УПРАВА ЗА ИНДИРЕКТНО ОПОРЕЗИВАЊЕ
Бана Лазаревића бб, Бања Лука

ПРАКТИЧНА ПРАВИЛА ПРУЖАЊА УСЛУГЕ ОВЈЕРАВАЊА ОВЈЕРИОЦА УПРАВЕ ЗА ИНДИРЕКТНО ОПОРЕЗИВАЊЕ

(*Certification Practices Statement - CPS*)

Верзија 1.0

САДРЖАЈ

На основу члана 61. Закона о управи („Службени гласник БиХ“, бр. 32/02, 102/09 и 72/17) и члана 5. Правилника о ближим условима за издавање квалификованих потврда („Службени гласник БиХ“, број: 14/17) директор Управе за индиректно опорезивање доноси

ПРАКТИЧНА ПРАВИЛА ПРУЖАЊА УСЛУГЕ ОВЈЕРАВАЊА ОВЈЕРИОЦА УПРАВЕ ЗА ИНДИРЕКТНО ОПОРЕЗИВАЊЕ

1. УВОД

Управа за индиректно опорезивање (у даљем тексту: УИО) је изградила инфраструктуру јавних криптографских кључева - *Public Key Infrastructure – PKI* и као овјерилац у смислу Закона о електронском потпису („Службени гласник БиХ“, број: 91/06) присутна је као овјерилац који пружа услуге издавања квалификованих и неквалификованих електронских потврда, управљања животним циклусом електронских потврда и издавање квалификованих електронских временских жигова, под именом: Овјерилац УИО.

Овјерилац УИО врши издавање квалификованих електронских потврда у складу са законским прописима, општим актима и упутствима Овјериоца УИО који регулишу ову област. Правни оквир за обављање дјелатности издавања квалификованих електронских потврда Овјериоца УИО чине следећи законски и подзаконски акти:

- Закон о електронском потпису („Службени гласник БиХ“, број 91/06),
- Закон о електронском документу („Службени гласник БиХ“, број 58/14),
- Правилник о ближим условима издавања квалификованих потврда („Службени гласник БиХ“, број 14/17)

Општа правила функционисања Овјериоца УИО садржана су у документима:

- Политика овјеравања Овјериоца Управе за индиректно опорезивање (*Certification Policy - CP*) (у даљем тексту Политика овјеравања),
- Практична правила пружања услуге овјеравања Овјериоца Управе за индиректно опорезивање (*Certification Practices Statement - CPS*.

Практична правила пружања услуге овјеравања Овјериоца Управе за индиректно опорезивање (у даљем тексту: Практична правила), представљају јавни документ који дефинише процес пружања услуге овјеравања и начин њиховог коришћења при издавању и управљању животним циклусом електронских потврда и електронских печата, оперативне процедуре у циљу испуњавања постављених захтјева и начин на који Овјерилац УИО испуњава техничке, организационе и процедуралне захтјеве пословања који су идентификовани у Политици овјеравања као и употребу електронске потврде од стране корисника.

Услуге повјерења које пружа Овјерилац УИО су опсег овог документа. Овај документ описује комплетан животни циклус квалификованих и неквалификованих електронских

потврда изданих на сигурним криптографским уређајима или у виду софтверских потврда од стране Овјериоца УИО. Политика овјеравања и Практична правила као јавни документи објављују се на званичној *Web* страници Овјериоца УИО.

Осим ових докумената корисницима и свим заинтересованим лицима, на званичној *Web* страници Овјериоца УИО доступни су:

- Обрасци уговора о издавању и коришћењу квалификованих електронских потврда,
- Обрасци уговора о издавању и коришћењу неквалификованих електронских потврда,
- Обрасци захтјева за издавање и коришћење квалификованих електронских потврда,
- Обрасци захтјева за издавање и коришћење неквалификованих електронских потврда,
- Обрасци захтјева за промјену статуса квалификованих електронских потврда,
- Обрасци захтјева за промјену статуса неквалификованих електронских потврда,
- Корисничка упутства,
- Остали акти везане за рад Овјериоца УИО.

