja (u daljnjem tekstu: Posebna pravila) kao interni dokumenti koji čuvaju poslovnu tajnu JP BH POŠTA.

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

1.1. Pregled

JP BH POŠTA, u svojoj infrastrukturi za izdavanje kvalificiranih potvrda, koristi sljedeće servere:

1. Korijenski ovjerilac: "JP BH POŠTA Root CA".
2. Podređeni ovjerilac za izdavanje potvrda koji je potpisan od strane "JP BH POŠTA Root CA": "JP BH POŠTA Issuing CA".

"JP BH POŠTA Root CA" server služi kao najviši ovjerilac i koristi samopotpisanu potvrdu (self-signed certificate) koja je generisana tokom ceremonije generisanja korijenskog kriptografskog ključa aplikacije Ovjerioca (Root Key Generation Ceremony). Ovaj server izdaje potvrde "JP BH POŠTA Issuing CA" Ovjeriocu u okviru infrastrukture JP BH POŠTA.

"JP BH POŠTA Issuing CA" server, koji je podređeni ovjerilac, izdaje kvalificirane elektronske potvrde fizičkim licima i fizičkim licima povezanim s pravnim licima. Osim toga, izdaje administrativne potvrde koje odražavaju uloge zaposlenika u JP BH POŠTA, također izdaje kvalificirane vremenske žigove.
CRL (Certificate Revocation List) lista se redovno izdaje svakih 24 sata, a njezina valjanost traje 3 dana.
Sistemskim administratorima izdaju se potvrde za potrebe administriranja "JP BH POŠTA Issuing CA" JP BH POŠTA servera.

Sve ove aktivnosti odvijaju se u potpunom skladu s Politikom ovjeravanja i Praktičnim pravilima koja su obvezujuća za Ovjerioca JP BH POŠTA, za osobe kojima je Ovjerilac JP BH POŠTA izdao kvalificiranu elektronsku potvrdu i za treća lica koja se oslanjaju na potvrde izdane od strane Ovjerioca JP BH POŠTA.
Korisnici kvalificiranih elektronskih potvrda Ovjerioca JP BH POŠTA posjeduju par kriptografskih ključeva, uključujući javni i privatni ključ. Privatni kriptografski ključ koristi se za kvalificirano elektronsko potpisivanje, dok se javni kriptografski ključ koristi za provjeru kvalificiranog elektronskog potpisa.

1.1.1. Profili potvrda Ovjerioca JP BH POŠTA

1.1.1.1. Tipovi potvrda koje izdaje Ovjerilac JP BH POŠTA

JP BH POŠTA potvrda korijenskog ovjerioca - JP BH POŠTA ROOT CA	
Naziv tipa potvrde	**Područje primjene potvrde**
Potvrda JP BH pošta korijenskog ovjerioca (JP BH POŠTA ROOT CA)	Izdavanje ca potvrda podređenom ovjeriocu, izdavanje CRL JP BH POŠTA
Potvrda JP BH POŠTA podređenog ovjerioca (JP BH POŠTA ISSUING CA)	Izdavanje korisničkih potvrda za fizička lica i fizčka lica povezana sa pravnim licima, potvrda za JP BH POŠTA servis izdavanja kvalificiranih vremenskih žigova, potpisivanje pripadajućih CRL. OID POLITIKE OVJERAVANJA: 1.3.6.1.4.1.59867.10.1.2

Tabela 1. Tipovi potvrda koje izdaje Ovjerilac JP BH POŠTA

1.1.1.2. Tipovi potvrda koje izdaje ovjerilac JP BH POŠTA Issuing CA

Popis tipova potvrda koje izdaje ovjerilac JP BH POŠTA ISSUING CA		
Naziv grupe	**Naziv tipa potvrde**	**Područje primjene potvrde**
Potvrde za fizička lica	JP BH POŠTA kvalificirana potvrda za elektronski potpis za fizička lica	Izdaje se fizičkim licima za izradu kvalificiranog elektronskog potpisa.
	OID politike ovjeravanja	1.3.6.1.4.1.59867.10.2.1.10.1.1
Potvrde za fizička lica povezane s pravnim licima	JP BH POŠTA kvalificirana potvrda za elektronski potpis za fizičke lica povezana sa pravnim licima	Izdaje se fizičkim licima povezanim s poslovnim licima za izradu kvalificiranog elektronskog potpisa koji će se koristiti u poslovne svrhe.
	OID politike ovjeravanja	1.3.6.1.4.1.59867.10.2.1.11.1.1
Potvrde za zaposlene	Kvalificirana potvrda za elektronski potpis za zaposlene	Izdaje se zaposlenima za izradu kvalificiranog elektronskog potpisa.
	OID politike ovjeravanja	1.3.6.1.4.1.59867.10.2.2.11.1.1
Potvrda za elektronski pečat	*KVALIFICIRANA POTVRDA ZA ELEKTRONSKI PEČAT*	Izdaje se pravnim licima za izradu kvalificiranog elektronskog pečata.
	OID politike ovjeravanja	1.3.6.1.4.1. 59867.10.2.1.12.1.1

Kvalificirani vremenski žigova	*Kvalificirana potvrda za vremenski žig*	Izdaje se pravnim licima za izradu kvalificiranog vremenskog žiga
	OID politike ovjeravanja	1.3.6.1.4.1. 59867.10.2.1.13.1.1

Tabela 2. Tipovi potvrda koje izdaje ovjerilac *JP BH POŠTA Issuing CA*

Osnovni podaci o CA potvrdama Ovjerioca JP BH POŠTA

1.1.1.2.1. Osnovni podaci o potvrdi JP BH POŠTA Root CA

JP BH POŠTA potvrda korijenskog ovjerioca - JP BH POŠTA ROOT CA		
Osnovna polja		
Polje	**Atribut**	**Vrijednost**
Issuer	commonName (CN)	BHP-RootCA
	organizationName (O)	JP BH POSTA doo
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 20 godina
Subject	commonName (CN)	BHP-RootCA
	organizationName (O)	JP BH POSTA doo
	countryName (C)	BA
SHA 256 thumbprint: 7BF9B84E1F8E57D58490783B07C88EE81134CAE796FD1F3A48A8ECCA066DC045 SHA 1 thumbprint: DBAAD3FDFC7A8E2F1E20CE09636A17B4711F7BFB		

Tabela 3 Osnovni podaci o potvrdi *JP BH POŠTA Root CA*

1.1.1.2.2. Osnovni podaci o potvrdi JP BH POŠTA Issuing CA

JP BH POŠTA potvrda podređenog ovjerioca-JP BH POŠTA ISSUING CA		
Osnovna polja		
Polje	**Atribut**	**Vrijednost**
Issuer	commonName (CN)	BHP-RootCA
	organizationName (O)	JP BH POSTA doo
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 15 godina
Subject	commonName (CN)	BHP-SubCA
	organizationName (O)	JP BH POŠTA
	countryName (C)	BA
Kvalificirane elektronske potvrde izdate do 18.09.2024. godine potpisane su sa potvrdom: SHA 256 thumbprint: 4AE1894AA02A5ABC24E9AA206912D08E7957D457FE78273D8E8A2D0B3FE739C3 SHA 1 thumbprint: 054D583910AB1729C30325BD155E289E9B77F9DA		
Kvalificirane elektronske potvrde izdate poslije 18.09.2024. godine potpisane su sa potvrdom: SHA 256 thumbprint: 2BCA9CDC4E087172E324986AC6F32E4762542A7007741D84DBE56F1A11337C58 SHA 1 thumbprint: 74F17A95262AF433B0F2816D185BA3EB9CD5DB72		

Tabela 4. Osnovni podaci o potvrdi *JP BH POŠTA Issuing CA*

1.2. Naziv i identifikacija dokumenta

Ovaj dokument nosi naziv "Praktična pravila pružanja usluge ovjeravanja ovjerioca u okviru JP BH POŠTA", kako je naznačeno na početnoj stranici dokumenta.

Organizacija IANA (Internet Assigned Numbers Authority) dodijelila je JP BH POŠTA d.o.o. Sarajevo OID 1.3.6.1.4.1.59867. JP BH POŠTA d.o.o. Sarajevo je temeljem tog OID-a dodijelila Ovjeriocu JP BH POŠTA OID 1.3.6.1.4.1.59867.10. Identifikacioni broj ovog dokumenta (OID) je 1.3.6.1.4.1.59867.10.1.2.1.0.

OID	**Objašnjenje**
1.3.6.1.4.1.59867	Jedinstveni identifikacioni broj dodijeljen JP BH POŠTA od strane organizacije IANA
1.3.6.1.4.1.59867.10	Jedinstveni identifikacioni broj Ovjerioca JP BH POŠTA dodijeljen od strane JP BH POŠTA
1.3.6.1.4.1.59867.10.1	Jedinstveni identifikacioni broj dodijeljen za dokumente Ovjerioca JP BH POŠTA
1.3.6.1.4.1.59867.10.2.1	Jedinstveni identifikacioni broj dodijeljen za potvrde Ovjerioca JP BH POŠTA

Tabela 5. Jedinstveni identifikacioni brojevi Ovjerioca JP BH POŠTA

Dokumenti	**Vrsta dokumenta**	**Verzija**	**Podverzija**
1.3.6.1.4.1.59867.10.1	1 za CP	1 za početnu verziju	0 za početnu podverziju
	2 za CPS	1 za početnu verziju	0 za početnu podverziju

Tabela 6. Struktura jedinstvenih identifikacionih brojeva dokumenata Ovjerioca JP BH POŠTA

Nepromjenjivi dio *OID*-a politike ovjeravanja	**Ovjerilac potvrde**	**Skupina profila potvrde**	**Profil potvrde**	**Način čuvanja privatnog ključa**
1.3.6.1.4.1.59867.10.1	0 – *JP BH POŠTA Root CA*	Skupine potvrda	Oznaka profila potvrde unutar skupine potvrda.	Način čuvanja privatnog ključa odgovara na pitanje da li

	1 – *JP BH POŠTA Issuing CA*	su definisane prema namjeni potvrda i Njihovim korisnicima. Oznake skupina potvrda su sljedeće: 10 - potvrde za fizička lica 11 - potvrde za fizička lica povezana sa pravnim licima 12 - potvrde za elektronski pečat	Vrijednost oznake profila potvrde počinje od broja 1.	se privatni ključ čuva na kriptografskom uređaju. Moguće vrijednosti su sljedeće: 0 privatni ključ povezan sa potvrdom se ne čuva u kriptografskom uređaju 1 privatni ključ povezan sa potvrdom se čuva u kriptografskom uređaju

Tabela 7. Struktura jedinstvenih identifikacionih brojeva potvrda Ovjerioca JP BH POŠTA

1.3. Učesnici PKI sistema

Učesnici PKI sistema su:

1. Ovjerilac JP BH POŠTA ,
2. Korisnici usluga,
3. Treća lica,
4. Ostali učesnici.

Ovjerilac JP BH POŠTA

Ovjerilac JP BH POŠTA sa sastoji od tri jedinice:

1. Tijelo za upravljanje radom (PMA – Policy Management Authority)
2. Tijelo za operativne poslove (OA – Operations Authority) i
3. Registracijsko tijelo (RA – Registration Authority).

Tijelo za upravljanje radom (PMA – Policy Management Authority)

Članovi Tijela za upravljanje radom
su:

1) Voditelj CA (predsjednik tijela)
2) Voditelj tijela za operativne poslove
3) Voditelj registracijskog tijela
4) Stručni saradnik za pravne poslove

Voditelj CA u slučaju odsustva imenuje nekog od članova Tijela kao zamjenika (vršioca dužnosti

Voditelja CA) tokom odsustva.

Zadaci ovog Tijela su:

- razvoj i održavanje pravila rada usluga povjerenja (CP/CPS)
- razvoj i održavanje ostalih relevantnih javnih dokumenata (javno dostupne informacije, ugovori, formular)
- praćenje poštivanja pravila rada Ovjerioca JP BH POŠTA
- praćenje relevantnog zakonodavstva
- rješavanje sporova između subjekata u okviru Ovjerioca JP BH POŠTA
- zaprima i obrađuje izvještaje o procjeni rada (audita)
- da kvartalno prikupi izvještaje o performansama servisa na osnovu kojih će donositi odluke o unaprjeđenju istih
- opoziv certifikata korisnika u slučajevima kada zahtjev za opoziv nije podnio korisnik, nadležni sud ili drugo nadležno tijelo ili pravni sljedbenik korisnika

Tijelo za operativne poslove (OA – Operations Authority)

Tijelo za operativne poslove je zaduženo za upravljanje i održavanje IKT infrastukture - hardverskih i softverskih komponenti CA rješenja.

Pored Voditelja tijela za operativne poslove, isti sačinjavaju sljedeći članovi:

- Zamjenik voditelja
- Mrežni administrator
- Sistemski administrator
- Administrator baze podataka
- Administrator aplikativnih CA rješenja
- HSM operater
- Inženjer za informacijsku sigurnost
- Helpdesk operater (min. 2 izvršioca)

Ova organizaciona jedinica unutar Ovjerioca JP BH POŠTA odgovorna je za pravilan rad opreme i softvera, posebno u vezi s izdavanjem elektronskih potvrda. Također, njihova odgovornost obuhvata kreiranje, potpisivanje i izdavanje potvrda, upravljanje trajanjem tih potvrda te, na kraju, povlačenje potvrda kada je to potrebno. Sve ove aktivnosti provode se u skladu s Praktičnim pravilima. Poslovni procesi opisani su načelno u Praktičnim pravilima, dok su detaljnije propisani internim pravilnicima Ovjerioca JP BH POŠTA.

Registracijsko tijelo (RA – Registration Authority)

Zadaci Registracijskog tijela su provjera identiteta naručilaca odnosno korisnika certifikata, obrada zahtjeva i odobrenje ili odbijanje zahtjeva za izdavanje, suspenziju ili opoziv certifikata.

Pored Voditelja registracijskog tijela, isti sačinjavaju sljedeći članovi:

- Zamjenik voditelja
- Kontrolori (veći broj izvršilaca)
- Šalterski radnici – operateri (veći broj izvršilaca)

Korisnici

Korisnici usluga Ovjerioca JP BH POŠTA su:

1. Fizičko lice, koje se identifikuje specifičnim atributima,
2. Fizičko lice koje je zaposleno u pravnom licu,
3. Pravno lice,
4. Zaposleni Ovjerioca JP BH POŠTA .

Ako Ovjerilac JP BH POŠTA ovjerava elektronsku potvrdu za fizičko lice koje je zaposleno u pravnom licu, tada će se unutar atributa koji identificiraju korisnika nalaziti i informacije koje označavaju ime tog pravnog lica.

Subjekti ovjeravanja

Subjekt koji se potvrđuje u dokumentu identificiran je kao subjekt i posjeduje privatni ključ koji je povezan s javnim ključem sadržanim u potvrdi.

U potvrdama koje izdaje Ovjerilac JP BH POŠTA, subjekti ovjeravanja su kako slijedi:

- U ličnim potvrdama za elektronski potpis, subjekt je fizičko lice.
- U poslovnim potvrdama za elektronski potpis, subjekt je fizičko lice koje je povezano s pravnim licem.
- U kvalificiranim potvrdama za elektronski pečat, subjekt je pravno lice.

Treća lica

Treća lica su subjekti koji koriste elektronske potvrde izdate od Ovjerioca JP BH POŠTA kao sredstvo za provjeru elektronskog potpisa i identiteta korisnika.

Treća lica mogu provjeriti status opozvanosti elektronskih potvrda putem registra opozvanih potvrda - CRL (Certificate Revocation List) Ovjerioca JP BH POŠTA, koji se redovno ažurira svaki dan.

CRL lista se generiše svakih 24 sata, a njen period važenja iznosi 3 dana.

Treća lica trebaju redovno provjeravati najnovije dostupne CRL registre opozvanih potvrda kako bi imala tačne i pravovremene informacije o opozivu i suspenziji potvrda.

Nikada se ne bi smjelo oslanjati na CRL registar opozvanih potvrda duže od maksimalnog perioda važenja te liste.

Ostali učesnici

Ostali subjekti su pravna lica koja na bilo koji način doprinose ili sudjeluju u osiguravanju kvalitete rada Ovjerioca JP BH POŠTA i pružanju usluga ovjeravanja. Ova kategorija obuhvaća proizvođače i distributere opreme i softvera, proizvođače, osiguravajuća društva i druge sudionike.

1.4. Upotreba potvrda

Područje primjene

Potvrda JP BH POŠTA Root CA koristi se za sljedeće svrhe:

- Izdavanje potvrda za podređenog Ovjerioca (JP BH POŠTA Issuing CA).
- Izdavanje registra opozvanih potvrda (CRL).

Potvrde od strane podređenog Ovjerioca JP BH POŠTA Issuing CA koriste se za:

- Izdavanje korisničkih potvrda.
- Izdavanje registra opozvanih potvrda (CRL).
- Izdavanje potvrda za JP BH POŠTA servis izdavanja kvalificiranih elektronskih žigova.

Područje primjene potvrda od Ovjerioca JP BH POŠTA, koje su izdane od strane certifikacijskog tijela JP BH POŠTA Issuing CA, uključuje:

- Izradu kvalificiranog elektronskog potpisa.
- Izradu kvalificiranog elektronskog pečata.
- Potpisivanje kvalificiranih vremenskih žigova od strane servisa za izdavanje kvalificiranih vremenskih žigova.

Privatni kriptografski ključevi pridruženi kvalificiranim elektronskim potvrdama koriste se u postupku kvalificiranog elektronskog potpisivanja elektronskih dokumenata. Ovaj postupak može se primjenjivati u komunikaciji između imaoca kvalificiranih elektronskih potvrda. Također, koristi se u pravnim poslovima i drugim pravnim radnjama te u upravnim, sudskim i drugim postupcima pred državnim organima i drugim institucijama, pod uvjetom da je Zakonom koji uređuje taj postupak propisana upotreba kvalificiranog elektronskog potpisa.

Kvalificirane elektronske potvrde služe kao potvrda veze između javnog kriptografskog ključa korisnika i identiteta tog korisnika koji je izvršio kvalificirano potpisivanje elektronskog dokumenta.

Nedozvoljene primjene

Svaka druga upotreba ovlaštenog elektronskog potvrđivanja koja nije precizno navedena u ovom dokumentu i nije u skladu s odredbama Zakona o elektronskom potpisu i drugim relevantnim propisima koji reguliraju ovu oblast strogo je zabranjena.

1.5. Politika administriranja dokumenta

Organizacija upravljanja dokumentom

Dokument Praktična pravila kreira i ažurira Ovjerilac JP BH POŠTA :

Adresa:

„JP BH POŠTA“ d.o.o. Sarajevo
Obala Kulina bana 8
71000, Sarajevo
Bosna i Hercegovina

Kontakt:

Telefon: +387 33 252 613
Faks: +387 33 252 743
e-mail: kabinet@posta.ba
web: www.posta.ba

Tekuću verziju i prethodne verzije dokumenta moguće je preuzeti sa web stranice Ovjerioca JP BH POŠTA dijelu *Dokumentacija* www.posta.ba/e-potpis/dokumentacija

Lica za kontakt

Lica koja se mogu kontaktirati radi ovjere JP BH POŠTA su Voditelj CA JP BH POŠTA, zaposlenici koji pružaju tehničku podršku te drugi zaposlenici ovlašteni za pružanje informacija u vezi primjene Praktičnih pravila i drugih akata JP BH POŠTA, u skladu s odgovarajućim procedurama i općim aktima JP BH POŠTA.

Kontakt informacije za osobe navedene u prethodnom paragrafu dostupne su na službenoj web stranici JP BH POŠTA.

Lica određena za usklađivanje dokumenta sa praksom izdavanja potvrda

Tijelo za upravljanje radom (PMA – Policy Management Authority) JP BH POŠTA usklađuje oblik i sadržaj ovih Praktičnih pravila sa eventualnim promjenama koje se mogu pojaviti u praksi izdavanja elektronskih potvrda.
Osim toga, Tijelo za upravljanje radom (PMA – Policy Management Authority) JP BH POŠTA redovno provjerava usklađenost ovih Praktičnih pravila sa trenutno važećim zakonima.

Procedure za odobrenje Praktičnih pravila

Nakon izmjene zakonskih propisa, poslovni proces vezan za izdavanje kvalificiranih potvrda ili bilo kakvih drugih promjena koje utječu na postupke u Praktičnim pravilima podložan je reviziji i usklađivanju od strane Tijela za upravljanje radom (PMA - Policy Management Authority) u JP BH POŠTA. Nakon što se proces usklađivanja provede, predsjednik tog tijela odobrava novo izdanje Praktičnih pravila i podnosi ga nadležnom organu na usvajanje.

