

UPRAVA ZA NEIZRAVNO OPOREZIVANJE
Bana Lazarevića bb, Banja Luka

POLITIKA OVJERAVANJA
OVJERITELJA UPRAVE ZA NEIZRAVNO
OPOREZIVANJE

(Certification Policy - CP)

Verzija 1.0

SADRŽAJ

1.	UVOD	3
2.	OBJAVLJIVANJE I LOKACIJA PODATAKA O USLUGAMA OVJERAVANJA	4
3.	IDENTIFIKACIJA I AUTENTIKACIJA	5
4.	OPERATIVNI ZAHTJEVI U PROCESU IZDAVANJA POTVRDA.....	5
5.	KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OVLAŠTENIH OSOBA	8
6.	KONTROLE TEHNIČKE ZAŠTITE	10
7.	SADRŽAJ POTVRDE, REGISTRA OPOZVANIH POTVRDA I OCSP PROFILI.....	11
8.	REVIZIJA USKLAĐENOSTI RADA UNO OVJERITELJA I DRUGE PROCJENE ..	12
9.	OSTALI POSLOVI I PRAVNA PITANJA.....	12

Temeljem članka 61. Zakona o upravi („Službeni glasnik BiH“, br. 32/02, 102/09 i 72/17) i članka 5. Pravilnika o bližim uvjetima za izdavanje kvalificiranih potvrda („Službeni glasnik BiH“, broj: 14/17) ravnatelj Uprave za neizravno oporezivanje donosi

POLITIKU OVJERAVANJA OVJERITELJA UPRAVE ZA NEIZRAVNO OPOREZIVANJE

1. UVOD

Uprava za neizravno oporezivanje (u daljnjem tekstu: UNO) je izgradila infrastrukturu javnih kriptografskih ključeva - *Public Key Infrastructure – PKI* i kao ovjeritelj u smislu Zakona o elektroničkom potpisu („Službeni glasnik BiH“, broj: 91/06) prisutna je kao ovjeritelj koji pruža usluge izdavanja kvalificiranih i nekvalificiranih elektroničkih potvrda, upravljanja životnim ciklusom elektroničkih potvrda i izdavanje kvalificiranih elektroničkih vremenskih žigova, pod imenom: Ovjeritelj UNO.

Ovjeritelj UNO vrši izdavanje kvalificiranih elektroničkih potvrda sukladno zakonskim propisima, općim aktima i uputama Ovjeritelja UNO koja reguliraju ovu oblast. Pravni okvir za obavljanje djelatnosti izdavanja kvalificiranih elektroničkih potvrda Ovjeritelja UNO čine sljedeći zakoni i podzakonski akti:

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

Opća pravila funkcioniranja Ovjeritelja UNO sadržana su u dokumentima:

- Politika ovjeravanja Ovjeritelja Uprave za neizravno oporezivanje (*Certification Policy - CP*) (u daljnjem tekstu Politika ovjeravanja),
- Praktična pravila pružanja usluge ovjeravanja Ovjeritelja Uprave za neizravno oporezivanje (*Certification Practices Statement - CPS*) (u daljnjem tekstu Praktična pravila).

Kvalificirane i nekvalificirane elektroničke potvrde i kvalificirani elektronički vremenski žigovi koje izdaje Ovjeritelj UNO su u skladu s eIDAS uredbom Europske unije („Uredba broj 910/2014 Europskog parlamenta i Vijeća o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ“) i odgovarajućim međunarodnim standardima i preporukama, kao i drugim standardima, dokumentima i preporukama, koje se odnose na izdavanje kvalificiranih elektroničkih potvrda.

Ovjeritelj UNO koristi u svojoj infrastrukturi za izdavanje kvalificiranih i nekvalificiranih elektroničkih potvrda hijerarhiju više CA (eng. *Certification Authority*) poslužitelja.

