



POLITIKA OVJERAVANJA
OVJERIOCA JP BH POŠTA

klasifikacija: javno

oznaka:

revizija: 01.11.2023

strana: 1/18

JP BH POŠTA d.o.o. Sarajevo
Obala Kulina bana 8, Sarajevo

POLITIKA OVJERAVANJA
OVJERIOCA JP BH POŠTE d.o.o. Sarajevo
(Certification Policy - CP)

Verzija 1.0

Informacije o dokumentu


Naziv dokumenta:	Politika ovjeravanja Ovjerioca JP BH POŠTA
OID dokumenta:	1.3.6.1.4.1.59867.10.1.1.1.0.
Tip dokumenta:	Pravilnik o postupcima certificiranja (<i>Certification Practice Statement, CPS</i>)

Istorija izmjena

Verzija	Datum	Razlog izmjene
1.0	30.11.2023	Inicijalna verzija

SADRŽAJ

Informacije o dokumentu	2
Istorija izmjena	2
1. UVOD	4
2. OBJAVLJIVANJE I LOKACIJA PODATAKA O USLUGAMA OVJERAVANJA	5
3. IDENTIFIKACIJA I AUTENTIKACIJA	6
4. OPERATIVNI ZAHTJEVI U PROCESU IZDAVANJA POTVRDA	7
5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OVLAŠTENIH OSOBA... ..	10
6. KONTROLE TEHNIČKE ZAŠTITE	12
7. SADRŽAJ POTVRDE I REGISTRA OPOZVANIH POTVRDA	14
8. REVIZIJA USKLAĐENOSTI RADA JP BH POŠTA OVJERIOCA I DRUGE PROCJENE	14
9. OSTALI POSLOVI I PRAVNA PITANJA	15

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	4/18

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.

POLITIKU OVJERAVANJA OVJERIOCA JP BH POŠTA

1. UVOD

„JP BH POŠTA“ d.o.o. Sarajevo (u daljnjem tekstu: JP BH POŠTA) je izgradila infrastrukturu javnih kriptografskih ključeva - *Public Key Infrastructure – PKI* i kao ovjerilac u smislu Zakona o elektronskom potpisu („Službeni glasnik BiH“, broj: 91/06) prisutna je kao ovjerilac koji pruža usluge izdavanja kvalificiranih elektronskih potvrda, upravljanja životnim ciklusom elektronskih potvrda i izdavanje kvalificiranih elektronskih vremenskih žigova, pod imenom: Ovjerilac JP BH POŠTA.


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

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

Opća pravila funkcioniranja Ovjerioca JP BH POŠTA sadržana su u dokumentima:

- Politika ovjeravanja Ovjerioca JP BH POŠTA (*Certification Policy - CP*) (u daljnjem tekstu: Politika ovjeravanja),
- Praktična pravila pružanja usluge ovjeravanja Ovjerioca JP BH POŠTA (*Certification Practices Statement - CPS*) (u daljnjem tekstu: Praktična pravila).

Kvalificirane elektronske potvrde koje izdaje Ovjerilac 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

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	5/18

unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ“) i odgovarajućim međunarodnim standardima i preporukama, kao i drugim standardima, dokumentima i preporukama, koje se odnose na izdavanje kvalificiranih elektronskih potvrda.

Ovjerilac JP BH POŠTA koristi u svojoj infrastrukturi za izdavanje kvalificiranih i nekvalificiranih elektronskih potvrda hijerarhiju više CA (eng. *Certification Authority*) servera. Dvorazinsku arhitekturu Infrastrukture Ovjerioca JP BH POŠTA čine dva CA servera:

- Korijski ovjerilac: „JP BH POŠTA Root CA“
- Podređeni ovjerilac za izdavanje potvrda koji je potpisan od strane "JP BH POŠTA Root CA": "JP BH POŠTA Issuing CA

Privatni kriptografski ključevi koji su pridruženi kvalificiranim elektronskim potvdama koriste se u procesu kvalificiranog elektronskog potpisivanja elektronskog dokumenta, koji se može koristiti u korespodenciji, u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom i drugim institucijama, ako je Zakonom kojim se utvrđuje taj postupak, propisana upotreba kvalificiranog elektronskog potpisa.

