UPRAVA ZA INDIREKTNO OPOREZIVANJE
Bana Lazarevića bb, Banja Luka

PRAKTIČNA PRAVILA PRUŽANJA USLUGE OVJERAVANJA OVJERIOCA UPRAVE ZA INDIREKTNO OPOREZIVANJE

(*Certification Practices Statement - CPS*)

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

PRAKTIČNA PRAVILA PRUŽANJA USLUGE 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*).

Praktična pravila pružanja usluge ovjeravanja Ovjerioca Uprave za indirektno oporezivanje (u daljnjem tekstu: Praktična pravila), predstavljaju javni dokument koji definira proces pružanja usluge ovjeravanja i način njihovog korištenja pri izdavanju i upravljanju životnim ciklusom elektronskih potvrda i elektronskih pečata, operativne procedure u cilju ispunjenja postavljenih zahtjeva i način na koji Ovjerilac UIO ispunjava tehničke, organizacione i proceduralne zahtjeve poslovanja koji su identificirani u Politici ovjeravanja, kao i upotrebu elektronske potvrde od strane korisnika.

Usluge povjerenja koje pruža Ovjerilac UIO jesu obim ovog dokumenta. Ovaj dokument opisuje kompletan životni ciklus kvalificiranih i nekvalificiranih elektronskih potvrda izdanih na sigurnim kriptografskim uređajima ili u vidu softverskih potvrda od strane Ovjerioca UIO. Politika ovjeravanja i Praktična pravila kao javni dokumenti objavljuju se na zvaničnoj *Web* stranici Ovjerioca UIO.

Osim ovih dokumenata, korisnicima i svim zainteresiranim licima, na zvaničnoj *Web* stranici Ovjerioca UIO dostupni su:

- Obrasci ugovora o izdavanju i korištenju kvalificiranih elektronskih potvrda,
- Obrasci ugovora o izdavanju i korištenju nekvalificiranih elektronskih potvrda,
- Obrasci zahtjeva za izdavanje i korištenje kvalificiranih elektronskih potvrda,
- Obrasci zahtjeva za izdavanje i korištenje nekvalificiranih elektronskih potvrda,
- Obrasci zahtjeva za promjenu statusa kvalificiranih elektronskih potvrda,
- Obrasci zahtjeva za promjenu statusa nekvalificiranih elektronskih potvrda,
- Korisnička uputstva,
- Ostali akti vezani za rad Ovjerioca UIO.

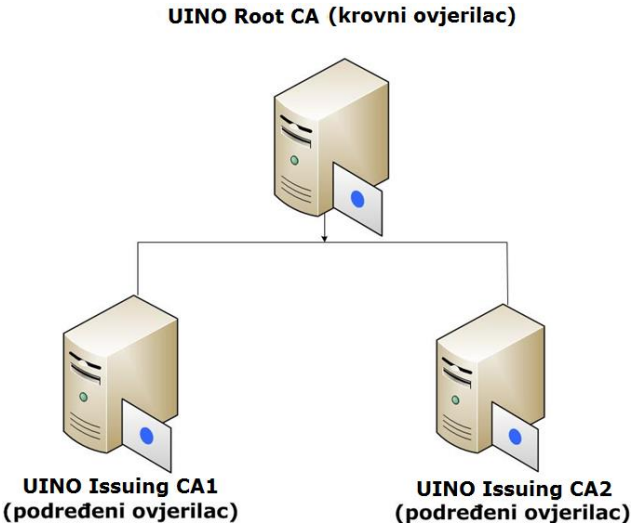
Ovjerilac UIO utvrđuje i Posebna interna pravila rada Ovjerioca UIO i zaštite sistema ovjeravanja (u daljnjem tekstu: Posebna pravila). Posebna pravila su interni dokumenti i predstavljaju poslovnu tajnu UIO.

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.

1.1. Pregled

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***“.



Slika 1. Hijerarhija Ovjerioca UIO

„*UINO Root CA*“ server radi kao krovni ovjerilac na osnovu potvrde izdate samom sebi (eng. *self-signed certificate*) u procesu generiranja privatnog kriptografskog ključa aplikacije ovjerioca (eng. *Root Key Generation Ceremony*). „*UINO Root CA*“ server izdaje potvrde njemu podređenim ovjeriocima *„UINO Issuing CA1“* i *„UINO Issuing CA2“* koji su dio infrastrukture Ovjerioca UIO, potvrdu za potpisivanje odgovora UIO OCSP servisa za provjeru statusa opozvanosti potvrda koje izdaje „*UINO Root CA*“, kao i administrativne potvrde u skladu sa ulogom koju zaposleni obavlja.

Za potrebe administriranja, „*UINO Root CA*“ server izdaje dvije potvrde *Security Officer*-ima i jednu potvrdu *Security Auditor*-u.

Serveri „*UINO Issuing CA1*“ i „*UINO Issuing CA2*“ izdaju potvrde krajnjim korisnicima.

„*UINO Issuing CA1*“ server kao podređeni ovjerilac (eng. *subordinate*) izdaje kvalificirane i nekvalificirane elektronske potvrde fizičkim licima i fizičkim licima povezanim sa pravnim licima u svrhu izrade kvalificiranog elektronskog potpisa i pečata, nekvalificiranog elektronskog potpisa, autentikaciju, autentikaciju *Web* stranica (*TLS*/*SSL* potvrde, potvrde za servere), kao i administrativne potvrde u skladu sa ulogom koju zaposleni obavlja. Pored ovoga, server izdaje potvrdu za potpis odgovora *OCSP* servisa za „*UINO Issuing CA1*“ i potvrdu servisu za izdavanje kvalificiranih vremenskih žigova.

„*UINO Issuing CA2*“ server kao podređeni ovjerilac (eng. *subordinate*) izdaje kvalificirane elektronske potvrde za zaposlene UIO u svrhu izrade elektronskog potpisa i autentikaciju, domensku autentikaciju, autentikaciju *Web* stranica, kao i administrativne potvrde u skladu sa ulogom koju zaposleni obavlja. Pored ovoga izdaje se potvrda internom servisu za izdavanje vremenskih žigova, potvrda za potpisivanje fajlova informacionih sistema UIO i potvrda za potpis odgovora *OCSP* servisa za „*UINO Issuing CA2*“.

Za potrebe administriranja „*UINO Issuing CA1*“ i „*UINO Issuing CA2*“ servera izdaju se po dvije potvrde *Security Officer*-ima i jedna potvrda *Security Auditor*-u.

Funkcioniranje hijerarhijske infrastrukture u potpunosti je u skladu sa Politikom ovjeravanja i Praktičnim pravilima koja su obavezujuća za Ovjerioca UIO, lica kojima je Ovjerilac UIO izdao elektronsku potvrdu i treća lica koja se pouzdaju u potvrdu izdanu od strane Ovjerioca

UIO. Korisnici kvalificiranih elektronskih potvrda Ovjerioca UIO, posjeduju jedan par kriptografskih ključeva (javni i privatni ključ). Privatni kriptografski ključ koristi se za kvalificirano elektronsko potpisivanje, a javni kriptografski ključ koristi se za verificiranje kvalificiranog elektronskog potpisa.

1.1.1. Profili potvrda Ovjerioca UIO

1.1.1.1. Tipovi potvrda koje izdaje ovjerilac „UINO Root CA“

POPIS TIPOVA POTVRDA KOJE IZDAJE UINO ROOT CA	
NAZIV TIPA POTVRDE	**PODRUČJE PRIMJENE POTVRDE**
POTVRDA UIO KORIJENSKOG OVJERIOCA (UINO ROOT CA)	IZDAVANJE CA POTVRDA PODREĐENIM OVJERIOCIMA, IZDAVANJE CRL I IZDAVANJE POTVRDE ZA UIO OCSP SERVIS
POTVRDA PRVOG UIO PODREĐENOG OVJERIOCA (UINO ISSUING CA1)	IZDAVANJE KORISNIČKIH POTVRDA ZA FIZIČKA LICA I FIZIČKA LICA POVEZANA SA PRAVNIM LICIMA, POTPISIVANJE PRIPADAJUĆIH CRL, POTVRDE ZA UIO SERVIS IZDAVANJA KVALIFICIRANIH VREMENSKIH ŽIGOVA, POTVRDA ZA UIO OCSP SERVIS
	OID POLITIKE OVJERAVANJA: 1.3.6.1.4.1.46134.10.1.2
POTVRDA DRUGOG UIO PODREĐENOG OVJERIOCA (UINO ISSUING CA2)	IZDAVANJE KORISNIČKIH POTVRDA ZA ZAPOSLENE UIO, POTPISIVANJE PRIPADAJUĆIH CRL, POTVRDE ZA UIO SERVIS IZDAVANJA VREMENSKIH ŽIGOVA, POTVRDA ZA UIO OCSP SERVIS
	OID POLITIKE OVJERAVANJA: 1.3.6.1.4.1.46134.10.1.2
POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA	POTVRDA ZA POTPIS ODGOVORA OCSP SERVISA ZA UINO ROOT CA
	OID POLITIKE OVJERAVANJA: 1.3.6.1.4.1.46134.10.2.0.16.1.1

Tabela 1. Tipovi potvrda koje izdaje ovjerilac *UINO Root CA*

1.1.1.2. Tipovi potvrda koje izdaje ovjerilac UINO Issuing CA1

POPIS TIPOVA POTVRDA KOJI IZDAJE UINO ISSUING CA1		
NAZIV GRUPE	**NAZIV TIPA POTVRDE**	**PODRUČJE PRIMJENE POTVRDE**
POTVRDE ZA FIZIČKA LICA	UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA FIZIČKA LICA (QCP-n-qscd)	IZDAJE SE FIZIČKIM LICIMA ZA IZRADU KVALIFICIRANOG ELEKTRONSKOG POTPISA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.10.1.1
	UIO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU FIZIČKIH LICA(NCP+)	IZDAJE SE FIZIČKIM LICIMA I KORISTI ZA JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.10.2.1
	UIO NEKVALIFICIRANA POTVRDA ZA FIZIČKA LICA ZA ELEKTRONSKI POTPIS I AUTENTIKACIJU (NCP+)	IZDAJE SE FIZIČKIM LICIMA I KORISTI ZA IZRADU ELEKTRONSKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.10.3.1
	UIO POTVRDA ZA ELEKTRONSKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKCS#12 FORMATA (NCP)	IZDAJE SE FIZIČKIM LICIMA ZA IZRADU ELEKTRONSKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.10.4.0
POTVRDE ZA FIZIČKA LICA	UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA FIZIČKE	IZDAJE SE FIZIČKIM LICIMA POVEZANIM S POSLOVNIM SUBJEKTOM

POVEZANE S PRAVNIM LICIMA	LICA POVEZANA SA PRAVNIM LICIMA (QCP-n-qscd)	ZA IZRADU KVALIFICIRANOG ELEKTRONSKOG POTPISA U POSLOVNE SVRHE.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.11.1.1
	UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA STRANCE POVEZANE SA PRAVNIM LICIMA (QCP-n-qscd)	IZDAJE SE STRANCIMA POVEZANIM S POSLOVNIM SUBJEKTOM ZA IZRADU KVALIFICIRANOG ELEKTRONSKOG POTPISA U POSLOVNE SVRHE.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.11.2.1
	UIO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU FIZIČKIH LICA POVEZANIH SA PRAVNIM LICIMA(NCP+)	IZDAJE SE FIZIČKIM LICIMA POVEZANIM S POSLOVNIM SUBJEKTOM ZA JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA U POSLOVNE SVRHE.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.11.3.1
	UIO NEKVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS I AUTENTIKACIJU ZA FIZIČKA LICA POVEZANA SA PRAVNIM LICIMA (NCP+)	IZDAJE SE FIZIČKIM LICIMA POVEZANIM SA POSLOVNIM SUBJEKTOM ZA IZRADU ELEKTRONSKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA U POSLOVNE SVRHE.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.11.4.1
	UIO POTVRDA ZA ELEKTRONSKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKSC#12 FORMATA ZA FIZIČKA LICA POVEZANA SA PRAVNIM LICIMA (NCP)	IZDAJE SE FIZIČKIM LICIMA POVEZANIM S POSLOVNIM SUBJEKTOM. KORISTI SE ZA POTREBE ELEKTRONSKOG POTPISIVANJA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.11.5.0
POTVRDA ZA ELEKTRONSKI PEČAT	UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI PEČAT (QCP-l-qscd)	IZDAJE SE PRAVNIM LICIMA ZA IZRADU KVALIFICIRANOG ELEKTRONSKOG PEČATA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.12.1.1
POTVRDA ZA AUTENTIKACIJU WEB STRANICA ZA PRAVNA LICA	POTVRDA ZA AUTENTIKACIJU WEB STRANICA (SSL) ZA PRAVNA LICA	IZDAJE SE PRAVNIM LICIMA ZA AUTENTIKACIJU WEB STRANICA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.13.1.0
POTVRDA ZA IT OPREMU ZA PRAVNA LICA	APLIKATIVNA POTVRDA ZA ELEKTRONSKO POTPISIVANJE ZA PRAVNA LICA (NCP)	IZDAJE SE APLIKACIJAMA I INFORMACIONIM SISTEMIMA PRAVNIH LICA ZA IZRADU ELEKTRONSKOG POTPISA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.14.1.0
POTVRDA ZA VREMENSKI ŽIG	UIO KVALIFICIRANA POTVRDA ZA VREMENSKI ŽIG	IZDAJE SE SERVISU ZA IZDAVANJE KVALIFICIRANIH VREMENSKIH ŽIGOVA I KORISTI ZA POTPISIVANJE KVALIFICIRANIH VREMENSKIH ŽIGOVA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.15.1.1
POTVRDA ZA OCSP SERVIS	UIO POTVRDA ZA OCSP SERVIS UINO ISSUING CA1	IZDAJE SE OCSP SERVISU ZA POTPIS OCSP ODGOVORA CA TIJELA UINO ISSUING CA1.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.1.16.1.1

Tabela 2. Tipovi potvrda koje izdaje ovjerilac *UINO Issuing CA1*

1.1.1.3. Tipovi potvrda koje izdaje ovjerilac UINO Issuing CA2

POPIS TIPOVA POTVRDA KOJE IZDAJE UINO ISSUING CA2		
NAZIV GRUPE	**NAZIV TIPA POTVRDE**	**PODRUČJE PRIMJENE POTVRDE**
POTVRDE ZA ZAPOSLENE	UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA ZAPOSLENE (QCP-n-qscd)	IZDAJE SE ZAPOSLENIMA ZA IZRADU KVALIFICIRANOG ELEKTRONSKOG POTPISA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.11.1.1
	UIO NEKVALIFICIRANA POTVRDA ZA AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	IZDAJE SE ZAPOSLENIMA ZA JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.11.2.1
	UIO NEKVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS I AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	IZDAJE SE ZAPOSLENIMA ZA IZRADU ELEKTRONSKOG POTPISA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.11.3.1
	UIO NEKVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS I DOMENSKU AUTENTIKACIJU ZA ZAPOSLENE (NCP+)	IZDAJE SE ZAPOSLENIMA ZA IZRADU ELEKTRONSKOG POTPISA I DOMENSKU AUTENTIKACIJU.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.11.4.1
	UIO POTVRDA ZA ELEKTRONSKO POTPISIVANJE I AUTENTIKACIJU U OBLIKU DATOTEKE PKSC#12 FORMATA (NCP) ZA ZAPOSLENE (NCP)	IZDAJE SE ZAPOSLENIMA, A KORISTI SE ZA POTREBE ELEKTRONSKOG POTPISIVANJA, JAKU AUTENTIKACIJU I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.11.5.0
POTVRDE ZA AUTENTIKACIJU WEB STRANICA I DRUGIH SERVISA	POTVRDA ZA AUTENTIKACIJU WEB STRANICA (SSL)	IZDAJE SE ZAPOSLENIMA-ADMINISTRATORIMA SERVERA ZA AUTENTIKACIJU WEB STRANICA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.13.1.0
	KERBEROS POTVRDA ZA DOMEN KONTROLER (DOMEN KONTROLER KDC)	IZDAJE SE ZAPOSLENIMA-ADMINISTRATORIMA ACTIVE DIRECTORY DOMENA ZA AUTENTIKACIJU DOMEN KONTROLERA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.13.10.0
POTVRDA ZA IT OPREMU	UIO APLIKATIVNA POTVRDA ZA AUTENTIKACIJU U OBLIKU DATOTEKE PKCS#12 FORMATA (NCP)	IZDAJE SE SOFTVERSKIM MODULIMA INFORMACIONOG SISTEMA UIO I KORISTI ZA NJIHOVU AUTENTIKACIJU DRUGIM MODULIMA I INFORMACIONIM SISTEMIMA UIO I ENKRIPCIJU KLJUČA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.14.1.0
POTVRDA ZA VREMENSKI ŽIG	POTVRDA ZA VREMENSKI ŽIG	IZDAJE SE INTERNOM SERVISU ZA IZDAVANJE VREMENSKIH ŽIGOVA I KORISTI ZA POTPISIVANJE VREMENSKIH ŽIGOVA.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.15.1.1

POTVRDA ZA OCSP SERVIS	UINO POTVRDA ZA OCSP SERVIS UINO ISSUING CA2	IZDAJE SE OCSP SERVISU ZA POTPIS OCSP ODGOVORA CA TIJELA UINO ISSUING CA2.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.16.1.1
POTVRDA ZA POTPISIVANJE KODA	POTVRDA ZA POTPISIVANJE KODA (NCP+)	IZDAJE SE ZAPOSLENIMA ZA POTPISIVANJE FAJLOVA INFORMACIONIH SISTEMA UIO.
	OID POLITIKE OVJERAVANJA	1.3.6.1.4.1.46134.10.2.2.17.1.1

Tabela 3. Tipovi potvrda koje izdaje ovjerilac *UINO Issuing CA2*

1.1.1.4. Osnovni podaci o CA potvrdama UIO Ovjerioca

1.1.1.4.1. Osnovni podaci o potvrdi UINO Root CA

UIO POTVRDA KORIJENSKOG OVJERIOCA - UINO ROOT CA		
OSNOVNA POLJA		
POLJE	**ATRIBUT**	**VRIJEDNOST**
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 20 godina
Subject	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
SHA-1 thumbprint: 30c40b7dfb76c4dccf4d2d77e21d984e11fd43ea		
SHA 256 thumbprint: c676695d64b5b5f7b3308a7ee41ba17fcaceff6baddbe27a5f9588ed75b1cb67		

Tabela 4. Osnovni podaci o potvrdi *UINO Root CA*

1.1.1.4.2. Osnovni podaci o potvrdi UINO Issuing CA1

UIO POTVRDA PRVOG PODREĐENOG OVJERIOCA-UINO ISSUING CA1		
OSNOVNA POLJA		
POLJE	**ATRIBUT**	**VRIJEDNOST**
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde

	notAfter	Vrijeme izdavanja potvrde + 20 godina
Subject	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
SHA-1 thumbprint: 44f227af9af01c3c119b35f49ad186076c1fc44a		
SHA 256 thumbprint: a6f1dd9fdb403dd08da4c0cfcb3d7e4837a749b4ceee26e7ac0967bb6fb0ce44		

Tabela 5. Osnovni podaci o potvrdi *UINO Issuing CA1*

1.1.1.4.3. Osnovni podaci o potvrdi UINO Issuing CA2

UIO POTVRDA DRUGOG PODREĐENOG OVJERIOCA – UINO ISSUING CA2		
OSNOVNA POLJA		
POLJE	**ATRIBUT**	**VRIJEDNOST**
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Vrijeme izdavanja potvrde
	notAfter	Vrijeme izdavanja potvrde + 20 godina
Subject	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
SHA-1 thumbprint: 7a5de606842c8068dfe5cf2224267493c84af0f6		
SHA 256 thumbprint: b2e7486187ae3611e88263eec309af19730b237e2b5dcc06a358164c2e0494f2		

Tabela 6. Osnovni podaci o potvrdi *UINO Issuing CA2*

1.2. Naziv i identifikacija dokumenta

Ovaj dokument nosi naziv **„PRAKTIČNA PRAVILA PRUŽANJA USLUGE OVJERAVANJA OVJERIOCA UPRAVE ZA INDIREKTNO OPOREZIVANJE“**, kao što je to označeno na početnoj strani dokumenta.