Dvorazinsku arhitekturu Infrastrukture Ovjeritelja UNO čine tri CA poslužitelja:

- Korijski ovjeritelj: „*UINO Root CA*“
- Podređeni ovjeritelji za izdavanje potvrda, potpisani od strane „*UINO Root CA*“:
 - o „*UINO Issuing CA1*“,
 - o „*UINO Issuing CA2*“.

Privatni kriptografski ključevi koji su pridruženi kvalificiranim elektroničkim potvdama koriste se u procesu kvalificiranog elektroničkog potpisivanja elektroničkog dokumenta, koji se može koristiti u općenju organa i općenju organa i stranaka, 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 uporaba kvalificiranog elektroničkog potpisa.

Kvalificirane elektroničke potvrde potvrđuju svezu između javnog kriptografskog ključa korisnika i identiteta korisnika koji je izvršio kvalificirano potpisivanje elektroničkog dokumenta.

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

2. OBJAVLJIVANJE I LOKACIJA PODATAKA O USLUGAMA OVJERAVANJA

Ovjeritelj UNO objavljuje podatke i svu dokumentaciju koja se odnosi na izdavanje elektroničkih potvrda na *Web* stranici <http://ca.uino.gov.ba>. *Web* stranica je javno dostupna, kao i svi podaci i sva dokumentacija koji se na njoj nalaze.

Ovjeritelj UNO objavljuje na svojoj službenoj *Web* stranici:

- Politiku ovjeravanja Ovjeritelja UNO,
- Praktična pravila pružanja usluge ovjeravanja Ovjeritelja UNO,
- Prethodne verzije Politike ovjeravanja Ovjeritelja UNO i Praktičnih pravila pružanja usluge ovjeravanja Ovjeritelja UNO,
- Obrazac ugovora o obavljanju usluga ovjeravanja,
- Obrazac zahtjeva za izdavanje i korištenje elektroničke potvrde,
- Obrazac zahtjeva za promjenu statusa potvrde,
- Definicije važećih profila potvrda Ovjeritelja UNO usklađenih sa eIDAS uredbom Europske unije,
- Korisničke upute,
- Potvrde ovjeritelja *UINO Root CA* i podređenih ovjeritelja (*UINO Issuing CA1* i *UINO Issuing CA2*) sa pridruženim *hash* vrijednostima,
- Registre opozvanih potvrda (*CRL* – eng. *Certificate Revocation List*) ovjeritelja *UINO Root CA*, *UINO Issuing CA1* i *UINO Issuing CA2*,
- Zakonsku regulativu iz područja elektroničkog potpisa i pružanja usluga povjerenja,

- Cjenik usluga ovjeravanja,
- Lokacije ureda Registracijskog tijela,
- Obavijesti korisnicima vezane uz davanje usluga ovjeravanja,
- Druge akte i obavještenja.

3. IDENTIFIKACIJA I AUTENTIKACIJA

Ovjeritelj UNO identificira korisnika na temelju identifikacijskog dokumenata koji korisnik podnosi (važeća osobna iskaznica, putovnica ili drugi). Korisnik mora osobno podnijeti cjelokupnu dokumentaciju.

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

Ovjeritelj UNO jamči jedinstvenost imena u svojoj domeni. Ovjeritelj UNO dodjeljuje svakom korisniku jedinstveno ime (*Distinguished Name - DN*), koje se upisuje u polje *Subject* elektroničke potvrde.

Imena kojima bi se kršila intelektualna ili autorska prava drugih nisu dozvoljena. Ovjeritelj UNO nije obvezan provjeriti da li je korištenje takvih imena zakonito. Odgovornost korisnika je osigurati zakonito korištenje odabranog imena.

Kvalificirana elektronička potvrda za elektronički potpis se može izdati samo fizičkoj osobi, sukladno Zakonu o elektroničkom potpisu. Fizička osoba ima pravo u ime pravne osobe koristiti kvalificiranu elektroničku potvrdu, ukoliko mu to dozvoli pravna osoba. Fizička osoba može biti zaposlena u pravnoj osobi. Kvalificirana potvrda za elektronički pečat može se izdati samo pravnoj osobi.