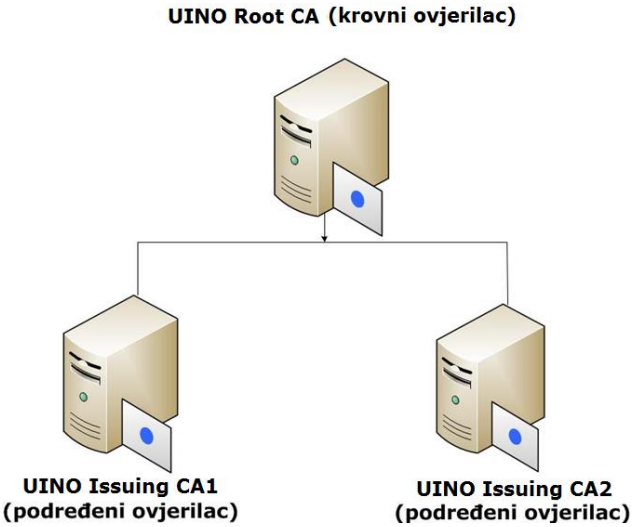
Овјерилац УИО утврђује и Посебна интерна правила рада Овјериоца УИО и заштите система овјеравања (у даљем тексту: Посебна правила). Посебна правила су интерни документи и представљају пословну тајну УИО.

Квалификоване и неквалификоване електронске потврде и квалификовани електронски временски жигови које издаје Овјерилац УИО су у складу с eIDAS уредбом Европске уније („Уредба број 910/2014 Европског парламента и Савјета о електронској идентификацији у унутрашњем тржишту и стављању ван снаге Директиве 1999/93/EZ“) и одговарајућим међународним стандардима и препорукама, као и другим стандардима, документима и препорукама, које се односе на издавање квалификованих електронских потврда.

1.1. Преглед

Овјерилац УИО користи у својој инфраструктури за издавање квалификованих и неквалификованих електронских потврда хијерархију више *CA* (енг. *Certification Authority*) сервера. Двонивовску архитектуру инфраструктуре Овјериоца УИО чине три CA сервера:

- Коријенски овјерилац: „***UINO Root CA***“
- Подређени овјериоци за издавање потврда, потписани од стране „*UINO Root CA*“:
  - „***UINO Issuing CA1***“,
  - „***UINO Issuing CA2***“.



Шема 1. приказује хијерархију Овјериоца УИО

„*UINO Root CA*“ сервер ради као *Root* овјерилац на основу потврде издате самом себи (енг. *self-signed certificate*) у процесу генерисања приватног криптографског кључа апликације овјериоца (енг. *Root Key Generation Ceremony*). „*UINO Root CA*“ сервер издаје потврде њему подређеним овјериоцима „*UINO IssuingCA1*“ и „*UINO Issuing CA2*“ који су дио инфраструктуре Овјериоца УИО, потврду за потписивање одговора УИО OCSP сервиса за провјеру статуса опозваности потврде које издаје „*UINO Root CA*“, као и административне потврде у складу са улогом коју запослени обавља.

За потребе администрирања „*UINO Root CA*“ сервер издаје двије потврде *Security Officer*-има и једну потврду *Security Auditor*-у.

Сервери „*UINO IssuingCA1*“ и „*UINO Issuing CA2*“ издају потврде крајњим корисницима.

„*UINO IssuingCA1*“ сервер као подређени овјерилац (енг. *subordinate*) издаје квалификоване и неквалификоване електронске потврде физичким лицима и физичким лицима повезаним са правним лицима у сврху израде квалификованог електронског потписа и печата, неквалификованог електронског потписа, аутентификацију, аутентификацију *Web* страница (*TLS*/*SSL* потврде, потврде за сервере), као и администраторске потврде у складу са улогом коју запослени обавља. Поред овога, сервер издаје потврду за потпис одговора *OCSP* сервиса за „*UINO IssuingCA1*“ и потврду сервису за издавање квалификованих временских жигова.