Kvalificirane elektronske potvrde potvrđuju vezu između javnog kriptografskog ključa korisnika i identiteta korisnika koji je izvršio kvalificirano potpisivanje elektronskog dokumenta.


Svaka druga upotreba kvalificirane elektronske potvrde koja nije definirana ovim dokumentom i nije u suglasnosti sa odredbama Zakona o elektronskom potpisu i drugim dokumentima koji reguliraju ovu oblast, nije dozvoljena.

2. OBJAVLJIVANJE I LOKACIJA 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/e-potpis. Web stranica je javno dostupna, kao i svi podaci i sva dokumentacija koji se na njoj nalaze.

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 ,
- Opšte uslove za pružanje usluge izdavanja kvalificiranih elektronskih potvrda – certifikata Ovjerioca JP BH POŠTA,
- Zahtjev za korištenje usluga ovjerioca za izdavanje kvalificiranih elektronskih

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	6/18

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.


3. IDENTIFIKACIJA I AUTENTIKACIJA

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.

Korisnici ne mogu da budu anonimni i ne mogu da koriste pseudonime.

Ovjerilac JP BH POŠTA garantira jedinstvenost imena u svojoj domeni. Ovjerilac JP BH POŠTA dodjeljuje svakom korisniku jedinstveno ime (*Distinguished Name - DN*), koje se upisuje u polje *Subject* elektronske potvrde.

Imena kojima bi se kršila intelektualna ili autorska prava drugih nisu dozvoljena. Ovjerilac JP BH POŠTA nije obavezan da verificira da li je korištenje takvih imena zakonito. Korisnik snosi odgovornost za to da osigura zakonito korištenje odabranog imena.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	7/18

Kvalificirana elektronska potvrda za elektronski potpis se može izdati samo fizičkom licu, u skladu sa Zakonom o elektronskom potpisu. Fizičko lice ima pravo da u ime pravnog lica koristi kvalificiranu elektronsku potvrdu, ukoliko mu to dozvoli pravno lice.

Kvalificirana potvrda za elektronski pečat može se izdati samo pravnom licu.

Ukoliko Ovjerilac JP BH POŠTA izdaje elektronsku potvrdu fizičkom licu koje je zaposleno u pravnom licu, u okviru atributa koji identifikuju korisnika nalaze se i podaci koji označavaju naziv pravnog lica i to poslovno ime pravnog lica i identifikator organizacije.

Korisnik mora biti fizički prisutan u toku registracije.

4. OPERATIVNI ZAHTJEVI U PROCESU IZDAVANJA POTVRDA

Za izdavanje elektronske potvrde, korisnik je dužan da:

- Popuni i potpiše zahtjev za izdavanje i korištenje elektronske potvrde i uz isti preda na uvid identifikacioni dokument (lična karta ili pasoš),
- Ispuni zahtjeve za identifikaciju,
- Ispuni finansijske obaveze prema cjenovniku,
- Potpiše ugovor o izdavanju i korištenju elektronske potvrde.

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.

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

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 ispunji uvjete iz prethodnog stava ili ako na bilo koji način povrijedi odredbe Praktičnih pravila, Ovjerilac JP BH POŠTA će odbiti zahtjev za izdavanje elektronske potvrde.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	8/18

Izdavanje elektronske potvrde vrši se na sljedeći način:

1. Korisnik preko *Web* stranice Ovjerioca JP BH POŠTA popunjava i štampa Zahtjev za izdavanje i korištenje elektronske potvrde,
2. Korisnik potpisuje Zahtjev za izdavanje i korištenje elektronske potvrde,
3. Korisnik, u postupku izdavanja potvrde, identificira se lično u Registracijskom tijelu JP BH POŠTA na unaprijed definisanim lokacijama,
4. Uposlenik Registracijskog tijela JP BH POŠTA unosi podatke o korisniku i kreira zahtjev u aplikaciji Registracijskog tijela i prosljeđuje verificiran zahtjev Kontroloru registracijskog tijela JP BH POŠTA,
5. Kontrolor Registracijskog tijela JP BH POŠTA provjerava zahtjev i prosljeđuje ga na odobrenje Voditelju Registracijskog tijela,
6. Na osnovu verificiranog i provjerenog zahtjeva Voditelj Registracijskog tijela isti odobrava i dostavlja Tijelu za operativne poslove na personalizaciju kriptografskog uređaja,
7. Korisnički privatni kriptografski ključ se generira u hardverskom kriptografskom modulu *QSCD* uređaja od strane HSM Operatera iz Tijela za operativne poslove,
8. Ovjerilac JP BH POŠTA šalje izdane korisničke potvrde na *QSCD* uređaju na lokaciju predaje zahtjeva,
9. Ovjerilac JP BH POŠTA šalje pripadajuću lozinku/*PIN* kod u zatvorenoj koverti Korisniku sa uputama da preuzme *QSCD* uređaj na lokaciji predaje zahtjeva.
10. 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 o preuzimanju elektronske potvrde na *QSCD* uređaju,


Ukoliko se naknadno utvrdi da u elektronskoj potvrdi postoje pogrešni podaci, korisnik je dužan da se obrati Ovjeriocu JP BH POŠTA radi izdavanja nove potvrde.

Ovjerilac JP BH POŠTA ne vrši produženje korištenja elektronske potvrde. Cijeli proces se izvršava izdavanjem nove elektronske potvrde.

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

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,

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	9/18

- 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.

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.


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

Registri opozvanih potvrda ovjerioca objavljuju se na svaka 24 sata.

Dostupnost CRL servisa je 24 sata na dan, 7 dana u sedmici.

U slučaju da prije redovne objave dođe do opoziva ili suspenzije elektronske potvrde, Ovjerilac JP BH POŠTA odmah objavljuje novi registar opozvanih potvrda i prije isteka važenja registra opozvanih potvrda.

Korisnici i treća lica su dužni da provjere status elektronske potvrde na osnovu javno dostupnog registra opozvanih potvrda Ovjerioca JP BH POŠTA.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	10/18

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

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.

Korisnik prestaje s korištenjem elektronske potvrde:

- Istekom roka važnosti elektronske potvrde,
- Opozivom elektronske potvrde,
- Tijekom trajanja suspenzije elektronske potvrde.


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

5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OVLAŠTENIH OSOBA

Oprema Ovjerioca JP BH POŠTA se nalazi u sigurnoj prostoriji koja je osigurana dvorazinskom elektronskom bravom u zgradi generalne direkcije JP BH POŠTA. Kontrola fizičkog pristupa Ovjeriocu JP BH POŠTA je implementirana u skladu sa Zakonom o elektronskom potpisu i podzakonskim aktima, i to na sljedeći način:

- Pristup u prostorije, sigurnu zonu, elektronski se bilježi i unosi u elektronski dnevnik za pristup prostorijama, i isti se pregleda,
- Brave, elektronski sistemi zaštite i sistemi protupožarne zaštite su u skladu sa važećim standardima,
- Prostor i sistem nadgledani su 24 sata, 7 dana u sedmici od strane ovlaštenih lica Ovjerioca JP BH POŠTA,
- Pristup se može provoditi isključivo uz prisutnost najmanje dva ovlaštena lica koja imaju pravo pristupa,
- Pristup zbog održavanja sistema mora biti unaprijed najavljen, osim u slučaju smetnji u radu sistema za koje Tijelo za operativne poslove utvrdi da zahtijevaju hitnu intervenciju,
- Svaki pristup zaštićenoj prostoriji evidentira se unutar elektronske evidencije.

Ovjerilac JP BH POŠTA osigurava da je pristup sistemu ovjeravanja ograničen isključivo na ovlaštene zaposlene.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	11/18

Prostorije u kojima se nalazi infrastruktura Ovjerioca JP BH POŠTA u generalnoj direkciji JP BH POŠTA su opremljene:

- Sistemom za besprekidno napajanje električnom energijom i stabilizaciju napona za računarsku i komunikacijsku opremu, koji je povezan sa agregatom,
- Neovisnim sistemom za klimatizaciju koji omogućava kontrolu temperature i vlažnosti vazduha unutar prostorija Ovjerioca JP BH POŠTA.

