UPRAVA ZA INDIREKTNO OPOREZIVANJE
Bana Lazarevića bb, Banja Luka

POLITIKA OVJERAVANJA OVJERIOCA UPRAVE ZA INDIREKTNO OPOREZIVANJE

(Certification Policy - CP)

Verzija 1.0

SADRŽAJ

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

POLITIKU OVJERAVANJA
OVJERIOCA UPRAVE ZA INDIREKTNO OPOREZIVANJE

1. UVOD

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

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

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

Opća pravila funkcioniranja Ovjerioca UIO sadržana su u dokumentima:

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

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

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

- Korijenski ovjerilac: „***UINO Root CA***“

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

Privatni kriptografski ključevi koji su pridruženi kvalificiranim elektronskim potvrdama koriste se u procesu kvalificiranog elektronskog potpisivanja elektronskog 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 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 UIO objavljuje podatke i svu dokumentaciju koja se odnosi na izdavanje elektronskih 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.

Ovjerilac UIO objavljuje na svojoj zvaničnoj *Web* stranici:

- Politiku ovjeravanja Ovjerioca UIO,
- Praktična pravila pružanja usluge ovjeravanja Ovjerioca UIO,
- Prethodne verzije Politike ovjeravanja Ovjerioca UIO i Praktičnih pravila pružanja usluge ovjeravanja Ovjerioca UIO,
- Obrazac ugovora o obavljanju usluga ovjeravanja,
- Obrazac zahtjeva za izdavanje i korištenje elektronske potvrde,
- Obrazac zahtjeva za promjenu statusa potvrde,
- Definicije važećih profila potvrda Ovjerioca UIO usklađenih sa eIDAS uredbom Evropske unije,
- Korisnička uputstva,
- Potvrde ovjerioca *UINO Root CA* i podređenih ovjerilaca (*UINO Issuing CA1* i *UINO Issuing CA2*) sa pridruženim *hash* vrijednostima,
- Registre opozvanih potvrda (*CRL* – eng. *Certificate Revocation List*) ovjerioca *UINO Root CA*, *UINO Issuing CA1* i *UINO Issuing CA2*,
- 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 UIO identifikuje korisnika na osnovu identifikacionog dokumenata koje korisnik podnosi (važeća lična karta, pasoš ili drugi). Korisnik mora lično da podnese cjelokupnu dokumentaciju.

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

Ovjerilac UIO garantira jedinstvenost imena u svojoj domeni. Ovjerilac UIO 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 UIO nije obavezan da verificira da li je korištenje takvih imena zakonito. Korisnik snosi odgovornost za to da osigura zakonito korištenje odabranog imena.

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. Fizičko lice može da bude zaposleno u pravnom licu. Kvalificirana potvrda za elektronski pečat može se izdati samo pravnom licu.

Ukoliko Ovjerilac UIO 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, odnosno porezni identifikacioni broj.

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 priloži ovjerenu fotokopiju identifikacionog dokumenta,
- 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 UIO 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 pet godina i vezuje se za dan izdavanja potvrde.

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

Izdavanje elektronske potvrde vrši se na sljedeći način:

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

Prvom upotrebom elektronske potvrde od strane korisnika, potvrda se smatra prihvaćenom.

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

Ovjerilac UIO 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 UIO je dužan da opozove elektronsku potvrdu iz sljedećih razloga:

- U slučaju da neka informacija sadržana u potvrdi postane netačna,
- Promjene podataka u potvrdi, koje zahtjevaju 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,
- U slučaju prestanka odnosa između potpisnika i poslovnog subjekta,
- Neispunjavanja obaveza korisnika potvrde određenih ovim Praktičnim pravilima i ugovorom,
- Ukoliko opoziv elektronske potvrde zahtjeva korisnik 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 obavljanju usluge ovjeravanja od strane korisnika,
- 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 UIO,
- 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.

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

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

U slučaju da prije redovne objave dođe do opoziva ili suspenzije elektronske potvrde, Ovjerilac UIO 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 UIO.

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.

Ovjerilac UIO 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 UIO 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 UIO se nalazi u sigurnoj prostoriji koja je osigurana dvorazinskom elektronskom bravom u zgradi glavnog ureda UIO. Kontrola fizičkog pristupa Ovjeriocu UIO 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 UIO,
- 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 Grupa za održavanje sistema PKI UIO utvrdi da zahtijevaju hitnu intervenciju,
- Svaki pristup zaštićenoj prostoriji evidentira se unutar elektronske evidencije.

Ovjerilac UIO osigurava da je pristup sistemu ovjeravanja ograničen isključivo na ovlaštene zaposlene.

Prostorije u kojima se nalazi infrastruktura Ovjerioca UIO u glavnom uredu UIO su opremljene:

- Sistemom za neprekidni izvor napajanja 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 UIO.