Sve promjene ili dopune Praktičnih pravila moraju biti izvedene u skladu s odredbama Zakona o elektronskom potpisu, podzakonskim aktima i relevantnom praksom te podliježu odobrenju nadležnog državnog organa.

1.6. Definicije i skraćenice

DEFINICIJA	ZNAČENJE DEFINICIJE
Autentikacija	Elektronski postupak kojim se potvrđuje identitet lica ili izvornost i cjelovitost podataka.
Aplikacija Ovjerioca	Aplikacija na serverima Ovjerioca JP BH POŠTA koja generira i potpisuje elektronske potvrde i registre opozvanih potvrda pomoću kriptografskih ključeva generiranih i pohranjenih u hardverskom kriptografskom modulu.
Aplikacija Registracijskog tijela	*Web* aplikacija koja služi za registriranje korisnika Ovjerioca JP BH POŠTA i obradu njihovih zahtjeva za izdavanje potvrda kao i zahtjeva za promjenu statusa potvrda.
Aplikacija Centralnog sistema	*Web* aplikacija koja omogućava centralizirano praćenje i upravljanje životnim ciklusom kriptografskih uređaja, kreiranje naloga za izdavanje kriptografskih uređaja.
Aktivacijski podaci	Tajni podaci koji se koriste za aktivaciju kriptografskih ključeva u hardverskom kriptografskom modulu ili pristup privatnim ključevima softverskih potvrda. Aktivacijski podatak može biti *PIN*, lozinka ili elektronski ključ.
Autor pečata	Pravno lice koje izrađuje elektronski pečat.
Dešifriranje	Kriptografski proces kojim se šifrirani podaci pretvaraju u razumljive podatke (otvoreni tekst), korištenjem ključa za dešifriranje i algoritma za dešifriranje.
Elektronski dnevnik	Elektronska forma zapisa o provedenim aktivnostima. Log datoteka.

Elektronski dokument	Dokument u elektronskom obliku koji se koristi u poslovnim i drugim radnjama.
Elektronski potpis	Skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektronskom obliku i koji služe za identifikaciju potpisnika i utvrđivanje vjerodostojnosti potpisanog elektronskog dokumenta. Elektronski potpis kreira fizičko lice.
Elektronski pečat	Skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektronskom obliku ili su logički povezani s njima radi osiguranja izvornosti i cjelovitosti tih podataka. Elektronski pečat kreira pravno lice.
Elektronski vremenski žig	Skup podataka u elektronskom obliku koji povezuje tačan datum i vrijeme kreiranja tog skupa podataka sa drugim podacima u elektronskom obliku.
Hardverski kriptografski modul (eng. *Hardware security module* – HSM)	Uređaj određenog nivoa sigurnosti koji: ▪ Generira par kriptografskih ključeva, ▪ Štiti kriptografske i druge povjerljive informacije, ▪ Izvršava kriptografske funkcije.
Infrastruktura javnih ključeva (PKI)	Arhitektura, organizacija, hardver, softver, pravila, operativni postupci i procedure koje zajednički podržavaju implementaciju i rad kriptografskog sistema javnog ključa za upravljanje životnim ciklusom elektronskih potvrda.
Javni ključ (eng. *Public Key*)	Javno dostupan kriptografski ključ koji odgovara uparenom privatnom ključu. Javni ključ se može koristiti za provjeru elektronskog potpisa (ako je javno objavljen kao ključ za dešifriranje) ili za šifriranje podatka (ako je javno objavljen kao ključ za šifriranje)
Kompromitiranje privatnog kriptografskog ključa	Narušene sigurnosti kojom se privatni kriptografski ključ izlaže mogućem neovlaštenom pristupu, kao što su neovlašteno otkrivanje, mijenjane ili korištenje.
Korisnik	Fizičko lice koje koristi elektronsku potvrdu izdanu od strane Ovjerioca i čiji se podaci nalaze u potvrdi.
Kvalificirana potvrda za elektronski potpis	Potvrda u elektronskom obliku koja je izdana od strane ovlaštenog Ovjerioca, a koja sadrži podatke predviđene Zakonom o elektronskom potpisu i koja povezuje podatke za verificiranje elektronskog potpisa sa određenim fizičkim licem i potvrđuje identitet tog lica.
Kvalificirani elektronski potpis	Skup podataka u elektronskom obliku koji prate druge podatke u elektronskom obliku ili su sa njima logički povezani. Istim se pouzdano garantira identitet potpisnika (fizičko lice), integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj koji ispunjava uvjete utvrđene zakonom.
Kvalificirani elektronski pečat	Skup podataka u elektronskom obliku koji prate druge podatke u elektronskom obliku ili su sa njima logički povezani. Istim se pouzdano garantira identitet pečatioca (pravno lice), integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj koji ispunjava uvjete utvrđene zakonom.
Kvalificirani elektronski vremenski žig	Elektronski vremenski žig u kojem su navedeni datum i vrijeme zasnovani na izvoru tačnog vremena povezanom s UTC-om i povezani sa podacima

	u elektronskom obliku na način kojim se u razumnoj mjeri isključuje mogućnost nezapažene izmjene tih podataka, a koji je potpisan korištenjem naprednog elektronskog potpisa kvalificiranog pružaoca usluge vremenskog žigosanja.
Kvalificirana sredstva za formiranje kvalificiranog elektronskog potpisa i pečata	Odgovarajuća tehnička sredstva (softver i hardver) koja se koriste za izradu kvalificiranog elektronskog potpisa, odnosno pečata, uz korištenje podataka za formiranje kvalificiranog elektronskog potpisa, odnosno pečata.
Kvalificirani ocjenjivač	Fizičko ili pravno lice koje zadovoljava zahtjeve propisane eIDAS uredbom Evropske unije.
Kvalificirani ovjerilac	Tijelo koje pruža jednu ili više kvalificiranih usluga povjerenja i kome je odgovarajuće nadzorno tijelo odobrilo status kvalificiranog Ovjerioca.
Ovjerilac	Tijelo koje izdaje i dodjeljuje kvalificirane elektronske potvrde a kojem vjeruje jedan ili više korisnika.
Opoziv potvrde	Trajni prestanak valjanosti potvrde prije isteka roka važenja navedenog u potvrdi.
Par ključeva	Dva matematički povezana kriptografska ključa (privatni ključ i njegov odgovarajući javni ključ) koja imaju sljedeća svojstva: ▪ Jedan ključ iz para ključeva može biti korišten za šifriranje podataka, a koji se mogu dešifrirati samo korištenjem drugog ključa iz istog para ključeva, ▪ U slučaju poznavanja samo jednog ključa nije moguće (u razumnom vremenu i uz poznatu tehnologiju) otkriti drugi ključ.
Podaci za formiranje kvalificiranog elektronskog potpisa ili pečata	Jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik, odnosno pečatilac koristi za izradu kvalificiranog elektronskog potpisa ili pečata.
Podaci za provjeru kvalificiranog elektronskog potpisa	Podaci, kao što su kodovi ili javni kriptografski ključevi, koji se koriste za provjeru kvalificiranog elektronskog potpisa, čime se potvrđuju izvornost i cjelovitost podataka zaštićenih tim potpisom, te neporecivost kreiranja potpisa od strane odgovarajućeg autora.
Potvrda	Skup podataka u elektronskom obliku koji: ▪ Imenuje i identifikuje korisnika navedenog u potvrdi, ▪ Sadrži korisnikov javni ključ, ▪ Ima upisan vremenski period valjanosti potvrde, ▪ Ima značenje u skladu sa važećim propisima i normama, ▪ Identifikuje Ovjerioca koji izdaje potvrde, ▪ Elektronski je potpisan od strane Ovjerioca, čime je zaštićen od nezapaženih promjena.
Potvrda Ovjerioca	Potvrda javnog ključa za *CA* kojeg je izdao drugi *CA* ili kojeg je izdao isti *CA*.
Privatni ključ (eng. *Private Key*)	Kriptografski ključ kojeg korisnik čuva u tajnosti, a koji odgovara uparenom javnom ključu. Koristi se za izradu elektronskog potpisa ili za dešifriranje podataka šifriranih odgovarajućim javnim ključem. Korisnik čuva u tajnosti, a koji odgovara njegovom javnom ključu.

Privatni kriptografski ključ aplikacije Ovjerioca	Privatni ključ Ovjerioca, zajedno sa javnim ključem koji je sadržan u potvrdi Ovjerioca predstavljaju par ključeva Ovjerioca. Privatni ključ je generiran prilikom inicijalizacije aplikacije Ovjerioca, a koristi se za potpisivanje izdanih elektronskih potvrda i registara opozvanih potvrda, što se radi pomoću *HSM*-a – hardverskog kriptografskog modula.
Povjerljive uloge	Uloge o kojima ovisi sigurnost rada pružatelja usluga povjerenja.
Potpisnik	Fizičko lice koje izrađuje elektronski potpis.
Registar opozvanih potvrda – CRL (eng. *Certificate Revocation List - CRL*)	Potpisana lista u koju se upisuju serijski brojevi i drugi podaci svih opozvanih potvrda koje je izdao ovjerilac.
Root CA	Ovjerilac najvišeg nivoa unutar domene pružaoca usluga povjerenja, potpisuje potvrde određenih Ovjerioca, vlastitu potvrdu, kao i administrativne potvrde.
Root potvrda Ovjerioca – Root CA potvrda	Potvrda koju ovjerilac izdaje sam sebi (eng. *self-signed certificate*), tj. subjekt potvrde je ovjerilac. *Root CA* potvrda sadrži javni ključ i naziv Ovjerioca koji je izdao potvrdu.
Reaktivacija potvrde	Radnja kojom se suspendirana potvrda čini ponovo valjanom.
Sigurno sredstvo za izradu elektronskog potpisa (eng. *Secure Signature Creation Device* – SSCD)	Sredstvo za izradu elektronskog potpisa koje osigurava: ▪ Da se podaci za izradu sigurnog elektronskog potpisa mogu pojaviti samo jednom, te da je ostvarena njihova sigurnost, ▪ Da se podaci za izradu sigurnog elektronskog potpisa ne mogu ponoviti, te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije, ▪ Da podatke za izradu sigurnog elektronskog potpisa korisnika može pouzdano zaštiti od neovlaštenog korištenja. Sredstvo za izradu sigurnog elektronskog potpisa ne smije pri izradi sigurnog elektronskog potpisa promijeniti podatke koji se potpisuju ili onemogućiti korisniku uvid u te podatke prije procesa izrade sigurnog elektronskog potpisa.
Sredstva za provjeru kvalificiranog elektronskog potpisa i pečata	Odgovarajuća tehnička sredstva (softver i hardver) koja služe za provjeru kvalificiranog elektronskog potpisa i pečata, uz korištenje podataka za provjeru elektronskog potpisa i pečata.
Suspenzija potvrde	Privremeni prestanak valjanosti potvrde prije isteka roka važenja navedenog u potvrdi.
Šifriranje	Proces u kriptografiji kojim se podaci mijenjaju tako da se informacije učine nerazumljivim za subjekte koji ne posjeduju odgovarajući ključ za dešifriranje. Upotrebom ključa za dešifriranje u postupku dešifriranja ove se informacije ponovo mogu učiniti razumljivim, tj. dovesti u oblik u kojem su postojale neposredno prije njihovog šifriranja.
Zaposleni	Lice u radnom odnosu sa JP BH POŠTA d.o.o. Sarajevo.
TSA sistem	Sistem za pružanje usluga izdavanja vremenskih žigova.
Validacija	Postupak potvrđivanja da su elektronski potpis ili pečat valjani.
Validacija potvrde	Postupak potvrđivanja da je potvrda valjana.
Validacija potpisa	Proces provjere kriptografske vrijednosti potpisa korištenjem podataka za verifikaciju potpisa.

Tabela 8. Definicije

Spisak skraćenica koje se pominju u dokumentu prikazan je u okviru Tabele 9.

Skraćenica	Puni naziv	Značenje
AES	*Advanced Encryption Standard*	Algoritam simetrične kriptografije namijenjen za šifriranje
CA	*Certification Authority*	Ovjerilac
CP	*Certification Policy*	Politika ovjeravanja koja ukazuje na primjenjivost potvrda za određenu skupinu sa zahtjevima za sigurnost.
CPS	*Certification Practice Statement*	Praktična pravila pružanja usluge ovjeravanja u kome su pobrojani operativni postupci koje ovjerilac provodi prilikom izdavanja i upravljanja životnim vijekom potvrde.
CRL	*Certificate Revocation List*	Registar opozvanih potvrda.
CMS	*Certificate Managament System*	Sistem za upravljanje životnim vijekom potvrda koje ovjerilac izdaje.
DN	*Distinguished Name*	Jedinstveno ime subjekta upisano u potvrdu kojim se identificira subjekt kojem je izdana potvrda.
EAL	*Evaluation Assurance Level*	Testiran nivo sigurnosti prema standardu ISO/IEC 15408. Postoji sedam (7) razina i to od EAL1 do EAL7.
ETSI	*European Telecommunications Standards Institute*	Evropski institut za standarde iz oblasti telekomunikacija.
HSM	*Hardware Security Module*	Hardverski kriptografski modul za kriptografske operacije.
ISO	*International organization for standardization*	Međunarodna organizacija za standardizaciju
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup javnom direktorijumu

NIST	*National institute of standards and technology*	Nacionalni institut za standarde i tehnologiju
NTP	*Network Time Protocol*	Protokol mrežnog vremena
OCSP	*Online Certificate Status Protocol*	Protokol za on-line provjeru statusa potvrda, opisan u dokumentu RFC 6960.
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Lični tajni broj za aktivaciju pametne kartice, pametnog *USB* tokena ili sličnog kriptografskog uređaja.
PKCS#10	*Public Key Cryptography Standard 10*	Standard za format zahtjeva za potvrdu.
PKI	*Public Key Infrastructure*	Infrastruktura javnih kriptografskih ključeva
QSCD	*Qualified Signature Creation Device*	Kvalificirano sredstvo za kreiranje elektronskih potpisa i pečata (pametni USB token).
RA	*Registration Authority*	Registracijsko tijelo
RFC	*Request for comment*	Dokumenti koji definiraju Internet standarde i preporuke.
UTC	*Coordinated Universal Time*	Koordinirano univerzalno vrijeme

Tabela 9. Spisak skraćenica

1.7. Standardi

- ISO 9001 – Quality management systems – Requirements
- ISO/IEC 15408 – Information technology – Security techniques – Evaluation criteria for IT security
- ISO 22301 – Business continuity management systems – Requirements
- ISO/IEC 27001 – Information technology – Security techniques – Information security management
- ETSI EN 319 401 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
- ETSI EN 319 411-1– Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
- ETSI EN 319 412-1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
- ETSI EN 319 412-2 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- ETSI EN 319 412-3 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- ETSI EN 319 412-5 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
- ETSI EN 319 403 – Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
- ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
- IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile

2. OBJAVLJIVANJE I LOKACIJA PODATAKA O USLUGAMA OVJERAVANJA

2.1. Lokacija za objavljivanje podataka o uslugama ovjeravanja

Ovjerilac JP BH POŠTA objavljuje podatke i svu dokumentaciju koja se odnosi na izdavanje elektronskih potvrda na Web stranici www.posta.ba Web stranica je javno dostupna, kao i svi podaci i sva dokumentacija koji se na njoj nalaze.

2.2. Objavljivanje podataka o uslugama ovjeravanja

Ovjerilac JP BH POŠTA objavljuje na svojoj zvaničnoj *Web* stranici:

- Politiku ovjeravanja Ovjerioca JP BH POŠTA ,
- Praktična pravila pružanja usluge ovjeravanja Ovjerioca JP BH POŠTA ,
- Prethodne verzije Politike ovjeravanja Ovjerioca JP BH POŠTA i Praktičnih pravila pružanja usluge ovjeravanja Ovjerioca JP BH POŠTA ,
- Opšti uslovi za pružanje usluge izdavanja kvalificiranih elektronskih potvrda – certifikata Ovjerioca JP BH POŠTA,
- Zahtjev za korištenje usluga ovjerioca za izdavanje kvalificiranih elektronskih potvrda,
- Ugovor o pružanju usluga ovjerioca za izdavanje kvalificiranih elektronskih potvrda,
- Zahtjev za izdavanje i korištenje kvalificirane elektronske potvrde za fizička lica,
- Zahtjev za izdavanje i korištenje kvalificirane elektronske potvrde za fizička lica u pravnom licu,
- Ugovor o izdavanju i korištenju kvalificirane elektronske potvrde za fizičko lice,
- Ugovor o izdavanju i korištenju kvalificirane elektronske potvrde za fizičko lice u pravnom licu,
- Zahtjev za promjenu statusa kvalificiranih elektronskih potvrda,
- Definicije važećih profila potvrda Ovjerioca JP BH POŠTA usklađenih sa eIDAS 910/2014 uredbom Evropske unije,
- Korisnička uputstva,
- Potvrde Ovjerioca JP BH POŠTA Root CA i podređenog Ovjerioca (JP BH POŠTA Issuing CA sa pridruženim hash vrijednostima,
- Registre opozvanih potvrda (CRL liste) Ovjerioca JP BH POŠTA Root CA, JP BHPOŠTA Issuing CA,
- Zakonsku regulativu iz područja elektronskog potpisa i pružanja usluga povjerenja,
- Cjenovnik usluga ovjeravanja,
- Lokacije ureda Registracijskog tijela,
- Obavještenja korisnicima vezane uz davanje usluga ovjeravanja,
- Druge akte i obavještenja.

Ovlašteni zaposlenik zadužen za ažuriranje sadržaja Web stranice po odobrenju obavlja objavljivanje dokumenata.

Ovjerilac JP BH POŠTA objavljuje korisnička uputstva i obrasce na web stranici, a prethodne verzije se zamjenjuju sa novim verzijama.

2.3. Učestalost objavljivanja podataka o uslugama ovjeravanja

Ovjerilac JP BH POŠTA ažurira objavljene podatke sljedećom dinamikom:

- Registri opozvanih potvrda (CRL) objavljuju se na svaka 24 sata. U slučaju opoziva i/ili suspenzije potvrde, ažurirani registar opozvanih potvrda se objavljuje odmah poslije opoziva i/ili suspenzije potvrda,
- Promjene na postojećim dokumentima objavljuju se u najkraćem roku poslije nastale promjene,
- Validnost CRL liste je 3 dana.

Dodatni dokumenti objavljuju se u najkraćem roku po odobravanju od strane nadležnih organa.

2.4. Kontrola pristupa podacima o uslugama ovjeravanja

Podaci koji su objavljeni na web stranici Ovjerioca JP BH POŠTA su javno dostupni. Pristup je ograničen na mogućnost čitanja. Svi koji pristupaju ovim podacima radi korištenja elektronskih potvrda dužni su se upoznati s odredbama ovih Praktičnih pravila.

Ovjerilac JP BH POŠTA ima postavljene logičke i fizičke sigurnosne mjere za zaštitu podataka na web stranicama od neovlaštenog brisanja i dodavanja ili neovlaštenih promjena.

3. IDENTIFIKACIJA I AUTENTIKACIJA

3.1. Određivanje imena

Vrste imena

Ovjerilac JP BH POŠTA Root CA i JP BH POŠTA Issuing CA, unose podatke o imenu ili nazivu subjekta za kojeg se izdaje potvrda u polje Subject potvrde. Jedinstveno ime (DN) u polju Subject u potvrdama usklađeno je s preporukom IETF RFC 5280 i normom X.520. Ovo jedinstveno ime mora biti unikatno unutar Ovjerioca JP BH POŠTA.

U elektronskim potvrdama koje izdaje Ovjerilac JP BH POŠTA, polje Issuer (vidi Tabelu 10, Tabelu 11 i Tabelu 12), koje sadrži ime Ovjerioca koji je izdao potvrdu, i polje Subject potvrde, koje sadrži ime korisnika potvrde, predstavljaju jedinstvena imena u obliku X.509 v3.

Komponenta imena	Vrijednost
Naziv CA servera (CN)	BHP-RootCA
Naziv organizacije (O)	JP BH POSTA doo
Naziv države (C)	BA

Tabela 10. Struktura imena potvrde Ovjerioca JP BH POŠTA Root CA u elektronskim potvrdama

Komponenta imena	Vrijednost
Naziv CA servera (CN)	BHP-SubCA
Naziv organizacije (O)	JP BH POSTA doo
Naziv države (C)	BA

Tabela 11. Struktura imena potvrde podređenog Ovjerioca JP BH POŠTA Issuing CA u elektronskim potvrdama

Struktura imena korisnika kvalificirane potvrde za elektronski potpis i pečat prikazana je u Tabeli 12, Tabeli 13 i Tabeli 14.