Oprema Ovjeritelja JP BH POŠTA smještena je na mjestu koje je osigurano od poplave.

Oprema Ovjerioca JP BH POŠTA zaštićena je automatskim sistemom protupožarne zaštite u skladu sa propisanom i važećom zakonskom regulativom.

Svi računarski mediji koji sadrže podatke o poslovima Ovjerioca JP BH POŠTA, uključujući i medije s rezervnim kopijama podataka, smještaju se u vatrootporne sigurne kase-kontejnere, od kojih se jedna nalazi na centralnoj lokaciji Ovjerioca JP BH POŠTA, a druga u drugoj sigurnoj lokaciji.

Ovjerilac JP BH POŠTA garantira da sve poslove koji se obavljaju u okviru propisane djelatnosti obavljaju lica od povjerenja s tačno propisanim obavezama i ovlaštenjima. Rad ovih lica je podložan stalnim provjerama.

Zaposleni Ovjerioca JP BH POŠTA moraju biti kvalificirani za obavljanje poslova iz Praktičnih pravila i podliježu provjeri stručne sposobnosti.


U slučaju izvršene ili sumnje na izvršene neautorizirane aktivnosti od strane ovlaštenog lica Ovjerioca JP BH POŠTA, istom će biti onemogućen daljnji pristup tehničkim sredstvima (hardveru i softveru) Ovjerioca JP BH POŠTA, a Ovjerilac JP BH POŠTA će analizirati i eventualno suspendirati ili opozvati sve važeće elektronske potvrde koje su izdate od tog lica.

Izvršene neautorizirane aktivnosti prijavljuju se nadležnim organizacijskim jedinicama JP BH POŠTA, državnim organima i institucijama, u skladu sa važećim zakonskim i internim propisima.

U slučaju štete nastale na tehničkim sredstvima (hardveru i softveru) ili podacima, pri čemu privatni kriptografski ključ aplikacije ovjerioca nije uništen ili oštećen, servisi aplikacije ovjerioca bit će ponovno uspostavljeni u najkraćem mogućem roku.

Ovjerilac JP BH POŠTA će u slučaju kompromitiranja privatnog kriptografskog ključa aplikacije ovjerioca odmah:

- Opozvati izdane elektronske potvrde,
- Opozvati potvrdu aplikacije ovjerioca,
- Objaviti registar opozvanih potvrda,

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	12/18

- Obavijestiti korisnike izdanih elektronskih potvrda.

Poslije prestanka katastrofe i otklanjanja njenog uzroka, Ovjerilac JP BH POŠTA će u najkraćem mogućem roku da dovede sistem u produkciono stanje i nastavi s radom.

Ovjerilac JP BH POŠTA u slučaju prestanka rada ima obavezu:

- Obavijestiti sve zainteresirane strane (nadležni organ i svoje korisnike) o prestanku rada,
- Prenijeti svoje obaveze drugom ovjeriocu, ukoliko postoje mogućnosti za to,
- Opozvati sve izdane elektronske potvrde kojima nije istekao rok važnosti ukoliko ne uspije da prenese svoje obaveze na drugog ovjerioca,
- Uništiti ili potpuno onemogućiti korištenje svojih privatnih ključeva, koji su korišteni za kreiranje potvrda i registra opozvanih potvrda, tako da se isti ne mogu rekonstruirati.

Korisnici izdatih elektronskih potvrda bit će obaviješteni o prestanku rada preko zvanične *Web* stranice Ovjerioca JP BH POŠTA ili na drugi način, posredstvom sredstava javnog informiranja ili elektronskom poštom.

6. KONTROLE TEHNIČKE ZAŠTITE

Tokom ceremonije generiranja para kriptografskih ključeva koristi se zaštita koja važi za prostorije Ovjerioca JP BH POŠTA, zaštita koju pruža hardverski kriptografski modul (eng. *Hardware Security Module – HSM*), operativni sistem, aplikacija ovjerioca i višestruka autentikacija ovlaštenih lica.


Par kriptografskih ključeva korisnika za potpisivanje i verificiranje kvalificiranog elektronskog potpisa generira se na *QSCD* uređaju, koji predstavlja sredstvo za formiranje kvalificiranog elektronskog potpisa.