„*UINO Issuing CA2*“ сервер као подређени овјерилац (енг. *subordinate*) издаје квалификоване електронске потврде за запослене УИО у сврху израде електронског потписа и аутентификацију, доменску аутентификацију, аутентификацију *Web* страница, као и администраторске потврде у складу са улогом коју запослени обавља. Поред овога издаје се потврда интерном сервису за издавање временских жигова, потврда за потписивање фајлова информационог система УИО и потврда за потпис одговора OCSP сервиса за „*UINO Issuing CA2*“.

За потребе администрирања „*UINO Issuing CA1*“ и „*UINO Issuing CA2*“ сервера издају се по двије потврде *Security Officer*-има и једну потврду *Security Auditor*-у.

Функционисање хијерархијске инфраструктуре у потпуности је у складу са Политиком овјеравања и Практичним правилима која су обавезујућа за Овјериоца УИО, лица којима је Овјерилац УИО издао електронску потврду и трећа лица која се поуздају у потврду издату од стране Овјериоца УИО. Корисници квалификованих електронских потврда Овјериоца УИО, посједују један пар криптографских кључева (јавни и приватни кључ). Приватни криптографски кључ користи се за квалификовано електронско потписивање, а јавни криптографски кључ користи се за верификовање квалификованог електронског потписа.

1.1.1. Профили потврда Овјериоца УИО

1.1.1.1. Типови потврда које издаје овјерилац „UINO Root CA“

ПОПИС ТИПОВА ПОТВРДА КОЈЕ ИЗДАЈЕ UINO ROOT CA	
НАЗИВ ТИПА ПОТВРДЕ	**ПОДРУЧЈЕ ПРИМЈЕНЕ ПОТВРДЕ**
ПОТВРДА УИО КОРИЈЕНСКОГ ОВЈЕРИОЦА (UINO ROOT CA)	ИЗДАВАЊЕ СА ПОТВРДА ПОДРЕЂЕНИМ ОВЈЕРИОЦИМА, ИЗДАВАЊЕ CRL И ИЗДАВАЊЕ ПОТВРДЕ ЗА УИО OCSP СЕРВИС
ПОТВРДА ПРВОГ УИО ПОДРЕЂЕНОГ ОВЈЕРИОЦА (UINO ISSUING CA1)	ИЗДАВАЊЕ КОРИСНИЧКИХ ПОТВРДА ЗА ФИЗИЧКА ЛИЦА И ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА, ПОТПИСИВАЊЕ ПРИПАДАЈУЋИХ CRL, ПОТВРДЕ ЗА УИО СЕРВИС ИЗДАВАЊА КВАЛИФИКОВАНИХ ВРЕМЕНСКИХ ЖИГОВА, ПОТВРДА ЗА УИО OCSP СЕРВИС
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА: 1.3.6.1.4.1.46134.10.1.2
ПОТВРДА ДРУГОГ УИО ПОДРЕЂЕНОГ ОВЈЕРИОЦА (UINO ISSUING CA2)	ИЗДАВАЊЕ КОРИСНИЧКИХ ПОТВРДА ЗА ЗАПОСЛЕНЕ УИО, ПОТПИСИВАЊЕ ПРИПАДАЈУЋИХ CRL, ПОТВРДЕ ЗА УИО СЕРВИС ИЗДАВАЊА ВРЕМЕНСКИХ ЖИГОВА, ПОТВРДА ЗА УИО OCSP СЕРВИС
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА: 1.3.6.1.4.1.46134.10.1.2
ПОТВРДА ЗА ПОТПИС ОДГОВОРА OCSP СЕРВИСА	ПОТВРДА ЗА ПОТПИС ОДГОВОРА OCSP СЕРВИСА ЗА UINO ROOT CA
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА: 1.3.6.1.4.1.46134.10.2.0.16.1.1