Ukoliko Ovjeritelj UNO izdaje elektroničku potvrdu fizičkoj osobi koja je zaposlena u pravnoj osobi, u okviru atributa koji identificiraju korisnika nalaze se i podaci koji označavaju naziv pravne osobe i to poslovno ime pravne osobe i identifikator organizacije, odnosno porezni identifikacijski broj.

Korisnik mora da bude fizički nazočan tijekom registracije.

4. OPERATIVNI ZAHTJEVI U PROCESU IZDAVANJA POTVRDA

Za izdavanje elektroničke potvrde, korisnik je dužan:

- Popuniti i potpisati zahtjev za izdavanje i korištenje elektroničke potvrde i uz isti priložiti ovjerenu fotokopiju identifikacijskog dokumenta,
- Ispuniti zahtjeve za identifikaciju,
- Ispuniti financijske obveze prema cjeniku,
- Potpisati ugovor o izdavanju i korištenju elektroničke potvrde.

Zahtjev za izdavanje i korištenje elektroničke potvrde sadrži podatke na temelju kojih Ovjeritelj UNO može stupiti u kontakt s korisnikom elektroničke potvrde.

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

Korištenje kvalificirane elektroničke potvrde se ugovara na rok od pet godina i vezuje se za dan izdavanja potvrde.

Ovjeritelj UNO će odobriti zahtjev za izdavanje elektroničke potvrde, ukoliko su ispunjeni sljedeći uvjeti:

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

Ako korisnik ne ispuni uvjete iz prethodnog stavka ili ako na bilo koji način povrijedi odredbe Praktičnih pravila, Ovjeritelj UNO će odbiti zahtjev za izdavanje elektroničke potvrde.

Izdavanje elektroničke potvrde vrši se na sljedeći način:

1. Korisnik preko *Web* sajta Ovjeritelja UNO preuzima Zahtjev za izdavanje elektroničke potvrde i popunjava ga,
2. Korisnik, u postupku izdavanja potvrde, identificira se osobno u Grupi za podršku korisnicima sustava PKI UNO u regionalnom centru,
3. Grupa za podršku korisnicima sustava PKI UNO u regionalnom centru unosi podatke o korisniku i kreira zahtjev u aplikaciji Registracijskog tijela i prosljeđuje verificiran zahtjev Grupi za održavanje sustava PKI UNO,
4. Grupa za održavanje sustava PKI UNO na temelju verificiranog zahtjeva kreira nalog za personalizaciju kriptografskog uređaja,
5. Korisnički privatni kriptografski ključ se generira u hardverskom kriptografskom modulu *SSCD* uređaja kod Ovjeritelja UNO,
6. Ovjeritelj UNO šalje izdane korisničke potvrde na *SSCD* uređaju u regionalni centar,
7. Korisnik potpisuje ugovor o izdavanju i korištenju elektroničke potvrde, preuzima elektroničku potvrdu na *SSCD* uređaju u Grupi za podršku korisnicima sustava PKI UNO u regionalnom centru i potpisuje izjavu o preuzimanju elektroničke potvrde na *SSCD* uređaju,
8. Korisnik preuzima pripadajuću zaporku/PIN kod u zatvorenoj koverti u Grupi za podršku korisnicima sustava PKI UNO u regionalnom centru.

Prvom uporabom elektroničke potvrde od strane korisnika, potvrda se smatra prihvaćenom.

Ukoliko se naknadno utvrdi da u elektroničkoj potvrdi postoje pogrešni podaci, korisnik je dužan da se obrati Ovjeritelju UNO radi izdavanja nove potvrde.

Ovjeritelj UNO ne vrši produženje korištenja elektroničke potvrde. Cijeli proces se izvršava izdavanjem nove elektroničke potvrde.

Zamjena javnog ključa u elektroničkoj potvrdi se ne vrši. Cijeli proces se izvršava izdavanjem nove elektroničke potvrde.