Dužine kriptografskih ključeva za koje Ovjerilac JP BH POŠTA izdaje elektronske potvrde su:

- Kriptografski ključevi aplikacije ovjerioca: *RSA* ključevi najmanje dužine 3072 bita,
- Korisnički ključevi: *RSA* ključevi najmanje dužine 2048 bita.

Generiranje parametara javnog kriptografskog ključa aplikacije ovjerioca vrši se u hardverskim kriptografskim modulima Ovjerioca JP BH POŠTA, a parametri javnih kriptografskih ključeva korisnika generiraju se u kriptografskim *QSCD* uređajima i softveru Ovjerioca JP BH POŠTA, ovisno od profila potvrde po kojem se izdaje potvrda.

Namjena javnog kriptografskog ključa kvalificirane elektronske potvrde ili pečata je verificiranje kvalificiranog elektronskog potpisa ili pečata i osiguravanje neporecivosti.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	13/18

Ovjerilac JP BH POŠTA ima implementiranu višestruku autorizaciju za pristup privatnom kriptografskom ključu aplikacija ovjerioca JP BH POŠTA *Root CA*, JP BH POŠTA *Issuing CA*.

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

Kreiranje kopija privatnih kriptografskih ključeva povezanih sa kvalificiranim elektronskim potvrdama korisnika se ne radi.

Rokovi važnosti potvrda Ovjerioca JP BH POŠTA su:

- Potvrde aplikacije ovjerioca: (20) dvadeset godina,
- Kvalificirane elektronske potvrde korisnika: (1) jedna ili (3) tri godine,
- Kvalificirana potvrda za elektronski pečat: (1) jedna ili (3) tri godine,


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

Na sistemu Ovjerioca JP BH POŠTA implementirane su tehničko-sigurnosne kontrole i mehanizmi, i to:

- Kontrola pristupa do sistemskih servisa aplikacije Ovjerioca JP BH POŠTA,
- Kontrola pristupa funkcijama aplikacije Ovjerioca JP BH POŠTA,
- Stroga podjela uloga između ovlaštenih lica Ovjerioca JP BH POŠTA,
- Upotreba kriptografskih modula za smještanje kriptografskih ključeva ovlaštenih lica Ovjerioca JP BH POŠTA,
- Sigurno arhiviranje podataka aplikacije Ovjerioca JP BH POŠTA i elektronskih dnevnika,
- Zaštita elektronskih dnevnika, odnosno podataka u istima o svim događajima koji se odnose na sigurnost,
- Uspostavljanje mehanizama obnove sistema, kriptografskih ključeva i baze podataka aplikacije Ovjerioca JP BH POŠTA.

Ovjerilac JP BH POŠTA ima mehanizme i procedure koje primjenjuje u kontroli i nadzoru svih tehničkih sistema. U slučaju narušene bezbjednosti sistema Ovjerioca JP BH POŠTA ili gubitka integriteta, Ovjerilac JP BH POŠTA će u roku od 24 sata o tome obavijestiti nadležni organ.

Računarsku mrežu Ovjerioca JP BH POŠTA čine povezani mrežni segmenti, na kojima se nalaze serveri i radne stanice. Segmenti su međusobno povezani mrežnim uređajima i *firewall*-ima. Sigurnosna pravila na *firewall*-ima i mrežnim uređajima dozvoljavaju promet samo između servera i radnih stanica po protokolima koji su potrebni za obavljanje djelatnosti Ovjerioca JP BH POŠTA i za pristup servisima Ovjerioca JP BH POŠTA.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	14/18

Elektronske potvrde i registri opozvanih potvrda imaju vremensku oznaku datuma i vremena izdavanja, datuma i vremena prestanka važenja potvrde i datuma i vremena izdavanja sljedećeg registra opozvanih potvrda. Vremenska oznaka nije kriptografski vremenski žig. Sistem tačnog vremena je putem *NTP* protokola (eng. *Network Time Protocol*) usklađen sa spoljnim *UTC* (*Coordinated Universal Time*) izvorom tačnog vremena koji u skladu sa zakonskom regulativom osigurava Institut za mjeriteljstvo BiH.