Komponenta imena	Vrijednost
Naziv korisnika (*CN*)	Ime Prezime (Ime i prezime kako je navedeno u identifikacionoj ispravi)
Serijski broj (*SERIALNUMBER*)	Kombinacija JIP i JMB (JIP je pseudoslučajno generirani broj zahtjeva)
Ime (G)	Ime (Ime kako je navedeno u identifikacionoj ispravi)

Prezime (SN)	Prezime (Prezime kako je navedeno u identifikacionoj ispravi)
Mjesto (L)	Mjesto prebivališta
Naziv države (C)	*BA*

Tabela 12. Struktura imena za fizičko lice u kvalificiranim elektronskim potvrdama

Komponenta imena	**Vrijednost**
Naziv korisnika (*CN*)	Ime Prezime (Ime i prezime kako je navedeno u identifikacionoj ispravi)
Serijski broj (*SERIALNUMBER*)	Kombinacija JIP i JMB (JIP je pseudoslučajno generirani broj zahtjeva)
Ime (G)	Ime (Ime kako je navedeno u identifikacionoj ispravi)
Prezime (SN)	Prezime (Prezime kako je navedeno u identifikacionoj ispravi)
Naziv organizacije (O)	Puni registrovani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registrovan
Identifikator organizacije (2.5.4.97)	IB (Jedinstveni identifikacioni broj pravnog lica)
Mjesto (L)	Mjesto sjedišta pravnog lica
Naziv države (C)	*BA*

Tabela 13. Struktura imena za korisnika u pravnom licu u kvalificiranim elektronskim potvrdama

Komponenta imena	**Vrijednost**
Naziv pravnog lica (*CN*)	Naziv koji pravno lice koristi za svoje predstavljanje
Serijski broj (*SERIALNUMBER*)	JIP-JIB (JIP je pseudoslučajno generirani broj zahtjeva, JIB je Jedinstveni identifikacioni broj pravnog lica)
Naziv organizacije (O)	Puni registrirani skraćeni naziv pravnog lica ili naziv pravnog lica ako skraćeni naziv nije registriran
Identifikator organizacije (2.5.4.97)	JIB (Jedinstveni identifikacioni broj pravnog lica)
Mjesto (L)	Mjesto sjedišta pravnog lica
Naziv države (C)	*BA*

Tabela 14. Struktura imena pravnog lica za kvalificirani elektronski pečat

Nomenklatura imena

U polje Subject kvalificirane potvrde upisuju se podaci o fizičkom licu kako su navedeni u važećem identifikacionom dokumentu. Kod fizičkog lica koje je povezano sa pravnim licem u okviru atributa koji identifikuje korisnika nalaze se i registrirani podaci pravnog lica.

U svaku potvrdu upisuju se podaci o imenu, odnosno nazivu subjekta ovjeravanja, te podatak o mjestu prebivališta i državi fizičkog lica, odnosno mjestu i državi sjedišta poslovnog subjekta. Podaci o imenu ili nazivu koji se upisuju u potvrdu odnose se na autentično ime ili naziv subjekta. Polje Subject u potvrdi usklađeno je s dokumentom IETF RFC 5280.

Polje Subject u potvrdama koje se izdaju za fizička lica sadrži ime i prezime lica. U poslovnim certifikatima polje Subject dodatno sadrži i puni registrirani naziv poslovnog subjekta i njegov identifikator.

Ukoliko bilo koji podatak koji se unosi u polje Subject sadrži posebne znakove ili slova koja nisu sadržana u službenim pismima Bosne i Hercegovine, takvi znakovi se zamjenjuju najbližim znakom engleske abecede.

Sadržaj ekstenzije Subject Alternative Name kod potvrde za fizička lica i fizička lica povezana sa pravnim licem može biti e-mail adresa subjekta.

Smislenost imena

Imena i nazivi u atributima polja *Subject* koji identificiraju fizičko lice i poslovni subjekt su smisleni. Za atribute u polju *Subject* u certifikatima koje izdaju Ovjerilac JP BH POŠTA primjenjuju se sljedeća pravila:

- Lično ime i prezime moraju biti kako su navedeni u identifikacionoj ispravi, odnosno u službenim matičnim registrima,
- Naziv poslovnog subjekta mora biti kako je naveden u službenim nadležnim nacionalnim registrima.

ODREĐIVANJE ELEMENATA POLJA SUBJECT U POTVRDAMA	
Naziv potvrde	**Atributi i vrijednosti polja subject**
JP BH POŠTA kvalificirana potvrda za elektronski potpis za fizičko lice	▪ **commonName (CN):** Ime i prezime ▪ **serialNumber:** Serijski broj potvrde ▪ **givenName (G):** Ime ▪ **surname (SN):** Prezime ▪ **localityName (L):** Mjesto prebivališta ▪ **countryName (C):** BA
JP BH POŠTA kvalificirana potvrda za elektronski pečat	▪ **commonName (CN):** Naziv koji subjekat koristi za svoje predstavljanje ▪ **serialNumber**: Serijski broj potvrde ▪ **organizationIdentifier (2.5.4.97)** : JIB ▪ **organizationName (O)**: Skraćeni naziv poslovnog subjekta ili puni registrirani naziv

	poslovnog subjekta ako skraćeni naziv nije registriran ▪ **localityName (L)**: Mjesto sjedišta poslovnog subjekta ▪ **countryName (C)**: BA
JP BH POŠTA kvalificirana potvrda za elektronski potpis za fizičko lice povezano sa pravnim licem	▪ **commonName (CN)**: Ime i prezime potpisnika ▪ **serialNumber**: Serijski broj potvrde ▪ **givenName (G)**: Ime ▪ **surname (SN)**: Prezime ▪ **organizationIdentifier (2.5.4.97)** : JIB ▪ **organizationName (O)**: Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran ▪ **localityName (L)**: Mjesto sjedišta poslovnog subjekta ▪ **countryName (C)**: *BA*

Tabela 15. Određivanje elemenata polja Subject u potvrdama

Pravila tumačenja raznih oblika imena

Tumačenje oblika imena u polju Subject po normi X.520 u Ovjeriocu JP BH POŠTA određeno je na sljedeći način:

- commonName (CN) – U potvrdama za fizička lica, fizička lica povezana sa pravnim licima i potvrdama za zaposlene ovaj atribut sadrži ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi.
- serialNumber – Ovaj atribut u polju Subject osigurava jedinstvenost imena subjekta. U potvrdama za fizička lica i fizička lica povezana sa pravnim licima pseudoslučajno generiranog broja potvrde (JIP) i jedinstvenog matičnog broja (JMB). U aplikacijskim potvrdama se ovo polje ne koristi.
- organizationIdentifier (2.5.4.97) – U potvrdama za fizička lica povezana sa pravnim licima i potvrdama za zaposlene sastoji se od oznake poreznog identifikacionog broja pravnog lica (PIB).
- localityName (L) – U potvrdama za fizička lica povezana sa pravnim licima atribut localityName sadrži naziv mjesta u kojem je sjedište poslovnog subjekta. U potvrdama za fizička lica atribut localityName sadrži mjesto prebivališta potpisnika. U aplikacijskim potvrdama atribut localityName sadrži naziv mjesta u kojem je sjedište poslovnog subjekta.
- countryName (C)– Sadrži oznaku dvoslovnog ISO koda Bosne i Hercegovine.

JP BH POŠTA kvalificirana potvrda za elektronski potpis za fizička lica		
Atribut	**Vrijednost**	**Opis**
commonName (CN)	Ime i prezime	Ime i prezime potpisnika kako je navedeno u identifikacionoj ispravi
serialNumber	JIP-JMB	JIP je pseudoslučajno generiran broj potvrde
givenName (G)	Ime	Ime (Ime kako je navedeno u identifikacionoj ispravi)
surname (SN)	Prezime	Prezime (Prezime kako je navedeno u identifikacionoj ispravi)
Locality (L)	Mjesto	Mjesto prebivališta
countryName (C)	*BA*	Dvoslovan ISO kod države prebivališta potpisnika, BA za Bosnu i Hercegovinu

Tabela 16. Tumačenje oblika imena po X.520 normi za JP BH POŠTA kvalificirane potvrde za elektronski potpis za fizička lica

JP BH POŠTA kvalificirana potvrda za elektronski potpis za fizička lica povezana sa pravnim licima		
ATRIBUT	**VRIJEDNOST**	**OPIS**
commonName (CN)	Ime i prezime	Ime i prezime potpisnika kako je navedeno u identifikacionoj ispravi
serialNumber	JIP-JMB	JIP je pseudoslučajno generiran broj potvrde
givenName (G)	Ime	Ime (Ime kako je navedeno u identifikacionoj ispravi)
surname (SN)	Prezime	Prezime (Prezime kako je navedeno u identifikacionoj ispravi)
organizationName (O)	Naziv poslovnog subjekta	Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran
organizationIdentifier (2.5.4.97)	JIB	Jedinstveni identifikacioni broj pravnog lica
Locality (L)	Mjesto	Mjesto sjedišta pravnog lica
countryName (C)	*BA*	Dvoslovan ISO kod države Bosne i Hercegovine

Tabela 17. Tumačenje oblika imena po X.520 normi za JP BH POŠTA kvalificirane potvrde za elektronski potpis za fizička lica povezana sa pravnim licima.

JP BH POŠTA kvalificirana potvrda za elektronski pečat		
Atribut	**Vrijednost**	**Opis**
commonName (CN)	Naziv poslovnog subjekta	Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran
serialNumber	JIP-JIB	JIP je pseudoslučajno generiran broj potvrde JIB je jedinstveni identifikacioni broj pravnog lica
organizationName (O)	Naziv poslovnog subjekta	Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran
organizationIdentifier (2.5.4.97)	JIB	Jedinstveni identifikacioni broj pravnog lica
Locality (L)	Mjesto	Mjesto sjedišta pravnog lica
countryName (C)	*BA*	Dvoslovčani ISO kod države Bosne i Hercegovine

Tabela 18. Tumačenje oblika imena za JP BH POŠTA kvalificirane potvrde za elektronski pečat.

Jedinstvenost imena

Jedinstveno ime subjekta jedinstveno je unutar Ovjerioca JP BH POŠTA i produkcijske hijerarhije zasnovane na serveru *JP BH POŠTA Root CA*. Jedinstvenost jedinstvenog imena osigurana je vrijednošću atributa *serialNumber* u polju *Subject* potvrde.

Ovjerilac JP BH POŠTA samostalno kontroliše i dodjeljuje vrijednost atributa *serialNumber* u jedinstvenom imenu da bi imena različitih subjekata bila jedinstvena. Atribut serialNumber se formira od broja zahtjeva korisnika za izdavanje digitalne potvrde i jedinstvenog matičnog broja (JMB).

Anonimnost ili pseudonimi korisnika

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

Ovjerilac JP BH POŠTA će odbiti svaki zahtjev za anonimnošću ili korištenjem pseudonima.

Pravila za tumačenje različitih vrsta imena

U kvalificiranim elektronskim potvrdama su imena korisnika vjerno predstavljena odgovarajućim latiničnim ili ćiriličnim slovima.
Znakovi koje nije dozvoljeno koristiti u imenima korisnika su: " (navodnici), ? (upitnik), \ (obrnuta kosa crta), # (ljestve), $ (dolar), % (postotak), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez).

Jedinstvenost imena

JP BH POŠTA, kao ovjerilac, jamči ekskluzivnost imena unutar svoje domene. Svaki korisnik će dobiti jedinstveno ime (Distinguished Name - DN), koje će biti upisano u Subject polje elektronske potvrde.

Priznavanje, autentikacija i uloga zaštitnog znaka

Imena koja bi povrijedila intelektualna ili autorska prava drugih osoba nisu dozvoljena. Ovlaštena osoba iz JP BH POŠTA nije obavezna provjeravati zakonitost korištenja takvih imena. Korisnik je odgovoran za osiguravanje da odabrano ime bude korišteno u skladu sa zakonom.

Ovlaštena osoba iz JP BH POŠTA će, u najkraćem mogućem roku, postupiti po svim sudskim nalozima koje su izdate u skladu sa zakonima, a koje se odnose na pravne mjere u slučaju povrede prava trećih strana prilikom izdavanja elektronskih potvrda prema ovim Praktičnim pravilima.

3.2. Početna provjera valjanosti identiteta

Početna provjera tačnosti identiteta je obavezni dio postupka podnošenja zahtjeva za izdavanje potvrde.

Metod dokazivanja posjeda privatnog ključa

Privatni kriptografski ključ korisnika kvalificiranih potvrda se generiše u Ovjeriocu JP BH POŠTA na QSCD uređaju.

Autentikacija identiteta fizičkog lica

U skladu s navedenim Praktičnim pravilima, neophodno je provesti postupak autentikacije identiteta fizičkog lica. Tokom procesa registracije, korisnik mora biti fizički prisutan.

Prilikom registracije, obavezno je da korisnik posjeduje važeći identifikacioni dokument sa svojom fotografijom, kao što su važeća lična karta ili pasoš. U tom trenutku će se napraviti kopija identifikacionog dokumenta korisnika.

Fotografija na identifikacionom dokumentu se detaljno upoređuje s fizičkim izgledom korisnika koji je prisutan tokom registracije. Ovo upoređivanje obuhvata karakteristike lica, starost, spol i slične relevantne informacije kako bi se osigurala autentičnost korisnikovog identiteta.

Autentikacija identiteta pravnog lica

Kvalificirana elektronska potvrda za elektronski potpis može biti izdana isključivo fizičkom licu, u skladu sa Zakonom o elektronskom potpisu. Fizičko lice ima pravo da u ime pravnog lica koristi kvalificiranu elektronsku potvrdu samo ako mu to pravno lice dozvoli. Fizičko lice može biti zaposleno u pravnom licu. Kvalificirana elektronska potvrda za elektronski pečat može biti izdata isključivo pravnom licu.

Ako Ovjerilac JP BH POŠTA izdaje elektronsku potvrdu fizičkom licu koje predstavlja pravno lice, unutar atributa koji identificiraju korisnika nalaze se i podaci koji označavaju naziv pravnog lica, njegovo poslovno ime i identifikator organizacije, odnosno porezni identifikacioni broj.

Kada je korisnik fizičko lice u pravnom licu, prije zaključivanja ugovora i izdavanja certifikata fizičkom licu u pravnom licu, potrebno je prvo zaključiti Ugovor o pružanju usluga ovjerioca za izdavanje kvalificiranih elektronskih potvrda sa pravnim licem.

Pravno lice sa web stranice Ovjerioca www.posta.ba/e-potpis u dijelu „Dokumentacija“ preuzima i popunjava Zahtjev za korištenje usluga ovjerioca i Ugovor o pružanju usluga ovjerioca za izdavanje kvalificiranih elektronskih potvrda i iste potpisane, uz Aktuelni Izvod iz sudskog registra (ne stariji od 12 mjeseci, original ili ovjerena kopija) ili drugi odgovarajući akt ili akte iz kojih je vidljiv naziv pravnog lica, lice ovlašteno za zastupanje, sjedište pravnog lica, JIB i sl. dostavlja na adresu Ovjerioca JP BH POŠTA.

Na osnovu zaključenog Ugovora o pružanju usluga ovjerioca fizičko lice u pravnom licu pristupa proceduri izdavanja certifikata tako što na jednoj od lokacija Registracijskog tijela Ovjerioca JP BH POŠTA podnosi Zahtjev za izdavanje i korištenje kvalificirane elektronske potvrde uz koji prilaže:

- Identifikacioni dokument (lična karta ili pasoš),
- Dokaz o uplati naknade, odnosno odgovarajući dokument o regulisanju finansijskih obaveza za izdavanje i korištenje kvalificirane elektronske potvrde
- Ovlaštenje pravnog lica za izdavanje i korištenje kvalificirane elektronske potvrde kojim ovlašteno lice pravnog lica ovlašćuje fizičko lice za korištenje kvalificirane elektronske potvrde za elektronski potpis.

Neprovjereni podaci o korisniku

Svi podaci o korisniku koje zahtijeva Zakon o elektronskom potpisu moraju biti adekvatno verificirani.

Provjera tačnosti podataka pravnog lica

Korisnik prilaže važeću dokumentaciju za ime pravnog lica, koje će se uključiti u elektronsku potvrdu. Riječi koje treba unijeti u potvrdu moraju biti identične riječima navedenim u priloženoj dokumentaciji.

Upotrebu imena pravnog lica moraju odobriti i ovlastiti odgovarajući predstavnici pravnog lica, i to na sljedeći način:

- Upotrebu imena pravnog lica registriranog u sudskom registru odobravaju odgovorna lica tog pravnog lica.
- Upotrebu imena pravnog lica koje ima jednog vlasnika mora odobriti sam vlasnik.
- Upotrebu imena pravnog lica koje je u vlasništvu više partnera mora odobriti partner naveden u ugovoru o partnerstvu.
- Upotrebu imena pravnog lica koje je u vlasništvu neke zajednice mora odobriti nadležna institucija.

Kriteriji za međusobnu saradnju

Ovjerilac JP BH POŠTA ne predviđa unakrsno ovjeravanje.

3.3. Identifikacija i autentikacija zahtjeva za obnovom ključa

Identifikacija i autentikacija zahtjeva za rutinskom obnovom ključa

U slučaju potrebe za rutinskom obnovom ključa, Ovjerilac JP BH POŠTA ne dopušta ovu radnju. Postupak se provodi izdavanjem nove elektronske potvrde prema već opisanom postupku.

Identifikacija i autentikacija zahtjeva za zamjenom ključa nakon opoziva

Nakon što je ključ opozvan, Ovjerilac JP BH POŠTA ne omogućava zamjenu istog. Cijeli proces se izvodi izdavanjem nove elektronske potvrde.

3.4. Identifikacija i autentikacija zahtjeva za opoziv i suspenziju potvrde

Korisnik može zahtijevati opoziv elektronske potvrde putem propisane procedure.

Korisnik lično dolazi i identificira se na jednoj od prethodno definisanih lokacija Ovjerioca JP BH POŠTA te predaje zahtjev za promjenu statusa kvalificirane elektornske potvrde s vlastitim potpisom.

Pravno lice zahtjev za promjenu statusa za zaposlenika podnosi na jednoj od prethodno definisanih lokacija Ovjerioca JP BH POŠTA u kojem slučaju zahtjev za promjenu statusa mora biti potpisan i opečaćen od strane ovlaštenog lica u pravnom licu.

4. OPERATIVNI ZAHTJEVI U PROCESU IZDAVANJA POTVRDA

4.1. Zahtjevi za izdavanje potvrda

Ko može da podnese zahtjev za izdavanje potvrde

Zahtjev može da podnese svako fizičko lice koje ispunjava uslove navedene u ovim Praktičnim pravilima.

Uslovi za izdavanje potvrde

Za izdavanje elektronske potvrde, korisnik je dužan da:

- Popuni i potpiše zahtjev za izdavanje i korištenje elektronske potvrde
- Ispuni zahtjeve za identifikaciju,
- Ispuni finansijske obaveze prema cjenovniku,
- Potpiše ugovor o izdavanju i korištenju elektronske potvrde.

Kvalificirana elektronska potvrda za elektronski potpis se izdaje isključivo fizičkom licu .

Kvalificirana elektronska potvrda za elektronski pečat se izdaje isključivo pravnom licu.

Zahtjev za izdavanje i korištenje elektronske potvrde sadrži podatke na osnovu kojih Ovjerilac JP BH POŠTA može da stupi u kontakt s korisnikom elektronske potvrde.

Ugovor sadrži uvjete izdavanja i korištenja potvrde, a stupa na snagu kada ga potpišu ugovorne strane.

U slučaju kada se potvrda izdaje fizičkom licu unutar pravnog lica, prvo se potpisuje ugovor s pravnim licem, a zatim pojedinačno sa svakim fizičkim licem unutar pravnog lica kojem se izdaje potvrda.

Kao dokaz da je pravno lice saglasno za izdavanje certifikata za fizičko lice uz Zahtjev za izdavanje i korištenje kvalificirane elektronske potvrde fizičko lice prilaže Ovlaštenje za izdavanje i korištenje kvalificirane elektronske potvrde kojim ovlašteno lice pravnog lica ovlašćuje fizičko lice za korištenje kvalificirane elektonske potvrde za elektronski potpis.