Табела 1. Типови потврда које издаје овјерилац *UINO Root CA*

1.1.1.2. Типови потврда које издаје овјерилац UINO Issuing CA1

ПОПИС ТИПОВА ПОТВРДА КОЈИ ИЗДАЈЕ UINO ISSUING CA1		
НАЗИВ ГРУПЕ	**НАЗИВ ТИПА ПОТВРДЕ**	**ПОДРУЧЈЕ ПРИМЈЕНЕ ПОТВРДЕ**
ПОТВРДЕ ЗА ФИЗИЧКА ЛИЦА	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА (QCP-n-qscd)	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.10.1.1
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА (NCP+)	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА И КОРИСТИ ЗА ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.10.2.1
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА И

	ЗА ФИЗИЧКА ЛИЦА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ (NCP+)	КОРИСТИ ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.10.3.1
	УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ PKCS#12 ФОРМАТА (NCP)	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.10.4.0
ПОТВРДЕ ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА С ПРАВНИМ ЛИЦИМА	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА (QCP-n-qscd)	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА У ПОСЛОВНЕ СВРХЕ.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.11.1.1
	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА СТРАНЦЕ ПОВЕЗАНЕ СА ПРАВНИМ ЛИЦИМА (QCP-n-qscd)	ИЗДАЈЕ СЕ СТРАНЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА У ПОСЛОВНЕ СВРХЕ.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.11.2.1
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ФИЗИЧКИХ ЛИЦА ПОВЕЗАНИХ СА ПРАВНИМ ЛИЦИМА (NCP+)	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ ЗА ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА У ПОСЛОВНЕ СВРХЕ.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.11.3.1
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА (NCP+)	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ СА ПОСЛОВНИМ СУБЈЕКТОМ ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА У ПОСЛОВНЕ СВРХЕ.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.11.4.1
	УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ PKSC#12 ФОРМАТА ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА (NCP)	ИЗДАЈЕ СЕ ФИЗИЧКИМ ЛИЦИМА ПОВЕЗАНИМ С ПОСЛОВНИМ СУБЈЕКТОМ. КОРИСТИ СЕ ЗА ПОТРЕБЕ ЕЛЕКТРОНСКОГ ПОТПИСИВАЊА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.11.5.0
ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ (QCP-l-qscd)	ИЗДАЈЕ СЕ ПРАВНИМ ЛИЦИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПЕЧАТА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.12.1.1
ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ WEB СТРАНИЦА ЗА ПРАВНА ЛИЦА	ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ WEB СТРАНИЦА (SSL) ЗА ПРАВНА ЛИЦА	ИЗДАЈЕ СЕ ПРАВНИМ ЛИЦИМА ЗА АУТЕНТИФИКАЦИЈУ WEB СТРАНИЦА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.13.1.0
ПОТВРДА ЗА ИТ ОПРЕМУ ЗА ПРАВНА ЛИЦА	АПЛИКАТИВНА ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ ЗА ПРАВНА ЛИЦА (NCP)	ИЗДАЈЕ СЕ АПЛИКАЦИЈАМА И ИНФОРМАЦИОНИМ СИСТЕМИМА ПРАВНИХ ЛИЦА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.14.1.0
ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ	ИЗДАЈЕ СЕ СЕРВИСУ ЗА ИЗДАВАЊЕ КВАЛИФИКОВАНИХ ВРЕМЕНСКИХ