Ovjeritelj UNO je dužan da opozove elektroničku potvrdu iz sljedećih razloga:

- U slučaju da neka informacija sadržana u potvrdi postane netočna,
- Promjene podataka u potvrdi, koje zahtjevaju izdavanje nove potvrde,
- Naknadnog utvrđivanja da podaci koje je dostavio korisnik pri identifikaciji nisu točni,
- Gubitka, oštećenja ili zlouporabe 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,
- U slučaju prestanka odnosa između potpisnika i poslovnog subjekta,
- Neispunjavanja obveza korisnika potvrde određenih Praktičnim pravilima i ugovorom,
- Ukoliko opoziv elektroničke potvrde zahtjeva korisnik potvrde,
- Ukoliko korisnik elektroničke potvrde prestane da postoji,
- Ukoliko korisnik izgubi poslovnu sposobnost ili pravna osoba kojoj pripada korisnik prestane da postoji,
- U slučaju da potvrda više nije sukladna općim pravilima,
- Ukoliko se promijene okolnosti koje bitno utječu na važenje potvrde,
- U slučaju otkaza ugovora o obavljanju usluge ovjeravanja od strane korisnika,
- Iz drugih razloga koji su utvrđeni Zakonom o elektroničkom potpisu i drugim propisima koji reguliraju ovu oblast.

Opoziv elektroničke potvrde može zahtijevati:

- Korisnik elektroničke potvrde – fizička osoba,
- Pravna osoba za zaposlene u toj pravnoj osobi,
- Ovjeritelj UNO,
- Nadležni državni organ na temelju zakona.

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

Registri opozvanih potvrda ovjerioca objavljuju se na svaka 24 sata.

Putem OCSP (eng. *Online Certificate Status Protocol*) servisa Ovjeritelja UNO dostupne su informacije o statusu opozvanosti potvrda koje su izdate od strane Ovjeritelja UNO.

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

U slučaju da prije redovite objave dođe do opoziva ili suspenzije elektroničke potvrde, Ovjeritelj UNO odmah objavljuje novi registar opozvanih potvrda i prije isteka važenja registra opozvanih potvrda.

Korisnici i treće osobe su dužne da provjere status elektroničke potvrde na temelju javno dostupnog registra opozvanih potvrda Ovjeritelja UNO.

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

Ovjeritelj UNO može suspendirati elektroničke potvrde tijekom provjeravanja okolnosti u svezi s mogućim opozivom potvrde.

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

Korisnik prestaje s korištenjem elektroničke potvrde:

- Istekom roka valjanosti elektroničke potvrde,
- Opozivom elektroničke potvrde,
- Tijekom trajanja suspenzije elektroničke potvrde.

Ovjeritelj UNO ne čuva privatne ključeve korisnika kvalificiranih elektroničkih potvrda i ne može da ih otkrije niti obnovi.

5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OVLAŠTENIH OSOBA

Oprema Ovjeritelja UNO se nalazi u sigurnoj prostoriji koja je osigurana dvorazinskom elektroničkom bravom u zgradi glavnog ureda UNO. Kontrola fizičkog pristupa Ovjeritelju UNO je implementirana sukladno Zakonu o elektroničkom potpisu i podzakonskim aktima, i to na sljedeći način:

- Pristup u prostorije, sigurnu zonu, elektronički se bilježi i unosi u elektronički dnevnik za pristup prostorijama, i isti se pregleda,
- Brave, elektronički sustavi zaštite i sustavi protupožarne zaštite su sukladni važećim standardima,
- Prostor i sustav nadgledani su 24 sata, 7 dana u tjednu od strane ovlaštenih osoba Ovjeritelja UNO,
- Pristup se može provoditi isključivo uz nazočnost najmanje dvije ovlaštene osobe koje imaju pravo pristupa,
- Pristup zbog održavanja sustava mora biti unaprijed najavljen, osim u slučaju smetnji u radu sustava za koje Grupa za održavanje sustava PKI UNO utvrdi da zahtijevaju hitnu intervenciju,
- Svaki pristup zaštićenoj prostoriji evidentira se unutar elektroničke evidencije.