Organizacija *IANA* (*Internet Assigned Numbers Authority*) dodijelila je Upravi za indirektno oporezivanje *OID* 1.3.6.1.4.1.46134. Uprava za indirektno oporezivanje je na osnovu tog *OID*-a dodijelila Ovjeriocu UIO *OID* 1.3.6.1.4.1.46134.10. Identifikacioni broj ovog dokumenta (*OID*) je 1.3.6.1.4.1.46134.10.1.2.1.0.

OID	OBJAŠNJENJE
1.3.6.1.4.1.46134	Jedinstveni identifikacioni broj dodijeljen Upravi za indirektno oporezivanje od strane organizacije IANA
1.3.6.1.4.1.46134.10	Jedinstveni identifikacioni broj Ovjerioca UIO dodijeljen od strane UIO
1.3.6.1.4.1.46134.10.1	Jedinstveni identifikacioni broj dodijeljen za dokumente Ovjerioca UIO
1.3.6.1.4.1.46134.10.2	Jedinstveni identifikacioni broj dodijeljen za potvrde Ovjerioca UIO

Tabela 7. Jedinstveni identifikacioni brojevi Ovjerioca UIO

DOKUMENTI	VRSTA DOKUMENTA	VERZIJA	PODVERZIJA
1.3.6.1.4.1.46134.10.1	1 za CP	1 za početnu verziju	0 za početnu podverziju
	2 za CPS	1 za početnu verziju	0 za početnu podverziju

Tabela 8. Struktura jedinstvenih identifikacionih brojeva dokumenata Ovjerioca UIO

NEPROMJENJIVI DIO *OID*-A POLITIKE OVJERAVANJA	OVJERILAC POTVRDE	SKUPINA PROFILA POTVRDE	PROFIL POTVRDE	NAČIN ČUVANJA PRIVATNOG KLJUČA
1.3.6.1.4.1.46134.10.2	0 – *UINO Root CA* 1 – *UINO Issuing CA1* 2 – *UINO Issuing CA2*	Skupine potvrda su definirane prema namjeni potvrda i njihovim korisnicima. Oznake skupina potvrda su sljedeće:	Oznaka profila potvrde unutar skupine potvrda. Vrijednost oznake profila potvrde počinje od broja 1.	Način čuvanja privatnog ključa odgovara na pitanje da li se privatni ključ čuva na kriptografskom uređaju. Moguće vrijednosti su sljedeće:
		10 – potvrde za fizička lica 11 – potvrde za fizička lica povezana s pravnim licima 12 – potvrde za		0 – privatni ključ povezan sa potvrdom se ne čuva u kriptografskom uređaju 1 – privatni ključ povezan sa potvrdom se čuva u

		elektronski pečat 13 – potvrde za autentikaciju *Web* stranica i drugih servisa 14 – potvrde za IT opremu 15 – potvrde za vremenski žig 16 – potvrde za OCSP servis 17 – potvrde za potpisivanje koda		kriptografskom uređaju

Tabela 9. Struktura jedinstvenih identifikacionih brojeva potvrda Ovjerioca UIO

1.3. Učesnici *PKI* sistema

Učesnici PKI sistema su:

- Ovjerilac UIO,
- Korisnici usluga,
- Treća lica,
- Ostali učesnici.

1.3.1. Ovjerilac UIO

U Odsjeku za elektronske potpise i certifikate Sektora za informacione tehnologije postoje sljedeće jedinice:

- Grupa za održavanje sistema PKI UIO – *CA*,
- Grupa za podršku korisnicima sistema PKI UIO – *RA*.

1.3.1.1. Odsjek za elektronske potpise i certifikate
Grupa za održavanje sistema PKI UIO – CA (eng. *Certification Authority*)

Ova organizaciona jedinica u okviru Ovjerioca UIO odgovorna je za ispravno funkcioniranje opreme i programa, a koji su u vezi s izdavanjem elektronskih potvrda. Također ova jednica je zadužena i za kreiranje, potpisivanje i izdavanje potvrda, upravljanje životnim vijekom potvrda, završno s opozivom potvrde. Organizaciona jedinica radi u skladu sa Praktičnim

pravilima, pri čemu su poslovni procesi načelno opisani u Praktičnim pravilima, a detaljno propisani internim pravilnicima Ovjerioca UIO.

Serverska infrastruktura *CA* obuhvata:

- ***UINO Root CA*** server, kao korijenski ovjerilac, samopotpisani krovni ovjerilac,
- ***UINO Issuing CA1*** server, kao prvi podređeni ovjerilac,
- ***UINO Issuing CA2*** server, kao drugi podređeni ovjerilac.

1.3.1.2. Odsjek za elektronske potpise i certifikate Grupa za podršku korisnicima sistema PKI UIO – RA (eng. *Registration Authority*)

Ova organizaciona jedinica u okviru Ovjerioca UIO izrađuje pravila vršenja usluga ovjeravanja, pripadajuću dokumentaciju i procedure.

Zaposleni u Grupi za podršku korisnicima sistema PKI UIO koji rade u regionalnim centrima Uprave za indirektno oporezivanje ovlašteni su za zaprimanje zahtjeva, provjeravanje identiteta korisnika i za unošenje zahtjeva za izdavanje elektronskih potvrda i zahtjeva za promjenu statusa potvrda u aplikaciji Registracijskog tijela Ovjerioca UIO.

1.3.2. Korisnici

Korisnici usluga UIO Ovjerioca su:

- Fizičko lice, koje se identifikuje specifičnim atributima,
- Fizičko lice koje je zaposleno u pravnom licu,
- Pravno lice,
- Zaposleni UIO.

Ukoliko Ovjerilac UIO izdaje elektronsku potvrdu fizičkom licu koje je zaposleno u pravnom licu, u okviru atributa koji identificiraju korisnika nalaze se i podaci koji označavaju naziv pravnog lica.

1.3.2.1. Subjekti ovjeravanja

Subjekt ovjeravanja je u potvrdi identificiran kao Subjekt te je nosilac privatnog ključa koji je povezan s javnim ključem sadržanim u potvrdi.

Subjekti ovjeravanja u potvrdama koje izdaju podređeni Ovjerioci UIO:

- U ličnim potvrdama za elektronski potpis je fizičko lice,
- U poslovnim potvrdama za elektronski potpis je fizičko lice koje je povezano sa pravnim licem,
- U kvalificiranim potvrdama za e-pečat je pravno lice,

- U potvrdama za autentikaciju *Web* stranica je server koji je identificiran nazivom domene i kojim upravlja pravno lice.

1.3.3. Treća lica

Treća lica su lica koja se pouzdaju u elektronske potvrde izdane od Ovjerioca UIO, u cilju verificiranja elektronskog potpisa i provjere identiteta korisnika.

Treća lica mogu provjeriti status opozvanosti elektronskih potvrda putem registra opozvanih potvrda – *CRL* (eng. *Certificate Revocation List*) ili preko *OCSP* (eng. *Online Certificate Status Protocol)* servisa Uprave za indirektno oporezivanje, koji se svaki dan ažuriraju.
Treća lica provjeravaju najnovije raspoložive registre opozvanih potvrda da bi imale kompletnu i pravovremenu informaciju o opozivu i suspenziji potvrda.

Ni pod kojim uvjetima se ne treba oslanjati na registar opozvanih potvrda duže od maksimalnog roka važenja registra opozvanih potvrda.

1.3.4. Ostali učesnici

Ostali učesnici su pravna lica koja, na neki način, doprinose ili učestvuju u osiguravanju kvaliteta rada Ovjerioca UIO i davanja usluga ovjeravanja. U ovu grupu spadaju proizvođači i distributeri opreme i softvera, proizvođači i distributeri smart kartica, osiguravajuće društvo, i drugi učesnici.

1.4. Upotreba potvrda

1.4.1. Područje primjene

UINO Root CA potvrda koristi se za:

- Izdavanje potvrda njemu podređenih ovjerilaca (*UINO Issuing CA1* i *UINO Issuing CA2*),
- Izdavanje registra opozvanih potvrda (*CRL*),
- Izdavanje potvrde za UIO *OCSP* servis sa kojom ovaj *OCSP* servis potpisuje odgovore za status potvrda njemu podređenih ovjerilaca i ostalih potvrda koje izdaje ovjerilac *UINO Root CA*.

Potvrde podređenih ovjerilaca *UINO Issuing CA*1 i *UINO Issuing CA2* se koriste za:

- Izdavanje korisničkih potvrda,
- Izdavanje registra opozvanih potvrda (*CRL*),
- Izdavanje potvrda za UIO servis izdavanja kvalificiranih elektronskih žigova,
- Izdavanje potvrda za UIO *OCSP* servis.

Područje primjene UIO potvrda izdanih od strane ovjerilaca *UINO Issuing CA1* i *UINO Issuing CA2*:

- Izrada elektronskog potpisa i kvalificiranog elektronskog potpisa,
- Izrada kvalificiranog elektronskog pečata,
- Autentikaciju korisnika i enkripcija ključa,
- Autentikaciju *Web* stranica, tj. za autentikaciju *Web* servera kojima se pristupa putem *TLS* ili *SSL* protokola,
- Izrada elektronskog potpisa od strane aplikacije informacionog sistema,
- Potpis odgovora *OCSP* servisa ovjerilaca,
- Potpisivanje kvalificiranih vremenskih žigova od strane servisa za izdavanje kvalificiranih vremenskih žigova,
- Domensku autentikaciju zaposlenih,
- Autentikaciju domen kontrolera,
- Potpisivanje fajlova informacionog sistema UIO.

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.

1.4.2. Nedozvoljene primjene

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.

1.5. Politika administriranja dokumenta

1.5.1. Organizacija upravljanja dokumentom

Dokument Praktična kreira i ažurira Ovjerilac UIO:

Adresa:

Uprava za indirektno oporezivanje
Bana Lazarevića bb
78000 Banja Luka

Kontakt:

Telefon: +387 51 335 100
Faks: +387 51 335 347
E-mail: pki.administrator@uino.gov.ba
Web: **http://ca.uino.gov.ba**

Tekuću verziju i prethodne verzije dokumenta moguće je preuzeti sa *Web* stranice Ovjerioca UIO **http://ca.uino.gov.ba,** u dijelu *Dokumentacija*.

1.5.2. Lica za kontakt

Lica za kontakt Ovjerioca UIO su šef Odsjeka za elektronske potpise i certifikate u Sektoru za informacione tehnologije UIO, zaposleni koji obavljaju poslove tehničke podrške i drugi zaposleni ovlašteni za davanje informacija u vezi primjene Praktičnih pravila i drugih akata Ovjerioca UIO.

Kontakt adrese lica iz stava 1. ove tačke su objavljene na zvaničnoj *Web* stranici Ovjerioca UIO.

1.5.3. Lica određena za usklađivanje dokumenta sa praksom izdavanja potvrda

Odsjek za elektronske potpise i certifikate Sektora za informacione tehnologije UIO usklađuje formu i sadržaj ovih Praktičnih pravila sa eventualnim promjenama nastalim u praksi izdavanja elektronskih potvrda.

Također, Odsjek za elektronske potpise i certifikate Sektora za informacione tehnologije UIO redovno procjenjuje usklađenost ovih Praktičnih pravila s važećim zakonima.

1.5.4. Procedure za odobrenje Praktičnih pravila

Nakon izmjene zakonske regulative, poslovnog procesa vezanog za izdavanje kvalificiranih potvrda ili drugih izmjena koje utiču na postupke iz obima dokumenta Praktična pravila, Odsjek za elektronske potpise i certifikate Sektora za informacione tehnologije UIO provodi reviziju ovog dokumenta i vrši njegovo usklađivanje. Nakon provedenog procesa usklađivanja šef Odsjeka za elektronske potpise i certifikate odobrava novi dokument Praktična pravila.

Izmjene ili dopune Praktičnih pravila se moraju obaviti u skladu sa odredbama Zakona o elektronskom potpisu, podzakonskim aktima i praksom, te zato mogu biti predmet davanja odobrenja nadležnog državnog organa.

1.6. Definicije i skraćenice

DEFINICIJA	ZNAČENJE DEFINICIJE
Autentikacija	Elektronski postupak kojim se potvrđuje identitet lica ili izvornost i cjelovitost podataka.
Aplikacija Ovjerioca	Aplikacija na serverima Ovjerioca UIO koja generira i potpisuje elektronske potvrde i registre opozvanih potvrda pomoću kriptografskih ključeva generiranih i pohranjenih u hardverskom kriptografskom modulu.
Aplikacija Registracijskog tijela	*Web* aplikacija koja služi za registriranje korisnika Ovjerioca UIO i obradu njihovih zahtjeva za izdavanje potvrda kao i zahtjeva za promjenu statusa potvrda.
Aplikacija Centralnog sistema	*Web* aplikacija koja omogućava centralizirano praćenje i upravljanje životnim ciklusom kriptografskih uređaja, kreiranje naloga za izdavanje kriptografskih uređaja, izdavanje softverskih potvrda i potvrda za autentikaciju *Web* stranica.
Aktivacijski podaci	Tajni podaci koji se koriste za aktivaciju kriptografskih ključeva u hardverskom kriptografskom modulu ili pristup privatnim ključevima softverskih potvrda. Aktivacijski podatak može biti *PIN*, lozinka ili elektronski ključ.
Autor pečata	Pravno lice koje izrađuje elektronski pečat.
Desktop aplikacija za personaliziranje kriptografskih uređaja	Desktop aplikacija namijenjena vizuelnoj i elektronskoj personalizaciji kriptografskih uređaja, kreiranju šablona za vizuelno personaliziranje kriptografskog uređaja, kontrolu kvaliteta personaliziranih kriptografskih uređaja, te štampanju *PIN* i *PUK* kodova kriptografskog uređaja korisnika Ovjerioca UIO.
Dešifriranje	Kriptografski proces kojim se šifrirani podaci pretvaraju u razumljive podatke (otvoreni tekst), korištenjem ključa za dešifriranje i algoritma za dešifriranje.
Elektronski dnevnik	Elektronska forma zapisa o provedenim aktivnostima. Log datoteka.
Elektronski dokument	Dokument u elektronskom obliku koji se koristi u poslovnim i drugim radnjama.
Elektronski potpis	Skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani s drugim podacima u elektronskom obliku i koji služe za identifikaciju potpisnika i utvrđivanje vjerodostojnosti potpisanog elektronskog dokumenta. Elektronski potpis kreira fizičko lice.
Elektronski pečat	Skup podataka u elektronskom obliku koji su pridruženi ili su **logički** povezani s drugim podacima u elektronskom obliku ili su logički povezani s njima radi osiguranja izvornosti i cjelovitosti tih podataka. Elektronski pečat kreira pravno lice.
Elektronski vremenski žig	Skup podataka u elektronskom obliku koji povezuje točan datum i vrijeme kreiranja tog skupa podataka sa drugim podacima u

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

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

***Private Key*)**	uparenom javnom ključu. Koristi se za izradu elektronskog potpisa ili za dešifriranje podataka šifriranih odgovarajućim javnim ključem.
Privatni kriptografski ključ aplikacije ovjerioca	Privatni ključ ovjerioca, zajedno sa javnim ključem koji je sadržan u potvrdi ovjerioca predstavljaju par ključeva ovjerioca. Privatni ključ je generiran prilikom inicijalizacije aplikacije ovjerioca, a koristi se za potpisivanje izdanih elektronskih potvrda i registara opozvanih potvrda, što se radi pomoću *HSM*-a – hardverskog kriptografskog modula.
Povjerljive uloge	Uloge o kojima ovisi sigurnost rada pružatelja usluga povjerenja.
Potpisnik	Fizičko lice koje izrađuje elektronski potpis.
Registar opozvanih potvrda – CRL (eng. *Certificate Revocation List - CRL*)	Potpisana lista u koju se upisuju serijski brojevi i drugi podaci svih opozvanih potvrda koje je izdao ovjerilac.
Root CA	Ovjerilac najvišeg nivoa unutar domene pružaoca usluga povjerenja, potpisuje potvrde podređenih ovjerioca, vlastitu potvrdu, kao i administrativne potvrde.
Root potvrda ovjerioca – Root CA potvrda	Potvrda koju ovjerilac izdaje sam sebi (eng. *self-signed certificate*), tj. subjekt potvrde je ovjerilac. *Root CA* potvrda sadrži javni ključ i naziv ovjerioca koji je izdao potvrdu.
Reaktivacija potvrde	Radnja kojom se suspendirana potvrda čini ponovo valjanom.
Sigurno sredstvo za izradu elektronskog potpisa (eng. *Secure Signature Creation Device* – SSCD)	Sredstvo za izradu elektronskog potpisa koje osigurava: ▪ Da se podaci za izradu sigurnog elektronskog potpisa mogu pojaviti samo jednom, te da je ostvarena njihova sigurnost, ▪ Da se podaci za izradu sigurnog elektronskog potpisa ne mogu ponoviti, te da je potpis zaštićen od krivotvorenja pri korištenju postojeće raspoložive tehnologije, ▪ Da podatke za izradu sigurnog elektronskog potpisa korisnika može pouzdano zaštititi od neovlaštenog korištenja. Sredstvo za izradu sigurnog elektronskog potpisa ne smije pri izradi sigurnog elektronskog potpisa promijeniti podatke koji se potpisuju ili onemogućiti korisniku uvid u te podatke prije procesa izrade sigurnog elektronskog potpisa.
Sredstva za provjeru kvalificiranog elektronskog potpisa i pečata	Odgovarajuća tehnička sredstva (softver i hardver) koja služe za provjeru kvalificiranog elektronskog potpisa i pečata, uz korištenje podataka za provjeru elektronskog potpisa i pečata.
Suspenzija potvrde	Privremeni prestanak valjanosti potvrde prije isteka roka važenja navedenog u potvrdi.