		ЖИГОВА И КОРИСТИ ЗА ПОТПИСИВАЊЕ КВАЛИФИКОВАНИХ ВРЕМЕНСКИХ ЖИГОВА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.15.1.1
ПОТВРДА ЗА OCSP СЕРВИС	УИО ПОТВРДА ЗА OCSP СЕРВИС UINO ISSUING CA1	ИЗДАЈЕ СЕ OCSP СЕРВИСУ ЗА ПОТПИС OCSP ОДГОВОРА СА ТИЈЕЛА UINO ISSUING CA1.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.1.16.1.1

Табела 2. Типови потврда које издаје овјерилац *UINO Issuing CA1*

1.1.1.3. Типови потврда које издаје овјерилац UINO Issuing CA2

ПОПИС ТИПОВА ПОТВРДА КОЈЕ ИЗДАЈЕ UINO ISSUING CA2		
НАЗИВ ГРУПЕ	**НАЗИВ ТИПА ПОТВРДЕ**	**ПОДРУЧЈЕ ПРИМЈЕНЕ ПОТВРДЕ**
ПОТВРДЕ ЗА ЗАПОСЛЕНЕ	УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ЗАПОСЛЕНЕ (QCP-n-qscd)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ИЗРАДУ КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ ПОТПИСА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.11.1.1
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ (NCP+)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.11.2.1
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ (NCP+)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.11.3.1
	УИО НЕКВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС И ДОМЕНСКУ АУТЕНТИФИКАЦИЈУ ЗА ЗАПОСЛЕНЕ (NCP+)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ИЗРАДУ ЕЛЕКТРОНСКОГ ПОТПИСА И ДОМЕНСКУ АУТЕНТИФИКАЦИЈУ.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.11.4.1
	УИО ПОТВРДА ЗА ЕЛЕКТРОНСКО ПОТПИСИВАЊЕ И АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ PKSC#12 ФОРМАТА (NCP) ЗА ЗАПОСЛЕНЕ (NCP)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА, А КОРИСТИ СЕ ЗА ПОТРЕБЕ ЕЛЕКТРОНСКОГ ПОТПИСИВАЊА, ЈАКУ АУТЕНТИФИКАЦИЈУ И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.11.5.0
ПОТВРДЕ ЗА АУТЕНТИФИКАЦИЈУ WEB СТРАНИЦА И ДРУГИХ СЕРВИСА	ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ WEB СТРАНИЦА (SSL)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА-АДМИНИСТРАТОРИМА СЕРВЕРА ЗА АУТЕНТИФИКАЦИЈУ WEB СТРАНИЦА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.13.1.0
	KERBEROS ПОТВРДА ЗА ДОМЕН КОНТРОЛЕР (ДОМЕН КОНТРОЛЕР KDC)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА-АДМИНИСТРАТОРИМА ACTIVE DIRECTORY ДОМЕНА ЗА АУТЕНТИФИКАЦИЈУ ДОМЕН КОНТРОЛЕРА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.13.10.0
ПОТВРДА ЗА ИТ ОПРЕМУ	УИО АПЛИКАТИВНА ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ У ОБЛИКУ ДАТОТЕКЕ PKCS#12 ФОРМАТА (NCP)	ИЗДАЈЕ СЕ СОФТВЕРСКИМ МОДУЛИМА ИНФОРМАЦИОНОГ СИСТЕМА УИО И КОРИСТИ ЗА

		ЊИХОВУ АУТЕНТИФИКАЦИЈУ ДРУГИМ МОДУЛИМА И ИНФОРМАЦИОНИМ СИСТЕМИМА УИО И ЕНКРИПЦИЈУ КЉУЧА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.14.1.0
ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ	ПОТВРДА ЗА ВРЕМЕНСКИ ЖИГ	ИЗДАЈЕ СЕ ИНТЕРНОМ СЕРВИСУ ЗА ИЗДАВАЊЕ ВРЕМЕНСКИХ ЖИГОВА И КОРИСТИ ЗА ПОТПИСИВАЊЕ ВРЕМЕНСКИХ ЖИГОВА.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.15.1.1