Ovjeritelj UNO osigurava da je pristup sustavu ovjeravanja ograničen isključivo na ovlaštene zaposlene.

Prostorije u kojima se nalazi infrastruktura Ovjeritelja UNO u glavnom uredu UNO su opremljene:

- Sustavom za neprekidni izvor napajanja električnom energijom i stabilizaciju napona za računarsku i komunikacijsku opremu, koji je povezan sa agregatom,
- Neovisnim sustavom za klimatizaciju koji omogućava kontrolu temperature i vlažnosti zraka unutar prostorija Ovjeritelja UNO.

Oprema Ovjeritelja UNO smještena je na mjestu koje je osigurano od poplave.

Oprema Ovjeritelja UNO zaštićena je automatskim sustavom protupožarne zaštite sukladno propisanoj i važećoj zakonskoj regulativi.

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

Ovjeritelj UNO jamči da sve poslove koji se obavljaju u okviru propisane djelatnosti obavljaju osobe od povjerenja s točno propisanim obvezama i ovlaštenjima. Rad ovih osoba je podložan stalnim provjerama.

Zaposleni Ovjeritelja UNO moraju biti kvalificirani za obavljanje poslova i podliježu provjeri stručne sposobnosti.

U slučaju izvršene ili sumnje na izvršene neovlaštene aktivnosti od strane ovlaštene osobe Ovjeritelja UNO, istoj će biti onemogućen daljnji pristup tehničkim sredstvima (hardveru i softveru) Ovjeritelja UNO, a Ovjeritelj UNO će suspendirati ili opozvati sve važeće elektroničke potvrde koje su izdate toj osobi.

Izvršene neovlaštene aktivnosti prijavljuju se nadležnim organizacijskim jedinicama UNO, državnim organima i institucijama, sukladno važećim zakonskim i internim propisima.

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

Ovjeritelj UNO će u slučaju kompromitiranja privatnog kriptografskog ključa aplikacije ovjeritelja odmah:

- Opozvati izdane elektroničke potvrde,
- Opozvati potvrdu aplikacije ovjeritelja,
- Objaviti registar opozvanih potvrda,
- Obavijestiti korisnike izdanih elektroničkih potvrda.

Poslije prestanka katastrofe i otklanjanja njenog uzroka, Ovjeritelj UNO će u najkraćem mogućem roku dovesti sustav u produkcijsko stanje i nastaviti s radom.

Ovjeritelj UNO u slučaju prestanka rada ima obvezu:

- Obavijestiti sve zainteresirane strane (nadležni organ i svoje korisnike) o prestanku rada,
- Prenijeti svoje obveze drugom ovjeritelju, ukoliko postoje mogućnosti za to,
- Opozvati sve izdane elektroničke potvrde kojima nije istekao rok valjanosti ukoliko ne uspije da prenese svoje obveze na drugog ovjeritelja,
- 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 elektroničkih potvrda bit će obaviješteni o prestanku rada preko službene *Web* stranice Ovjeritelja UNO ili na drugi način, posredstvom sredstava javnog informiranja ili elektroničkom poštom.

6. KONTROLE TEHNIČKE ZAŠTITE

Tijekom ceremonije generiranja para kriptografskih ključeva koristi se zaštita koja važi za prostorije Ovjeritelja UNO, zaštita koju pruža hardverski kriptografski modul (eng. *Hardware Security Module – HSM*), operacijski sustav, aplikacija ovjeritelja i višestruka autentikacija ovlaštenih osoba.

Par kriptografskih ključeva korisnika za potpisivanje i verifikaciju kvalificiranog elektroničkog potpisa generira se na *SSCD* uređaju, koji predstavlja sredstvo za formiranje kvalificiranog elektroničkog potpisa.