Šifriranje	Proces u kriptografiji kojim se podaci mijenjaju tako da se informacije učine nerazumljivim za subjekte koji ne posjeduju odgovarajući ključ za dešifriranje. Upotrebom ključa za dešifriranje u postupku dešifriranja ove se informacije ponovo mogu učiniti razumljivim, tj. dovesti u oblik u kojem su postojale neposredno prije njihovog šifriranja.
Zaposleni	Lice u radnom odnosu sa Upravom za indirektno oporezivanje.
TSA sistem	Sistem za pružanje usluga izdavanja vremenskih žigova.
Validacija	Postupak potvrđivanja da su elektronski potpis ili pečat valjani.
Validacija potvrde	Postupak potvrđivanja da je potvrda valjana.
Validacija potpisa	Proces provjere kriptografske vrijednosti potpisa korištenjem podataka za verifikaciju potpisa.

Tabela 10. Definicije

Spisak skraćenica koje se pominju u dokumentu prikazan je u okviru tabele 11.

SKRAĆENICA	PUNI NAZIV	ZNAČENJE
AES	*Advanced Encryption Standard*	Algoritam simetrične kriptografije namijenjen za šifriranje
CA	*Certification Authority*	Ovjerilac
CP	*Certification Policy*	Politika ovjeravanja koja ukazuje na primjenjivost potvrda za određenu skupinu sa zahtjevima za sigurnost.
CPS	*Certification Practice Statement*	Praktična pravila pružanja usluge ovjeravanja u kome su pobrojani operativni postupci koje ovjerilac provodi prilikom izdavanja i upravljanja životnim vijekom potvrde.
CRL	*Certificate Revocation List*	Registar opozvanih potvrda.
CMS	*Certificate Managament System*	Sistem za upravljanje životnim vijekom potvrda koje ovjerilac izdaje.

DN	*Distinguished Name*	Jedinstveno ime subjekta upisano u potvrdu kojim se identificira subjekt kojem je izdana potvrda.
EAL	*Evaluation Assurance Level*	Testiran nivo sigurnosti prema standardu ISO/IEC 15408. Postoji sedam (7) razina i to od EAL1 do EAL7.
ETSI	*European Telecommunications Standards Institute*	Evropski institut za standarde iz oblasti telekomunikacija.
HSM	*Hardware Security Module*	Hardverski kriptografski modul za kriptografske operacije.
IETF	*Internet engineering task force*	Radna grupa za Internet inženjering
ISO	*International organization for standardization*	Međunarodna organizacija za standardizaciju
LDAP	*Lightweight Directory Access Protocol*	Protokol za pristup javnom direktorijumu
NIST	*National institute of standards and technology*	Nacionalni institut za standarde i tehnologiju
NTP	*Network Time Protocol*	Protokol mrežnog vremena
OCSP	*Online Certificate Status Protocol*	Protokol za on-line provjeru statusa potvrda, opisan u dokumentu RFC 6960.
OID	*Object Identifier*	Identifikator objekta
PIN	*Personal Identification Number*	Lični tajni broj za aktivaciju pametne kartice, pametnog *USB* tokena ili sličnog kriptografskog uređaja.
PKCS#10	*Public Key Cryptography Standard 10*	Standard za format zahtjeva za potvrdu.
PKI	*Public Key Infrastructure*	Infrastruktura javnih kriptografskih ključeva
QSCD	*Qualified Signature Creation Device*	Kvalificirano sredstvo za kreiranje elektronskih potpisa i pečata (pametna kartica, pametni USB token, i slično).
RA	*Registration Authority*	Registracijsko tijelo
RFC	*Request for comment*	Dokumenti koji definiraju Internet standarde i preporuke.

SSCD	*Secure Signature Creation Device*	Sredstvo za formiranje kvalificiranog elektronskog potpisa (pametna kartica, pametni *USB* token, i slično).
UTC	*Coordinated Universal Time*	Koordinirano univerzalno vrijeme

Tabela 11. Spisak skraćenica

1.7. Standardi

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

- IETF RFC 3647 – Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework

- IETF RFC 5280 (2008) – Internet X.509 Public Key Infrastructure; Certificate and Certificate Revocation List (CRL) Profile

- IETF RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (2013)

2. OBJAVLJIVANJE I LOKACIJA PODATAKA O USLUGAMA OVJERAVANJA

2.1. Lokacija za objavljivanje 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.

2.2. Objavljivanje podataka o uslugama ovjeravanja

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* liste) ovjerilaca *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.

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

Ovjerilac Uprave za indirektno oporezivanje objavljuje korisnička uputstva i obrasce na *Web* stranici, a prethodne verzije se zamjenjuju sa novim verzijama.

2.3. Učestalost objavljivanja podataka o uslugama ovjeravanja

Ovjerilac UIO ažurira objavljene podatke sljedećom dinamikom:

- Registri opozvanih potvrda (*CRL*) objavljuju se na svaka 24 sata. U slučaju opoziva i/ili suspenzije potvrde, ažurirani registar opozvanih potvrda se objavljuje odmah poslije opoziva i/ili suspenzije potvrda,
- Promjene na postojećim dokumentima objavljuju se u najkraćem roku poslije nastale promjene,
- Dodatni dokumenti objavljuju se u najkraćem roku po odobravanju od strane nadležnih organa.

2.4. Kontrola pristupa podacima o uslugama ovjeravanja

Podaci koji su objavljeni na *Web* stranici Ovjerioca UIO su javno dostupni. Pristup je ograničen na mogućnost čitanja. Svi koji pristupaju ovim podacima radi korištenja elektronskih potvrda dužni su da se upoznaju s odredbama ovih Praktičnih pravila.

Ovjerilac UIO ima uspostavljene logičke i fizičke sigurnosne mjere za zaštitu podataka na *Web* stranicama od neovlaštenog brisanja i dodavanja ili neovlaštenih promjena.

3. IDENTIFIKACIJA I AUTENTIKACIJA

3.1. Određivanje imena

3.1.1. Vrste imena

Ovjerilac *UINO Root CA* i njemu podređeni ovjerioci UIO u potvrdu upisuju podatke o imenu, odnosno nazivu subjekta za kojeg se potvrda izdaje u polje *Subject* potvrde. Razlikovno ime (eng. *Distinguished Name - DN*) u polju *Subject* u potvrdama usklađeno je s preporukom IETF RFC 5280 i normom X.520 i ono mora biti jedinstveno unutar Ovjerioca UIO.

U elektronskim potvrdama koje izdaje Ovjerilac UIO, polje *Issuer* **(**tabela 12, tabela 13 i tabela 14) potvrde, koje sadrži ime ovjerioca koji je izdao potvrdu, i polje *Subject* potvrde, koje sadrži ime korisnika potvrde, su jedinstvena imena (eng. *Distinguished Name - DN*) u obliku *X.509* v3.

KOMPONENTA IMENA	VRIJEDNOST
Naziv CA servera (CN)	*UINO Root CA*
Naziv organizacije (O)	*Uprava za indirektno-neizravno oporezivanje*
Naziv države (C)	*BA*

Tabela 12. Struktura imena potvrde ovjerioca *UINO Root CA* Uprave za indirektno oporezivanje (UIO) u elektronskim potvrdama

KOMPONENTA IMENA	VRIJEDNOST
Naziv CA servera (CN)	*UINO Issuing CA1*
Naziv organizacije (O)	*Uprava za indirektno-neizravno oporezivanje*
Naziv države (C)	*BA*

Tabela 13. Struktura imena potvrde podređenog ovjerioca *UINO Issuing CA1* Uprave za indirektno oporezivanje (UIO) u elektronskim potvrdama

KOMPONENTA IMENA	VRIJEDNOST
Naziv CA servera (CN)	*UINO Issuing CA2*
Naziv organizacije (O)	*Uprava za indirektno-neizravno oporezivanje*
Naziv države (C)	*BA*

Tabela 14. Struktura imena potvrde podređenog ovjerioca *UINO Issuing CA2* Uprave za indirektno oporezivanje (UIO) u elektronskim potvrdama

Struktura imena korisnika kvalificirane potvrde za elektronski potpis prikazana je u tabeli 15 i tabeli 16.

KOMPONENTA IMENA	VRIJEDNOST
Naziv korisnika (*CN*)	Ime Prezime (Ime i prezime kako je navedeno u identifikacionoj ispravi)
Serijski broj (*SERIALNUMBER*)	*CA:BA*-JIP (JIP je pseudoslučajno generirani broj potvrde)
Ime (G)	Ime (Ime potpisnika kako je navedeno u identifikacionoj ispravi)
Prezime (SN)	Prezime (Prezime potpisnika kako je navedeno u identifikacionoj ispravi)
Mjesto (L)	Mjesto prebivališta potpisnika
Naziv države (C)	*BA*

Tabela 15. Struktura imena za fizičko lice u kvalificiranim elektronskim potvrdama

KOMPONENTA IMENA	VRIJEDNOST
Naziv korisnika (*CN*)	Ime Prezime (Ime i prezime kako je navedeno u identifikacionoj ispravi)
Serijski broj (*SERIALNUMBER*)	*CA:BA*-JIP (JIP je pseudoslučajno generirani broj potvrde)
Ime (G)	Ime (Ime potpisnika kako je navedeno u identifikacionoj ispravi)
Prezime (SN)	Prezime (Prezime potpisnika kako je navedeno u identifikacionoj ispravi)
Identifikator organizacije (2.5.4.97)	*VATBA*-PIB (Porezni identifikacioni broj - PIB broj pravnog lica)
Naziv organizacije (O)	Puni registrirani skraćeni naziv poslovnog subjekta ili naziv poslovnog subjekta ako skraćeni naziv nije registriran.
Mjesto (L)	Mjesto sjedišta pravnog lica registriranog u Bosni i Hercegovini.
Naziv države (C)	*BA*

Tabela 16. Struktura imena za korisnika u pravnom licu u kvalificiranim elektronskim potvrdama

KOMPONENTA IMENA	VRIJEDNOST
Naziv pravnog lica (*CN*)	Naziv koji pravno lice koristi za svoje predstavljanje
Serijski broj (*SERIALNUMBER*)	*CA:BA*-JIP (JIP je pseudoslučajno generirani broj za datog subjekta)
Identifikator organizacije (2.5.4.97)	*VATBA*-PIB (Porezni identifikacioni broj - PIB broj pravnog lica).
Naziv organizacije (O)	Puni registrirani skraćeni naziv pravnog lica ili naziv pravnog lica ako skraćeni naziv nije registriran.
Mjesto (L)	Mjesto sjedišta pravnog lica registriranog u Bosni i Hercegovini.
Naziv države (C)	*BA*

Tabela 17. Struktura imena pravnog lica za kvalificirani elektronski pečat

3.1.2. Nomenklatura imena

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

U svaku potvrdu upisuju se podaci o imenu, odnosno nazivu subjektu ovjeravanja, te podatak o mjestu prebivališta i državi fizičkog lica, odnosno mjestu i državi sjedišta poslovnog subjekta. Podaci o imenu ili nazivu koji se upisuju u potvrdu odnose se na autentično ime ili naziv subjekta. Polje *Subject* u potvrdi usklađeno je s dokumentom IETF RFC 5280.
Polje *Subject* u potvrdama koje se izdaju za fizička lica sadrži ime i prezime lica. U poslovnim certifikatima i certifikatima za elektronski pečat polje *Subject* dodatno sadrži i puni registrirani naziv poslovnog subjekta i njegov identifikator.

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

Kod potvrda za autentikaciju *Web* stranica polje *Subject* i ekstenzija *Subject Alternative Name* sadrže puni kvalificirani naziv servera (FQDN).

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

3.1.3. Smislenost imena

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

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

ODREĐIVANJE ELEMENATA POLJA SUBJECT U POTVRDAMA	
NAZIV POTVRDE	**ATRIBUTI I VRIJEDNOSTI POLJA SUBJECT**
UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA FIZIČKO LICE	▪ **commonName (CN)**: Ime i prezime potpisnika ▪ **serialNumber**: *CA*:*BA*-JIP ▪ **givenName (G)**: Ime potpisnika ▪ **surname (SN)**: Prezime potpisnika ▪ **localityName (L)**: Mjesto prebivališta potpisnika ▪ **countryName (C)**: *BA*
UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA FIZIČKO LICE POVEZANO SA PRAVNIM LICEM	▪ **commonName (CN)**: Ime i prezime potpisnika ▪ **serialNumber**: *CA*:*BA*-JIP ▪ **givenName (G)**: Ime potpisnika ▪ **surname (SN)**: Prezime potpisnika ▪ **organizationIdentifier (2.5.4.97)** : VATBA-PIB ▪ **organizationName (O)**: Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran ▪ **localityName (L)**: Mjesto sjedišta poslovnog subjekta ▪ **countryName (C)**: *BA*

ODREĐIVANJE ELEMENATA POLJA SUBJECT U POTVRDAMA	
NAZIV POTVRDE	**ATRIBUTI I VRIJEDNOSTI POLJA SUBJECT**
UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA ZAPOSLENE	▪ **commonName (CN)**: Ime i prezime potpisnika ▪ **serialNumber**: *CA*:*BA*-JIP ▪ **givenName (G)**: Ime potpisnika ▪ **surname (SN)**: Prezime potpisnika ▪ **organizationIdentifier (2.5.4.97)** : *VATBA*-PIB UIO ▪ **organizationName (O)**: Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran ▪ **localityName (L)**: Mjesto sjedišta UIO ▪ **countryName (C)**: *BA*
UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI PEČAT	▪ **commonName (CN)**: Naziv koji subjekat koristi za svoje predstavljanje ▪ **serialNumber**: *CA*:*BA*-JIP ▪ **organizationIdentifier (2.5.4.97)** : *VATBA*-PIB ▪ **organizationName (O)**: Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran ▪ **localityName (L)**: Mjesto sjedišta poslovnog subjekta ▪ **countryName (C)**: *BA*
UIO POTVRDA ZA AUTENTIKACIJU WEB STRANICA	▪ **commonName**: FQDN servera ▪ **organizationIdentifier (2.5.4.97)**:*VATBA*-PIB ▪ **organizationName**: Naziv pravnog lica ▪ **localityName**: Mjesto sjedišta pravnog lica ▪ **countryName**: *BA*

Tabela 18. Određivanje elemenata polja *Subject* u potvrdama

3.1.4. Pravila tumačenja raznih oblika imena

Tumačenje oblika imena u polju *Subject* po normi X.520 u Ovjeriocu UIO određeno je na sljedeći način:

- commonName – U potvrdama za fizička lica, fizička lica povezana sa pravnim licima i potvrdama za zaposlene ovaj atribut sadrži ime i prezime fizičkog lica kako je navedeno u identifikacionoj ispravi. U potvrdama za autentikaciju *Web* stranica stavlja se samo jedan puni kvalificirani naziv servera (*FQDN*).
- serialNumber – Ovaj atribut u polju *Subject* osigurava jedinstvenost imena subjekta. U potvrdama za fizička lica, fizička lica povezana sa pravnim licima i potvrdama za zaposlene sastoji se od skraćenice Ovjerioca (*CA*), dvoslovčanog ISO koda države prebivališta potpisnika (BA) i pseudoslučajno generiranog broja potvrde (JIP). U aplikacijskim potvrdama se ovo polje ne koristi.
- givenName – Sadrži ime fizičkog lica kako je navedeno u identifikacionoj ispravi.
- surname – Sadrži prezime fizičkog lica kako je navedeno u identifikacionoj ispravi.
- organizationIdentifier – U potvrdama za fizička lica povezana sa pravnim licima i potvrdama za zaposlene sastoji se od oznake VAT, dvoslovčanog ISO koda države prebivališta potpisnika (BA) i poreznog identifikacionog broja pravnog lica (PIB).
- localityName – U potvrdama za fizička lica povezana sa pravnim licima atribut *localityName* sadrži naziv mjesta u kojem je sjedište poslovnog subjekta. U potvrdama za fizička lica atribut *localityName* sadrži mjesto prebivališta potpisnika. U aplikacijskim potvrdama atribut *localityName* sadrži naziv mjesta u kojem je sjedište poslovnog subjekta.
- countryName – Sadrži oznaku dvoslovčanog ISO koda Bosne i Hercegovine.