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

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

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

Ovjerilac UIO 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 UIO 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 UIO, istom će biti onemogućen daljnji pristup tehničkim sredstvima (hardveru i softveru) Ovjerioca UIO, a Ovjerilac UIO će suspendirati ili opozvati sve važeće elektronske potvrde koje su izdate tom licu.

Izvršene neautorizirane aktivnosti prijavljuju se nadležnim organizacijskim jedinicama UIO, 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 UIO će u slučaju kompromitiranja privatnog kriptografskog ključa aplikacije ovjerioca odmah:

- Opozvati izdane elektronske potvrde,
- Opozvati potvrdu aplikacije ovjerioca,
- Objaviti registar opozvanih potvrda,
- Obavijestiti korisnike izdanih elektronskih potvrda.

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

Ovjerilac UIO 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 UIO 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 UIO, 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 *SSCD* uređaju, koji predstavlja sredstvo za formiranje kvalificiranog elektronskog potpisa.

Dužine kriptografskih ključeva za koje Ovjerilac UIO izdaje elektronske potvrde su:

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

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

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

Ovjerilac UIO ima implementiranu višestruku autorizaciju za pristup privatnom kriptografskom ključu aplikacija ovjerioca *UINO Root CA, UINO Issuing CA1* i *UINO Issuing CA2* Ovjerioca UIO.

Ovjerilac UIO 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 UIO su:

- Potvrde aplikacije ovjerioca: dvadeset (20) godina,
- Kvalificirane elektronske potvrde korisnika: pet (5) godina,
- Potvrda za potpis odgovora *OCSP* servisa: jedna (1) godina,
- Kvalificirana potvrda za elektronski pečat: pet (5) godina,
- Potvrda za autentikaciju *Web* stranica za pravna lica: 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 elektronske potvrde je odgovoran za čuvanje lozinke svog *SSCD* uređaja.

Na sistemu Ovjerioca UIO implementirane su tehničko-sigurnosne kontrole i mehanizmi, i to:

- Kontrola pristupa do sistemskih servisa aplikacije Ovjerioca UIO,
- Kontrola pristupa funkcijama aplikacije Ovjerioca UIO,
- Stroga podjela uloga između ovlaštenih lica Ovjerioca UIO,
- Upotreba kriptografskih modula za smještanje kriptografskih ključeva ovlaštenih lica Ovjerioca UIO,
- Sigurno arhiviranje podataka aplikacije Ovjerioca UIO 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 UIO.

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

Računarsku mrežu Ovjerioca UIO 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 UIO i za pristup servisima Ovjerioca UIO.

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, REGISTRA OPOZVANIH POTVRDA I OCSP PROFILI

Ovjerilac UIO izdaje potvrde sukladne specifikaciji *X.509* verzije 3.

Dokument s opisom profila potvrda Ovjerioca UIO dostupan je na *Web* stranici Ovjerioca UIO pod nazivom „UIO 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)*.

Ovjerilac UIO 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 UIO OVJERIOCA I DRUGE PROCJENE

Ovjerilac UIO 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 UIO 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.

Šef Odsjeka za elektronske potpise i certifikate u Sektoru za informacione tehnologije UIO odgovoran je za provođenje unutarnjih revizija i određivanje lica koja ih provode.

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

- Tehnologije infrastrukture javnih kriptografskih ključeva,
- Vršenja 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 UIO i ne objavljuje se javno. Namijenjen je isključivo ovlaštenim licima Ovjerioca UIO za potrebe otklanjanja eventualno pronađenih nedostataka.

9. OSTALI POSLOVI I PRAVNA PITANJA

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

Ovjerilac UIO snosi finansijsku odgovornost za obavljanje svoje djelatnosti u skladu sa važećim zakonskim propisima.

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

Sva prava intelektualne svojine Ovjerioca UIO, uključujući zaštitne znake i autorska prava, ostaju isključivo vlasništvo Ovjerioca UIO.

Ovjerilac UIO garantira pružanje usluge ovjeravanja, u skladu sa zakonom, drugim propisima, Praktičnim pravilima i drugim aktima Uprave za indirektno oporezivanje koji su usklađeni s važećim propisima Bosne i Hercegovine.

Ovjerilac UIO 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 UIO.

Ovjerilac UIO 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.

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

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

Ovjerilac UIO 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 UIO i korisnika.

U slučaju prestanka rada, Ovjerilac UIO 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 smart kartice. Smart kartica 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 UIO i korisnika kvalifikovane elektronske potvrde, odnosno trećih lica u vezi međusobnih prava i obaveza i tumačenja ugovora i ovih Praktičnih pravila, UIO će nastojati da spor riješi mirnim putem, sporazumno, a ukoliko do sporazuma ne dođe, spor će rješavati nadležni sud u Banjoj Luci.

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

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

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

Direktor
Uprave za indirektno oporezivanje

_____

dr. Miro Džakula