Dužine kriptografskih ključeva za koje Ovjeritelj UNO izdaje elektroničke potvrde su:

- Kriptografski ključevi aplikacije ovjeritelja: *RSA* ključevi najmanje dužine 4096 bita,
- Korisnički ključevi: *RSA* ključevi najmanje dužine 2048 bita.

Generiranje parametara javnog kriptografskog ključa aplikacije ovjeritelja vrši se u hardverskim kriptografskim modulima Ovjeritelja UNO, a parametri javnih kriptografskih ključeva korisnika generiraju se u kriptografskim *SSCD* uređajima i softveru Ovjeritelja UNO, u zavisnosti od profila potvrde po kojem se izdaje potvrda.

Namjena javnog kriptografskog ključa kvalificirane elektroničke potvrde ili pečata korisnika je verifikacija kvalificiranog elektroničkog potpisa ili pečata i osiguravanje neporecivosti.

Ovjeritelj UNO ima implementiranu višestruku autorizaciju za pristup privatnom kriptografskom ključu aplikacija ovjeritelja *UINO Root CA*, *UINO Issuing CA1* i *UINO Issuing CA2* Ovjeritelja UNO.

Ovjeritelj UNO ne nudi mogućnost otkrivanja privatnog kriptografskog ključa.

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

Rokovi valjanosti potvrda Ovjeritelja UNO su:

- Potvrde aplikacije ovjeritelja: dvadeset (20) godina,
- Kvalificirane elektroničke potvrde korisnika: pet (5) godina,
- Potvrda za potpis odgovora OCSP servisa: jedna (1) godina,
- Kvalificirana potvrda za elektronički pečat: pet (5) godina,
- Potvrda za autentikaciju *Web* stranica za pravne osobe: 398 dana,
- Potvrda za autentikaciju *Web* stranica i *Kerberos* potvrda za domen kontroler: dvije (2) godine,
- Potvrda za potpisivanje koda: tri (3) godine.

Svaki korisnik kvalificirane elektroničke potvrde je odgovoran za čuvanje zaporke svog *SSCD* uređaja.

Na sustavu Ovjeritelja UNO implementirane su tehničko-sigurnosne kontrole i mehanizmi, i to:

- Kontrola pristupa do sistemskih servisa aplikacije Ovjeritelja UNO,
- Kontrola pristupa funkcijama aplikacije Ovjeritelja UNO,
- Stroga podjela uloga između ovlaštenih osoba Ovjeritelja UNO,
- Uporaba kriptografskih modula za smještanje kriptografskih ključeva ovlaštenih osoba Ovjeritelja UNO,
- Sigurno arhiviranje podataka aplikacije Ovjeritelja UNO i elektroničkih dnevnika,
- Zaštita elektroničkih dnevnika, odnosno podataka u istima o svim događajima koji se odnose na sigurnost,
- Uspostavljanje mehanizama obnove sustava, kriptografskih ključeva i baze podataka aplikacije Ovjeritelja UNO.

Ovjeritelj UNO ima mehanizme i procedure koje primjenjuje u kontroli i nadzoru svih tehničkih sustava. U slučaju narušavanja sigurnosti sustava Ovjeritelja UNO ili gubitka integriteta, Ovjeritelj UNO će u roku od 24 sata o tome obavijestiti nadležni organ.

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

Elektroničke 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. Sustav točnog vremena je putem *NTP* protokola (eng. *Network Time Protocol*) usklađen sa vanjskim *UTC* (*Coordinated Universal Time*) izvorom točnog vremena koji sukladno zakonskoj regulativi osigurava Institut za mjeriteljstvo BiH.

7. SADRŽAJ POTVRDE, REGISTRA OPOZVANIH POTVRDA I OCSP PROFILI

Ovjeritelj UNO izdaje potvrde sukladne specifikaciji *X.509* verzije 3.