Ekstenzija *Subject Alternative Name* sadrži barem jedan *FQDN* servera u potvrdama za autentikaciju *Web* stranica, odnosno *e-mail* adresu potpisnika ili *e-mail* adresu povezanu s IT sistemom, aplikacijom ili servisom u ostalim potvrdama.

UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA FIZIČKA LICA		
ATRIBUT	**VRIJEDNOST**	**OPIS**
commonName (CN)	Ime i prezime	Ime i prezime potpisnika kako je navedeno u identifikacionoj ispravi
serialNumber	*CA*:*BA*-JIP	JIP je pseudoslučajno generiran broj potvrde
givenName (G)	Ime potpisnika	Ime potpisnika kako je navedeno u identifikacionoj ispravi
surname (SN)	Prezime potpisnika	Prezime potpisnika kako je navedeno u identifikacionoj ispravi
localityName (L)	Mjesto prebivališta potpisnika	Mjesto prebivališta fizičkog lica
countryName (C)	*BA*	Dvoslovčani ISO kod države prebivališta potpisnika, BA za Bosnu i Hercegovinu

Tabela 19. Tumačenje oblika imena po X.520 normi za UIO kvalificirane potvrde za elektronski potpis za fizička lica

UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA FIZIČKA LICA POVEZANA SA PRAVNIM LICIMA		
ATRIBUT	**VRIJEDNOST**	**OPIS**
commonName (CN)	Ime i prezime	Ime i prezime potpisnika kako je navedeno u identifikacionoj ispravi
serialNumber	*CA:BA*-JIP	JIK je pseudoslučajno generiran broj potvrde
givenName (G)	Ime potpisnika	Ime potpisnika kako je navedeno u identifikacionoj ispravi
surname (SN)	Prezime potpisnika	Prezime potpisnika kako je navedeno u identifikacionoj ispravi
organizationIdentifier (2.5.4.97)	*VATBA*-PIB	PIB je porezni identifikacioni broj pravnog lica
organizationName (O)	Naziv poslovnog subjekta	Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran
localityName (L)	Mjesto sjedišta poslovnog subjekta	Mjesto sjedišta poslovnog subjekta
countryName (C)	*BA*	Dvoslovčani ISO kod države Bosne i Hercegovine

Tabela 20. Tumačenje oblika imena po X.520 normi za UIO kvalificirane potvrde za elektronski potpis za fizička lica povezana sa pravnim licima

UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI POTPIS ZA ZAPOSLENE		
ATRIBUT	**VRIJEDNOST**	**OPIS**
commonName (CN)	Ime i prezime	Ime i prezime potpisnika kako je navedeno u identifikacionoj ispravi
serialNumber	*CA:BA*-JIP	JIP je pseudoslučajno generiran broj potvrde
givenName (G)	Ime potpisnika	Ime potpisnika kako je navedeno u identifikacionoj ispravi
surname (SN)	Prezime potpisnika	Prezime potpisnika kako je navedeno u identifikacionoj ispravi
organizationIdentifier (2.5.4.97)	*VATBA*-PIB UIO	PIB UIO je porezni identifikacioni broj Uprave za indirektno-neizravno oporezivanje
organizationName (O)	*Uprava za indirektno-neizravno oporezivanje*	Naziv poslovnog subjekta
localityName (L)	Mjesto sjedišta UIO ili regionalnog centra	Mjesto sjedišta UIO ili regionalnog centra
countryName (C)	*BA*	Dvoslovčani ISO kod države Bosne i Hercegovine

Tabela 21. Tumačenje oblika imena po X.520 normi za UIO kvalificirane potvrde za elektronski potpis za zaposlene

UIO KVALIFICIRANA POTVRDA ZA ELEKTRONSKI PEČAT		
ATRIBUT	**VRIJEDNOST**	**OPIS**
commonName (CN)	Naziv poslovnog subjekta	Naziv koji poslovni subjekat koristi za svoje predstavljanje
serialNumber	*CA*:*BA*-JIP	JIP je pseudoslučajno generiran broj potvrde
organizationIdentifier (2.5.4.97)	*VATBA*-PIB	PIB je porezni identifikacioni broj pravnog lica
organizationName (O)	Naziv poslovnog subjekta	Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran
localityName (L)	Mjesto sjedišta poslovnog subjekta	Mjesto sjedišta poslovnog subjekta
countryName (C)	*BA*	Dvoslovčani ISO kod države Bosne i Hercegovine

Tabela 22. Tumačenje oblika imena po X.520 normi za UIO kvalificirane potvrde za elektronski pečat

UIO POTVRDA ZA AUTENTIKACIJU WEB STRANICA		
ATRIBUT	**VRIJEDNOST**	**OPIS**
commonName (CN)	Puni kvalificirani naziv servera (FQDN)	Samo jedan puni kvalificirani naziv servera (FQDN)
organizationIdentifier (2.5.4.97)	*VATBA*-PIB	PIB je porezni identifikacioni broj pravnog lica
organizationName	Naziv poslovnog subjekta	Skraćeni naziv poslovnog subjekta ili puni registrirani naziv poslovnog subjekta ako skraćeni naziv nije registriran
localityName (L)	Mjesto sjedišta poslovnog subjekta	Mjesto sjedišta poslovnog subjekta
countryName (C)	*BA*	Dvoslovčani ISO kod države Bosne i Hercegovine

Tabela 23. Tumačenje oblika imena po X.520 normi za UIO potvrde za autentikaciju *Web* stranica

3.1.5. Jedinstvenost imena

Razlikovno ime subjekta jedinstveno je unutar Ovjerioca UIO i produkcijske hijerarhije zasnovane na serveru *UINO Root CA*. Jedinstvenost razlikovnog imena osigurana je vrijednošću atributa *serialNumber* u polju *Subject* potvrde.

Ovjerilac UIO samostalno kontrolira i dodjeljuje vrijednost atributa *serialNumber* u razlikovnom imenu da bi imena različitih subjekata bila jedinstvena.

U aplikacijskim potvrdama jedinstvenost imena osigurava se na način da se u atribut *commonName* razlikovnog imena potvrde upisuje naziv aplikacije koji unutar istog poslovnog subjekta mora biti jedinstven.

Jedinstvenost razlikovnog imena u administrativnim potvrdama osigurana je vrijednošću atributa *serialNumber* u polju *Subject* potvrde.

3.1.6. Anonimnost ili pseudonimi korisnika

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

Ovjerilac UIO odbija bilo koji zahtjev za anonimnošću ili za korištenjem pseudonima.

3.1.7. Pravila za tumačenje različitih vrsta imena

U kvalificiranim elektronskim potvrdama su imena korisnika vjerno predstavljena odgovarajućim latiničnim ili ćiriličnim slovima.

Znakovi koje nije dozvoljeno koristiti u imenima korisnika su: " (navodnici), ? (upitnik), \ (obrnuta kosa crta), # (ljestve), $ (dolar), % (postotak), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez).

3.1.8. Jedinstvenost imena

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.

3.1.9. Priznavanje, autentikacija i uloga zaštitnog znaka

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.

Ovjerilac UIO će, što je moguće prije, izvršiti sve sudske naloge koji su izdati u skladu sa zakonima, a koji se tiču pravnih lijekova za bilo kakvo kršenje prava trećih lica prilikom izdavanja elektronskih potvrda po ovim Praktičnim pravilima.

3.2. Početna provjera valjanosti identiteta

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

3.2.1. Metod dokazivanja posjeda privatnog ključa

Privatni kriptografski ključ korisnika kvalificiranih potvrda se generira u Ovjeriocu UIO na *SSCD* uređaju.

3.2.2. Autentikacija identiteta fizičkog lica

Korisnik mora biti identifikovan u skladu sa ovim Praktičnim pravilima.

Korisnik mora biti fizički prisutan u toku registracije.

U toku registracije korisnik mora da posjeduje važeći identifikacioni dokument sa fotografijom (važeća lična karta, pasoš ili drugi). Prilikom registracije korisnik treba priložiti ovjerenu fotokopiju identifikacionog dokumenta.

Fotografija u dokumentu za identificiranje se poredi s korisnikom koji je fizički prisutan (karakteristike lica, starost, spol i sl.).

3.2.3. Autentikacija identiteta pravnog lica

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.

Ukoliko je korisnik fizičko lice koje je zaposleno u pravnom licu, neophodno je:

- Utvrditi tačan identitet pravnog lica i autorizovanje korištenja njenog imena,
- Priložiti službene dokumente o tom pravnom licu prilikom podnošenja zahtjeva (Rješenje o registraciji pravnog lica – original ili ovjerena fotokopija), radi potvrđivanja valjanosti imena pravnog lica,
- Dokazati da je korisnik ovlašten od strane pravnog lica za dobijanje elektronske potvrde.

Ukoliko je korisnik fizičko lice-stranac koje je zaposleno u pravnom licu registriranom u Bosni i Hercegovini, neophodno je:

- Utvrditi tačan identitet fizičkog lica i autorizovanje korištenja njegovog imena,
- Potvrditi valjanost imena fizičkog lica, tokom čega podnosilac zahtjeva mora osigurati sljedeće službene dokumente o tom fizičkom licu:
  - Valjan identifikacioni dokument neophodan za ulazak u Bosnu i Hercegovinu,
  - Prijavu boravka izdatu od strane nadležnog organa,
  - Potvrdu o prijavi rada izdatu od strane nadležnog organa,
  - Radnu dozvolu izdatu od strane nadležnog organa,
  - Ugovor o radu (izdaje pravno lice registrirano u Bosni i Hercegovini u kojem će raditi fizičko lice-stranac),
- Dokazati da je korisnik ovlašten od strane pravnog lica za dobijanje elektronske potvrde.

3.2.4. Neprovjereni podaci o korisniku

Svi podaci o korisniku koje zahtjeva Zakon o elektronskom potpisu moraju da budu propisno provjereni.

3.2.5. Provjera tačnosti podataka pravnog lica

Korisnik dostavlja važeću dokumentaciju za ime pravnog lica, koje će biti uključeno u elektronsku potvrdu. Izbor riječi u imenu pravnog lica koje treba upisati u potvrdu mora da bude identičan riječima u dostavljenoj dokumentaciji.

Korištenje imena pravnog lica moraju dozvoliti i autorizovati odgovorni predstavnici pravnog lica, i to:

- Korištenje imena pravnog lica koje je registrirano u sudskom registru moraju da autorizuju odgovorna lica tog pravnog lica,
- Korištenje imena pravnog lica koje ima jednog vlasnika mora da autorizuje sam vlasnik,
- Korištenje imena pravnog lica koje je u vlasništvu više partnera mora da autorizuje partner koji je naveden u ugovoru o partnerstvu,
- Korištenje imena pravnog lica koje je vlasništvo neke zajednice mora da autorizuje nadležna institucija.

3.2.6. Kriteriji za međusobnu saradnju

Ovjerilac UIO ne predviđa unakrsno ovjeravanje.

3.3. Identifikacija i autentikacija zahtjeva za obnovom ključa

3.3.1. Identifikacija i autentikacija zahtjeva za rutinskom obnovom ključa

Ovjerilac UIO ne dozvoljava obnovu ključa. Cijeli proces se izvršava izdavanjem nove elektronske potvrde na prethodno opisani način.

3.3.2. Identifikacija i autentikacija zahtjeva za zamjenom ključa poslije opoziva

Ovjerilac UIO ne dozvoljava zamjenu ključa poslije opoziva. Cijeli proces se izvršava izdavanjem nove elektronske potvrde.

3.4. Identifikacija i autentikacija zahtjeva za opozivom i suspenzijom potvrde

Korisnik zahtijeva opoziv elektronske potvrde po jednoj od sljedećih procedura:

- Korisnik se identifikuje lično i predaje svojeručno potpisan zahtjev Grupi za podršku korisnicima sistema PKI UIO u regionalnom centru ili sjedištu UIO,
- Korisnik šalje elektronski potpisan zahtjev elektronskom poštom (*e-mail*) Grupi za održavanje sistema PKI UIO, na unaprijed određenu adresu elektronske pošte. Grupa za održavanje sistema PKI UIO priznaje samo elektronski potpisane zahtjeve s važećom kvalificiranom elektronskom potvrdom izdatom od strane Ovjerioca UIO. Zahtjev se može poslati samo sa *e-mail* adrese koja je navedena prilikom registracije korisnika u njegovom zahtjevu i koja se nalazi u izdatoj potvrdi.

4. OPERATIVNI ZAHTJEVI U PROCESU IZDAVANJA POTVRDA

4.1. Zahtjevi za izdavanje potvrda

4.1.1. Ko može da podnese zahtjev za izdavanje potvrde

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

4.1.2. Uvjeti za izdavanje potvrde

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.

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

Zahtjev za izdavanje i korištenje elektronske potvrde sadrži podatke na osnovu kojih Ovjerilac 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.

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

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

4.2. Obrada zahtjeva za izdavanje potvrda

4.2.1. Obavljanje funkcija identifikacije i potvrđivanja autentičnosti

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

4.2.2. Odobrenje ili odbijanje zahtjeva za izdavanje potvrda

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.

4.2.3. Vrijeme obrade zahtjeva za izdavanje potvrde

Ovjerilac UIO vrši obradu zahtjeva poslije prispjeća zahtjeva od strane Grupe za podršku korisnicima sistema PKI UIO u regionalnim centrima. Obrada zahtjeva može da traje najduže 30 radnih dana od dana prijema zahtjeva.

4.3. Izdavanje potvrda

4.3.1. Aktivnosti u toku izdavanja potvrde

Izdavanje elektronske potvrde vrši se na sljedeći način:

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**.**

4.3.2. Obavještavanje korisnika o izdavanju potvrde

Ovjerilac UIO poziva korisnika da u Grupi za podršku korisnicima sistema PKI UIO u regionalnom centru preuzme elektronsku potvrdu na *SSCD* uređaju.

4.4. Preuzimanje potvrda

4.4.1. Postupak preuzimanja potvrda

Korisniku se kvalificirana elektronska potvrda uručuje lično 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.

4.4.2. Objavljivanje potvrda

Elektronska potvrda se javno ne objavljuje od strane Ovjerioca UIO.

4.4.3. Obavještavanje o izdavanju potvrda trećih lica

Treća lica se ne obavještavaju o izdavanju elektronske potvrde.

4.5. Korištenje para kriptografskih ključeva i potvrde

4.5.1. Korištenje privatnog ključa i potvrde od strane korisnika

Privatni kriptografski ključevi potvrde *UINO Root CA, UINO Issuing CA1* i *UINO Issuing CA2* koriste se za potpisivanje potvrda i *CRL*-ova.

Privatni kriptografski ključ korisnika se koristi za kreiranje kvalificiranog elektronskog potpisa ili pečata, a kvalificirana elektronska potvrda za verificiranje kvalificiranog elektronskog potpisa ili pečata.

4.5.2. Korištenje javnog ključa i potvrda od strane trećeg lica

Treće lice koristi javni ključ i elektronsku potvrdu za verificiranje elektronskog potpisa.

4.6. Produžetak korištenja potvrde

Ovjerilac UIO ne vrši produženje korištenja elektronske potvrde. Cijeli proces se izvršava izdavanjem nove elektronske potvrde.

4.7. Zamjena javnog ključa u potvrdi

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

4.7.1. Okolnosti za zamjenu javnog ključa u potvrdi

Ne vrši se.

4.7.2. Ko može da zahtijeva zamjenu javnog ključa u potvrdi

Ne vrši se.

4.7.3. Obrada zahtjeva za zamjenu javnog ključa u potvrdi

Ne vrši se.

4.7.4. Obavještavanje korisnika o zamjeni javnog ključa u potvrdi

Ne vrši se.

4.7.5. Postupak prihvaćanja obavještenja o zamjeni javnog ključa u potvrdi

Ne vrši se.

4.7.6. Objavljivanje potvrde kod koje je izvršena zamjena javnog ključa

Ne vrši se.

4.7.7. Obavještavanje trećih lica o izdavanju potvrda

Ne vrši se.

4.8. Promjena podataka u potvrdi

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

4.8.1. Okolnosti za promjenu podataka u potvrdi

Ne vrši se.

4.8.2. Ko može da zahtijeva promjenu podataka u potvrdi

Ne vrši se.

4.8.3. Obrada zahtjeva za promjenu podataka u potvrdi

Ne vrši se.

4.8.4. Obavještenje korisnika o promjeni podataka u potvrdi

Ne vrši se.

4.8.5. Postupak prihvaćanja obavještenja o promjeni podataka u potvrdi

Ne vrši se.

4.8.6. Objavljivanje potvrda kod koga je izvršena promjena podataka

Ne vrši se.

4.8.7. Obavještenje trećih lica o izdavanju potvrda

Ne vrši se.

4.9. Opoziv i suspenzija potvrda

4.9.1. Okolnosti opoziva potvrda

4.9.1.1. Okolnosti opoziva potvrda Ovjerioca UIO

Ovjerilac UIO će opozvati potvrdu Ovjerioca UIO u roku od 5 (pet) dana:

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

4.9.1.2. Okolnosti opoziva korisničkih potvrda

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.

4.9.2. Ko može da zahtijeva opoziv potvrde

Opoziv elektronske potvrde može da zahtijeva:

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

4.9.3. Procedure za opoziv potvrde

4.9.3.1. Opoziv potvrde zbog kompromitiranja privatnog kriptografskog ključa

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

1. Korisnik zahtijeva opoziv elektronske potvrde po jednoj od sljedećih procedura:

    - Korisnik preko *Web* sajta Ovjerioca UIO preuzima Zahtjev za promjenu statusa kvalificirane elektronske potvrde i popunjava ga. Korisnik se identifikuje lično u Grupi za podršku korisnicima sistema PKI UIO u regionalnom centru u kojoj predaje svojeručno potpisan zahtjev. Poslije uspješne identifikacije, Grupa za podršku korisnicima sistema PKI UIO u regionalnom centru UIOsi zahtjev u aplikaciju Registracijskog tijela i prosljeđuje ga Grupi za održavanje sistemu PKI UIO.
    - Korisnik šalje zahtjev koji je elektronski potpisan kvalificiranom elektronskom potvrdom elektronskom poštom (*e-mail*) Grupi za održavanje sistema PKI UIO na unaprijed određenu adresu elektronske pošte. Grupa za održavanje sistema PKI UIO priznaje samo elektronski potpisane zahtjeve sa važećom kvalificiranom elektronskom potvrdom izdanom korisniku od strane Ovjerioca UIO. Zahtjev se može poslati samo sa *e-mail* adrese koja je navedena prilikom registracije korisnika u njegovom zahtjevu i koja se nalazi u izdatoj potvrdi.