Korištenje kvalificirane elektronske potvrde se ugovara na rok od 1 (jedne) ili 3 (tri) godine i vezuje se za dan kreiranja potvrde.

4.1. Obrada zahtjeva za izdavanje potvrda

Obavljanje funkcija identifikacije i potvrđivanja autentičnosti

Ovjerilac JP BH POŠTA identifikuje korisnika na osnovu identifikacionog dokumenata koje korisnik podnosi (važeća lična karta ili pasoš). Korisnik mora lično da podnese cjelokupnu dokumentaciju.

4.2.2. Odobrenje ili odbijanje zahtjeva za izdavanje potvrda

Ovjerilac JP BH POŠTA će odobriti zahtjev za izdavanje elektronske potvrde, ukoliko su ispunjeni sljedeći uvjeti:

- Korisnik je lično podnio potrebnu dokumentaciju,
- Podnesena dokumentacija je provjerena,
- Svi podaci unijeti u zahtjev smatraju se odgovarajućim i kompletnim.

Ako korisnik ne ispuni navedene uvjete ili ako na bilo koji način povrijedi odredbe ovih Praktičnih pravila, Ovjerilac JP BH POŠTA će odbiti zahtjev za izdavanje elektronske potvrde.

4.2.3. Vrijeme obrade zahtjeva za izdavanje potvrde

Obrada zahtjeva može da traje najduže 10 radnih dana od dana prijema zahtjeva.

4.3. Izdavanje potvrda

4.3.1. Aktivnosti u toku izdavanja potvrde

Izdavanje elektronske potvrde vrši se na sljedeći način:

- Korisnik preko Web stranici Ovjerioca JP BH POŠTA preuzima Zahtjev za izdavanje elektronske potvrde i popunjava ga,
- Korisnik, u postupku izdavanja potvrde, identificira se lično u Registracijskom tijelu (RA – Registration Authority) JP BH POŠTA na unaprijed definisanim lokacijama,
- Uposlenik Registracijskog tijela JP BH POŠTA unosi podatke o korisniku i kreira zahtjev u aplikaciji Registracijskog tijela i prosljeđuje verificiran zahtjev Kontroloru registracijskog tijela PKI JP BH POŠTA ,
- Kontrolor registracijskog tijela PKI JP BH POŠTA na osnovu verificiranog zahtjeva kreira nalog za personalizaciju kriptografskog uređaja,
- Korisnički privatni kriptografski ključ se generira u hardverskom kriptografskom modulu QSCD uređaja od strane HSM Operatera iz Tijela za operativne poslove,
- Ovjerilac JP BH POŠTA šalje izdane korisničke potvrde na QSCD uređaju na lokaciju predaje zahtjeva,
- Ovjerilac JP BH POŠTA šalje pripadajuću lozinku/PIN kod u zatvorenoj koverti Korisniku sa uputama da preuzme QSCD uređaj na lokaciji predaje zahtjeva.
- Korisnik potpisuje ugovor o izdavanju i korištenju elektronske potvrde, preuzima elektronsku potvrdu na QSCD uređaju od uposlenika Registracijskog tijela PKI JP BH POŠTA i potpisuje izjavu (otpremnicu) o preuzimanju elektronske potvrde na QSCD uređaju.

4.3.2. Obavještavanje korisnika o izdavanju potvrde

Ovjerilac JP BH POŠTA šalje PIN preporučenom poštom uz obavještenje korisnika o mjestu na kojem može preuzeti elektronsku potvrdu putem QSCD uređaja.

4.4. Preuzimanje potvrda

4.4.1. Postupak preuzimanja potvrda

Korisnicima kvalificirane elektronske potvrde uručuje ih uposlenik Registracijskog tijela PKI JP BH POŠTA. Ako se naknadno utvrdi da elektronska potvrda sadrži netočne podatke, korisnik je dužan kontaktirati Ovjerioca JP BH POŠTA radi izdavanja nove potvrde.

4.4.2. Objavljivanje potvrda

Ovjerilac JP BH POŠTA javno ne objavljuje elektronske potvrde.

4.4.3. Obavještavanje o izdavanju potvrda trećim licima

Treća lica se ne obavještavaju o izdavanju elektronskih potvrda.

4.5. Korištenje para kriptografskih ključeva i potvrda

4.5.1. Korištenje privatnog ključa i potvrde od strane korisnika

Privatni kriptografski ključevi izdani od strane JP BH POŠTA Root CA i JP BH POŠTA Issuing CA koriste se za potpisivanje potvrda i CRL-ova. Privatni kriptografski ključ korisnika koristi se za stvaranje kvalificiranog elektronskog potpisa ili pečata, dok se kvalificirana elektronska potvrda koristi za verifikaciju kvalificiranog elektronskog potpisa ili pečata.

4.5.2. Korištenje javnog ključa i potvrda od strane trećih lica

Treća lica koriste javni ključ i elektronsku potvrdu za verifikaciju elektronskih potpisa.

4.6. Produžetak korištenja potvrde

JP BH POŠTA ne produžuje korištenje elektronske potvrde. Cijeli proces zamjenjuje izdavanjem nove elektronske potvrde.

4.7. Zamjena javnog ključa u potvrdi

Zamjena javnog ključa u elektronskoj potvrdi se ne vrši. Cijeli proces zamjenjuje izdavanjem nove elektronske potvrde.

4.7.1. Okolnosti za zamjenu javnog ključa u potvrdi

Ne vrši se.

4.7.2. Ko može da zahtijeva zamjenu javnog ključa u potvrdi

Ne vrši se.

4.7.3. Obrada zahtjeva za zamjenu javnog ključa u potvrdi

Ne vrši se.

4.7.4. Obavještavanje korisnika o zamjeni javnog ključa u potvrdi

Ne vrši se.

4.7.5. Postupak prihvaćanja obavještenja o zamjeni javnog ključa u potvrdi

Ne vrši se.

4.7.6. Objavljivanje potvrde kod koje je izvršena zamjena javnog ključa

Ne vrši se.

4.7.7. Obavještavanje trećih lica o izdavanju potvrda

Ne vrši se.

4.8. Promjena podataka u potvrdi

Izmjena podataka u elektronskoj potvrdi se ne vrši. Cijeli proces se izvršava izdavanjem nove elektronske potvrde.

4.8.1. Okolnosti za promjenu podataka u potvrdi

Ne vrši se.

4.8.2. Ko može da zahtijeva promjenu podataka u potvrdi

Ne vrši se.

4.8.3. Obrada zahtjeva za promjenu podataka u potvrdi

Ne vrši se.

4.8.4. Obavještenje korisnika o promjeni podataka u potvrdi

Ne vrši se.

4.8.5. Postupak prihvaćanja obavještenja o promjeni podataka u potvrdi

Ne vrši se.

4.8.6. Objavljivanje potvrda kod koga je izvršena promjena podataka

Ne vrši se.

4.8.7. Obavještenje trećih lica o izdavanju potvrda

Ne vrši se.

4.9. Opoziv i suspenzija potvrda

4.9.1. Okolnosti opoziva potvrda

4.9.1.1. Okolnosti opoziva potvrda Ovjerioca JP BH POŠTA

Ovjerilac JP BH POŠTA će opozvati potvrdu Ovjerioca JP BH POŠTA u roku od 24 sata od prijama zahtjeva:

- Ako se zaprimi dokaz da je privatni ključ povezan sa javnim ključem u potvrdi Ovjerioca JP BH POŠTA kompromitiran,
- U slučaju potrebe za promjenom kriptografskog algoritma i pripadajuće dužine ključa,
- U slučaju dokaza o zloupotrebi potvrde Ovjerioca JP BH POŠTA ,
- Ako ovlašteno lice Ovjerioca JP BH POŠTA podnese pisani zahtjev za opoziv potvrde Ovjerioca JP BH POŠTA .

4.9.1.2. Okolnosti opoziva korisničkih potvrda

Ovjerilac JP BH POŠTA je dužan da opozove elektronsku potvrdu iz sljedećih razloga:

- U slučaju da neka informacija sadržana u potvrdi postane netačna,
- Promjene podataka u potvrdi, koje zahtijevaju izdavanje nove potvrde,
- Naknadnog utvrđivanja da podaci koje je dostavio korisnik pri identifikaciji nisu tačni,
- Gubitka, oštećenja ili zloupotrebe tehničkih sredstava (hardvera ili softvera) ili privatnog kriptografskog ključa, odnosno kompromitiranja ili sumnje u kompromitiranje privatnog kriptografskog ključa,
- U slučaju trajne nedostupnosti privatnog ključa,
- U slučaju ako privatni ključ ili aktivacijski podaci nisu više u posjedu potpisnika, odnosno pečatioca,
- Neispunjavanja obaveza korisnika potvrde određenih ovim Praktičnim pravilima i ugovorom,
- Ukoliko opoziv elektronske potvrde zahtjeva korisnik potvrde,
- Ukoliko opoziv elektronske potvrde zahtjeva pravno lice za zaposlenika kao korisnika potvrde,
- Ukoliko korisnik elektronske potvrde prestane da postoji,
- Ukoliko korisnik izgubi poslovnu sposobnost ili pravno lice kojoj pripada korisnik prestane da postoji,
- U slučaju da potvrda više nije u skladu sa općim pravilima,
- Ukoliko se promijene okolnosti koje bitno utiču na važenje potvrde,
- U slučaju otkaza ugovora o izdavanju i korištenju kvalificirane elektronske potvrde od strane korisnika potvrde,
- U slučaju otkaza ugovora o pružanju usluga ovjerioca za izdavanje kvalificiranih elektronskih potvrda od strane pravnog lica,
- Iz drugih razloga koji su utvrđeni Zakonom o elektronskom potpisu i drugim propisima koji reguliraju ovu oblast.

4.9.2. Ko može da zahtijeva opoziv potvrde

Opoziv elektronske potvrde može da zahtijeva:

- Korisnik elektronske potvrde – fizičko lice,
- Pravno lice za zaposlene u tom pravnom licu,
- Ovjerilac JP BH POŠTA ,
- Nadležni državni organ na osnovu zakona.

4.9.3. Procedure za opoziv potvrde

4.9.3.1. Opoziv potvrde zbog kompromitiranja privatnog kriptografskog ključa

Opoziv elektronske potvrde zbog kompromitiranja ili sumnje u kompromitiranje privatnog kriptografskog ključa, vrši se na sljedeći način:

Korisnik potvrde pristupa web stranici Ovjerioca https://ca-posta.ba/ i online popunjava tražene podatke za promjenu statusa digitalnog certifikata u kojem pod „Vrsta promjene statusa“ treba izabrati „opoziv“. Nakon kreiranja zahtjeva za opoziv digitalnog certifikata korisnik potvrde dobija poruku da je uspješno popunio prijavu za opoziv digitalnog certifikat te zahtjev preuzima, štampa i svojeručno potpisuje i isti lično podnosi na jednoj od lokacija Registracijskog tijela Ovjerioca JP BH POŠTA, kojom prilikom je obavezan radi identifikacije ovlaštenom šalterskom radniku dati na uvid identifikacioni dokument (lična karta ili pasoš).

Pravno lice može izvršiti opoziv certifikata za zaposlenika tako što pristupa web stranici Ovjerioca https://ca-test.posta.ba/revoke i online popunjava tražene podatke za promjenu statusa digitalnog certifikata u kojem pod „Vrsta promjene statusa“ treba izabrati „opoziv“. Nakon kreiranja zahtjeva za opoziv digitalnog certifikata zaposlenika, pravno lice dobija poruku da je uspješno popunilo prijavu za opoziv digitalnog certifikat nakon čega zahtjev preuzima i štampa te se potpisan i opečaćen od strane ovlaštenog lica u pravnom licu podnosi na jednoj od lokacija Registracijskog tijela Ovjerioca „JP BH POŠTA“ d.o.o. Sarajevo.

Zaposlenik Registracijskog tijela šalje verificiran zahtjev Voditelju Registracijskog tijela internom poštom. Dodatno, uposlenik Registracijskog tijela šalje skeniran zahtjev email-om Voditelju Registracijskog tijela. Voditelj Registracijskog tijela bez odlaganja provodi proceduru realizacije zahtjeva te izdaje nalog za opoziv koji uz zahtjev za opoziv dostavlja Voditelju tijela za operativne poslove internom poštom i šalje skeniran zahtjev email-om. Voditelj OA zaprimljeni nalog za opoziv uz zahtjev za opoziv prosljeđuje na realizaciju HSM Operteru internom poštom i šalje skeniran zahtjev email-om.

Radno vrijeme Registracijskog tijela je ponedjeljak – petak od 08:00 sati do 15:00 sati, a Tijela za operativne poslove JP BH POŠTA je ponedjeljak – petak od 08.00 do 16:00 sati.

Tijelo za operativne poslove inicijalno izvršava suspenziju, a naknadno nakon kompletiranja procesa verifikacije zahtjeva korisnika potvrde ili pravnog lica opoziva elektronsku potvrdu.

Tijelo za operativne poslove obavještava Voditelja Registracijskog tijela o izvršenju. Voditelj Registracijskog tijela obavještava korisnika potvrde o opozivu elektronskom poštom. Ako se radi o korisniku potvrde u pravnom licu o opozivu se obaviještava i pravno lice. U slučaju da korisnik potvrde ili pravno lice ne posjeduju adresu elektronske pošte, obavještenje o opozivu bit će poslano poštom na adresu naznačenu u ugovoru.

Ovjerilac JP BH POŠTA može da se odluči za opoziv elektronske potvrde i bez zahtjeva korisnika, ukoliko ustanovi da je došlo ili sumnja da je došlo do kompromitiranja privatnog kriptografskog ključa povezanog s tom potvrdom.

Poslije opoziva elektronske potvrde, korisnik može da zahtijeva izdavanje nove elektronske potvrde.

4.9.3.2. Povlačenje potvrde zbog promjene podataka u potvrdi

Povlačenje elektronske potvrde zbog promjene podataka u potvrdi obavlja se na isti način kako je navedeno u tački 4.9.3.1.

Ovlašteni predstavnik JP BH POŠTA može odlučiti povući elektronsku potvrdu i bez zahtjeva korisnika, ako uoči promjenu podataka u potvrdi koja zahtijeva izdavanje nove elektronske potvrde.

Nakon povlačenja elektronske potvrde, korisnik može zatražiti izdavanje nove elektronske potvrde.

4.9.3.3. Povlačenje potvrde zbog nepoštivanja obaveza korisnika

U situacijama gdje korisnik ne ispunjava svoje preuzete obaveze Ovjerilac JP BH POŠTA ima pravo povući elektronsku potvrdu korisnika.

Ovjerilac JP BH POŠTA obavještava korisnika o povlačenju elektronske potvrde putem elektronske pošte. Ukoliko korisnik nije u posjedu elektronske adrese, obavještenje o povlačenju će biti poslato putem poštanskog servisa na adresu koja je navedena u ugovoru.

Nakon povlačenja elektronske potvrde, korisnik ima pravo podnijeti zahtjev za izdavanje nove elektronske potvrde.

4.9.4. Period od podnošenja zahtjeva do opoziva potvrde

Nakon što korisnik podnese zahtjev za opoziv elektronske potvrde, JP BH POŠTA Ovjerilac će odmah pristupiti obradi zahtjeva za opozivom potvrde bez zadržavanja.

4.9.5. Vremenski okvir za obradu zahtjeva za opoziv potvrde

Operativni tim Ovjerioca će provesti opoziv elektronske potvrde i odmah objaviti novi registar opozvanih potvrda čim primi zahtjev za opoziv potvrde od strane Kontrolora Registracijskog tijela.

4.9.6. Zahtjev za provjeru opozvanosti potvrda od strane trećih strana

Prilikom rukovanja elektronskim potvrdama izdanim od strane Ovjerioca JP BH POŠTA, treća lica su obavezna redovito provjeravati opozvanost potvrda.

4.9.7. Učestalost objavljivanja registra opozvanih potvrda

Registri opozvanih potvrda Ovjerioca JP BH POŠTA Root CA objavljuju se svakih 12 mjeseci i prilikom opoziva podređenih Ovjerioca JP BH POŠTA Root CA. Registar opozvanih potvrda Ovjerioca CERTIFIKACIJSKOG TIJELA JP BH POŠTA Issuing CA objavljuje se svakih 24 sata. U slučaju prijevremenog opoziva ili suspenzije elektronske potvrde, Ovjerilac JP BH POŠTA će odmah objaviti novi registar opozvanih potvrda prije isteka važenja prethodnog registra opozvanih potvrda.

4.9.8. Maksimalno kašnjenje u objavljivanju registra opozvanih potvrda

Najveće dopušteno kašnjenje u objavljivanju CRL liste u javnom repozitoriju iznosi 5 (pet) minuta. U slučaju nepredviđenih okolnosti koje rezultiraju dužim kašnjenjem u objavi CRL liste, Ovjerilac JP BH POŠTA će obavijestiti korisnike o razlozima kašnjenja i vremenskom periodu u kojem validna CRL lista nije objavljena.

4.9.9. Druge dostupne forme registra opozvanih potvrda

Registar opozvanih potvrda je dostupan na web stranici Ovjerioca JP BH POŠTA. CRL servis je dostupan 24 sata dnevno, 7 dana u sedmici.

4.9.10. Zahtjevi za online provjeru opozvanosti potvrda

Korisnici i treće strane su obavezni provjeravati status elektronske potvrde na osnovu javno dostupnog registra opozvanih potvrda Ovjerioca JP BH POŠTA.

4.9.11. Druge forme registra opozvanih potvrda

Registar opozvanih potvrda je raspoloživ i na Web stranici Ovjerioca JP BH POŠTA.

4.9.12. Posebni zahtjevi u slučaju kompromitiranja ključa

Ako korisnik zna ili sumnja u kompromitaciju njegovog privatnog ključa dužan je da odmah prestane sa njegovim korištenjem i podnese zahtjev za opoziv elektronske potvrde.

4.9.13. Okolnosti suspenzije i prekida suspenzije potvrde

Suspenzija je privremeno deaktiviranje elektronske potvrde izdane korisniku.

Ovjerilac JP BH POŠTA može da suspendira elektronske potvrde tokom provjeravanja okolnosti u vezi s mogućim opozivom potvrde.

Prekidom (ukidanjem) suspenzije elektronska potvrda postaje aktivna (važeća), tako da ima sve funkcionalnosti koje je imala i prije suspenzije.

4.9.14. Ko može da zahtijeva suspenziju i prekid suspenzije potvrde

Suspenziju elektronske potvrde može da zahtijeva:

- Korisnik elektronske potvrde – fizičko lice,
- Pravno lice za zaposlene u tom pravnom licu,
- Ovjerilac JP BH POŠTA ,
- Nadležni državni organ na osnovu zakona.

Prekid suspenzije može da zahtijeva:

- Korisnik elektronske potvrde, kada ustanovi da su razlozi za suspenziju prestali,
- Pravno lice, nakon prestanka razloga suspenzije potvrde,
- Ovjerilac JP BH POŠTA , kada ustanovi da su razlozi za suspenziju prestali,
- Nadležni državni organ, na osnovu zakona.

4.9.15. Procedure za suspenziju i prekid suspenzije potvrde

Suspenzija ili prekid suspenzije elektronske potvrde, vrši se na sljedeći način:

Korisnik potvrde pristupa web stranici Ovjerioca https://ca.posta.ba/ i online popunjava tražene podatke za promjenu statusa digitalnog certifikata u kojem pod „Vrsta promjene statusa“ treba izabrati „suspenzija“ ili „prekid suspenzije“. Nakon kreiranja zahtjeva za suspenziju ili prekid suspenzije digitalnog certifikata korisnik potvrde, dobija poruku da je uspješno popunio prijavu za suspenziju ili prekid suspenzije digitalnog certifikat te zahtjev preuzima, štampa i svojeručno potpisuje i isti lično podnosi na jednoj od lokacija Registracijskog tijela Ovjerioca JP BH POŠTA, kojom prilikom je obavezan radi identifikacije ovlaštenom šalterskom radniku dati na uvid identifikacioni dokument (lična karta ili pasoš).

Pravno lice može izvršiti suspenziju ili prekid suspenzije certifikata za zaposlenika tako što pristupa web stranici Ovjerioca https://ca.posta.ba/revoke i online popunjava tražene podatke za promjenu statusa digitalnog certifikata u kojem pod „Vrsta promjene statusa“ treba izabrati „suspenzija“ ili „prekid suspenzije“. Nakon kreiranja zahtjeva za suspenziju ili prekid suspenzije digitalnog certifikata zaposlenika, pravno lice dobija poruku da je uspješno popunilo prijavu za suspenziju ili prekid suspenzije digitalnog certifikat nakon čega zahtjev preuzima i štampa te se potpisan i opečaćen od strane ovlaštenog lica u pravnom licu podnosi na jednoj od lokacija Registracijskog tijela Ovjerioca „JP BH POŠTA“ d.o.o. Sarajevo.