7. SADRŽAJ POTVRDE I REGISTRA OPOZVANIH POTVRDA

Ovjerilac JP BH POŠTA izdaje potvrde sukladne specifikaciji *X.509* verzije 3.

Ovjeritelj JP BH POŠTA potpisuje kvalificirane elektroničke potvrde i registre opozvanih potvrda primjenom algoritma SHA256 (OID 1.3.6.1.4.1.59867.10.1.2) sukladno dokumentima *RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, *RFC 4055 – Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* i *RFC 6931 – Additional XML Security Uniform Resource Identifiers (URIs)*.

Ovjerilac JP BH POŠTA izdaje *X.509* registre opozvanih potvrda (eng. *Certificate Revocation List – CRL*) verzije 2. Profil registra opozvanih potvrda je u skladu sa dokumentom *RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

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


Ovjerilac JP BH POŠTA vrši analizu rizika kojom identifikuje kritične servise koji zahtijevaju korištenje sigurnih sistema i visok nivo sigurnosti:

- Prije početka obavljanja usluga ovjeravanja,
- U toku operativnog rada po potrebi, a najmanje svakih 6 mjeseci.

Ovjerilac JP BH POŠTA izvršava redovne unutarnje revizije rada dva puta godišnje.

Moguće je izvršiti i više od dvije revizije godišnje ukoliko je to zahtijevano od nadležnog organa ili ako je to posljedica nezadovoljavajućih rezultata prethodne revizije.

Interna revizija JP BH POŠTA je odgovorna za provođenje unutarnjih revizija i određivanje lica koja ih provode.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	15/18

Unutarnja revizija se provodi angažiranjem stručnog lica iz ili izvan Ovjerioca JP BH POŠTA koja mora da ima iskustva na području:

- Tehnologije infrastrukture javnih kriptografskih ključeva,
- Vršnja djelatnosti ovjerioca,
- Provođenja revizije ovjerioca ili drugog informacijsko-komunikacijskog sistema.

U slučaju utvrđenih nedostataka, provode se aktivnosti na otklanjanju istih u što kraćem roku.

Izveštaj revizije predstavlja interni dokument Ovjerioca JP BH POŠTA i ne objavljuje se javno. Namijenjen je isključivo ovlaštenim licima Ovjerioca JP BH POŠTA za potrebe otklanjanja eventualno pronađenih nedostataka.

9. OSTALI POSLOVI I PRAVNA PITANJA

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

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


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:

- 1) 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,
- 2) 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.

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.

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

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	16/18

Sva prava intelektualne svojine Ovjerioca JP BH POŠTA, uključujući zaštitne znake i autorska prava, ostaju isključivo vlasništvo Ovjerioca JP BH POŠTA.

Ovjerilac JP BH POŠTA garantira pružanje usluge ovjeravanja, u skladu sa zakonom, drugim propisima, Praktičnim pravilima i drugim aktima Ovjerioca, koji su usklađeni s važećim propisima Bosne i Hercegovine.


Ovjerilac JP BH POŠTA ima obavezu:

- Izvršiti provjeru identiteta korisnika u postupku 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 kvalificiranu elektronsku potvrdu, u skladu sa zakonom,
- Osigurati da kvalificirana elektronska potvrda sadrži sve potrebne podatke, u skladu sa zakonom,
- Unijeti u kvalificiranu elektronsku potvrdu osnovne podatke o svom identitetu i o identitetu korisnika, kao i javni kriptografski ključ korisnika koji je par njegovom privatnom kriptografskom ključu,
- Osigurati vidljiv podatak u elektronskoj potvrdi o tačnom datumu i vremenu (sat i minut) izdavanja potvrde,
- Usvojiti ili odbiti izvršenje zahtjeva za promjenu statusa kvalificirane elektronske potvrde, u skladu sa zakonom,
- Voditi ažuran, tačan i sigurnim mjerama zaštićen registar opozvanih potvrda i da isti bude javno dostupan,
- Osigurati vidljiv podatak u registru opozvanih potvrda o tačnom datumu i vremenu (sat i minut) opoziva elektronske potvrde,
- Vršiti nadzor nad radom organizacijskih jedinica u sastavu Ovjerioca JP BH POŠTA.