2. Grupa za održavanje sistema PKI UIO verifikuje zahtjev korisnika (dobijen od korisnika elektronskom poštom ili dobijen od Grupe za podršku korisnicima sistema PKI UIO u regionalnom centru) i opoziva elektronsku potvrdu.

Grupa za održavanje sistema PKI UIO obavještava korisnika o opozivu elektronske potvrde elektronskom poštom. U slučaju da korisnik ne posjeduje adresu elektronske pošte, obavještenje o opozivu bit će mu poslato poštom na adresu naznačenu u ugovoru.

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

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

4.9.3.2. Opoziv potvrde zbog promjene podataka u potvrdi

Opoziv elektronske potvrde zbog promjene podataka u potvrdi vrši se na isti način kako je određeno u tački 4.9.3.1.

Ovjerilac UIO može da se odluči za opoziv elektronske potvrde i bez zahtjeva korisnika, ukoliko procijeni da je došlo do promjene podataka u potvrdi, koje zahtijevaju izdavanje nove elektronske potvrde.

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

4.9.3.3. Opoziv potvrde zbog neispunjenja obaveza korisnika

U slučaju da korisnik ne ispunjava svoje obaveze, Grupa za održavanje sistema PKI UIO u Ovjeriocu UIO vrši opoziv elektronske potvrde korisnika.

Grupa za održavanje sistema PKI UIO obavještava korisnika o opozivu elektronske potvrde elektronskom poštom. U slučaju da korisnik ne posjeduje adresu elektronske pošte, obavještenje o opozivu bit će mu poslato poštom na adresu naznačenu u ugovoru.

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

4.9.4. Vrijeme od prijave do opoziva potvrde

Poslije podnošenja zahtjeva za opoziv elektronske potvrde od strane korisnika Ovjerilac UIO će pristupiti obradi zahtjeva za opozivom potvrde, bez odgađanja.

4.9.5. Vremenski rok u kome ovjerilac provodi zahtjev za opoziv potvrde

Grupa za održavanje sistema PKI UIO izvršava opoziv elektronske potvrde odmah po prijemu zahtjeva za opoziv potvrde i objavljuje novi registar opozvanih potvrda.

4.9.6. Zahtjev za provjeru opozvanosti potvrda od strane trećih lica

U toku rada sa elektronskim potvrdama izdanim od strane Ovjerioca UIO, treća lica imaju obavezu da provjeravaju opozvanost potvrda.

4.9.7. Učestalost objavljivanja registra opozvanih potvrda

Registri opozvanih potvrda ovjerioca *UINO Root CA* objavljuju se na svakih 6 mjeseci i prilikom opoziva podređenog ovjerioca ili potvrde za potpisivanje odgovora *OCSP* servisa ovjerioca *UINO Root CA*.

Registri opozvanih potvrda ovjerilaca *UINO Issuing CA1* i *UINO Issuing CA2* objavljuju se na svaka 24 sata.

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.

4.9.8. Maksimalno kašnjenje u objavljivanju registra opozvanih potvrda

Maksimalno kašnjenje objave *CRL* liste u javnom repozitoriju jeste jedan minut. U slučaju nepredviđenih okolnosti koje rezultuju dužim kašnjenjem objave *CRL* liste, Ovjerilac UIO će obavijestiti korisnike o razlogu kašnjenja i vremenskom intervalu unutar koga nije objavljena validna *CRL* lista.

4.9.9. Raspoloživost on-line provjere opozvanosti/statusa potvrda

Registar opozvanih potvrda i *OCSP* servis su stalno dostupani za *on-line* provjeru opozvanosti elektronskih potvrda.

Putem *OCSP* servisa Ovjerioca UIO dostupne su informacije o statusu opozvanosti potvrda koje su izdate od strane Ovjerioca UIO.

Adresa UIO *OCSP* servisa je http://ocsp.uino.gov.ba, a sadržana je u ekstenziji *Authority Information Access* svake potvrde koju izdaju *UINO Root CA* i podređeni *UINO Issuing CA1* i *UINO Issuing CA2*.

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

4.9.10. Zahtjevi za on-line provjeru opozvanosti potvrda

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

4.9.11. Druge forme registra opozvanih potvrda

Registar opozvanih potvrda je raspoloživ i na *Web* stranici Ovjerioca UIO.

4.9.12. Posebni zahtjevi u slučaju kompromitiranja ključa

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

4.9.13. Okolnosti suspenzije i prekida suspenzije potvrde

Suspenzija je privremeno deaktiviranje elektronske potvrde izdane korisniku.

Ovjerilac 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.

4.9.14. Ko može da zahtijeva suspenziju i prekid suspenzije potvrde

Suspenziju elektronske potvrde može da zahtijeva:

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

Prekid suspenzije može da zahtijeva:

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

4.9.15. Procedure za suspenziju i prekid suspenzije potvrde

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

1. Korisnik podnosi zahtjev za suspenziju ili prekid suspenzije elektronske potvrde po jednoj od sljedećih procedura:

    - Korisnik preko *Web* sajta Ovjerioca UIO preuzima Zahtjev za promjenu statusa elektronske potvrde i popunjava ga. Korisnik se identifikuje lično u Grupi za podršku korisnicima sistema PKI UIO u regionalnom centru u kojem predaje svojeručno potpisan zahtjev. Poslije uspješne identifikacije, Grupa za podršku korisnicima sistema PKI UIO unosi zahtjev u aplikaciju Registracijskog tijela i proslijeđuje ga Grupi za održavanje sistema PKI.
    - Korisnik šalje zahtjev koji je elektronski potpisan kvalificiranom elektronskom potvrdom elektronskom poštom (*e-mail*) Grupi za održavanje sistema PKI UIO na unaprijed određenu adresu elektronske pošte. Grupa za održavanje sistema PKI UIO priznaje samo elektronski potpisane zahtjeve sa važećom kvalificiranom elektronskom potvrdom izdanom korisniku od strane Ovjerioca UIO. Zahtjev se može poslati samo sa *e-mail* adrese koja je navedena prilikom registracije korisnika u njegovom zahtjevu.

2. Grupa za održavanje sistema PKI UIO verificira zahtjev korisnika (dobijen od korisnika elektronskom poštom ili dobijen od Grupe za podršku korisnicima sistema PKI UIO) i izvršava suspenziju ili prekid suspenzije elektronske potvrde i o tome obavještava korisnika putem elektronske pošte.

Ukoliko Ovjerilac UIO sumnja da je došlo do kompromitacije privatnog kriptografskog ključa ili da je došlo do promjene podataka u potvrdi korisnika, može da suspendira elektronsku potvrdu i bez zahtjeva korisnika.

4.9.16. Ograničenje perioda na koji se potvrda suspenduje

Period suspenzije elektronske potvrde je maksimalno 30 dana.

4.10. Usluge o statusu potvrda

4.10.1. Operativne karakteristike

Ovjerilac UIO pruža uslugu provjere statusa opozvanosti elektronske potvrde posredstvom registra opozvanih potvrda.

4.10.2. Dostupnost usluge

Registar opozvanih potvrda je stalno dostupan.

4.10.3. Dodatne karakteristike

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

4.11. Prestanak korištenja potvrde

Korisnik prestaje s korištenjem elektronske potvrde:

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

4.12. Otkrivanje i obnova privatnog ključa korisnika

4.12.1. Politika otkrivanja i obnove privatnog ključa korisnika

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

4.12.2. Politika enkapsulacije ključa sesije i obnove

Ne vrši se.

5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OVLAŠTENIH LICA

Ovo poglavlje opisuje kontrolu fizičkog okruženja, procedura i ovlaštenih lica, koja je implementirana kod Ovjerioca UIO da bi se zaštitilo funkcioniranje sistema.

Procedure su definirane u politici informacijske sigurnosti koja se dokumentira, provodi i održava, a obuhvata sigurnosne kontrole i operativne postupke za objekte, sisteme i informatičku opremu u skladu sa standardom ISO/IEC 27001.

UIO definira politiku informacijske sigurnosti koju odobrava uprava UIO i određuje način upravljanja svojom informacijskom sigurnošću. O promjenama politike sigurnosti informacija saopćavat će se trećim stranama, prema potrebi. Ovo uključuje sve pouzdajuće strane, tijela za ocjenjivanje, nadzorna ili druga regulatorna tijela.

Radi se prepoznavanje, analiziranje i procjena poslovnih i tehničkih rizika na osnovu standarda ISO 9001 i ISO/IEC 27001. UIO provodi sve sigurnosne zahtjeve i operativne postupke, kako su dokumentirani u politici informacijske sigurnosti, na osnovu odabrane mjere smanjenja rizika.

UIO vodi popis sve informacijske imovine i dodjeljuje klasifikaciju u skladu s procjenom rizika.

Politika informacijske sigurnosti i popis informacione opreme pregledavaju se u planiranim intervalima (najmanje jednom svake godine) radi očuvanja svrhe i efikasnosti politike informacijske sigurnosti, te u slučaju značajnih promjena. Sve promjene koje mogu uticati na pružen nivo sigurnosti odobrava uprava UIO.

5.1. Kontrola fizičkog pristupa

Ovjerilac UIO kao vršilac usluga izdavanja kvalificiranih elektronskih potvrda primjenjuje mjere fizičke zaštite sistema u skladu sa ovim pravilima, važećim zakonskim i podzakonskim propisima i međunarodnim preporukama u skladu sa standardom ISO/IEC 27001.

Ovjerilac UIO primjenjuje mjere fizičke zaštite sistema izdavanja elektronskih potvrda na osnovu procjene rizika radi ograničavanja pristupa hardverskim i softverskim komponentama sistema kao što su serveri, radne stanice, kriptografski moduli, mrežni uređaji i pripadajući softver i arhivi.

5.1.1. Lokacija i razmještaj prostorija (okolišna sigurnost)

Provode se kontrole kako bi se izbjegao gubitak, oštećenje ili ugrožavanje imovine i prekid poslovne aktivnosti. 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.

5.1.2. Kontrola fizičkog pristupa za pojedince

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

Zaposleni u Ovjeriocu UIO mora se pridržavati sljedećih obaveza:

- Izvršavati svoje administratorske dužnosti u sigurnoj zoni. Ulazak u sigurnu zonu je moguć isključivo uz identifikaciju beskontaktnom karticom. Otvaranje ormara u kome je smještena oprema Ovjerioca UIO je moguć isključivo uz identifikaciju sa posebnom beskontaktnom karticom, čiji je nosilac drugo ovlašteno lice,
- Štititi beskontaktnu karticu za ulazak u sigurnu zonu i za otvaranje ormara sa opremom,
- Smještati kartice *HSM* administratora i *HSM* operatora i druge medije koji sadrže kriptografske ključeve, pristupne parametre korisničkih računa ili druge povjerljive podatke u sigurnu kasu-kontejner. Za otvaranje kase-kontejnera potreban je par ključeva,
- Štititi lozinke koje omogućavaju pristup privatnim kriptografskim ključevima,
- Smještati rezervne kopije privatnog ključa u sigurnu kasu-kontejner,
- Zaposleni sa odgovarajućom ulogom u sistemu štite svoju smart karticu za pristup Centralnom sistemu *CMS*-a, koji omogućava centralizirano praćenje i upravljanje životnim ciklusom kriptografskih uređaja,
- Zaposleni sa odgovarajućom ulogom u sistemu štite svoju smart karticu za pristup *Desktop* aplikaciji koja služi za vizuelno i elektronsko personaliziranje kriptografskih uređaja,
- Zaposleni po završetku rada sa aplikacijama Centralnog sistema i *Desktop* aplikacije za personaliziranje kriptografskih uređaja odlažu smart kartice kojima pristupaju aplikacijama na sigurno mjesto,
- Zaposleni sa odgovarajućom ulogom u sistemu štite *PIN* kod smart kartice koju koriste za prijavu na aplikaciju Centralnog sistema *CMS*-a i Desktop aplikaciju *CMS*-a za personaliziranje kriptografskih uređaja, ovisno od uloge koja im je dodijeljena,
- Odjavljivati se sa svih aplikacija u slučaju da napušta računar, a računar ostaje bez nadzora.

Zaposleni koji obavlja poslove prijema zahtjeva za izdavanje elektronske potvrde i prijema zahtjeva za promjenu statusa potvrde u regionalnom centru, dužan je da se pridržava sljedećih obaveza:

- Izvršavati svoje dužnosti u zoni prijema,
- Štititi svoju smart karticu koju koristi za prijavljivanje na aplikaciju Registracijskog tijela,
- Štititi *PIN* kod smart kartica koje omogućavaju prijavljivanje na aplikaciju Registracijskog tijela,
- Odjavljivati se sa svih aplikacija u slučaju da napušta računar, a računar ostaje bez nadzora,
- Nakon prestanka sa radom sa aplikacijom Registracijskog tijela odlagati svoju smart karticu na sigurno mjesto.

5.1.3. Napajanje i klimatizacija

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.

5.1.4. Zaštita od poplave

Oprema Ovjerioca UIO smještena je na mjestu koje je osigurano od poplave.

5.1.5. Zaštita od vatre

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

5.1.6. Smještanje medija

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.

5.1.7. Odlaganje nepotrebnih podataka

Nepotrebna papirna dokumentacija i računarski mediji za smještaj podataka se komisijski sijeku na komadiće i fizički uništavaju.

Podaci sa medija, kao što su kriptografski ključevi, podaci za aktiviranje ili elektronski

dnevnici, nepovratno se brišu, prije nego što se mediji pošalju na uništavanje.

Uništavanje medija na kojima se nalaze povjerljivi podaci, te uništavanje podataka i ključeva povezanih s *HSM* modulima provodi se u skladu sa internim procedurama UIO.
Brisanje i uništavanje podataka *HSM* modula provodi se i prije njihovog eventualnog slanja na servis ili popravak, kao i prilikom svakog njihovog uklanjanja iz sigurne zone Ovjerioca UIO i njihovog transportovanja na druge lokacije UIO.

5.1.8. Smještaj rezervnih kopija podataka na udaljenoj lokaciji

Ovjerilac UIO koristi sigurnu udaljenu lokaciju za smještaj medija sa podacima. Mediji se smještaju u kasu-kontejner. Prostoriju u kojoj je smještena vatrootporna sigurna kasa-kontejner na pomenutoj udaljenoj lokaciji nadziru ovlaštena lica Ovjerioca UIO.

5.2. Kontrola procedura

5.2.1. Povjerljive uloge ovlaštenih lica

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.

Ovlaštenea lica Ovjerioca UIO, ovisno od dodijeljene uloge, mogu da obavljaju poslove na:

- *HSM* modulu,
- Serverima Ovjerioca UIO,
- Aplikacijama ovjerioca,
- Aplikaciji Registracijskog tijela *CMS*-a,
- Aplikaciji Centralnog Sistema *CMS*-a,
- *Desktop* aplikaciji *CMS*-a za personaliziranje kriptografskih uređaja,
- Mrežnim uređajima i pristupnim listama.

Privilegije određenih korisničkih računa na operativnim sistemima računara i korisničkih računa u aplikacijama, ograničavaju pristup ovlaštenim licima Ovjerioca UIO na radnje koje su im potrebne u obavljanju njihovih dužnosti.

Unutar Ovjerioca UIO postoje sljedeće sigurnosne funkcije:

- Glavni administrator sigurnosti – administrira i implementira sigurnosne funkcije i procedure, upravlja aktivnostima na dodatnom unaprjeđenju poslova izdavanja, opoziva i suspenzije elektronskih potvrda,
- Administrator sistema – odgovoran je za instalaciju, konfiguraciju i održavanje sigurnih sistema Ovjerioca UIO za registraciju korisnika, izdavanje elektronskih potvrda i distribuiranje tačnog vremena. Osigurava sredstva za formiranje sigurnog elektronskog potpisa za korisnike i upravljanje opozivom elektronskih potvrda,
- Operator sistema – odgovoran je za rad sigurnih sistema na dnevnom nivou i ima autoriziranu odgovornost za implementaciju sistema za formiranje rezervnih kopija i procedure oporavka,

- Evidentičar sistema – odgovoran je za pregledanje i održavanje arhiva i log fajlova sigurnih sistema Ovjerioca UIO.

5.2.2. Potreban broj ovlaštenih lica za operativne poslove

Ovjerilac UIO ima implementiranu dvostruku autorizaciju za ključne operativne poslove u aplikaciji ovjerioca i to na način opisan u ovom poglavlju.

Dvije autorizacije Administratora ovjerioca su potrebne da bi se izvršili sljedeći poslovi, i to:

- Promjena lozinke Administratora ovjerioca,
- Podešavanje broja autorizacija Administratora ovjerioca na jednu autorizaciju,
- Generiranje privatnog kriptografskog ključa aplikacije ovjerioca, odnosno obnova profila ovjerioca,
- Konfiguriranje potvrda aplikacije ovjerioca,
- Opoziv potvrda aplikacije ovjerioca,
- Podešavanje broja autorizacija za *Security Officer*-e na jednu autorizaciju,
- Kreiranje i obnova profila *Security Officer*-a,
- Promjena *hash* algoritma za potvrde.

Dvije *Security Officer* autorizacije potrebne su da bi se izvršili sljedeći poslovi, i to:

- Registriranje korisnika u aplikaciji Ovjerioca UIO,
- Provođenje operacija za promjenu statusa potvrde,
- Podešavanje ili promjena roka važnosti potvrde,
- Podešavanje ili promjena pravila u vezi korištenja potvrde,
- Podešavanje ili promjena administratorskih pravila,
- Kreiranje, promjena ili brisanje korisničkih računa sa ulogom *Security Officer*.