Zaposlenik Registracijskog tijela šalje verificiran zahtjev Voditelju Registracijskog tijela internom poštom. Dodatno, uposlenik Registracijskog tijela šalje skeniran zahtjev email-om Voditelju Registracijskog tijela. Voditelj Registracijskog tijela bez odlaganja provodi proceduru realizacije zahtjeva te izdaje nalog za suspenziju ili prekid suspenzije koji uz zahtjev za suspenziju ili prekid suspenzije dostavlja Voditelju tijela za operativne poslove internom poštom i šalje skeniran zahtjev email-om. Voditelj OA zaprimljeni nalog za suspenziju ili prekid suspenzije uz zahtjev za suspenziju ili prekid suspenzije prosljeđuje na realizaciju HSM Operteru internom poštom i šalje skeniran zahtjev email-om.

Radno vrijeme Registracijskog tijela je ponedjeljak – petak od 08:00 sati do 15:00 sati, a Tijela za operativne poslove JP BH POŠTA je ponedjeljak – petak od 08.00 do 16:00 sati.

Tijelo za operativne poslove verifikuje zahtjev korisnika potvrde ili pravnog lica dobijen od Voditelja Registracijskog tijela izvršava suspenziju ili prekid suspenzije elektronske potvrde te obavještava Voditelja Registracijskog tijela o izvršenju. Voditelj Registracijskog tijela

obavještava korisnika potvrde o suspenziji ili prekidu suspenizije elektronskom poštom. Ako se radi o korisniku potvrde u pravnom licu o suspenziji ili prekidu suspenzije se obaviještava i pravno lice. U slučaju da korisnik potvrde ili pravno lice ne posjeduju adresu elektronske pošte, obavještenje o opozivu bit će poslato poštom na adresu naznačenu u ugovoru.

4.9.16. Ograničenje perioda na koji se potvrda suspenduje

Period suspenzije elektronske potvrde je maksimalno 30 dana.

4.10. Usluge o statusu potvrda

4.10.1. Operativne karakteristike

Ovjerilac JP BH POŠTA pruža uslugu provjere statusa opozvanosti elektronske potvrde posredstvom registra opozvanih potvrda.

4.10.2. Dostupnost usluge

Registar opozvanih potvrda je stalno dostupan.

4.10.3. Dodatne karakteristike

U registru opozvanih potvrda pored podataka o serijskom broju, datumu i vremenu opoziva elektronske potvrde upisan je i razlog opoziva potvrde.

4.11. Prestanak korištenja potvrde

Korisnik prestaje s korištenjem elektronske potvrde:

- Istekom roka važnosti elektronske potvrde,
- Opozivom elektronske potvrde ili tijekom trajanja suspenzije elektronske potvrde.

4.12. Otkrivanje i obnova privatnog ključa korisnika

4.12.1. Politika otkrivanja i obnove privatnog ključa korisnika

Ovjerilac JP BH POŠTA ne čuva privatne ključeve korisnika kvalificiranih elektronskih potvrda i ne može da ih otkrije niti obnovi.

4.12.2. Politika enkapsulacije ključa sesije i obnove

Ne vrši se.

5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURE I OVLAŠTENIH LICA

Ovaj segment opisuje nadzor fizičkog pristupa, procedure i ovlaštena lica primijenjena u JP BH POŠTA kako bi se osiguralo nesmetano funkcioniranje sistema.

JP BH POŠTA usvojila je politiku informacijske sigurnosti, koja je odobrena od strane Uprave Društva, kako bi usmjeravala upravljanje sigurnošću informacija. Eventualne promjene u politici informacijske sigurnosti bit će obavještene treće strane po potrebi, uključujući pouzdane partnere, ocjenjivače tijela i regulatorna tijela.

Identificiraju se, analiziraju i procjenjuju poslovni i tehnički rizici u skladu s ISO 9001 i ISO/IEC 27001 standardima. JP BH POŠTA primjenjuje sve sigurnosne zahtjeve i operativne postupke dokumentirane u politici informacijske sigurnosti kako bi smanjila rizike.

JP BH POŠTA vodi inventar svih informacijskih sredstava i dodjeljuje im klasifikaciju prema ocjeni rizika.

Politika informacijske sigurnosti i inventar informacijske opreme redovito se pregledavaju (najmanje jednom godišnje) kako bi se osigurala njihova svrsishodnost i učinkovitost, te u slučaju značajnih promjena. Sve promjene koje bi mogle utjecati na razinu sigurnosti moraju dobiti odobrenje od Tijela za upravljanje radom JP BH POŠTA.

5.1. Kontrola fizičkog pristupa

JP BH POŠTA, kao pružatelj usluga izdavanja kvalificiranih elektronskih potvrda, primjenjuje mjere fizičke sigurnosti sistema u skladu s ovim pravilima, važećim zakonima i propisima te međunarodnim preporukama u skladu sa standardom ISO/IEC 27001.

Mjere fizičke sigurnosti sistema izdavanja elektronskih potvrda temelje se na procjeni rizika kako bi se ograničio pristup hardverskim i softverskim komponentama sistema, uključujući servere, radne stanice, kriptografske module, mrežne uređaje i pripadajući softver te arhive.

5.1.1. Lokacija i raspored prostorija (okolišna sigurnost)

Provode se kontrole kako bi se spriječili gubitak, oštećenje ili ugrožavanje imovine i prekid poslovnih aktivnosti. Oprema JP BH POŠTA smještena je u sigurnoj prostoriji koja je osigurana dvoslojnom električnom bravom u zgradi Generalne direkcije JP BH POŠTA. Kontrola fizičkog pristupa JP BH POŠTI provodi se u skladu sa Zakonom o elektronskom potpisu i podzakonskim aktima na sljedeći način:

Pristup prostorijama bilježi se elektronski i evidentira se u elektronskom dnevniku za pristup prostorijama, a isti se pregledava.

Brave, elektronski sistemi zaštite i sistemi protupožarne zaštite su usklađeni s važećim standardima.

Prostor i sistem nadziru se 24 sata, 7 dana u sedmici od strane ovlaštenih osoba JP BH POŠTA.

Pristup je moguć samo uz prisustvo najmanje dvije ovlaštene osobe s pravom pristupa.

Pristup zbog održavanja sistema mora biti unaprijed najavljen, osim u slučaju smetnji u radu sistema, za koje Tijelo za operativne poslove JP BH POŠTA utvrdi da zahtijevaju hitnu intervenciju.

Svaki pristup zaštićenim prostorijama bilježi se unutar elektronskog evidencijskog sistema.

5.1.2. Kontrola fizičkog pristupa za pojedince

Ovjerilac JP BH POŠTA jamči da samo ovlašteni zaposlenici imaju pristup sistemu ovjeravanja.

Zaposlenici u Ovjeriocu JP BH POŠTA moraju se pridržavati sljedećih obveza:

Izvršavati svoje administratorske dužnosti u sigurnoj zoni. Ulazak u sigurnu zonu moguć je isključivo uz identifikaciju putem beskontaktne kartice. Otvaranje ormara u kojima se čuva oprema Ovjerioca JP BH POŠTA dopušteno je samo uz identifikaciju s posebnom beskontaktnom karticom, koju posjeduje drugo ovlašteno lice.

Čuvati beskontaktnu karticu koja omogućuje ulazak u sigurnu zonu i otvaranje ormara s opremom.

Pohranjivati kartice HSM administratora i HSM operatora te druge medije koji sadrže kriptografske ključeve, pristupne parametre korisničkih računa ili druge povjerljive podatke u sigurnom kasu-kontejneru. Za otvaranje kasu-kontejnera potrebno je imati par ključeva.

Zaštititi lozinke koje omogućuju pristup privatnim kriptografskim ključevima.

Čuvati rezervne kopije privatnih ključeva u sigurnom kasa-kontejneru.

Zaposlenici s odgovarajućim ulogama u sistemu trebaju štititi svoje identifikacijske uređaje za pristup sistemu, što omogućuje centralizirano praćenje i upravljanje životnim ciklusom kriptografskih uređaja.

Zaposlenici s odgovarajućim ulogama u sistemu trebaju štititi svoje identifikacijske uređaje za pristup Desktop aplikaciji koja služi za elektronsku personalizaciju kriptografskih uređaja.

Nakon završetka rada s aplikacijama, zaposlenici trebaju pohraniti svoje identifikacijske uređaje na sigurno mjesto.

Odjavljivati se iz svih aplikacija kada napuste računar, a računar ostaje bez nadzora.

Zaposlenici koji obavljaju poslove prijema zahtjeva za izdavanje elektronske potvrde i prijema zahtjeva za promjenu statusa potvrde u regionalnom centru dužni su pridržavati se sljedećih obveza:

Izvršavati svoje dužnosti u zoni prijema.

Čuvati autentikacijske podatke koji omogućavaju prijavljivanje na aplikaciju Registracijskog tijela.

Odjavljivati se iz svih aplikacija kada napuste računar, a računar ostane bez nadzora.

5.1.3. Napajanje i klimatizacija

Prostorije u kojima se nalazi infrastruktura Ovjerioca JP BH POŠTA u glavnom uredu opremljene su:

- Sistemom za neprekidno napajanje električnom energijom i stabilizaciju napona za računarsku i komunikacijsku opremu, koji je povezan s generatorom,
- Nezavisnim sistemom za klimatizaciju koji omogućava kontrolu temperature i vlažnosti zraka unutar prostorija Ovjerioca JP BH POŠTA.

5.1.4. Zaštita od poplava

Oprema Ovjerioca JP BH POŠTA smještena je na mjestu koje je osigurano od poplava.

5.1.5. Zaštita od požara

Oprema Ovjerioca JP BH POŠTA je zaštićena automatskim sistemom za protupožarnu zaštitu u skladu s važećom zakonskom regulativom.

5.1.6. Smještanje medija

Svi računarski mediji koji sadrže podatke o poslovima Ovjerioca JP BH POŠTA, uključujući i medije s rezervnim kopijama podataka, pohranjuju se u vatrootporne sigurne kase-kontejnere. Jedan se nalazi na centralnoj lokaciji Ovjerioca JP BH POŠTA, a drugi u drugoj sigurnosnoj zoni JP BH POŠTA.

5.1.7. Odlaganje nepotrebnih podataka

Nepotrebna papirna dokumentacija i računarski mediji koji sadrže podatke uništavaju se uz komisijski nadzor. Podaci s medija, kao što su kriptografski ključevi, podaci za aktiviranje ili elektronski dnevnici, nepovratno se brišu prije slanja medija na uništavanje. Uništavanje medija na kojima se nalaze povjerljivi podaci, kao i uništavanje podataka i ključeva povezanih s HSM modulima, provodi se u skladu s internim procedurama JP BH POŠTA, prema Uputstvu o popisu sredstava i obaveza i rashodovanju imovine, broj U.D.-01.3.1-18508/19 od 06.12.2019. godine. Brisane i uništavanje podataka HSM modula provodi se i prije njihovog eventualnog slanja na servis ili popravak, kao i prilikom svakog njihovog uklanjanja iz sigurne zone Ovjerioca JP BH POŠTA i njihovog transportovanja na druge lokacije JP BH POŠTA.

5.1.8. Smještaj rezervnih kopija podataka

Ovjerilac JP BH POŠTA koristi lokaciju u drugoj sigurnosnoj zoni za smještaj medija s podacima. Mediji se čuvaju u kasa-kontejneru. Prostoriju u kojoj je smještena vatrootporna sigurna kasa-kontejner nadziru ovlaštena lica JP BH POŠTA.

5.2. Kontrola procedura

5.2.1. Povjerljive uloge ovlaštenih lica

Ovlaštenici JP BH POŠTA jamče da će svi poslovi unutar propisane djelatnosti biti obavljeni od strane osoba od povjerenja s precizno definiranim obvezama i ovlastima. Rad tih osoba će biti redovno provjeravan.

Ovisno o dodijeljenim ulogama, ovlašteni članovi JP BH POŠTA mogu obavljati poslove na sljedećim područjima:

- HSM modulima,
- Serverima JP BH POŠTA,
- Aplikacijama JP BH POŠTA,
- Aplikaciji Registracijskog tijela,
- Desktop aplikaciji za personalizaciju kriptografskih uređaja,
- Mrežnim uređajima i pristupnim listama.

Prava pristupa određenih korisničkih računa na računarskim operativnim sistemima i korisničkih računa u aplikacijama ograničena su kako bi omogućila ovlaštenim osobama Ovjerioca JP BH POŠTA izvođenje samo potrebnih radnji u okviru svojih zadataka.

Unutar Ovjerioca JP BH POŠTA postoji nekoliko sigurnosnih funkcija:

Sistemski administrator - odgovoran za instalaciju, konfiguraciju i održavanje sigurnih sistema JP BH POŠTA za registraciju korisnika, izdavanje elektronskih potvrda i distribuciju tačnog vremena. Osigurava sredstva za stvaranje sigurnih elektronskih potpisa za korisnike i upravljanje opozivom elektronskih potvrda. Odgovoran je za provedbu sigurnosnih postupaka za stvaranje sigurnosnih kopija.

Mrežni administrator sistema - odgovoran je za konfiguraciju i održavanje mrežnih elemenata sistema (Firewall, Switch). Osigurava da je konfguracija optimizirana sa sigurnosnog aspekta. Redovno provodi stvaranje sigurnosnih kopija konfiguracija mrežnih uređaja.

Inženjer za informacijsku sigurnost - upravlja sigurnosnim funkcijama i postupcima, nadzire aktivnosti u vezi s izdavanjem, opozivom i suspenzijom elektronskih potvrda.

5.2.2. Potreban broj ovlaštenih lica za operativne poslove

JP BH POŠTA primjenjuje dvostruku autorizaciju za ključne operativne zadatke u aplikaciji Ovjerioca, kako je opisano u ovom odjeljku.

Za izvođenje sljedećih zadataka potrebno je dvostruko odobrenje administratora Ovjerioca:

- Generiranje privatnih kriptografskih ključeva za aplikaciju Ovjerioca i obnavljanje ovjeriteljevih profila,
- Konfiguracija HSM uređaja,
- Zamjena lozinke kartica za upravljanje HSM uređajima,
- Zamjena jedne ili više setova operaterskih kartica,
- Analiza sistemskih poruka na HSM uređajima,
- Dodavanje drugih čitača kartica na HSM uređaje,
- Promjena trajanja CRL liste,
- Obnova profila i resetiranje zaboravljenih lozinki korisnika za izdavanje digitalnih potvrda.

Isto tako, dvostruka autorizacija se koristi za pristup sigurnim trezorima/kasama.

Svi ostali zadaci, koji nisu navedeni u ovom tački, izvršavaju se uz odobrenje jednog ovlaštenog lica JP BH POŠTA.

5.2.3. Identifikacija i autentifikacija ovlaštenih lica

JP BH POŠTA provodi verifikaciju svojih zaposlenika prije nego što im dodijeli odgovarajuće ovlasti, kao što su:

- Upis na odgovarajuću listu za pristup sigurnim prostorijama JP BH POŠTA,
- Identifikacijske beskontaktne kartice za pristup sigurnoj zoni,
- Identifikacijske beskontaktne kartice za pristup serverskom ormaru,
- Korisnički račun na operativnom sistemu servera i radnih stanica JP BH POŠTA,
- Administratorske i operaterske kartice za HSM,
- Korisnički račun u aplikaciji Ovjerioca JP BH POŠTA,
- Korisnički račun u aplikaciji Registracijskog tijela i
- Korisnički račun u Desktop aplikaciji za personalizaciju kriptografskih uređaja.

Svi korisnički računi, kartice i potvrde za ovlaštena lica JP BH POŠTA-a stvaraju se posebno za svaku ovlaštenu osobu.

Zabranjeno je zajedničko korištenje korisničkih računa, kartica ili potvrda između ovlaštenih osoba u JP BH POŠTA.

5.2.4. Razgraničenje ovlasti ovlaštenih lica

Aktivnosti zaposlenih u JP BH POŠTA ograničene su prema ovlastima definiranim na razini:

- Hardverskih kriptografskih uređaja (HSM),
- Operativnih sistema servera i radnih stanica,
- Aplikacija Ovjerioca JP BH POŠTA,
- Aplikacija za upravljanje potvrdama i izdavanje potvrda,
- Aplikacija za personalizaciju kriptografskih uređaja,
- Aplikacija Registracijskog tijela.

5.3. Kontrola ovlaštenih lica

Poslove unutar Ovjerioca JP BH POŠTA, u skladu s Praktičnim pravilima, obavljaju zaposlenici koji su u radnom odnosu u JP BH POŠTA. Zaposlenici Ovjerioca JP BH POŠTA moraju biti kvalificirani za obavljanje poslova navedenih u ovim Praktičnim pravilima i podliježu ocjeni njihovih stručnih sposobnosti.

Zaposlenici Ovjerioca JP BH POŠTA ne smiju otkrivati povjerljive informacije o sigurnosti Ovjerioca JP BH POŠTA ili informacije o korisnicima elektronskih potvrda neovlaštenim osobama.

Zaposlenicima Ovjerioca JP BH POŠTA ne dodjeljuju se zadaci izvan njihovog opsega poslova za koje su angažirani, a koji bi mogli stvoriti sukob interesa s njihovim trenutnim poslovima.

Zaposlenicima Ovjerioca JP BH POŠTA od strane Voditelja CA dostavljaju se detaljni postupci koje moraju slijediti .

5.3.1. Zahtjevi za kvalifikacije, iskustvo i provjeru ovlaštenih lica

Zaposlenici Ovjerioca JP BH POŠTA moraju ispunjavati specifične zahtjeve u vezi s njihovom stručnom kvalifikacijom za svaku poziciju za koju su angažirani, kao i u pogledu njihovog radnog iskustva i iskustva na sličnim radnim mjestima. Prilikom zapošljavanja uzima se u obzir da osoba koja se zaposli nije osuđivana za djela povezana s poslovima koje obavlja u JP BH POŠTA.

5.3.2. Postupci za provjeru prethodnih radnih iskustava

Provjeru prethodnih radnih iskustava osoba koje rade u Ovjerioca JP BH POŠTA provodi se u skladu s važećim zakonima i propisima u toj oblasti.

5.3.3. Obuka

Obuka zaposlenika u JP BH POŠTA obuhvaća:

- Upoznavanje s infrastrukturom JP BH POŠTA,
- Razumijevanje postupaka zaštite infrastrukture i podataka,
- Osposobljavanje za upotrebu aplikacija JP BH POŠTA, u skladu s dodijeljenom ulogom,
- Osposobljavanje za izradu sigurnosnih kopija podataka,
- Postupci oporavka sistema nakon štete,
- Razumijevanje drugih zadataka vezanih za rad u JP BH POŠTA.

Zaposlenicima koji zaprimaju zahtjeve također se pruža obuka koja uključuje:

- Upoznavanje s aktivnostima Ovjerioca JP BH POŠTA, vrstama potvrda i zahtjevima za promjenu statusa potvrda,
- Osposobljavanje za upotrebu aplikacije Registracijskog tijela,
- Razumijevanje drugih zadataka vezanih za rad u Ovjeriocu JP BH POŠTA.

Za polaznike obuke osigurava se relevantna literatura u skladu s temom obuke.

5.3.4. Učestalost ponovnih obuka

Zaposlenici u Ovjeriocu JP BH POŠTA redovno pohađaju obuke za obnavljanje i unapređenje svojih znanja najmanje jednom godišnje. Dodatno, vanredne obuke organiziraju se kada dođe do promjena u tehničkim sredstvima (hardveru i softveru) Ovjerioca JP BH POŠTA ili u načinu obavljanja poslova.

5.3.5. Učestalost i redoslijed rotacije poslova ovlaštenih lica

Ovjerilac JP BH POŠTA nije uspostavio pravila rotacije poslova kako bi se izbjeglo narušavanje pravila u vezi s obavljanjem različitih ovlaštenja i dužnosti. Ovo je učinjeno kako bi se očuvala integritet različitih povjerljivih uloga zaposlenih u Ovjeriocu JP BH POŠTA.