Ovjerilac JP BH POŠTA pruža usluge u skladu sa važećim propisima i internim aktima.

Korisnik je obavezan:

- Čuvati sredstva i podatke za formiranje kvalificiranog elektronskog potpisa od neovlaštenog pristupa i upotrebe,
- Dostaviti sve potrebne podatke i informacije o svom identitetu i o promjenama koje utiču ili mogu uticati na tačnost utvrđivanja njegovog identiteta odmah, a najkasnije u roku od 24 (dvadesetčetiri) sata od trenutka nastanka promjene,
- Odmah zatražiti opoziv svoje kvalificirane elektronske potvrde u svim slučajevima gubitka ili oštećenja sredstava ili podataka za formiranje kvalificiranog elektronskog potpisa,
- Namjenski koristiti kvalificiranu elektronsku potvrdu,
- Ispunjavati druge obaveze u skladu sa zakonom i zaključenom ugovoru koji je sačinjen u skladu sa važećim propisima.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	17/18

Svakom učesniku garantira se da Ovjerilac JP BH POŠTA usluge ovjeravanja pruža u skladu sa zakonom, ovim Praktičnim pravilima i drugim važećim propisima Ovjerioca JP BH POŠTA.

Ovjerilac JP BH POŠTA ne odgovara za štetu nastalu zbog nepoštivanja prava i obveza propisanih zakonom, važećim podzakonskim propisima i Praktičnim pravilima.

Ovjerilac JP BH POŠTA je dužan da na propisan način izdaje kvalificirane elektronske potvrde i odgovoran je za štetu pričinjenu licu koje se pouzdalo u tu potvrdu, u skladu sa zakonom, aktima ovjerioca i ugovorom zaključenim između Ovjerioca JP BH POŠTA i korisnika.

U slučaju prestanka rada, Ovjerilac JP BH POŠTA će:


- Obavijestiti sve korisnike putem *Web* stranice i nadležnog tijela državne uprave najmanje šest mjeseci prije planiranog prekida rada,
- Osigurati 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 osigura nastavak pružanja usluga povjerenja preko drugog davatelja usluga povjerenja,
- Osigurati dostupnost popisa opozvanih potvrda u roku od godine dana nakon opoziva svih potvrda,
- Arhivirati sve podatke u skladu s razdobljem propisanim relevantnim zakonom od posljednjeg dana rada ovjerioca.

Korisnik je odgovoran za štetu koja je nastala njegovom krivicom.

Korisnik je odgovoran ako s namjerom ili iz nehata obriše potvrdu i/ili pripadajući privatni ključ sa QSCD uređaja. QSCD uređaj sa koje je obrisana potvrda i/ili pripadajući privatni ključ ne podliježe reklamaciji, ni garanciji.

Korisnik nije odgovoran za štetu, ako dokaže da je postupao u skladu sa zakonom, podzakonskim aktima i zaključenom ugovoru.

Ukoliko dođe do spora između JP BH POŠTA i korisnika kvalifikovane elektronske potvrde, odnosno trećih lica u vezi međusobnih prava i obaveza i tumačenja ugovora i ovih Praktičnih pravila, JP BH POŠTA će nastojati da spor riješi mirnim putem, sporazumno, a ukoliko do sporazuma ne dođe, spor će rješavati nadležni sud u Sarajevu.

	POLITIKA OVJERAVANJA OVJERIOCA JP BH POŠTA	klasifikacija:	javno
		oznaka:	
		revizija:	30.11.2023
		strana:	18/18

Ovjerilac JP BH POŠTA se oslobađa odgovornosti za bilo koju štetu pričinjenu korisniku, drugom učesniku ili trećem licu, prilikom pružanja usluge ovjeravanja, ukoliko je do štete došlo uslijed razloga koji su izvan kontrole Ovjerioca JP BH POŠTA, odnosno uslijed više sile.

Ova Politika ovjeravanja stupa na snagu danom donošenja, a počinje sa primjenom osmoga dana od dana objave na *Web* stranici Ovjerioca JP BH POŠTA.

Broj dokumenta

Datum

Direktor JP BH POŠTA d.o.o. Sarajevo