Dvije autorizacije se koriste i za sljedeće poslove:

- Pristup sigurnim kasama,
- Generiranje kriptografskog ključa aplikacije ovjerioca,
- Kreiranje i obnova profila HSM administratora i HSM operatora,
- Promjena zaboravljene lozinke HSM administratora i HSM operatora.

Ostali poslovi koji nisu navedeni u ovoj tački, izvršavaju se uz autorizaciju jednog ovlaštenog lica Ovjerioca UIO.

5.2.3. Identifikacija i autentikacija ovlaštenih lica

Ovjerilac UIO vrši provjeru svojih zaposlenih, prije nego što im dodijeli određene privilegije koje mogu da budu:

- Upis u odgovarajuću pristupnu listu za ulazak u zaštićene prostorije Ovjerioca UIO,
- Identifikacijska beskontaktna kartica za ulazak u sigurnu zonu,
- Identifikacijska beskontaktna kartica za pristup serverskom ormaru,
- Korisnički račun na operativnom sistemu servera i radnim stanica Ovjerioca UIO,

- Administratorske i operatorske kartice za *HSM*,
- Korisnički račun na aplikaciji Ovjerioca UIO,
- Korisnički račun na aplikaciji Registracijskog tijela *CMS*-a i smart kartica sa elektronskom potvrdom za pristup aplikaciji Registracijskog tijela,
- Korisnički račun na aplikaciji Centralnog sistema *CMS*-a za upravljanje i izdavanje kriptografskog uređaja u glavnom uredu i smart kartica sa elektronskom potvrdom za pristup aplikaciji Centralnog sistema *CMS*-a,
- Korisnički račun na *Desktop* aplikaciji *CMS*-a za personalizaciju kriptografskih uređaja i smart kartica sa elektronskom potvrdom za pristup *Desktop* aplikaciji *CMS*-a,
- Korisnički računi, kartice i potvrde iz stava 1. ove tačke kreiraju se posebno za svako ovlašteno lice Ovjerioca UIO.

Zabranjeno je zajedničko korištenje korisničkih računa, kartica ili potvrda između ovlaštenih lica Ovjerioca UIO.

5.2.4. Razgraničenje ovlaštenja ovlaštenih lica

Aktivnosti zaposlenih unutar Ovjerioca UIO ograničene su ovlaštenjima definiranim na nivou:

- Hardverskog kriptografskog uređaja (*HSM*),
- Operativnog sistema servera i radnih stanica,
- Aplikacije Ovjerioca UIO,
- Aplikacije za upravljanje potvrdama i izdavanje potvrda,
- Aplikacije za personalizaciju kriptografskih uređaja,
- Aplikacije Registracijskog tijela.

5.3. Kontrola ovlaštenih lica

Poslove Ovjerioca UIO, u smislu Praktičnih pravila, obavljaju zaposleni koji su u radnom odnosu u UIO. Zaposleni Ovjerioca UIO moraju biti kvalificirani za obavljanje poslova iz ovih Praktičnih pravila i podliježu provjeri stručne sposobnosti.

Zaposleni Ovjerioca UIO ne smiju objavljivati, odnosno saopćavati neovlaštenim licima, povjerljive informacije vezane za sigurnost Ovjerioca UIO ili informacije o korisnicima elektronskih potvrda.

Zaposlenima Ovjerioca UIO ne dodjeljuju se poslovi izvan djelokruga poslova za koje su angažirani, a koji bi mogli da dovedu do sukoba interesa sa ovim poslovima.

Zaposleni Ovjerioca UIO dobijaju od šefa Odsjeka za elektronske potpise i certifikate dokumentaciju s detaljnim opisom procedura kojih su se dužni pridržavati.

5.3.1. Zahtjevi u vezi s kvalifikacijama, iskustvom i provjera ovlaštenih lica

Zaposleni Ovjerioca UIO moraju da zadovolje određene zahtjeve u pogledu stručne kvalifikacije za svako radno mesto na koje se angažiraju, kao i u pogledu radnog iskustva i iskustva na sličnim radnim dužnostima.

Prilikom zapošljavanja uzima se u obzir da lice koje se angažira nije bilo osuđivano za radnje koje su u vezi s poslovima koje obavlja kod Ovjerioca UIO.

5.3.2. Postupci za provjeru prethodnog radnog angažiranja

Provjera prethodnog radnog angažiranja lica za rad kod Ovjerioca UIO vrši se u skladu sa zakonom i propisima iz ove oblasti.

5.3.3. Obuka

Obuka zaposlenih u Ovjeriocu UIO obuhvata:

- Upoznavanje sa infrastrukturom Ovjerioca UIO,
- Upoznavanje s postupcima zaštite infrastrukture i podataka,
- Osposobljavanje za korištenje aplikacija Ovjerioca UIO, u skladu sa dodijeljenom ulogom,
- Osposobljavanje za kreiranje rezervnih kopija podataka,
- Poduzimanje postupaka za oporavak sistema poslije štete,
- Upoznavanje s drugim dužnostima vezanim za rad Ovjerioca UIO.

Za zaposlene koji zaprimaju zahtjeve u regionalnim centrima, obuka uključuje:

- Upoznavanje sa djelatnošću Ovjerioca UIO, vrstama potvrda i zahtjevima za promjenu statusa potvrda,
- Osposobljavanje za korištenje aplikacije Registracijskog tijela,
- Upoznavanje sa drugim dužnostima vezanim za rad Ovjerioca UIO.

Licima koja pohađaju obuku osigurava se odgovarajuća literatura, u skladu sa temom obuke.

5.3.4. Učestalost ponovnih obuka

Zaposleni kod Ovjerioca UIO pohađaju obuke za obnavljanje i usavršavanje znanja najmanje jednom godišnje, a vanredno kada se izvrše promjene tehničkih sredstava (hardvera i softvera) Ovjerioca UIO i način obavljanja djelatnosti.

5.3.5. Učestalost i redoslijed rotacije poslova ovlaštenih lica

Ovjerilac UIO nije ustanovio pravila rotacije poslova, kako ne bi došlo do narušavanja pravila vršenja različitih ovlaštenja i dužnosti, u svezi sa različitim povjerljivim ulogama zaposlenih u Ovjeriocu UIO.

5.3.6. Sankcije za neautorizirane aktivnosti

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.

5.3.7. Zahtjevi za vanjske saradnike

U slučaju da se dodijeli povjerljiva uloga vanjskom saradniku, za to lice važe isti uvjeti kao za stalno zaposlena lica Ovjerioca UIO.

5.3.8. Dokumentacija za potrebe zaposlenih

Zaposlenima se daje odgovarajuća dokumentacija s detaljnim opisom procedura kojih se moraju pridržavati.

5.4. Procedure nadgledanja rada sistema

Događaji koji se odnose na obavljanje djelatnosti Ovjerioca UIO zapisuju se u elektronske dnevnike (*audit log*) i evidencije koje se ručno vode, s datumom i vremenom događanja.

5.4.1. Vrste događaja koji se evidentiraju

Događaji koji se evidentiraju su u vezi sa:

- Izdavanjem potvrde ovjerioca *UINO Root CA* i potvrda njemu podređenih ovjerilaca,
- Izdavanjem potvrda za potpis odgovora *OCSP* servisa,
- Upravljanjem životnim ciklusom ključeva ovjerioca *UINO Root CA* i ključeva povezanih s potvrdom za *OCSP* servis,
- Upravljanjem životnim ciklusom harderskog kriptografskog uređaja,
- Opozivanjem potvrda koje izdaje ovjerilac *UINO Root CA*,
- Korisničkim kriptografskim ključevima i elektronskim potvrdama: izdavanje, preuzimanje, opoziv, suspenzija, prekid suspenzije, deaktiviranje, arhiviranje i drugi,
- Kriptografskim ključevima aplikacije ovjerioca,
- Tehničkim sredstvima (hardver i softver) Ovjerioca UIO,
- Administracijom, kreiranjem rezervnih kopija, sigurnosnim pravilima i korištenjem aplikacija ovjerioca,
- Fizičkim pristupom sistemu Ovjerioca UIO, uspješni i neuspješni pristup sistemu Ovjerioca UIO,
- Pokretanjem i zaustavljanjem servisa Ovjerioca UIO,
- Podizanjem i spuštanjem sistema, kvar hardvera,

- Kadrovskim promjenama u okviru Ovjerioca UIO.

5.4.2. Učestalost pregleda elektronskih dnevnika i ručnih evidencija

Ovlašteni administratori Ovjerioca UIO pregledaju elektronske dnevnike i ručne evidencije jednom sedmično.

Pod pregledom podrazumijeva se:

- Prikupljanje svih elektronskih dnevnika i ručnih evidencija od posljednjeg pregleda,
- Pregled i analiza zapisa u elektronskim dnevnicima i ručnim evidencijama,
- Razrješavanje eventualnih problema ili prijava šefu Odsjeka za elektronske potpise i certifikate, koji preuzima daljnje korake u cilju rješavanja problema.

5.4.3. Vrijeme čuvanja evidencija

Kopije elektronskih dnevnika i ručnih evidencija se čuvaju najmanje 10 godina.

5.4.4. Zaštita elektronskih dnevnika

Elektronski dnevnici i ručne evidencije štite se mehanizmima i postupcima koji osiguravaju povjerljivost i integritet dnevnika.

Novi zapisi elektronskih dnevnika i ručnih evidencija sistema ne smiju se automatski zapisivati preko postojećih zapisa.

Tako zaštićeni elektronski dnevnici i ručne evidencije sistema su na zahtjev raspoloživi samo ovlaštenim licima.

5.4.5. Kreiranje rezervnih kopija elektronskih dnevnika

Elektronski dnevnici svakodnevno se ažuriraju. Za kreiranje rezervnih kopija zadužena su ovlaštena lica Ovjerioca UIO. Rezervne kopije elektronskih dnevnika čuvaju se u glavnom uredu UIO.

5.4.6. Sistem prikupljanja podataka za elektronske dnevnike i ručne evidencije

Sistem prikupljanja podataka za elektronske dnevnike i ručne evidencije svih sistema u Ovjeriocu UIO je interni sistem koji je kombinacija automatskih i ručnih procesa koji se izvode na serverima Ovjerioca UIO i koje pokreće, odnosno nadgleda zaposlene Ovjerioca UIO s povjerljivim ulogama.

DOGAĐAJI KOJI SE ZAPISUJU U ELEKTRONSKE DNEVNIKE I RUČNE EVIDENCIJE	NAČIN PRIKUPLJANJA PODATAKA	ODGOVORNO LICE ILI SISTEM
Događaji povezani sa elektronskim potvrdama	automatsko	aplikacija Ovjerioca UIO
Registar izdatih elektronskih potvrda	automatsko, ručno	aplikacija Ovjerioca UIO, zaposleni Ovjerioca UIO
Događaji povezani sa aplikacijama Ovjerioca UIO	automatsko	aplikacije Ovjerioca UIO
Događaji na operativnom sistemu	automatsko	operativni sistem
Događaji na računarskoj mreži	automatsko	*firewall*-i, operativni sistem
Kreiranje rezervnih kopija i obnova baze korisnika elektronskih potvrda	automatsko, ručno	operativni sistem, aplikacija Ovjerioca UIO, zaposleni Ovjerioca UIO
Kreiranje rezervnih kopija konfiguracije i obnova logova PKI infrastrukture Ovjerioca UIO	automatsko, ručno	operativni sistem, aplikacija Ovjerioca UIO
Fizički pristup do PKI infrastrukture Ovjerioca UIO	ručno, automatsko	zaposleni Ovjerioca UIO, sistem za kontrolu pristupa
Pristup sefu u kome su smještene administratorske i operatorske kartice HSM uređaja	ručno	zaposleni Ovjerioca UIO
Pristup sefu u kome su smještene lozinke administratorskih računa servera PKI okruženja, lozinke administratorskih i operatorskih kartica HSM uređaja, lozinke za pristup aplikacijama UIO Ovjerioca	ručno	zaposleni Ovjerioca UIO
Promjene hardvera i softvera na sistemu	ručno	zaposleni Ovjerioca UIO
Održavanje rada na sistemu i prostoru	ručno	zaposleni Ovjerioca UIO
Kadrovske promjene	ručno	zaposleni Ovjerioca UIO

Tabela 24. Događaji koji se zapisuju u elektronske dnevnike i ručne evidencije i načini prikupljanja zapisa o tim događajima

5.4.7. Obavještavanje o incidentnom događaju

O incidentnom događaju se obavještava šef Odsjeka za elektronske potpise i certifikate. Lice koje je izazvalo događaj se ne obavještava.

Ovjerilac UIO djeluje blagovremeno i koordinirano kako bi brzo reagirao na incidente i ograničio uticaj kršenja sigurnosti.

Definirani su zaposleni čija uloga je da prate upozorenja o potencijalno kritičnim sigurnosnim događajima i koje treba osigurati da se prijavljuju relevantni incidenti u skladu s procedurama standarda ISO/IEC 27001.

Ovjerilac UIO izvještava nadležno tijelo u skladu s primjenjivim regulatornim pravilima o bilo kojem kršenju sigurnosti ili gubitku integriteta u roku od 24 sata od utvrđivanja kršenja.

Ako povreda sigurnosti ili gubitak integriteta može negativno uticati na fizičko ili pravno lice kojem je pružena pouzdana usluga, također se obavještava i fizičko ili pravno lice o kršenju sigurnosti ili gubitku integriteta bez nepotrebnog odgađanja.

Svaka kritična ranjivost koju ovjerilac UIO prethodno nije riješio rješava se u roku od 48 sati nakon otkrića.

5.4.8. Procjena ranjivosti sistema

Procjena ranjivosti sistema se vrši u sklopu svakodnevnih aktivnosti koje se provode na sistemu, analizama rizika, razmjenom iskustava sa ovjeriocima iz okruženja i pregledom elektronskih dnevnika i ručnih evidencija.

5.5. Arhiviranje podataka

5.5.1. Vrste podataka koji se arhiviraju

Ovjerilac UIO arhivira sljedeće podatke i dokumenta:

- Elektronske dnevnike,
- Ugovore i dokumentaciju korisnika,
- Zahtjeve za izdavanje i korištenje elektronske potvrde,
- Zahtjeve za promjenu statusa elektronske potvrde (opoziv, suspenzija, prekid suspenzije i drugo),
- Elektronske potvrde,
- Registre opozvanih potvrda,
- Interne akte Ovjerioca UIO vezane za obavljanje djelatnosti Ovjerioca UIO.

5.5.2. Period čuvanja podataka u arhivi

Ovjerilac osigurava trajno čuvanje svih relevantnih podataka koji se tiču elektronskih potvrda, u skladu sa važećim propisima.

5.5.3. Zaštita arhive

Arhiva dokumenata se čuva na centralnoj lokaciji Ovjerioca UIO (Središnji ured UIO) i u uredima Registracijskog tijela.

Arhiva je zaštićena s odgovarajućim sigurnosnim mehanizmima Ovjerioca UIO (fizičko-tehničkom zaštitom i nadzorom, ograničenim pristupom, šiframa i ključevima). Pristup arhivama dozvoljen je samo ovlaštenim licima.

Ovjerilac UIO osigurava tajnost tekućih i arhiviranih zapisa o elektronskim potvrdama.

5.5.4. Procedure arhiviranja

Papirni dokumenti arhiviraju se na centralnoj lokaciji Ovjerioca UIO (Središnji ured UIO) i u uredima Registracijskog tijela.

Ovjerilac UIO svakodnevno radi arhiviranja izrađuje kopije elektronskih dnevnika i podataka.

5.5.5. Vremenska oznaka arhiviranih podataka

Arhivirani podaci nose vremensku oznaku sa servera koji je sinhroniziran s izvorom tačnog vremena.

5.5.6. Sistem arhiviranja (interni ili eksterni)

Ovjerilac UIO koristi kombinirani sistem arhiviranja (interni i eksterni). Arhiviranje elektronskih podataka izvršava zaposleni u Ovjeriocu UIO, tehničkim sredstvima za arhiviranje koja su u vlasništvu Ovjerioca UIO.

5.5.7. Procedure kontrole pristupa arhiviranim podacima

Arhivirani elektronski podaci čuvaju se u kasama-kontejnerima za čije otvaranje su potrebna dva ključa. Kase-kontejneri se nalaze u zaštićenim prostorijama. Prostorije su sa restriktivnim i autoriziranim pristupom.

5.6. Generiranje novih ključeva ovjerioca

Generiranje novih ključeva Ovjerioca UIO vrši se pet godina prije isteka roka važnosti postojećih ključeva. Generiranje ključeva moguće je provesti i ranije, iz sljedećih razloga:

- Potrebno je promijeniti kriptografski algoritam kojim ovjerilac potpisuje potvrde i registre opozvanih potvrda,
- Potrebno je promijeniti dužinu ključeva ovjerioca,
- Potrebno je promijeniti rok važnosti ključeva ovjerioca,
- Potrebno je promijeniti *hash* algoritam ovjerioca, primjenom koga se izračunava *hash* vrijednost potvrde i registra opozvanih potvrda,
- Potrebno je promijeniti sadržaj postojećih polja ili ekstenzija potvrde ovjerioca ili dodati nove ekstenzije potvrdi ovjerioca,
- Privatni ključ ovjerioca je oštećen ili je kompromitiran.

5.7. Oporavak sistema poslije katastrofe

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

Procedure se obnavljaju u skladu s planom kontinuiteta nakon rješavanja bilo kojeg uzroka katastrofe koji se može ponoviti (npr. sigurnosna ranjivost) i odgovarajućim mjerama sanacije u skladu sa standardom ISO 22301.

5.7.1. Procedure rada u slučaju katastrofe ili prilikom kompromitiranja sistema

Ovjerilac UIO ima planove za očuvanje i oporavak sistema ovjeravanja nakon katastrofe. Internim planovima obuhvaćeni su postupci očuvanja i oporavka sistema za slučaj katastrofe uzrokovane kvarom opreme, ljudskom pogreškom, otuđenjem ili kompromitiranjem opreme i podataka, požarom, prirodnom katastrofom, terorističkim činom, i sl.