5.3.6. Sankcije za neautorizirane aktivnosti

U slučaju izvršenih ili sumnji na izvršene neautorizirane aktivnosti od strane ovlaštenog lica u Ovjeriocu JP BH POŠTA, tom licu će biti onemogućen daljnji pristup tehničkim sredstvima (hardveru i softveru) Ovjerioca JP BH POŠTA, a Ovjerilac JP BH POŠTA će suspendirati ili opozvati sve važeće elektronske potvrde koje su izdate tom licu. Sve neautorizirane aktivnosti prijavljuju se nadležnim organizacijskim jedinicama JP BH POŠTA, državnim organima i institucijama, u skladu sa važećim zakonskim i internim pravilima.

5.3.7. Zahtjevi za vanjske saradnike

U slučaju dodjele povjerljive uloge vanjskom saradniku, isti uvjeti vrijede kao i za stalno zaposlena lica u Ovjeriocu JP BH POŠTA.

5.3.8. Dokumentacija za potrebe zaposlenih

Zaposlenicima se pruža odgovarajuća dokumentacija s detaljnim opisom procedura koje moraju slijediti u svojem radu.

5.4. Postupak nadgledanja rada sistema

Sve aktivnosti koje se odnose na obavljanje zadataka Ovjerioca u JP BH POŠTA detaljno se bilježe u elektronskim dnevnicima (audit logovima) i ručno vođenim evidencijama, zajedno s datumom i vremenom događaja.

5.4.1. Vrste događaja koje se evidentiraju

Evidentiraju se različite vrste događaja, uključujući:

- Izdavanje potvrda Ovjerioca JP BH POŠTE i potvrda Ovjerioca koji mu je podređen.
- Upravljanje životnim ciklusom ključeva Ovjerioca u JP BH POŠTI.
- Upravljanje životnim ciklusom hardverskih kriptografskih uređaja.
- Opozivanje potvrda koje izdaje Ovjerilac JP BH POŠTA Root CA.
- Radnje s korisničkim kriptografskim ključevima i elektronskim potvrdama, uključujući izdavanje, preuzimanje, opoziv, suspenziju, prekid suspenzije, deaktivaciju, arhiviranje itd.

- Upravljanje kriptografskim ključevima aplikacije Ovjerioca.
- Održavanje tehničke opreme (hardver i softver) Ovjerioca JP BH POŠTA.
- Administracija, uključujući izradu rezervnih kopija, primjenu sigurnosnih pravila i korištenje aplikacija Ovjerioca.
- Fizički pristup sistemu Ovjerioca JP BH POŠTA, uključujući i uspješne i neuspješne pokušaje pristupa.
- Pokretanje i zaustavljanje servisa Ovjerioca JP BH POŠTA.
- Održavanje sistema, reagiranje na kvarove hardvera.
- Promjene u kadrovskoj strukturi Ovjerioca JP BH POŠTA.

5.4.2. Periodičnost pregleda elektronskih dnevnika i ručnih evidencija

Ovlašteni administratori u JP BH POŠTI pregledavaju elektronske dnevnike i ručne evidencije jednom sedmično. Ovaj pregled obuhvata:

Sakupljanje svih elektronskih dnevnika i ručnih evidencija od posljednjeg pregleda.

Pregled i analiza zapisa u elektronskim dnevnicima i ručnim evidencijama.

Rješavanje eventualnih problema ili prijava koje se šalju Voditelju CA, a koji preduzima daljnje korake za njihovo rješavanje.

5.4.3. Retencija evidencija

Kopije elektronskih dnevnika i ručnih evidencija čuvaju se najmanje godinu dana.

5.4.4. Zaštita elektronskih dnevnika

Elektronski dnevnici i ručne evidencije štite se mehanizmima i postupcima koji garantiraju povjerljivost i integritet tih zapisa. Novi zapisi se ne smiju automatski upisivati preko postojećih zapisa. Pristup takvim zaštićenim elektronskim dnevnicima i ručnim evidencijama dostupan je samo ovlaštenim osobama na zahtjev.

5.4.5. Kreiranje rezervnih kopija elektronskih dnevnika

Elektronski dnevnici se ažuriraju svakodnevno, a za kreiranje rezervnih kopija odgovorne su ovlaštene osobe u JP BH POŠTI. Rezervne kopije elektronskih dnevnika čuvaju se u Generalnoj direkciji JP BH POŠTA.

5.4.6. Sistem prikupljanja podataka za elektronske dnevnike i ručne evidencije

Sistem prikupljanja podataka za elektronske dnevnike i ručne evidencije u svim sistemima Ovjerioca JP BH POŠTA je interni sistem koji kombinira automatizirane i ručne procese. Taj sistem se izvršava na serverima Ovjerioca JP BH POŠTA i kontroliraju ga zaposlenici Ovjerioca JP BH POŠTA s povjerljivim ulogama.

Događaji koji se zapisuju u elektronske dnevnike i ručne evidencije	**Način prikupljanja podataka**	**Odgovorno lice ili sistem**
Događaji povezani sa elektronskim potvrdama	automatsko	aplikacija Ovjerioca JP BH POŠTA
Registar izdatih elektronskih potvrda	automatsko, ručno	aplikacija Ovjerioca JP BH POŠTA, zaposleni Ovjerioca JP BH POŠTA
Događaji povezani sa aplikacijama Ovjerioca JP BH POŠTA	automatsko	aplikacije Ovjerioca JP BH POŠTA
Događaji na operativnom sistemu	automatsko	operativni sistem
Događaji na računarskoj mreži	automatsko	*firewall*-i, operativni sistem
Kreiranje rezervnih kopija i obnova baze korisnika elektronskih potvrda	automatsko	operativni sistem, aplikacija Ovjerioca JP BH POŠTA, zaposleni Ovjerioca JP BH POŠTA
Kreiranje rezervnih kopija konfiguracije i infrastrukture Ovjerioca JP BH POŠTA	automatsko	operativni sistem, aplikacija Ovjerioca JP BH POŠTA
Fizički pristup do PKI infrastrukture Ovjerioca JP BH POŠTA	automatsko	zaposleni Ovjerioca JP BH POŠTA, sistem za kontrolu pristupa
Pristup sefu u kome su smještene administratorske i operatorske kartice HSM uređaja	ručno	zaposleni Ovjerioca JP BH POŠTA
Pristup sefu u kome su smještene lozinke administratorskih računa servera PKI okruženja, lozinke administratorskih i operatorskih kartica HSM uređaja, lozinke za pristup aplikacijama JP BH POŠTA Ovjerioca	ručno	zaposleni Ovjerioca JP BH POŠTA
Promjene hardvera i softvera na sistemu	ručno	zaposleni Ovjerioca JP BH POŠTA

Održavanje rada na sistemu i prostoru	ručno	zaposleni Ovjerioca JP BH POŠTA
Kadrovske promjene	ručno	zaposleni Ovjerioca JP BH POŠTA

Tabela 19. Događaji koji se zapisuju u elektronske dnevnike i ručne evidencije i načini prikupljanja zapisa o tim događajima

5.4.7. Obavještavanje o incidentnim događajima

Voditelj Certifikacijskog Autoriteta (CA) mora biti obaviješten o svakom incidentnom događaju. Osoba koja je uzrokovala incident neće biti obaviještena.

Ovlašteni predstavnik Ovjerioca JP BH POŠTA djeluje promptno i koordinirano kako bi brzo reagirao na incidente i ograničio njihov uticaj na sigurnost.

Definirani su zaposlenici čija je odgovornost praćenje upozorenja o potencijalno ozbiljnim sigurnosnim incidentima i obavezno prijavljivanje relevantnih incidenta.

Ovlašteni predstavnik Ovjerioca JP BH POŠTA izvještava nadležno tijelo u skladu s važećim regulatornim pravilima o svakom sigurnosnom prekršaju ili gubitku integriteta, u roku od 24 sata od trenutka utvrđivanja prekršaja.

Ukoliko incident ugrozi sigurnost ili integritet fizičkih ili pravnih osoba kojima je pružena pouzdana usluga, isto tako će se obavijestiti te osobe o incidentu bez nepotrebnog odlaganja.

Svaka ozbiljna ranjivost koju ovlašteni predstavnik JP BH POŠTA prethodno nije riješio bit će sanirana u roku od 48 sati od njenog otkrivanja.

5.4.8. Procjena ranjivosti sistema

Procjena ranjivosti sistema se sprovodi kao deo svakodnevnih aktivnosti koje se izvode na sistemu, analiziranjem rizika, razmenom iskustava sa ovjeriocima iz okoline i pregledom elektronskih dnevnika i ručnih evidencija.

5.5. Arhiviranje podataka

5.5.1. Vrste podataka koje se arhiviraju

Ovjerilac JP BH POŠTA arhivira sljedeće podatke i dokumenta:

- Ugovore i dokumentaciju korisnika,
- Zahtjeve za korištenje usluga ovjerioca za izdavanje elektronskih potvrda
- Zahtjeve za izdavanje i korišćenje elektronske potvrde,
- Zahtjeve za promjenu statusa elektronske potvrde (opoziv, suspenzija, prekid suspenzije i drugo),
- Registre opozvanih potvrda,
- Interni akti Ovjerioca JP BH POŠTA vezani za obavljanje delatnosti Ovjerioca JP BH POŠTA.

5.5.2. Period čuvanja podataka u arhivi

Ovjerilac obezbjeđuje trajno čuvanje svih relevantnih podataka koji se odnose na elektronske potvrde, u skladu sa važećim propisima.

5.5.3. Zaštita arhive

Arhiva dokumenata se čuva na centralnoj lokaciji Ovjerioca JP BH POŠTA (generalna direkcija JP BH POŠTA).

Arhiva je zaštićena odgovarajućim sigurnosnim mehanizmima Ovjerioca JP BH POŠTA (fizičkom i tehničkom zaštitom, ograničenim pristupom, šiframa i ključevima). Pristup arhivama je dozvoljen samo ovlaštenim licima.

Arhiva se čuva na centralnoj lokaciji Ovjerioca JP BH POŠTA (generalna direkcija JP BH POŠTA).

5.5.4. Procedure arhiviranja rezervnih kopija

Arhiva se čuva na centralnoj lokaciji Ovjerioca JP BH POŠTA (generalna direkcija JP BH POŠTA

5.5.5. Vremenska oznaka arhiviranih podataka

Arhivirani podaci sadrže vremensku oznaku sa servera koji je sinhronizovan sa izvorom tačnog vremena.

5.5.6. Sistem arhiviranja (interni ili eksterni)

Arhiviranje elektronskih podataka sprovode zaposleni u Ovjeriocu JP BH POŠTA, interno, koristeći tehnička sredstva za arhiviranje koja su u vlasništvu Ovjerioca JP BH POŠTA.

5.5.7. Procedure kontrole pristupa arhiviranim podacima

Arhivirani elektronski podaci se čuvaju u kasama-kontejnerima za čije otvaranje su potrebna dva ključa. Kase-kontejneri se nalaze u zaštićenim prostorijama. Pristup arhivama je dozvoljen samo ovlaštenim licima.

5.6. Generiranje novih ključeva Ovjerioca

Generiranje novih ključeva Ovjerioca JP BH POŠTA vrši se pet godina prije isteka roka važnosti postojećih ključeva. Generiranje ključeva može se sprovesti i ranije iz sledećih razloga:

- Potrebno je promijeniti kriptografski algoritam kojim ovjerilac potpisuje potvrde i registre opozvanih potvrda,
- Potrebno je promijeniti dužinu ključeva Ovjerioca,
- Potrebno je promijeniti rok važnosti ključeva Ovjerioca,
- Potrebno je promijeniti hash algoritam Ovjerioca, primjenom koga se izračunava hash vrijednost potvrde i registra opozvanih potvrda,

- Potrebno je promijeniti sadržaj postojećih polja ili ekstenzija potvrde Ovjerioca ili dodati nove ekstenzije potvrdi Ovjerioca,
- Privatni ključ Ovjerioca je oštećen ili kompromitiran.

5.7. Oporavak sistema nakon katastrofe

Održava se plan kontinuiteta rada za reagiranje u slučaju katastrofe, uključujući kompromitaciju privatnog ključa za potpis ili neku drugu kompromitaciju.

Procedure se obnavljaju u skladu s planom kontinuiteta nakon rješavanja bilo kojeg uzroka katastrofe koji se može ponoviti (npr. sigurnosna ranjivost) i odgovarajućim mjerama sanacije.

5.7.1. Procedure rada u slučaju katastrofe ili prilikom kompromitiranja sistema

Ovjerilac JP BH POŠTA ima planove za očuvanje i oporavak sistema ovjeravanja nakon katastrofe. Internim planovima obuhvaćeni su postupci očuvanja i oporavka sistema u slučaju katastrofe uzrokovane kvarom opreme, ljudskom greškom, otuđenjem ili kompromitiranjem opreme i podataka, požarom, prirodnom katastrofom, terorističkim aktima itd.

Internim planovima obuhvaćeni su i postupci koje treba preduzeti kako bi se sistem oporavio i kako bi se ponovno uspostavili prvobitni sigurnosni uslovi sistema Ovjerioca.

5.7.2. Oštećenja u računarskim resursima, programima i/ili podacima

U slučaju štete nastale na tehničkim sredstvima (hardveru i softveru) ili podacima, pri čemu privatni kriptografski ključ aplikacije Ovjerioca nije uništen ili oštećen, usluge aplikacije Ovjerioca će biti ponovno uspostavljene u najkraćem mogućem roku.

U slučaju uništenja ili oštećenja privatnog kriptografskog ključa aplikacije Ovjerioca, nakon što se otkloni uzrok uništenja ili oštećenja, sprovodi se postupak rekonstrukcije ključa.

5.7.3. Kompromitiranje privatnog kriptografskog ključa aplikacije Ovjerioca

U slučaju da dođe do kompromitiranja privatnog kriptografskog ključa aplikacije Ovjerioca, Ovjerilac JP BH POŠTA će odmah preduzeti sljedeće korake:

- Povući izdate elektronske potvrde.
- Povući potvrdu aplikacije Ovjerioca.
- Javno objaviti registar povučenih potvrda.
- Obavijestiti korisnike izdatih elektronskih potvrda.

Nakon što uzrok kompromitiranja bude uklonjen, Ovjerilac JP BH POŠTA će:

- Generirati nove kriptografske ključeve za aplikaciju Ovjerioca.
- Izdati korisnicima nove elektronske potvrde.

5.7.4. Nastavak rada poslije katastrofe

Nakon što se katastrofa završi i njen uzrok otkloni, Ovjerilac JP BH POŠTA će se potruditi da što prije vrati sistem u produktivno stanje i nastavi s radom.

5.8. Prestanak rada Ovjerioca

U slučaju prestanka rada, Ovjerilac JP BH POŠTA će preduzeti sljedeće obaveze:

- Obavijestiti sve relevantne strane, uključujući nadležne organe i svoje korisnike, o prestanku rada.
- Pokušati prenijeti svoje obaveze na drugog Ovjerioca, ako je to moguće.
- Povući sve izdate elektronske potvrde koje nisu istekle ukoliko ne uspije prenijeti svoje obaveze na drugog Ovjerioca.
- Uništiti ili potpuno onemogućiti korištenje svojih privatnih ključeva koji su korišteni za kreiranje potvrda i registra povučenih potvrda, kako bi se spriječila njihova rekonstrukcija.
- Ovjerilac JP BH POŠTA će obavijestiti svoje korisnike i nadležne državne organe o planiranom prestanku obavljanja usluga elektronskog potpisa i ovjeravanja u skladu s važećim propisima.
- Ovjerilac JP BH POŠTA će uložiti sve napore kako bi osigurao nastavak pružanja usluge kod drugog Ovjerioca za svoje korisnike.
- Ovjerilac JP BH POŠTA ima obavezu dostaviti svu postojeću dokumentaciju i arhivu Ovjeriocu kod kojeg je osigurao nastavak pružanja usluge prema svojim korisnicima.

Ukoliko nije moguć prijenos obaveza na drugog Ovjerioca, Ovjerilac JP BH POŠTA će raskinuti ugovore o izdavanju i korištenju elektronskih potvrda sa svojim korisnicima i povući sve važeće elektronske potvrde, o čemu će obavijestiti korisnike i nadležne državne organe.

Ovjerilac JP BH POŠTA će elektronskom poštom obavijestiti korisnike elektronskih potvrda i priznate Ovjerioce JP BH POŠTA, kao i Ovjerioce koji priznaju Ovjerioca JP BH POŠTA, o prestanku rada u skladu s važećim propisima.

Korisnici izdatih elektronskih potvrda bit će obaviješteni o prestanku rada putem zvanične web stranice Ovjerioca JP BH POŠTA ili na drugi način, putem sredstava javnog informiranja ili elektronske pošte.

6. KONTROLE TEHNIČKE ZAŠTITE

6.1. Generisanje parova kriptografskih ključeva i instalacija

6.1.1. Generisanje parova kriptografskih ključeva

JP BH POŠTA, u svojstvu Ovjerioca, održava aplikacije koje izvršavaju Root CA i Issuing CA JP BH POŠTA, a parovi njihovih kriptografskih ključeva generišu se tokom procesa ceremonije generisanja ključeva prema precizno definisanoj proceduri. Tokom ceremonije generisanja parova kriptografskih ključeva primjenjuju se mjere zaštite koje važe za prostorije Ovjerioca JP BH POŠTA, zaštitu koju pruža hardverski kriptografski modul (HSM), operativni sistem, aplikacija Ovjerioca i višestruka autentikacija ovlaštenih osoba.

Učesnici u Ceremoniji generisanja ključeva su ovlaštene osobe Ovjerioca JP BH POŠTA sa povjerljivim ulogama, a prisustvuje i revizor koji svjedoči da je Ceremonija generisanja parova ključeva sprovedena u skladu sa dokumentom "Ceremonija kreiranja PKI ključeva" JP BH POŠTA, koji služi kao protokol za generisanje ključeva i sadrži dokumentirane korake koji se preduzimaju tokom pomenute ceremonije.

Auditor potpisuje ovaj dokument na kraju ceremonije i tako potvrđuje da je postupak generisanja parova ključeva izvršen u skladu sa protokolom.

Sva lica koja su učestvovala u ceremoniji generisanja ključeva potpisuju ovaj dokument.

Kriptografski ključevi korisnika, koji se koriste za potpisivanje i verifikaciju kvalifikovanog elektronskog potpisa, generišu se na QSCD uređaju, koji predstavlja sredstvo za kreiranje kvalifikovanog elektronskog potpisa. Par kriptografskih ključeva povezanih sa korisničkom potvrdom za kreiranje kvalifikovanog elektronskog potpisa nikada se ne čuvaju na hardverskoj ili softverskoj opremi Ovjerioca JP BH POŠTA.

6.1.2. Uručenje privatnog kriptografskog ključa korisniku

Uručenje privatnog ključa korisniku vrši se putem QSCD uređaja u prostorijama Ovjerioca JP BH POŠTA, na mjestu podnošenja korisničkog zahtjeva.

6.1.3. Dostavljanje javnog kriptografskog ključa korisnika Ovjeriocu

Korisnički kriptografski javni ključ za izradu kvalifikovanog elektronskog potpisa generiše se zajedno sa privatnim ključem u Ovjeriocu JP BH POŠTA na QSCD uređaju, i nije potrebno da korisnik dostavlja javni kriptografski ključ Ovjeriocu.

6.1.4. Uručenje javnog kriptografskog ključa trećim licima

Javni kriptografski ključ aplikacije Ovjerioca u obliku potvrde je javno dostupan na web stranici Ovjerioca JP BH POŠTA.

Korisničkih javnih kriptografskih ključeva i potvrda Ovjerilac JP BH POŠTA ne objavljuje niti ih dostavlja trećim licima.

6.1.5. Dužine kriptografskih ključeva

Dužine kriptografskih ključeva koje Ovjerilac JP BH POŠTA koristi za izdavanje elektronskih potvrda su:

Kriptografski ključevi aplikacije Ovjerioca: RSA ključevi minimalne dužine od 3072 bita,

Korisnički ključevi: RSA ključevi minimalne dužine od 2048 bita.

6.1.6. Generisanje parametara javnog kriptografskog ključa i provjera kvaliteta

Generisanje parametara javnog kriptografskog ključa aplikacije Ovjerioca vrši se u hardverskim kriptografskim modulima Ovjerioca JP BH POŠTA, dok se parametri javnih kriptografskih ključeva korisnika generišu na kriptografskim QSCD uređajima i softveru Ovjerioca JP BH POŠTA, u skladu sa profilima potvrda.

Odgovorno lice Ovjerioca JP BH POŠTA postavlja parametre javnih ključeva aplikacije Ovjerioca i korisnika, kako je definisano u profilima potvrda.