Dokument s opisom profila potvrda Ovjeritelja UNO dostupan je na *Web* stranici Ovjeritelja UNO pod nazivom „UNO profili potvrda“.

Ovjeritelj UNO potpisuje kvalificirane elektroničke potvrde i registre opozvanih potvrda primjenom algoritma *SHA512RSA* (*OID* 1.2.840.113549.1.1.13) 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)*.

Ovjeritelj UNO izdaje X.509 registre opozvanih potvrda (eng. *Certificate Revocation List – CRL*) verzije 2. Profil registra opozvanih potvrda je sukladan dokumentu *RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile*.

8. REVIZIJA USKLAĐENOSTI RADA UNO OVJERITELJA I DRUGE PROCJENE

Ovjeritelj UNO vrši analizu rizika kojom identificira kritične servise koji zahtijevaju korištenje sigurnih sustava i visoku razinu sigurnosti:

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

Ovjeritelj UNO izvršava redovite 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.

Šef Odsjeka za elektroničke potpise i certifikate u Sektoru za informatičke tehnologije UNO odgovoran je za provođenje unutarnjih revizija i određivanje osoba koje ih provode.

Unutarnja revizija se provodi angažiranjem stručne osobe iz ili izvan Ovjeritelja UNO koja mora da ima iskustva na području:

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

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

Izvešće revizije predstavlja interni dokument Ovjeritelja UNO i ne objavljuje se javno. Namijenjen je isključivo ovlaštenim osobama Ovjeritelja UNO za potrebe otklanjanja eventualno pronađenih nedostataka.

9. OSTALI POSLOVI I PRAVNA PITANJA

Ovjeritelj UNO naplaćuje izdavanje elektroničke potvrde na temelju cjenika koji je objavljen na *Web* stranici Ovjeritelja UNO.

Ovjeritelj UNO snosi financijsku odgovornost za obavljanje svoje djelatnosti sukladno važećim zakonskim propisima.

Ovjeritelj UNO je dužan da osigura najniži iznos osiguranja od odgovornosti za moguću štetu nastalu vršenjem usluga izdavanja kvalificirane elektroničke potvrde sukladno 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 uporabom jedne kvalificirane elektroničke potvrde u jednom aktu u pravnom prometu;
- 2) Ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti ovjeritelja kumulativno na godišnjoj razini, po svim štetnim događajima, ne može biti niža od 1.500.000,00 KM.

Zaposleni Ovjeritelja UNO i korisnici obvezuju 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.

Ovjeritelj UNO je dužan da se u svom poslovanju pridržava odredbi Zakona o zaštiti osobnih podataka.

Sva prava intelektualne svojine Ovjeritelja UNO, uključujući zaštitne znake i autorska prava, ostaju isključivo vlasništvo Ovjeritelja UNO.

Ovjeritelj UNO jamči pružanje usluge ovjeravanja, sukladno zakonu, drugim propisima, Praktičnim pravilima i drugim aktima Uprave za neizravno oporezivanje koji su usklađeni s važećim propisima Bosne i Hercegovine.

Ovjeritelj UNO ima obvezu:

- Izvršiti provjeru identiteta korisnika u postupku izdavanja ili promjene statusa elektroničke potvrde, kao i točnost podataka u zahtjevu za izdavanje i korištenje elektroničke potvrde, odnosno zahtjevu za promjenu statusa elektroničke potvrde,
- Izdati kvalificiranu elektroničku potvrdu, sukladno zakonu,
- Osigurati da kvalificirana elektronička potvrda sadrži sve potrebne podatke, sukladno zakonu,
- Unijeti u kvalificiranu elektroničku 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 elektroničkoj potvrdi o točnom datumu i vremenu (sat i minut) izdavanja potvrde,
- Izvršiti ili odbiti izvršenje zahtjeva za promjenu statusa kvalificirane elektroničke potvrde, sukladno zakonu,
- Voditi ažuran, točan i sigurnim mjerama zaštićen registar opozvanih potvrda i da isti bude javno dostupan,
- Osigurati vidljiv podatak u registru opozvanih potvrda o točnom datumu i vremenu (sat i minut) opoziva elektroničke potvrde,
- Vršiti nadzor nad radom organizacijskih jedinica u sastavu Ovjeritelja UNO.