Internim planovima obuhvaćeni su i postupci koje treba poduzeti u cilju oporavka i uspostave prvobitnih sigurnosnih prilika sistema ovjerioca.

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

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

U slučaju uništenja ili oštećenja privatnog kriptografskog ključa aplikacije ovjerioca, poslije otklanjanja uzroka uništenja ili oštećenja provodi se postupak rekonstruiranja ključa.

5.7.3. Kompromitiranje privatnog kriptografskog ključa aplikacije ovjerioca

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.

Ovjerilac UIO će u slučaju kompromitiranja privatnog kriptografskog ključa aplikacije ovjerioca, poslije otklanjanja uzroka kompromitiranja:

- Generirati nove kriptografske ključeve aplikacije ovjerioca,
- Izdati korisnicima nove elektronske potvrde.

5.7.4. Nastavak rada poslije katastrofe

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

5.8. Prestanak rada ovjerioca

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.

Ovjerilac UIO će o planiranom prestanku obavljanja poslova vezanih za elektronski potpis i ovjeravanje obavijestiti svoje korisnike i nadležni državni organ u skladu sa važećim propisima.

Ovjerilac UIO će poduzeti sve što mogućnosti u datom trenutku budu dozvoljavale, kako bi osigurao nastavak obavljanja usluge kod drugog ovjerioca za svoje korisnike.

Ovjerilac UIO ima obvezu da ovjeriocu, kod koga je osigurao nastavak pružanja usluge prema svojim korisnicima, dostavi svu postojeću dokumentaciju i arhivu, koja se odnosi na obavljanje usluge vezane za elektronski potpis i ovjeravanje.

Ako se ne postigne prijenos obaveza na drugog ovjerioca, Ovjerilac UIO ima obavezu da svu postojeću dokumentaciju i arhivu, koja se odnosi na obavljanje usluga vezanih za elektronski potpis i ovjeravanje dostavi nadležnom državnom organu.

Ukoliko nema mogućnosti za prijenos obaveza pružanja usluge vezane za elektronski potpis i ovjeravanje na drugog ovjerioca, Ovjerilac UIO će raskinuti ugovore o izdavanju i korištenju elektronskih potvrda sa svojim korisnicima i opozvati sve važeće elektronske potvrde, o čemu će obavijestiti korisnike i nadležni državni organ.

Ovjerilac UIO će elektronskom poštom obavijestiti korisnike elektronskih potvrda i ovjerioce priznate od strane Ovjerioca UIO, odnosno ovjerioce koji priznaju Ovjerioca UIO kao ovjerioca, o prestanku rada u skladu sa važećim propisima.

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

6.1. Generiranje para kriptografskih ključeva i instalacija

6.1.1. Generiranje para kriptografskih ključeva

Ovjerilac UIO održava aplikacije ovjerioca koje izvršavaju *UINO Root CA, UINO Issuing CA1* i *UINO Issuing CA2*, a parovi njihovih kriptografskih ključeva su generirani tokom procesa ceremonije generiranja ključeva (eng. *Key Generation Ceremony*) po precizno definiranoj proceduri. 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.

U Ceremoniji generiranja ključeva učestvovala su ovlaštena lica Ovjerioca UIO sa povjerljivim ulogama i revizor koji svjedoči da je Ceremonija generiranja parova ključeva izvršena u skladu sa dokumentom Uprave za indirektno oporezivanje Ceremonija generiranja kriptografskih ključeva UIO koja služi kao protokol za generiranje ključeva u kome su dokumentirani koraci koji se izvode prilikom pomenute ceremonije.

Revizor potpisuje ovaj dokument na kraju ceremonije i time svjedoči da je postupak generiranja parova ključeva proveden u skladu sa protokolom.

U dokument se potpisuju sva lica koja su učestvovala u ceremoniji generiranja ključeva.

Par kriptografskih ključeva korisnika za potpisivanje i verificiranje kvalificiranog elektronskog potpisa generira se na *SSCD* uređaju, koji predstavlja sredstvo za formiranje kvalificiranog elektronskog potpisa. Par kriptografskih ključeva povezan sa korisničkom potvrdom za kreiranje kvalificiranog elektronskog potpisa se nikada ne smješta na hardversku ili softversku opremu Ovjerioca UIO.

6.1.2. Uručenje privatnog kriptografskog ključa korisniku

Uručenje privatnog ključa korisniku vrši se uručivanjem *SSCD* uređaja u prostorijama Ovjerioca UIO, u sjedištu ili u regionalnom centru UIO.

6.1.3. Dostavljanje javnog kriptografskog ključa korisnika ovjeriocu

Korisnički kriptografski javni ključ potvrde za izradu kvalificiranog elektronskog potpisa se zajedno sa privatnim ključem generira u Ovjeriocu UIO na *SSCD* uređaju i nema potrebe da korisnik dostavlja javni kriptografski ključ ovjeriocu.

Korisnički kriptografski javni ključ potvrde u obliku datoteke PKCS#12 formata se zajedno sa privatnim ključem generira u Ovjeriocu UIO i nema potrebe da korisnik dostavlja javni kriptografski ključ ovjeriocu.

Kriptografski javni ključ potvrde za autentikaciju *Web* stranica se dostavlja Ovjeriocu UIO u obliku datoteke PKCS#10 formata i podvrgava se temeljnoj provjeri prije izdavanja odgovarajuće potvrde.

6.1.4. Uručenje javnog kriptografskog ključa trećim licima

Javni kriptografski ključ aplikacije ovjerioca u formi potvrde je javno dostupan i na *Web* stranici Ovjerioca UIO.

Korisničke javne kriptografske ključeve i potvrde Ovjerilac UIO javno ne objavljuje niti uručuje trećim licima.

6.1.5. Dužine kriptografskih ključeva

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.

6.1.6. Generiranje parametara javnog kriptografskog ključa i provjera kvaliteta

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.

Odgovorno lice Ovjerioca UIO zadaje parametre javnih ključeva aplikacije ovjerioca i korisnika, kao što je navedeno u definicijama profila potvrda.

6.1.7. Namjena ključa

Za potpisivanje elektronskih potvrda, potvrda za servis Ovjerioca UIO za izdavanje vremenskih žigova, pripadajućeg registra opozvanih potvrda i potpis odgovora *OCSP* servisa upotrebljava se isključivo privatni kriptografski ključ aplikacije ovjerioca kojeg održava Ovjerilac UIO.

Javni kriptografski ključ aplikacije ovjerioca upotrebljava se za validaciju elektronskog potpisa elektronske potvrde i registra opozvanih potvrda (*Key Usage = Certificate Signing, Off-line CRL Signing, CRL Signing*).

Privatni ključevi potvrde UIO *OCSP* servisa namijenjeni su samo za potpisivanje odgovora UIO OCSP servisa (*Key Usage = digitalSignature, nonRepudiation, extKeyUsage = OCSPSigning).*

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

Vrsta potvrda	Sadržaj ekstenzije *Key Usage*
Kvalificirane elektronske potvrde Ovjerioca UIO	*Certificate Signing, Off-line CRL Signing, CRL Signing*
Kvalificirana elektronska potvrda za elektronski potpis na smart kartici	*Non-Repudiation*
Kvalificirana elektronska potvrda za elektronski pečat na smart kartici	*Digital Signature*
Potvrda za UIO OCSP servis	*Key Usage = digitalSignature, nonRepudiation, extKeyUsage = OCSPSigning*
Kvalificirana elektronska potvrda za elektronski vremenski žig	*Key Usage = digitalSignature, nonRepudiation, extKeyUsage = timeStamping*

Tabela 25. Sadržaj ekstenzije *Key Usage* u kvalificiranim elektronskim potvrdama koje izdaje Ovjerilac UIO

6.2. Zaštita privatnog kriptografskog ključa

6.2.1. Standardi za hardverski kriptografski modul

Sve operacije za generiranje kriptografskih ključeva i potpisivanje potvrda Ovjerioca UIO vrše se na hardverskom kriptografskom modulu, koji zadovoljava sigurnosne standarde ISO/IEC 15408 (Common Criteria) EAL4+.

Kvalificirano sredstvo za kreiranje elektronskog potpisa i pečata korisnika zadovoljava standard EAL4+.

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

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.

Pristup korisničkom privatnom kriptografskom ključu ograničen je samo na korisnika.

6.2.3. Otkrivanje privatnog kriptografskog ključa

Ovjerilac UIO ne nudi mogućnost otkrivanja privatnog kriptografskog ključa.

6.2.4. Kreiranje kopije privatnog kriptografskog ključa

Poslije generiranja kriptografskih ključeva aplikacije ovjerioca, uz prisutnost ovlaštenih lica Ovjerioca UIO, kreira se kopija privatnog kriptografskog ključa aplikacije ovjerioca. Privatni kriptografski ključ aplikacije ovjerioca je šifriran *AES* (*Rijndael*) algoritmom i nikad se ne

nalazi izvan hardverskog kriptografskog modula u dešifriranom obliku. Dešifriranje privatnog kriptografskog ključa je moguće samo u hardverskom kriptografskom modulu, na osnovu kopije privatnog kriptografskog ključa, uz pomoć dvije administratorske smart kartice za pristup hardverskom kriptografskom modulu i njihovih lozinki.

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

6.2.5. Arhiviranje privatnog kriptografskog ključa

Ovjerilac UIO arhivira kopiju privatnog kriptografskog ključa aplikacije ovjerioca poslije njegovog kreiranja, na lokaciji Ovjerioca UIO i drugoj udaljenoj lokaciji, u zaštićenim prostorijama u kasama-kontejnerima za dugotrajno čuvanje.

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

6.2.6. Prebacivanje privatnog ključa u kriptografski modul ili iz njega

Privatni kriptografski ključ aplikacije ovjerioca je generiran u hardverskom kriptografskom modulu. Samo ukoliko nastupi hardverski kvar hardverskog kriptografskog modula aplikacije ovjerioca, on će biti zamijenjen drugim modulom, a privatni ključ prebačen (importiran) u taj modul, uz pisanu odluku odgovornog lica Ovjerioca UIO i uz višestruku autorizaciju zaposlenih Ovjerioca UIO.

Privatni kriptografski ključ povezan sa kvalificiranom elektronskom potvrdom korisnika je generiran u hardverskom kriptografskom *SSCD* uređaju i ne eksportuje se.

6.2.7. Čuvanje privatnog kriptografskog ključa u kriptografskom modulu

Kriptografski ključevi se čuvaju u kriptografskim modulima i mogu da se koriste samo ukoliko su na pravilan način aktivirani.

6.2.8. Postupak za aktiviranje privatnog kriptografskog ključa

Za rekonstrukciju i aktiviranje privatnog kriptografskog ključa aplikacije ovjerioca potrebna je autorizacija dva *HSM* administratora sa svojim karticama i lozinkama i dva *HSM* operatera sa svojom karticom i lozinkom. Privatni kriptografski ključ aplikacije ovjerioca se aktivira poslije startovanja aplikacije ovjerioca.

Korisnički privatni kriptografski ključevi se aktiviraju poslije uspješne autentikacije korisnika sa lozinkom u korisničkoj aplikaciji prilikom elektronskog potpisivanja ili pečatiranja.

6.2.9. Postupak za deaktiviranje privatnog kriptografskog ključa

Privatni kriptografski ključ aplikacije ovjerioca se deaktivira zaustavljanjem aplikacije ovjerioca i deaktiviranjem *HSM*-a.

Korisničke aplikacije deaktiviraju privatni kriptografski ključ poslije elektronskog potpisivanja i izvlačenja smart kartice iz čitača kartica, ili istekom vremena korisničke sesije.

6.2.10. Postupak za uništavanje privatnog kriptografskog ključa

Privatni kriptografski ključ aplikacije ovjerioca se uništava samo u slučaju planiranog prestanka rada ovjerioca, a što se provodi samo uz pisanu odluku odgovornog lica Ovjerioca UIO.

Privatni kriptografski ključ korisnika se uništava ukoliko ga korisnik obriše sa smart kartice, fizički ošteti smart karticu.

6.2.11. Klasificiranje kriptografskih modula

Standard za kriptografske module prema kojima može da se vrši njihovo klasificiranje je ISO/IEC 15408 EAL, i navedeni su u tački 6.2.1.

6.3. Ostali aspekti administriranja nad parom kriptografskih ključeva

6.3.1. Arhiviranje javnog kriptografskog ključa

Ovjerilac UIO arhivira javni kriptografski ključ aplikacije ovjerioca i javne kriptografske ključeve korisnika.

6.3.2. Rok važnosti potvrda i kriptografskih ključeva

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.

6.4. Podaci za aktiviranje

6.4.1. Generiranje i upotreba podataka za aktiviranje

Podaci za aktiviranje privatnog ključa aplikacije ovjerioca generiraju se prilikom generiranja kriptografskih ključeva i mogu da ih koriste isključivo ovlaštena lica Ovjerioca UIO.

Lozinku za aktiviranje privatnog ključa (*PIN* kod) korisnika generira generator lozinki. Lozinka ima četiri ili više numeričkih karaktera. Korisnik ima mogućnost promjene lozinke i njene dužine.

Ukoliko korisnik uzastopno pet puta unese pogrešnu lozinku (*PIN* kod), dolazi do zaključavanja smart kartice. Smart karticu je moguće otključati sa *PUK* kodom koji se korisniku dostavlja zajedno sa lozinkom (*PIN* kodom) u zatvorenoj koverti.

6.4.2. Zaštita podataka za aktiviranje

Ovlaštena lica Ovjerioca UIO su dužna da čuvaju lozinke koje se koriste za aktiviranje ključeva.

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

6.4.3. Ostali vidovi podataka za aktiviranje

Ne postoje.

6.5. Sigurnosni zahtjevi za rad

Osjetljivi podaci moraju biti zaštićeni od otkrivanja ponovnim korištenjem objekata za pohranu (npr. izbrisanih datoteka) dostupnim neovlaštenim korisnicima.

Integritet svih sistema i informacija zaštićen je od virusa, zlonamjernog i neovlaštenog softvera.

6.5.1. Sigurnosne zakrpe

Sigurnosne zakrpe primjenjuju se u razumnom roku nakon što postanu dostupne (30 dana).

Sigurnosne zakrpe ne primjenjuju se ako uvode dodatne ranjivosti ili nestabilnosti koje nadmašuju prednosti njihove primjene. Svi razlozi zbog kojih se ne primjenjuju sigurnosne zakrpe su dokumentirani.

6.6. Sigurnosni zahtjevi za računare

6.6.1. Specifični računarski tehničko-sigurnosni zahtjevi

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.

Da bi se otkrili, zabilježili i spriječili pokušaji nedozvoljenog pristupa resursima sistema, Ovjerilac UIO kontinuirano prati sistem.

6.6.2. Nivo zaštite računara

Operativni sistem na serverima Ovjerioca UIO je u skladu sa standardom zaštite ISO/IEC 15408 EAL4+, kako bi se omogućio siguran rad aplikacije Ovjerioca UIO.

6.7. Tehnički nadzor tokom obavljanja djelatnosti

6.7.1. Razvoj sistema

Ovjerilac UIO koristi i oslanja se na aplikaciju ovjerioca, koja je razvijena po strogim kriterijima standarda ISO/IEC 15408 i certificirana prema razini EAL4+. Dodatni softver (CMS) koji se koristi prilikom pružanja usluge izdavanja elektronske potvrde je od pouzdane firme i sve nove verzije softvera se testiraju na testnom okruženju prije nego što se implementiraju na produkcijskom okruženju.

6.7.2. Upravljanje sigurnošću

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.

6.7.3. Nadzor sigurnosti tokom upotrebe sistema

Sigurnosna kontrola se periodično izvršava provjeravanjem rada komponenata Ovjerioca UIO.

6.8. Nadzor sigurnosti računarske mreže

Ovjerilac UIO štiti mrežu i sisteme od napada, segmentira svoje sisteme u mreže ili zone temeljene na procjeni rizika uzimajući u obzir funkcionalni, logički i fizički (uključujući lokaciju) odnos između pouzdanih sistema i usluga. Iste sigurnosne kontrole primjenjuju se na sve sisteme u istoj zoni.

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.

Razdvaja se namjenska mreža za administraciju IT sistema i operativna mreža Ovjerioca UIO.

Razdvajaju se proizvodni sistemi za usluge od sistema koji se koriste u razvoju i ispitivanju (npr. Sistemi za razvoj, testiranje i postupno postavljanje).

Uspostavlja se komunikaciju između različitih pouzdanih sistema samo putem pouzdanih kanala koji se logično razlikuju od ostalih komunikacijskih kanala i pružaju sigurnost identifikacije njegovih krajnjih tačaka i zaštita podataka kanala od modifikacije ili otkrivanja. Ako je potreban visok nivo dostupnosti vanjskog pristupa povjerljivoj usluzi, vanjska mrežna veza bit će redudantna kako bi se osigurala dostupnost usluga u slučaju kvara jedne mrežne veze.

Provodi se redovno skeniranje (svakih 90 dana) ranjivosti na javnim i privatnim IP adresama i bilježe dokazi da je svako skeniranje ranjivosti izvršilo lice ili entitet koji posjeduje vještine, alate, stručnost, etički kodeks i neovisnost potrebne za pružanje pouzdanog izvještaja.

Provodi se redovan (jedanput svake godine ili pri postavljanju i nakon nadogradnje/izmjene infrastrukture ili aplikacije za koje ovjerilac UIO utvrđuje da su značajne) test prodora (*penetration test*). Bilježe se dokazi da je svaki prodorni test provelo lice ili subjekt s vještinama, alatima, poznavanjem, etičkim kodeksom i neovisnošću potrebnim za pružanje pouzdanog izvještaja.

6.9. Vremenska oznaka

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

7.1. Profil potvrde

7.1.1. Verzija potvrde

Ovjerilac UIO izdaje potvrde sukladne specifikaciji *X.509* verzije 3. Profil kvalificirane elektronske potvrde u skladu je sa standardima navedenim na početku ovog dokumenta.

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

Potvrde Ovjerioca UIO sadrže osnovna polja *X.509* potvrde (tabela 26).