6.1.7. Namjena ključeva

Privatni kriptografski ključ aplikacije Ovjerioca, kojeg održava Ovjerilac JP BH POŠTA, koristi se isključivo za potpisivanje elektronskih potvrda i potvrda za servis Ovjerioca JP BH POŠTA pripadajućeg registra opozvanih potvrda.

Javni kriptografski ključ aplikacije Ovjerioca koristi se za validaciju elektronskog potpisa elektronskih potvrda i registra opozvanih potvrda (Key Usage = Certificate Signing, Off-line CRL Signing, CRL Signing).

Tabela 20. Sadržaj ekstenzije Key Usage u kvalificiranim elektronskim potvrdama koje izdaje Ovjerilac JP BH POŠTA

Vrsta potvrda	**Sadržaj ekstenzije *Key Usage***
Kvalificirane elektronske potvrde Ovjerioca JP BH POŠTA	*Certificate Signing, Off-line CRL Signing, CRL Signing*
Kvalificirana elektronska potvrda za elektronski potpis na QSCD USB tokenu	*Non-Repudiation*
Kvalificirana elektronska potvrda za elektronski pečat na QSCD USB tokenu	*Digital Signature*
Kvalificirana elektronska potvrda za elektronski vremenski žig	*Key Usage = digitalSignature, nonRepudiation, extKeyUsage = timeStamping*

6.2. Zaštita privatnog kriptografskog ključa

6.2.1. Standardi za hardverski kriptografski modul

Sve radnje vezane za generisanje kriptografskih ključeva i potpisivanje potvrda od strane Ovjerioca JP BH POŠTA obavljaju se putem hardverskog kriptografskog modula koji zadovoljava sigurnosne standarde ISO/IEC 15408 (Common Criteria) EAL4+.

Kvalifikovano sredstvo za kreiranje elektronskog potpisa korisnika također ispunjava standard EAL4+.

6.2.2. Kontrola pristupa privatnom ključu od strane n od m ovlaštenih lica

Ovjerilac JP BH POŠTA je implementirao višestruku autorizaciju za pristup privatnom kriptografskom ključu aplikacija Ovjerioca JP BH POŠTA Root CA, JP BH POŠTA Issuing CA Ovjerioca JP BH POŠTA.

Pristup korisničkom privatnom kriptografskom ključu ograničen je samo na korisnika.

6.2.3. Otkrivanje privatnog kriptografskog ključa

Ovjerilac JP BH POŠTA ne pruža mogućnost otkrivanja privatnog kriptografskog ključa.

6.2.4. Kreiranje kopije privatnog kriptografskog ključa

Nakon generisanja kriptografskih ključeva aplikacija Ovjerioca, uz prisustvo ovlaštenih lica Ovjerioca JP BH POŠTA, pravi se kopija privatnog kriptografskog ključa aplikacije Ovjerioca. Privatni kriptografski ključ aplikacije Ovjerioca šifriran je AES (Rijndael) algoritmom i nikada nije dostupan u dešifriranom obliku izvan hardverskog kriptografskog modula. Dešifriranje privatnog kriptografskog ključa moguće je samo unutar hardverskog kriptografskog modula, uz upotrebu dva administratorska autorizacijska sredstva za pristup hardverskom kriptografskom modulu i njihove lozinke.

Kreiranje kopija privatnih kriptografskih ključeva povezanih sa kvalifikovanim elektronskim potvrdama korisnika ne obavlja se.

6.2.5. Arhiviranje privatnog kriptografskog ključa

Ovjerilac JP BH POŠTA arhivira kopiju privatnog kriptografskog ključa aplikacije Ovjerioca nakon njegovog kreiranja, na lokaciji Ovjerioca JP BH POŠTA i na drugoj sigurnosnoj lokaciji u JP BH POŠTA, u zaštićenim prostorijama u kasama-kontejnerima za dugotrajno čuvanje.

Arhiviranje privatnih kriptografskih ključeva povezanih sa kvalifikovanim elektronskim potvrdama korisnika ne obavlja se.

6.2.6. Prebacivanje privatnog ključa u kriptografski modul ili iz njega

Privatni kriptografski ključ aplikacije Ovjerioca generiše se u hardverskom kriptografskom modulu. Samo u slučaju hardverskog kvara hardverskog kriptografskog modula aplikacije Ovjerioca, on će biti zamijenjen drugim modulom, a privatni ključ će biti prebačen (u taj modul, uz pisanu odluku

odgovornog lica Ovjerioca JP BH POŠTA i uz višestruku autorizaciju zaposlenih Ovjerioca JP BH POŠTA.

Privatni kriptografski ključ povezan sa kvalifikovanim elektronskim potvrdama korisnika generiše se u hardverskom kriptografskom QSCD uređaju i ne iznosi se izvan njega.

6.2.7. Čuvanje privatnog kriptografskog ključa u kriptografskom modulu

Kriptografski ključevi čuvaju se u kriptografskim modulima i mogu se koristiti samo ako su ispravno aktivirani.

6.2.8. Postupak za aktiviranje privatnog kriptografskog ključa

Za rekonstrukciju i aktiviranje privatnog kriptografskog ključa aplikacije Ovjerioca potrebna je autorizacija dva HSM administratora sa svojim karticama i lozinkama. Privatni kriptografski ključ aplikacije Ovjerioca aktivira se nakon pokretanja aplikacije Ovjerioca.

Korisnički privatni kriptografski ključevi aktiviraju se nakon uspješne autentikacije korisnika putem lozinke u korisničkoj aplikaciji tokom elektronskog potpisivanja.

6.2.9. Postupak za deaktiviranje privatnog kriptografskog ključa

Privatni kriptografski ključ aplikacije Ovjerioca deaktivira se zaustavljanjem aplikacije Ovjerioca i deaktivacijom HSM-a.

Korisničke aplikacije deaktiviraju privatni kriptografski ključ nakon elektronskog potpisivanja i izdavanja identifikacijskog sredstva ili nakon isteka korisničke sesije.

6.2.10. Postupak za uništavanje privatnog kriptografskog ključa

Privatni kriptografski ključ aplikacije Ovjerioca uništava se samo u slučaju planiranog prestanka rada Ovjerioca, što se vrši isključivo uz pisanu odluku odgovornog lica Ovjerioca JP BH POŠTA.

Privatni kriptografski ključ korisnika uništava se ako ga korisnik obriše sa QSCD uređaja ili fizički ošteti QSCD uređaj.

6.2.11. Klasifikacija kriptografskih modula

Standard za klasifikaciju kriptografskih modula je ISO/IEC 15408 EAL, a više informacija se može naći u tački 6.2.1.

6.3. Ostali aspekti upravljanja kriptografskim ključevima

6.3.1. Arhiviranje javnih kriptografskih ključeva

Ovjerilac JP BH POŠTA čuva kriptografske ključeve aplikacije Ovjerioca, ali ne čuva javne kriptografske ključeve korisnika.

6.3.2. Rokovi važenja potvrda i kriptografskih ključeva

Rok važenja potvrda Ovjerioca JP BH POŠTA su:

- Potvrda korijenskog ovjerioca: 20 godina,
- Povrda podređenog ovjerioca: 15 godine
- Kvalifikovane elektronske potvrde korisnika: 1 ili 3 godine.

6.4. Podaci za aktiviranje

6.4.1. Generisanje i upotreba podataka za aktiviranje

Podaci za aktiviranje privatnih ključeva aplikacije Ovjerioca generišu se prilikom generisanja kriptografskih ključeva i mogu koristiti samo ovlašteni zaposlenici Ovjerioca JP BH POŠTA.

Lozinka za aktiviranje privatnog ključa (PIN kod) korisnika generiše se pomoću generatora lozinki. Lozinka sadrži šest numeričkih karaktera. Korisnik ima mogućnost promjene lozinke i njenog dužeg formata.

Ako korisnik tri puta unese netačnu lozinku (PIN kod) za redom, dolazi do blokade QSCD uređaja. Pristup QSCD uređaju može se omogućiti koristeći PUK kod koji se dostavlja korisniku zajedno s lozinkom (PIN kodom) u zatvorenoj koverti. Ukoliko korisnik unese netačan PUK pet puta uzastopno QSCD uređaj je trajno blokiran i više nije moguće njegovo korištenje.

6.4.2. Zaštita podataka za aktiviranje

Ovlašteni zaposlenici Ovjerioca JP BH POŠTA su odgovorni za čuvanje lozinki koje se koriste za aktiviranje ključeva.

Svaki korisnik kvalifikovane elektronske potvrde odgovoran je za čuvanje lozinke svog QSCD uređaja.

6.4.3. Ostali oblici podataka za aktiviranje

Nema drugih oblika podataka za aktiviranje.

6.5. Sigurnosni zahtjevi za rad

Osjetljivi podaci moraju biti zaštićeni od otkrivanja putem ponovne upotrebe resursa za skladištenje, kao što su izbrisani fajlovi, dostupni neovlaštenim korisnicima.

Integritet svih sistema i informacija štiti se od virusa, zlonamjernog i neovlaštenog softvera.

6.5.1. Sigurnosne zakrpe

Sigurnosne zakrpe primjenjuju se u razumnom roku nakon što postanu dostupne, obično unutar 30 dana.

Sigurnosne zakrpe ne primjenjuju se ako unose dodatne ranjivosti ili nestabilnosti koje premašuju koristi njihove primjene. Svi razlozi za nepostavljanje sigurnosnih zakrpa dokumentiraju se.

6.6. Sigurnosni zahtjevi za računarstvo

6.6.1. Specifični tehničko-sigurnosni zahtjevi za računarstvo

Sistem Ovjerioca JP BH POŠTA uključuje tehničke sigurnosne kontrole i mehanizme, uključujući:

- Kontrolu pristupa sistemskim servisima aplikacije Ovjerioca JP BH POŠTA,
- Kontrolu pristupa funkcijama aplikacije Ovjerioca JP BH POŠTA,
- Strogu podjelu uloga među ovlaštenim zaposlenicima Ovjerioca JP BH POŠTA,
- Upotrebu kriptografskih modula za skladištenje kriptografskih ključeva ovlaštenih zaposlenika Ovjerioca JP BH POŠTA,
- Redovno sigurnosno kopiranje podataka aplikacije Ovjerioca JP BH POŠTA i elektronskih dnevnika,
- Postavljanje mehanizama obnove sistema, kriptografskih ključeva i baze podataka aplikacije Ovjerioca JP BH POŠTA.

Da bi se otkrili, zabilježili i spriječili pokušaji neovlaštenog pristupa resursima sistema, Ovjerilac JP BH POŠTA kontinuirano prati sistem.

6.6.2. Nivo zaštite računarstva

Operativni sistem na serverima Ovjerioca JP BH POŠTA usklađen je s ISO/IEC 15408 EAL4+ standardom kako bi se osigurao siguran rad aplikacije Ovjerioca JP BH POŠTA.

6.7. Tehnički nadzor tokom obavljanja djelatnosti

6.7.1. Razvoj sistema

Ovjerilac JP BH POŠTA oslanja se na aplikaciju Ovjerioca koja je razvijena prema strogim standardima. Dodatni softver (CMS) koji se koristi za izdavanje elektronskih potvrda dolazi od pouzdane firme, a sve nove verzije softvera se testiraju na testnom okruženju prije implementacije na produkcijskom okruženju.

6.7.2. Upravljanje sigurnošću

Ovjerilac JP BH POŠTA primjenjuje mehanizme i procedure za kontrolu i nadzor svih tehničkih sistema. U slučaju narušavanja sigurnosti sistema Ovjerioca JP BH POŠTA ili gubitka integriteta, Ovjerilac JP BH POŠTA će u roku od 24 sata obavijestiti nadležne organe.

6.7.3. Nadzor sigurnosti tokom upotrebe sistema

Sigurnosni nadzor se redovno vrši provjerom rada komponenata Ovjerioca JP BH POŠTA.

6.8. Nadzor sigurnosti računarske mreže

Ovjerilac JP BH POŠTA štiti mrežu i sisteme od napada segmentirajući svoje sisteme u mreže ili zone na osnovu procjene rizika, uzimajući u obzir funkcionalne, logičke i fizičke (uključujući lokaciju) odnose između pouzdanih sistema i usluga. Isti sigurnosni kontrolni mehanizmi primjenjuju se na sve sisteme unutar iste zone.

Računarsku mrežu Ovjerioca JP BH POŠTA čine povezani mrežni segmenti koji sadrže servere i radne stanice. Segmenti su međusobno povezani mrežnim uređajima i firewall-ima. Sigurnosna pravila na firewall-ima i mrežnim uređajima dozvoljavaju komunikaciju samo između servera i radnih stanica putem protokola koji su neophodni za obavljanje poslovanja Ovjerioca JP BH POŠTA i za pristup njegovim uslugama.

Postoji namjenska mreža za administraciju IT sistema i operativnu mrežu Ovjerioca JP BH POŠTA.

Proizvodni sistemi za pružanje usluga su fizički razdvojeni od sistema koji se koriste za razvoj i testiranje (npr. sistemi za razvoj, testiranje i postupno implementiranje).

Komunikacija između različitih pouzdanih sistema uspostavlja se samo putem pouzdanih kanala koji su logički razdvojeni od drugih komunikacijskih kanala i pružaju identifikaciju krajnjih tačaka i zaštitu podataka kanala od modifikacije ili otkrivanja. Ako je potrebno, vanjski pristup pouzdanom servisu ima redundantnu mrežnu vezu kako bi se osigurala dostupnost usluga u slučaju kvara jedne mrežne veze.

Redovno se skeniraju ranjivosti na javnim i privatnim IP adresama svakih 120 dana, a dokazi se dokumentiraju kako bi se osiguralo da svako skeniranje ranjivosti vrše osobe ili entiteti s potrebnim vještinama, alatima, stručnošću, etičkim kodeksom i nepristrasnošću za pružanje pouzdanih izvještaja.

6.9. Vremenska oznaka

Elektronske potvrde i registri opozvanih potvrda sadrže vremenske oznake za datum i vrijeme izdavanja, datum i vrijeme prestanka važenja potvrde, i datum i vrijeme izdavanja narednog registra opozvanih potvrda. Napomena: Vremenska oznaka nije kriptografski vremenski žig. Sistem tačnog vremena je usklađen putem NTP protokola s internim firewall-om Fortgate 100F NTP servisima, koji su u skladu s zakonskom regulativom Institut za mjeriteljstvo BiH, kao izvorom tačnog vremena.

7. SADRŽAJ POTVRDE I REGISTRA OPOZVANIH POTVRDA

7.1. Struktura potvrde

7.1.1. Verzija potvrde

Ovjerilac JP BH POŠTA izdaje potvrde u skladu s X.509 verzijom 3 specifikacije. Profil kvalifikovane elektronske potvrde je usklađen s standardima navedenim na početku ovog dokumenta.

Potvrde Ovjerioca JP BH POŠTA sadrže osnovna polja X.509 potvrde (vidi Tabelu 21).

Naziv polja	Opis polja
Version	Verzija specifikacije *X.509* potvrde.
Serial Number	Jedinstven serijski broj elektronske potvrde.
Signature Algorithm	*Hash* algoritam i asimetrični kriptografski algoritam korišteni za potpisivanje potvrde od strane aplikacije Ovjerioca.
Issuer	Jedinstveno ime Ovjerioca.
Valid From	Datum i vrijeme početka važenja elektronske potvrde.
Valid To	Datum i vrijeme prestanka važenja elektronske potvrde.
Subject	Jedinstveno ime korisnika potvrde.
Public Key	Naziv algoritma javnog ključa i parametri javnog kriptografskog ključa korisnika potvrde.

Tabela 21. Osnovna polja X.509 potvrde

7.1.2. Ekstenzije potvrde

Nazivi ekstenzija X.509 potvrda koje aplikacija Ovjerioca upisuje u kvalificirane elektronske potvrde i njihov opis dati su u sljedećoj tabeli (Tabela 22).

Naziv polja - ekstenzije	Opis polja - ekstenzije
Enhanced Key Usage (EKU)	Pokazuje da se javni ključ može koristiti za jednu ili više svrha (proširena mogućnost korištenja ključa).
Authority Information Access	Adresa potvrde „ JP BH POŠTA IssuingCA“
Certificate Policies	Identifikacija CPS-a i adresa *Web* stranice na kojoj se nalaze ova Praktična pravila.
Subject Alternative Name	Alternativna imena korisnika (*e-mail*, itd).
CRL Distribution Points	Lokacija na kojoj se nalaze registri opozvanih potvrda.
Authority Key Identifier	Identifikator javnog kriptografskog ključa Ovjerioca.
Subject Key Identifier	Identifikator javnog kriptografskog ključa korisnika potvrde.
Key Usage	Namjena javnog kriptografskog ključa korisnika kvalificirane elektronske potvrde.
Basic Constraints	Oznaka koja ukazuje na vrstu potvrde (potvrda Ovjerioca ili korisnička potvrda).
Qualified Certificate Statements	Oznaka da je potvrda izdana kao kvalificirana elektronska

	potvrda.

Tabela 22. Ekstenzije X.509 potvrde

7.1.3. Identifikacijska oznaka algoritma

Ovjerilac JP BH POŠTA koristi algoritam SHA256RSA za potpisivanje kvalificiranih elektronskih potvrda i registara opozvanih potvrda, u skladu s RFC 5280 - Internet X.509 Infrastructure Certificate i Certificate Revocation List (CRL) Profile, RFC 4055 - Dodatni algoritmi i identifikatori za RSA kriptografiju za upotrebu u Internet X.509 Public Key Infrastructure Certificate i Certificate Revocation List (CRL) Profile i RFC 6931 - Dodatni XML Security Uniform Resource Identifiers (URIs).

7.1.4. Forme imena

Potvrde JP BH POŠTA Root CA i potvrde izdane od JP BH POŠTA Issuing CA sadrže puna jedinstvena imena (Distinguished Name - DN) izdavaoca i korisnika potvrde u poljima Izdavač i Subjekt.

U elektronskim potvrdama koje izdaje Ovjerilac JP BH POŠTA, imena Ovjerioca JP BH POŠTA u polju Izdavač i imena korisnika potvrde u polju Subjekt su jedinstvena imena (Distinguished Name - DN). Za ime korisnika (Common Name - CN) u elektronskoj potvrdi primjenjuje se UTF8 String kodiranje.

7.1.5. Ograničenja u imenima

Specijalni znakovi kao što su ? (upitnik), \ (backslash), # (ljestve), $ (dolar), % (postotak), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez) nisu dozvoljeni u imenima. Potrebno je izostaviti ili zamijeniti ih drugim znakovima.

7.1.6. Identifikacijska oznaka politike ovjeravanja

Sve potvrde izdate od strane Ovjerioca JP BH POŠTA sadrže OID politike ovjeravanja na osnovu koje je izdata potvrda. OID za svaku politiku ovjeravanja je definisan u poglavljima 1.1.1 i 1.2.

7.1.7. Upotreba ekstenzije za razdvajanje politika

Ekstenzija za razdvajanje politika se ne koristi.

7.1.8. Kvalifikatori politike ovjeravanja

Ovjerilac JP BH POŠTA koristi polje Policy Qualifier=CPS ekstenzije Certificate Policies potvrda, u kojem se objavljuje adresa web stranice na kojoj se nalaze Praktična pravila i drugi akti Ovjerioca JP BH POŠTA.

7.1.9. Procesiranje kritičnih ekstenzija potvrda

Korisničke aplikacije su obavezne da procesiraju kritične ekstenzije potvrda.

7.2. Profil registra opozvanih potvrda

7.2.1. Verzija registra opozvanih potvrda

Ovjerilac JP BH POŠTA izdaje X.509 registre opozvanih potvrda (Certificate Revocation List - CRL) verzije 2. Profil registra opozvanih potvrda je u skladu s RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Registri opozvanih potvrda Ovjerioca JP BH POŠTA sadrže osnovna polja X.509 registra (Tabela 28) i ekstenzije X.509 registra (Tabela 23).

Naziv polja	**Opis polja**
Version	Verzija specifikacije *X.509* registra opozvanih potvrda.
Signature Algorithm	*Hash* algoritam i asimetrični kriptografski algoritam korišteni za potpisivanje registra opozvanih potvrda od strane aplikacije Ovjerioca.
Issuer	Jedinstveno ime Ovjerioca.
Effective Date (This Update)	Datum i vrijeme izdavanja registra opozvanih potvrda.
Next Update	Datum i vrijeme sljedećeg izdavanja registra opozvanih potvrda.
Revoked Certificates	Spisak serijskih brojeva opozvanih potvrda (eng. *serial number*) i datuma i vremena njihovog opozivanja (eng. *revocation date*).