Ovjeritelj UNO pruža usluge sukladno važećim propisima i internim aktima.

Korisnik je obavezan:

- Čuvati sredstva i podatke za formiranje kvalificiranog elektroničkog potpisa od neovlaštenog pristupa i uporabe,
- Dostaviti sve potrebne podatke i informacije o svom identitetu i o promjenama koje utječu ili mogu utjecati na točnost utvrđivanja njegovog identiteta odmah, a najkasnije u roku od 24 (dvadesetčetiri) sata od trenutka nastanka promjene,
- Odmah zatražiti opoziv svoje kvalificirane elektroničke potvrde u svim slučajevima gubitka ili oštećenja sredstava ili podataka za formiranje kvalificiranog elektroničkog potpisa,
- Namjenski koristiti kvalificiranu elektroničku potvrdu,
- Ispunjavati druge obveze sukladno zakonu i zaključenom ugovoru koji je sačinjen sukladno važećim propisima.

Svakom sudioniku jamči se da Ovjeritelj UNO usluge ovjeravanja pruža sukladno zakonu, Praktičnim pravilima i drugim važećim propisima Ovjeritelja UNO.

Ovjeritelj UNO ne odgovara za štetu nastalu zbog nepoštivanja prava i obveza propisanih zakonom, važećim podzakonskim propisima i Praktičnim pravilima.

Ovjeritelj UNO je dužan da na propisan način izdaje kvalificirane elektroničke potvrde i odgovoran je za štetu pričinjenu osobi koja se pouzdala u tu potvrdu, sukladno zakonu, aktima ovjeritelja i ugovorom zaključenim između Ovjeritelja UNO i korisnika.

U slučaju prestanka rada, Ovjeritelj UNO 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 pružatelja usluga povjerenja svim korisnicima kojima je već izdao potvrde i dostaviti svu dokumentaciju vezanu za pružanje povjerljivih usluga tom pružatelju usluga povjerenja,
- Opozvati sve izdane 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 sukladno razdobljima propisanim relevantnim zakonom od posljednjeg dana rada ovjeritelja.

Korisnik je odgovoran za štetu koja je nastala njegovom krivicom.

Korisnik je odgovoran ako s namjerom ili iz nemara obriše potvrdu i/ili pripadajući privatni ključ sa smart kartice. Smart kartica sa koje je obrisana potvrda i/ili pripadajući privatni ključ ne podliježe reklamaciji, ni jamstvu.

Korisnik nije odgovoran za štetu, ako dokaže da je postupao sukladno zakonu, podzakonskim aktima i zaključenom ugovoru.

Ukoliko dođe do spora između UNO i korisnika kvalifikovane elektroničke potvrde, odnosno trećih osoba u svezi međusobnih prava i obveza i tumačenja ugovora i Praktičnih pravila, UNO će nastojati da spor riješi mirnim putem, sporazumno, a ukoliko do sporazuma ne dođe, spor će rješavati nadležni sud u Banjoj Luci.

Ovjeritelj UNO se oslobađa odgovornosti za bilo koju štetu pričinjenu korisniku, drugom sudioniku ili trećoj osobi, prilikom pružanja usluga ovjeravanja, ukoliko je do štete došlo usljed razloga koji su izvan kontrole Ovjeritelja UNO, odnosno usljed više sile.

Ova Politika ovjeravanja stupa na snagu danom donošenja, a počinje sa primjenom osmoga dana od dana objave na *Web* stranici Ovjeritelja UNO.

Broj: 01-02-2-160-7/21
Datum: 12.03.2021.

Ravnatelj
Uprave za neizravno oporezivanje

dr. Miro Džakula