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

Tabela 26. Osnovna polja *X.509* potvrde

7.1.2. Ekstenzije potvrde

Nazivi ekstenzija *X.509* potvrda koje aplikacija ovjerioca upisuje u kvalificirane elektronske potvrde i njihov opis dati su u sljedećoj tabeli (tabela 27).

NAZIV POLJA - EKSTENZIJE	OPIS POLJA - EKSTENZIJE
Enhanced Key Usage (EKU)	Pokazuje da se javni ključ može koristiti za jednu ili više svrha (proširena mogućnost korištenja ključa).
Authority Information Access	Adresa potvrde „UIO IssuingCA1“ ili „UIO IssuingCA2“ servera i URI OCSP servisa.
Certificate Policies	Identifikacija CPS-a i adresa *Web* stranice na kojoj se nalaze ova Praktična pravila.
Subject Alternative Name	Alternativna imena korisnika (*e-mail*, itd).
CRL Distribution Points	Lokacija na kojoj se nalaze registri opozvanih potvrda.
Authority Key Identifier	Identifikator javnog kriptografskog ključa ovjerioca.
Subject Key Identifier	Identifikator javnog kriptografskog ključa korisnika potvrde.
Key Usage	Namjena javnog kriptografskog ključa korisnika kvalificirane elektronske potvrde.
Basic Constraints	Oznaka koja ukazuje na vrstu potvrde (potvrda ovjerioca ili korisnička potvrda).
Qualified Certificate Statements	Oznaka da je potvrda izdana kao kvalificirana elektronska potvrda.

Tabela 27. Ekstenzije *X.509* potvrde

7.1.3. Identifikacijska oznaka algoritma

Ovjerilac UIO potpisuje kvalificirane elektronske potvrde i registre opozvanih potvrda primjenom algoritma *SHA512RSA* (*OID* 1.2.840.113549.1.1.13) u skladu sa 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).*

7.1.4. Forme imena

Potvrde *UINO Root CA* i potvrde njemu podređenih ovjerilaca (*UINO Issuing CA1* i *UINO Issuing CA2*) u poljima Issuer i Subject sadrže puno razlikovno ime (eng. *Distinguished name*) izdavaoca potvrde.

U elektronskim potvrdama koje izdaje Ovjerilac UIO, ime Ovjerioca UIO koje je navedeno u polju *Issuer* i ime korisnika potvrde koje je navedeno u polju *Subject* su jedinstvena imena (eng. *Distinguished Name – DN*). Na ime korisnika (eng. *Common Name – CN*) u elektronskoj potvrdi se primjenjuje *UTF8 String* kodiranje.

7.1.5. Ograničenja u imenima

Specijalni znaci čije korištenje u imenima nije dozvoljeno su: ? (upitnik), \ (*backslash*), # (ljestve), $ (dolar), % (postotak), = (jednako), + (plus), | (uspravna crta), ; (tačka-zarez), < (manje), > (veće) i , (zarez). Iste je potrebno izostaviti ili zamijeniti drugim znacima.

7.1.6. Identifikacijska oznaka politike ovjeravanja

Sve potvrde izdane od strane Ovjerioca UIO sadrže *OID* politike ovjeravanja na osnovu koje je izdana potvrda. *OID* za svaku politiku ovjeravanja definiran je u poglavljima 1.1.1 i 1.2.

7.1.7. Upotreba ekstenzije za razdvajanje politika

Ne koristi se.

7.1.8. Kvalifikatori politike ovjeravanja

Ovjerilac UIO koristi potpolje *Policy Qualifier=CPS* ekstenzije *Certificate Policies* potvrde, u kojem objavljuje adresu *Web* stranice na kojoj se nalaze ova Praktična pravila i drugi akti Ovjerioca UIO.

7.1.9. Procesiranje kritičnih ekstenzija potvrda

Korisničke aplikacije moraju da procesuiraju ekstenzije potvrda koje su označene kao kritične (eng. *critical*).

7.2. Profil registra opozvanih potvrda

7.2.1. Verzija registra opozvanih potvrda

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*. Registri opozvanih

potvrda Ovjerioca UIO sadrže osnovna polja *X.509* registra (tabela 28) i ekstenzije *X.509* registra (tabela 29).

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

Tabela 28. Osnovna polja *X.509* registra opozvanih potvrda

7.2.2. Ekstenzije registra opozvanih potvrda

Nazivi ekstenzija *X.509* registra opozvanih potvrda koje aplikacija ovjerioca upisuje u registre i njihov opis dati su u sljedećoj tabeli (tabela 29).

NAZIV EKSTENZIJE	OPIS EKSTENZIJE
Authority Key Identifier	Identifikator javnog kriptografskog ključa ovjerioca.
CRL Number	Redni broj registra opozvanih potvrda (*OID* 2.5.29.20).

Reason Code	Razlog opoziva potvrde. Mogući razlozi opoziva potvrda (prema dokumentu *RFC* 5280) su: - *unspecified (0),* - *keyCompromise (1),* - *cACompromise (2),* - *affiliationChanged (3),* - *superseded (4),* - *cessationOfOperation (5),* - *certificateHold (6),* - *removeFromCRL (8),* - *privilegeWithdrawn* (9), - *aACompromise*(10).
Expired Certs On CRL	CRL koja sadrži ovu extenziju uključivat će informacije o statusu opoziva za potvrde koje su već istekle.
Invalidity Date	Datum kompromitiranja ili sumnje u kompromitiranje privatnog kriptografskog ključa ili datum kada je elektronska potvrda na neki drugi način prestala da bude važeća (*OID* 2.5.29.24).

Tabela 29. Ekstenzije *X.509* registra opozvanih potvrda

7.3. OCSP profil

Ovjerilac UIO omogućava internetsku provjeru statusa opoziva izdanih potvrda putem *OCSP* servisa čiji je rad usklađen s dokumentom IETF RFC 6960.

Podaci o statusu opoziva potvrda putem *OCSP* servisa dostupni su u stvarnom vremenu.

7.3.1. Verzija OCSP-a

Profil odgovora *OCSP* servisa Ovjerioca UIO sukladan je verziji 1 prema dokumentu IETF *RFC* 6960.

7.3.2. OCSP ekstenzije

Ekstenzije odgovora OCSP servisa Ovjerioca UIO prikazane su u tabeli 30.

NAZIV EKSTENZIJE	KRITIČNO	OPIS
Nonce	NE	Vrijednost nonce-a iz zahtijeva za statusom potvrde.
Extended Revoked Definition	NE	Kod razloga opoziva potvrde (eng. *reason code*).

Tabela 30. Ekstenzije odgovora OCSP servisa Ovjerioca UIO

8. REVIZIJA USKLAĐENOSTI RADA OVJERIOCA UIO I DRUGE PROCJENE

Ovjerilac UIO izvršava redovne unutarnje revizije rada (*internal audit*).

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

8.1. Učestalost revizije i analiza rizika

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.

8.2. Kvalifikacija lica koje vrši reviziju

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.

8.3. Odnos lica koje vrši reviziju prema predmetu revizije

Lice koje vrši reviziju postupa u skladu sa važećim propisima i međunarodnim standardima. Reviziju može vršiti lice zaposleno u Ovjeriocu UIO ili vanjsko stručno lice.

8.4. Sadržaj revizije

U okviru unutarnje revizije provjeravaju se:

- Sadržaj Politike ovjeravanja,
- Sadržaj Praktičnih pravila,

- Sukladnost obavljanja djelatnosti Ovjerioca UIO važećim propisima, Politikom ovjeravanja, Praktičnim pravilima i internim aktima (vezanim za procedure pristupa prostorijama Ovjerioca UIO, upravljanja aplikacijom Ovjerioca UIO, objavljivanja registra opozvanih potvrda, kreiranja rezervnih kopija i drugim internim aktima),
- Tehnički procesi i procedure,
- Fizička sigurnost,
- Primijenjene mjere informacione sigurnosti.

8.5. Poduzete aktivnosti kao rezultat utvrđenih nedostataka

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

8.6. Objavljivanje izvještaja revizije

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

9.1. Cjenovnik

Ovjerilac UIO objavljuje cjenovnik za izdavanje elektronskih potvrda na svojoj *Web* stranici.

Svaka promjena cijena izdavanja elektronskih potvrda objavljuje se na *Web* stranici Ovjerioca UIO i bit će dostupna svim zainteresiranim licima.

9.1.1. Naknada za izdavanje potvrda

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

9.1.2. Naknada za pristup potvrdama

Ovjerilac UIO ne objavljuje elektronske potvrde, tako da one nisu javno dostupne, pa ne može ni da naplaćuje pristup elektronskoj potvrdi.

9.1.3. Naknada za provjeru opozvanosti statusa potvrda

Provjera opozvanosti elektronske potvrde i dobijanje informacija o statusu potvrde korištenjem registra opozvanih potvrda ili *OCSP* servisa se ne naplaćuje.

9.1.4. Naknada za druge usluge

Ovjerilac UIO zadržava pravo da naplaćuje različite usluge ovisno od pruženih usluga u svakom konkretnom slučaju.

9.1.5. Povrat uplaćenih sredstava

U slučaju da Ovjerilac UIO raskine ugovor, a prethodno ne izda elektronsku potvrdu korisniku, korisnik može da traži povrat uplaćenih sredstava na iznos cijene potvrde.

9.2. Finansijska odgovornost

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

9.2.1. Osiguranje

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.

9.2.2. Drugi fondovi

Nije primijenjeno.

9.2.3. Osiguranje ili garancija za krajnje korisnike

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

9.3. Tajnost poslovnih podataka

9.3.1. Obim tajnih podataka

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

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

9.3.2. Podaci koji se ne smatraju tajnim

Podaci koji se ne smatraju tajnim su:

- Registri opozvanih potvrda, kao i podaci koje oni sadrže,
- Politika ovjeravanja,
- Praktična pravila,
- Podaci i dokumenta koja su objavljena na zvaničnoj *Web* stranici Ovjerioca UIO, a za koje postoji pisana suglasnost za javno objavljivanje.

9.3.3. Odgovornost za zaštitu tajnih podataka

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.

9.4. Čuvanje ličnih podataka

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

9.4.1. Plan čuvanja ličnih podataka

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

9.4.2. Lični podaci koji se smatraju tajnim

Svi podaci o korisnicima koji su zaštićeni zakonom smatraju se povjerljivim ličnim podacima.

9.4.3. Lični podaci koji se ne smatraju tajnim

Svi podaci koji su javno dostupni.

9.4.4. Odgovornost za zaštitu ličnih podataka

Ovjerilac UIO je odgovoran za lične podatke i zaštitu tih podataka, u skladu sa tačkom 9.3.3.

9.4.5. Upozorenje i suglasnost za korištenje ličnih podataka

Ovjerilac UIO će koristiti za potrebe pružanja usluge ovjeravanja lične podatke samo ako korisnik da suglasnost tokom procesa registracije. Smatra se da je korisnik dao suglasnost ukoliko je potpisao Ugovor o izdavanju i korištenju kvalificirane elektronske potvrde.

9.4.6. Otkrivanje ličnih podataka nadležnim organima

Ovjerilac UIO će otkriti ili dostaviti lične podatke na zahtjev nadležnog organa i u drugim slučajevima kada je to u skladu sa zakonom.

9.4.7. Druge okolnosti za otkrivanje ličnih podataka

Ovjerilac UIO će otkriti lične podatke zaštićene zakonom uz prethodnu suglasnost korisnika ili na zahtjev nadležnog organa i u drugim slučajevima predviđenim zakonom.

9.5. Zaštita prava intelektualne svojine

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

Softver treće strane Ovjerilac UIO koristi u skladu sa odredbama važeće licence.

9.6. Prava i obaveze

9.6.1. Prava i obaveze ovjerioca

Ovjerilac UIO garantira pružanje usluge ovjeravanja, u skladu sa zakonom, drugim propisima, ovim 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.

9.6.2. Prava i obaveze Grupe za podršku korisnicima sistema PKI UIO

Grupa za podršku korisnicima sistema PKI UIO, ima prava i obaveze da:

- Provjeri identitet korisnika u postupku izdavanja elektronske potvrde i tačnost podataka u zahtjevu za izdavanje i korištenje elektronske potvrde,
- Provjeri identitet korisnika i tačnost podataka u zahtjevu za promjenu statusa elektronske potvrde,
- Proslijedi podatke za izdavanje i promjenu statusa elektronske potvrde, kao i svu dokumentaciju Grupi za održavanje sistema PKI UIO.

9.6.3. Prava i obaveze korisnika

Ovjerilac UIO osigurava poštivanje i ostvarivanje svih prava i obaveza korisnika, koja su utvrđena propisima, a odnose se na kvalificiranu elektronsku potvrdu uključujući i ova pravila.

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.

9.6.4. Prava i obaveze trećih lica

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

Obaveze trećih lica, prije nego što se pouzdaju u kvalificiranu elektronsku potvrdu izdanu od strane Ovjerioca UIO su:

- Provjeravanje statusa potvrde,
- Upoznati se sa odgovornostima i ograničenjima Ovjerioca UIO definiranim u ovim Praktičnim pravilima i drugim aktima objavljenim na zvaničnoj *Web* stranici Ovjerioca UIO.

9.6.5. Prava i obaveze drugih učesnika

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

9.7. Izuzeće od odgovornosti

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

9.8. Odgovornost i ograničenja od odgovornosti

9.8.1. Odgovornost i ograničenja od odgovornosti ovjerioca

Ovjerilac 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.

Ovjerilac UIO je dužan da čuva dokaze o tome da je postupao u skladu sa važećim propisima.

9.8.2. Završetak rada

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.

9.8.3. Odgovornost i ograničenja od odgovornosti korisnika elektronske potvrde

Korisnik je odgovoran za štetu koja je nastala njegovom krivicom, odnosno zbog neispunjavanja obaveza utvrđenih u tački 9.6.3. ovih Praktičnih pravila.

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.

9.9. Naknade

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

9.10. Stupanje na snagu i prestanak važenja pravnih akata

9.10.1. Stupanje na snagu pravnih akata

Pravni akti Ovjerioca UIO stupaju na snagu u roku utvrđenom u svakom od tih akata u skladu sa zakonom.

Politika ovjeravanja Ovjerioca UIO i ova Praktična pravila objavljuju se i javno su dostupna svim zainteresiranim licima na *Web* stranici Ovjerioca UIO.

9.10.2. Period važenja

Primjena ovih Praktičnih pravila nije vremenski ograničena i ista će biti na snazi do objavljivanja novih pravila.

9.10.3. Efekat trajanja

Ovjerilac UIO će i poslije prestanka važenja elektronske potvrde štititi povjerljivost ličnih i drugih podataka korisnika, kao i poslije prestanka važenja svojih akata.

9.11. Pojedinačna obavještenja i komunikacija s korisnicima

Ovjerilac UIO komunicira sa korisnicima putem elektronske pošte, pisanim putem i *Web* stranice, osim ako nije drugačije određeno ovim Praktičnim pravilima.

9.12. Dopune Praktičnih pravila

9.12.1. Postupak za dopunu

Ovjerilac UIO će u slučaju promjene zakonske regulative i procedure rada izvršiti usklađivanje svojih važećih akata s istim.

Izmjene i dopune Praktičnih pravila, koje se odnose na rad Ovjerioca UIO i izdavanje elektronskih potvrda po pravilu se usvajaju trideset dana prije početka primjene. Izmjene i dopune Praktičnih pravila, koje po procjeni Ovjerioca UIO ne utiču bitno na korisnike, usvajaju se osam dana prije početka primjene.

9.12.2. Mehanizam i period obavještavanja

O izmjenama i dopunama Praktičnih pravila i ostalih dokumenata vezanih za Praktična pravila, Ovjerilac UIO obavještava Ministarstvo komunikacija i transporta BiH i iste objavljuje na *Web* stranici Ovjerioca UIO.

9.12.3. Okolnosti pod kojima *OID* mora da se promijeni

Promjena *OID*-a će se izvršiti ukoliko Ovjerilac UIO odluči da izvrši izmjene u Politici ovjeravanja i Praktičnim pravilima, a koje zahtijevaju promjenu *OID*-a.

9.13. Rješavanja u slučaju spora

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.

9.14. Mjerodavno pravo

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

9.15. Usklađenost s važećim zakonodavstvom

Pravni akti Ovjerioca UIO su u skladu sa zakonom i drugim propisima Bosne i Hercegovine koji reguliraju ovu oblast.

9.16. Ostale odredbe

9.16.1. Ugovor s korisnicima

Pružanje usluga ovjeravanja (izdavanje i korištenje elektronske potvrde) regulira se posebnim ugovorom između Ovjerioca UIO i korisnika, u skladu sa zakonom i drugim propisima.

9.16.2. Prenošenje prava

Korisnik elektronske potvrde ne može prava iz zaključenog ugovora sa Ovjeriocem UIO u cjelini ili djelimično prenositi na treća lica.

Ovjerilac UIO prava i obaveze iz ugovora zaključenog sa korisnikom, može u potpunosti ili djelimično, bez suglasnosti korisnika, prenijeti na drugog registriranog ovjerioca u BiH ili nadležni organ.

9.16.3. Izmjena ovih Praktičnih pravila

Izmjene ili dopune pojedinih odredbi ovih Praktičnih pravila ili akata donesenih na osnovu ovih Praktičnih pravila ne utiču na važenje ostalih odredbi ovih Praktičnih pravila.

9.16.4. Primjenjivost za advokatske naknade i odricanje od prava

Nije primjenjivo.

9.16.5. Viša sila

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.

Višu silu predstavljaju izvanredne okolnosti i nepredvidive situacije kao što su prirodne katastrofe, terorizam, nedostatak napajanja ili prekid telekomunikacijskih veza, požar, nepredvidivi incidenti kao što su virusi ili napadi s ciljem onemogućavanja servisa, greške u kriptografskim algoritmima i sl.

9.17. Stupanje na snagu

Ova Praktična pravila stupaju na snagu danom donošenja, a počinju sa primjenom osmoga dana od dana objave na *Web* stranici Ovjerioca UIO.

Direktor
Uprave za indirektno oporezivanje

Broj: 01-02-2-160-8/21
Datum: 12.03.2021.

dr. Miro Džakula