Tabela 23. Osnovna polja X.509 registra opozvanih potvrda

7.2.2. Ekstenzije registra opozvanih potvrda

Nazivi ekstenzija X.509 registra opozvanih potvrda koje aplikacija Ovjerioca upisuje u registre i njihov opis dati su u sljedećoj tabeli (Tabela 24).

Naziv ekstenzije	**Opis ekstenzije**
Authority Key Identifier	Identifikator javnog kriptografskog ključa Ovjerioca.
CRL Number	Redni broj registra opozvanih potvrda (*OID* 2.5.29.20).
Reason Code	Razlog opoziva potvrde. Mogući razlozi opoziva potvrda (prema dokumentu *RFC* 5280) su: - *unspecified (0),* - *keyCompromise (1),* - *cACompromise (2),* - *affiliationChanged (3),* - *superseded (4),* - *cessationOfOperation (5),* - *certificateHold (6),* - *removeFromCRL (8),* - *privilegeWithdrawn* (9), - *aACompromise*(10).
Expired Certs On CRL	CRL koja sadrži ovu extenziju uključivat će informacije o statusu opoziva za potvrde koje su već istekle.
Invalidity Date	Datum kompromitiranja ili sumnje u kompromitiranje privatnog kriptografskog ključa ili datum kada je elektronska potvrda na neki drugi način prestala da bude važeća (OID 1.3.6.1.4.1.59867.10.1.2)

Tabela 24. Ekstenzije X.509 registra opozvanih potvrda

8. REVIZIJA USKLAĐENOSTI RADA OVJERIOCA JP BH POŠTA I DRUGE PROCJENE

Ovjerilac JP BH POŠTA redovno provodi internu reviziju rada.

Nadležni organ, u skladu sa zakonom i podzakonskim aktima, ima pravo izvršiti reviziju, a Ministarstvo komunikacija i transporta Bosne i Hercegovine je taj nadležni organ.

8.1. Učestalost revizije i analiza rizika

Ovjerilac JP BH POŠTA izvodi analizu rizika kako bi identificirao ključne usluge koje zahtijevaju upotrebu sigurnih sistema i visok stupanj sigurnosti:

- Prije početka pružanja usluga ovjeravanja.
- Tijekom operativnog rada, prema potrebi, ali najmanje svakih 6 mjeseci.
- Ovjerilac JP BH POŠTA provodi redovne interne revizije dvaput godišnje.

Ako to zahtijeva nadležni organ ili ako su rezultati prethodne revizije nezadovoljavajući, moguće je provesti više od dvije revizije godišnje.

8.2. Kvalifikacije osoba koje vrše reviziju

Internu reviziju JP BH POŠTA provodi Interna revizija koja također određuje tko će provoditi reviziju.

Reviziju može provesti osoba zaposlena unutar ili izvan Ovjerioca JP BH POŠTA, ali ta osoba mora imati relevantno iskustvo u:

- Tehnologiji infrastrukture javnih kriptografskih ključeva.
- Ovjeravanju.
- Provođenju revizija, uključujući revizije Ovjerioca ili drugih informacijsko-komunikacijskih sistema.

8.3. Odnos osoba koje vrše reviziju prema predmetu revizije

Osobe koje provode reviziju pridržavaju se važećih propisa i međunarodnih standarda. Reviziju može provesti zaposlena osoba unutar Ovjerioca JP BH POŠTA ili vanjski stručnjak.

8.4. Sadržaj revizije

Interna revizija obuhvaća sljedeće aspekte:

- Sadržaj Politike ovjeravanja.
- Sadržaj Praktičnih pravila.
- Uspješnost izvođenja djelatnosti Ovjerioca JP BH POŠTA u skladu s važećim propisima, Politikom ovjeravanja, Praktičnim pravilima i internim aktima (uključujući postupke za pristup prostorijama Ovjerioca JP BH POŠTA, upravljanje aplikacijom Ovjerioca JP BH POŠTA, objavljivanje registra opozvanih potvrda, izradu sigurnosnih kopija i druga interna pravila).
- Tehnički procesi i postupci.
- Fizička sigurnost.
- Primijenjene sigurnosne mjere informacijske sigurnosti.

8.5. Poduzete aktivnosti kao rezultat utvrđenih nedostataka

Ako se utvrde nedostaci, poduzimaju se aktivnosti za njihovo rješavanje u najkraćem mogućem roku.

8.6. Objavljivanje izvještaja revizije

Izvještaj revizije je interni dokument Ovjerioca JP BH POŠTA i ne objavljuje se javno. Namijenjen je isključivo ovlaštenim osobama unutar Ovjerioca JP BH POŠTA radi otklanjanja eventualno pronađenih nedostataka.

9. OSTALI POSLOVI I PRAVNA PITANJA

9.1. Cjenovnik

Ovjerilac JP BH POŠTA objavljuje cjenovnik za izdavanje elektronskih potvrda na svojoj web stranici.

Svaka promjena cijena izdavanja elektronskih potvrda bit će objavljena na web stranici Ovjerioca JP BH POŠTA i bit će dostupna svim zainteresiranim licima.

9.1.1. Naknada za izdavanje potvrda

Ovjerilac JP BH POŠTA naplaćuje izdavanje elektronske potvrde na osnovu cjenovnika koji je objavljen na web stranici Ovjerioca JP BH POŠTA.

9.1.2. Naknada za pristup potvrdama

Ovjerilac JP BH POŠTA ne objavljuje elektronske potvrde, tako da one nisu javno dostupne, pa ne može ni naplaćivati pristup elektronskoj potvrdi.

9.1.3. Naknada za provjeru opozvanosti statusa potvrda

Provjera opozvanosti elektronske potvrde i dobivanje informacija o statusu potvrde korištenjem registra opozvanih potvrda se ne naplaćuje.

9.1.4. Naknada za druge usluge

Ovjerilac JP BH POŠTA zadržava pravo da naplaćuje različite usluge ovisno o pruženim uslugama u svakom konkretnom slučaju.

9.1.5. Povrat uplaćenih sredstava

U slučaju da Ovjerilac JP BH POŠTA raskine ugovor, a prethodno ne izda elektronsku potvrdu korisniku, korisnik može tražiti povrat uplaćenih sredstava u iznosu cijene potvrde.

9.2. Finansijska odgovornost

Ovjerilac JP BH POŠTA snosi finansijsku odgovornost za obavljanje svoje djelatnosti u skladu sa važećim zakonskim propisima.

9.2.1. Osiguranje

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

- Osigurana suma na koju mora biti ugovoreno osiguranje po jednom štetnom događaju ne može iznositi manje od 50.000,00 KM, podrazumijevajući pri tom kao štetni događaj pojedinačnu štetu nastalu upotrebom jedne kvalificirane elektronske potvrde u jednom aktu u pravnom prometu;
- Ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti Ovjerioca kumulativno na godišnjem nivou, po svim štetnim događajima, ne može biti niža od 1.500.000,00 KM.

9.2.2. Drugi fondovi

Nije primijenjeno.

9.2.3. Osiguranje ili garancija za krajnje korisnike

Osiguranje ili garancija za krajnje korisnike opisani su u okviru tačke 9.2.1.

9.3. Tajnost poslovnih podataka

9.3.1. Obim tajnih podataka

Tajni podaci su svi podaci koje Ovjerilac JP BH POŠTA pribavi i kreira u obavljanju svoje djelatnosti kao ovjerilac.

Pristup podacima koji se smatraju tajnim može biti odobren ovlaštenim licima Ovjerioca JP BH POŠTA i nadležnim državnim organima, ako su ispunjeni zakonom propisani uvjeti.

9.3.2. Podaci koji se ne smatraju tajnim

Podaci koji se ne smatraju tajnim su:

- Registri opozvanih potvrda, kao i podaci koje oni sadrže,
- Politika ovjeravanja,
- Praktična pravila,
- Podaci i dokumenti koja su objavljena na zvaničnoj web stranici Ovjerioca JP BH POŠTA, a za koje postoji pisana saglasnost za javno objavljivanje.

9.3.3. Odgovornost za zaštitu tajnih podataka

Ovlaštena lica Ovjerioca JP BH POŠTA i korisnici obavezuju se:

- Da čuvaju tajnost podataka primjenom mjera koje koriste za zaštitu svojih tajnih podataka i da će ih koristiti samo za potrebe zbog kojih su bili prikupljeni ili formirani u odnosu na odredbe Praktičnih pravila,
- Da neće neovlašteno otkrivati tajne podatke, bez prethodnog odobrenja u pisanoj formi koje daje korisnik ili nadležni organ.

9.4. Čuvanje ličnih podataka

Ovjerilac JP BH POŠTA je dužan da se u svom poslovanju pridržava odredbi Zakona o zaštiti ličnih podataka.

9.4.1. Plan čuvanja ličnih podataka

Lični podaci se čuvaju u skladu sa Zakonom o zaštiti ličnih podataka i podzakonskim aktima za provođenje istog.

9.4.2. Lični podaci koji se smatraju tajnim

Lični podaci koji se čuvaju smatraju se tajnim, osim u slučajevima kada je zahtjev za njihovim dostavljanjem izdat u pisanoj formi od strane korisnika ili nadležnog organa.

9.4.3. Lični podaci koji se ne smatraju tajnim

Svi podaci koji su javno dostupni.

9.4.4. Odgovornost za zaštitu ličnih podataka

Ovlaštena lica Ovjerioca JP BH POŠTA i korisnici obavezuju se:

- Da čuvaju lične podatke primjenom mjera koje koriste za zaštitu svojih ličnih podataka i da će ih koristiti samo za potrebe zbog kojih su bili prikupljeni ili formirani u odnosu na odredbe Praktičnih pravila,
- Da neće neovlašteno otkrivati lične podatke, bez prethodnog odobrenja u pisanoj formi koje daje korisnik ili nadležni organ.

JP BH POŠTA odgovara za lične podatke i njihovu zaštitu, u skladu s tačkom 9.3.3.

9.4.5. Upozorenje i saglasnost za korištenje ličnih podataka

JP BH POŠTA će koristiti lične podatke isključivo u svrhu pružanja usluge ovjere, pod uslovom da korisnik da saglasnost tokom procesa registracije. Smatra se da je korisnik dao saglasnost ukoliko je potpisao Ugovor o izdavanju i korištenju kvalifikovane elektronske potvrde.

9.4.6. Otkrivanje ličnih podataka nadležnim organima

JP BH POŠTA će otkriti ili dostaviti lične podatke na zahtjev nadležnih organa i u drugim slučajevima kada je to u skladu sa zakonom.

9.4.7. Drugi slučajevi otkrivanja ličnih podataka

JP BH POŠTA će otkriti lične podatke koji su zaštićeni zakonom uz prethodnu saglasnost korisnika ili na zahtjev nadležnih organa i u drugim slučajevima predviđenim zakonom.

9.5. Prava intelektualne svojine

JP BH POŠTA zadržava sva prava intelektualne svojine nad svim elementima CA JP BH POŠTA.

9.6. Prava i obaveze

9.6.1. Prava i obaveze Ovjerioca

CA JP BH POŠTA pruža uslugu ovjere u skladu sa važećim zakonima i propisima BiH, ovim Pravilima i drugim aktima JP BH POŠTA. Ovjerilac JP BH POŠTA ima obavezu:

- Provjeriti identitet korisnika u procesu izdavanja ili promjene statusa elektronske potvrde, kao i tačnost podataka u zahtjevu za izdavanje i korištenje elektronske potvrde, odnosno zahtjevu za promjenu statusa elektronske potvrde,
- Izdati kvalifikovanu elektronsku potvrdu u skladu sa zakonom,
- Obezbijediti da kvalifikovana elektronska potvrda sadrži sve neophodne podatke, u skladu sa zakonom,
- Unijeti u kvalifikovanu elektronsku potvrdu osnovne podatke o svom identitetu i o identitetu korisnika, kao i javni kriptografski ključ korisnika koji se podudara sa njegovim privatnim kriptografskim ključem,
- Obezbijediti vidljiv podatak u elektronskoj potvrdi o tačnom datumu i vremenu (sat i minut) izdavanja potvrde,
- Prihvatiti ili odbiti zahtjeve za promjenom statusa kvalifikovane elektronske potvrde, u skladu sa zakonom,
- Voditi ažuran, tačan i bezbjedan registar opozvanih potvrda i omogućiti javni pristup istom,
- Obezbijediti vidljiv podatak u registru opozvanih potvrda o tačnom datumu i vremenu (sat i minut) opoziva elektronske potvrde,
- Nadgledati rad organizacionih jedinica koje su dio JP BH POŠTA.
- Ovjerilac JP BH POŠTA pruža usluge u skladu sa važećim propisima i internim aktima.

9.6.2. Prava i obaveze Registracijskog tijela JP BH POŠTA

Registracijsko tijelo JP BH POŠTA ima prava i obaveze da:

- Provjeri identitet korisnika u procesu izdavanja elektronske potvrde i tačnost podataka u zahtjevu za izdavanje i korištenje elektronske potvrde,
- Provjeri identitet korisnika i tačnost podataka u zahtjevu za promjenu statusa elektronske potvrde,
- Proslijedi podatke za izdavanje i promjenu statusa elektronske potvrde, kao i svu dokumentaciju Tijelu za operativne poslove JP BH POŠTA.

9.6.3. Prava i obaveze korisnika

Svi korisnici potvrda koje izdaje Ovjerilac JP BH POŠTA imaju prava i obaveze da ih koriste u skladu sa zakonima, propisima i ovim Pravilima.

Korisnici potvrda koje izdaje Ovjerilac JP BH POŠTA imaju obavezu da:

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

9.6.4. Prava i obaveze trećih lica

Treća lica koja koriste kvalifikovane potvrde za provjeru valjanosti elektronskih potpisa imaju garanciju od strane Ovjerioca JP BH Pošta da njihov CA pruža uslugu ovjere u skladu sa važećim zakonima i propisima BiH i ovim Pravilima. Treća lica imaju pravo koristiti ove kvalifikovane potvrde koje izdaje Ovjerilac JP BH POŠTA u skladu sa važećim zakonima i propisima BiH i ovim Pravilima. Treća lica su dužna provjeriti status potvrde prije nego je koriste za provjeru valjanosti elektronskih potpisa.

9.6.5. Prava i obaveze drugih učesnika

Ovjerilac JP BH POŠTA ne definiše prava i obaveze drugih učesnika, već samo potvrđuje da pruža uslugu ovjere u skladu sa važećim zakonima i propisima BiH, ovim Pravilima i drugim aktima Ovjerioca JP BH POŠTA.

9.7. Odricanje od odgovornosti za prava i obaveze

Ovjerilac JP BH POŠTA ne snosi odgovornost za štetu nastalu uslijed nepoštivanja prava i obaveza propisanih zakonom, važećim podzakonskim propisima i ovim Praktičnim pravilima.

9.8. Odgovornost i ograničenja od odgovornosti

9.8.1. Odgovornost i ograničenja od odgovornosti Ovjerioca

Ovjerilac JP BH POŠTA prihvata i ograničava svoju odgovornost na pružanje usluge ovjere u skladu sa važećim zakonima i propisima BiH, ovim Pravilima i drugim aktima JP BH POŠTA.

9.8.2. Završetak rada

U slučaju prestanka rada, Ovjerilac JP BH POŠTA će:

- Obavijestiti sve korisnike putem Web stranice i nadležnog organa državne uprave najmanje šest mjeseci prije planiranog prekida rada,

- Obezbijediti nastavak pružanja povjerljivih usluga kod drugog pružaoca usluga povjerenja svim korisnicima kojima je već izdao potvrde i dostaviti svu dokumentaciju vezanu za pružanje povjerljivih usluga tom pružaocu usluga povjerenja,
- Opozvati sve izdate potvrde u najkraćem mogućem roku, a najkasnije u roku od 48 sati, obavijestiti nadležno tijelo državne uprave i dostaviti svu dokumentaciju vezanu za izvršene usluge, u slučaju da ne obezbijedi nastavak pružanja usluga povjerenja preko drugog pružaoca usluga povjerenja,
- Obezbijediti dostupnost popisa opozvanih potvrda u roku od godine dana nakon opoziva svih potvrda,
- Arhivirati sve podatke u skladu sa zakonom od posljednjeg dana rada Ovjerioca.

9.8.3. Odgovornost i ograničenja od odgovornosti korisnika elektronske potvrde

Korisnik je odgovoran za štetu koja je nastala njegovim postupkom ili propustom, odnosno zbog nepoštivanja obaveza utvrđenih u tački 9.6.3. ovih Praktičnih pravila.

Korisnik ne odgovara za štetu ako dokaže da je postupao u skladu sa zakonom, podzakonskim aktima i zaključenim ugovorom.

9.9. Naknade

Za pružanje usluga Ovjerioca JP BH POŠTA, korisnik plaća naknade u skladu sa tačkom 9.1. ovih Praktičnih pravila.

9.10. Stupanje na snagu i prestanak važenja pravnih akata

9.10.1. Stupanje na snagu pravnih akata

Pravni akti Ovjerioca JP BH POŠTA stupaju na snagu u roku utvrđenom u svakom od tih akata u skladu sa zakonom. Politika ovjere Ovjerioca JP BH POŠTA i ova Praktična pravila objavljuju se i javno su dostupna svim zainteresiranim licima na Web stranici Ovjerioca JP BH POŠTA.

9.10.2. Period važenja

Dokumenti Ovjerioca JP BH POŠTA ne prestaju važiti do objavljivanja novih.

9.10.3. Efekt trajanja

Ovjerilac JP BH POŠTA će i nakon prestanka važenja elektronske potvrde štititi povjerljivost ličnih i drugih podataka korisnika, kao i nakon prestanka važenja svojih akata.

9.11. Individualne obavijesti i komunikacija sa sudionicima

Ovjerilac JP BH POŠTA komunicira individualno sa svojim korisnicima i ostalim sudionicima putem elektronski potpisane e-pošte. Javna obavještenja se objavljuju na web stranici Ovjerioca JP BH POŠTA.

9.12. Izmjene i dopune

9.12.1. Postupak za izmjenu i dopunu

Ova pravila revidiraju se najmanje jednom godišnje ili u slučaju promjene zakona i podzakonskih akata BiH iz ove oblasti.

9.12.2. Mehanizam i period obavještavanja

Ispravke, ažuriranja ili izmjene se javno objavljuju na isti način na koji su i originalna Pravila objavljena.

9.12.3. Okolnosti pod kojima OID mora da se promijeni

Promjena OID-a će se izvršiti ukoliko Ovjerilac JP BH POŠTA odluči da izmijeni Politiku ovjere i Praktična pravila, a koje zahtijevaju promjenu OID-a.

9.13. Rješavanje sporova

Sporovi se rješavaju mirnim putem, a ako to nije moguće, nadležan je sud u Sarajevu.

9.14. Mjerodavno pravo

Za tumačenje i primjenu ovih Praktičnih pravila mjerodavno je zakonodavstvo Federacije BiH i zakonodavstvo Bosne i Hercegovine.

9.15. Usklađenost s važećim zakonodavstvom

Dokumenti i rad Ovjerioca JP BH POŠTA u skladu su sa važećim zakonima i propisima Federacije BiH i BiH.

9.16. Ostale odredbe

9.16.1. Ugovor s korisnicima

Pružanje usluga korisnicima uređuje se posebnim ugovorom između korisnika i Ovjerioca JP BH POŠTA koji je u skladu sa važećim zakonima i propisima BiH.

9.16.2. Prenošenje prava

Korisnici nemaju pravo prenosa prava iz ugovora sa Ovjeriocem JP BH POŠTA na treća lica. Ovjerilac JP BH POŠTA zadržava pravo da prava iz obaveze iz ugovora sa korisnikom, djelimično ili u cijelosti, prenese na drugu registrovanu CA u BiH ili nadležni organ.

9.16.3. Izmjena ovih Praktičnih pravila

U slučaju potrebe za izmjenom nekog dijela ovih Pravila, ostatak Pravila ostaje na snazi.

9.16.4. Primjenjivost na advokatske naknade i odricanje od prava

Nije primjenjivo.

9.16.5. Viša sila

Ovjerilac JP BH POŠTA se oslobađa odgovornosti za bilo kakvu štetu nastalu korisnicima, trećim licima i ostalim sudionicima u korištenju kvalifikovanih potvrda u slučaju djelovanja više sile van kontrole Ovjerioca JP BH POŠTA.

9.17. Stupanje na snagu

Ova Praktična pravila stupaju na snagu danom donošenja, objavljuju se na web stranici Ovjerioca JP BH POŠTA, a počinju se primjenjivati osam dana nakon dana donošenja.