ПОТВРДА ЗА OCSP СЕРВИС	УИО ПОТВРДА ЗА OCSP СЕРВИС UINO ISSUING CA2	ИЗДАЈЕ СЕ OCSP СЕРВИСУ ЗА ПОТПИС OCSP ОДГОВОРА СА ТИЈЕЛА UINO ISSUING CA2.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.16.1.1
ПОТВРДА ЗА ПОТПИСИВАЊЕ КОДА	ПОТВРДА ЗА ПОТПИСИВАЊЕ КОДА (NCP+)	ИЗДАЈЕ СЕ ЗАПОСЛЕНИМА ЗА ПОТПИСИВАЊЕ ФАЈЛОВА ИНФОРМАЦИОНИХ СИСТЕМА УИО.
	OID ПОЛИТИКЕ ОВЈЕРАВАЊА	1.3.6.1.4.1.46134.10.2.2.17.1.1

Табела 3. Типови потврда које издаје овјерилац *UINO Issuing CA2*

1.1.1.4. Основни подаци о CA потврдама УИО Овјериоца

1.1.1.4.1. Основни подаци о потврди UINO Root CA

УИО ПОТВРДА КОРИЈЕНСКОГ ОВЈЕРИОЦА - UINO ROOT CA		
ОСНОВНА ПОЉА		
ПОЉЕ	**АТРИБУТ**	**ВРИЈЕДНОСТ**
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 20 година
Subject	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
SHA-1 thumbprint: 30c40b7dfb76c4dccf4d2d77e21d984e11fd43ea		
SHA 256 thumbprint: c676695d64b5b5f7b3308a7ee41ba17fcaceff6baddbe27a5f9588ed75b1cb67		

Табела 4. Основни подаци о потврди *UINO Root CA*

1.1.1.4.2. Основни подаци о потврди UINO Issuing CA1

УИО ПОТВРДА ПРВОГ ПОДРЕЂЕНОГ ОВЈЕРИОЦА-UINO ISSUING CA1		
ОСНОВНА ПОЉА		
ПОЉЕ	**АТРИБУТ**	**ВРИЈЕДНОСТ**
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 20 година
Subject	commonName (CN)	UINO Issuing CA1
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
SHA-1 thumbprint: 44f227af9af01c3c119b35f49ad186076c1fc44a		
SHA 256 thumbprint: a6f1dd9fdb403dd08da4c0cfcb3d7e4837a749b4ceee26e7ac0967bb6fb0ce44		

Табела 5. Основни подаци о потврди *UINO Issuing CA1*

1.1.1.4.3. Основни подаци о потврди UINO Issuing CA2

УИО ПОТВРДА ДРУГОГ ПОДРЕЂЕНОГ ОВЈЕРИОЦА – UINO ISSUING CA2		
ОСНОВНА ПОЉА		
ПОЉЕ	**АТРИБУТ**	**ВРИЈЕДНОСТ**
Issuer	commonName (CN)	UINO Root CA
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
Validity	notBefore	Вријеме издавања потврде
	notAfter	Вријеме издавања потврде + 20 година
Subject	commonName (CN)	UINO Issuing CA2
	organizationName (O)	Uprava za indirektno-neizravno oporezivanje
	countryName (C)	BA
SHA-1 thumbprint: 7a5de606842c8068dfe5cf2224267493c84af0f6		
SHA 256 thumbprint: b2e7486187ae3611e88263eec309af19730b237e2b5dcc06a358164c2e0494f2		

Табела 6. Основни подаци о потврди *UINO Issuing CA2*

1.2. Назив и идентификација документа

Овај документ носи назив „**ПРАКТИЧНА ПРАВИЛА ПРУЖАЊА УСЛУГЕ ОВЈЕРАВАЊА ОВЈЕРИОЦА УПРАВЕ ЗА ИНДИРЕКТНО ОПОРЕЗИВАЊЕ**“, као што је то означено на почетној страни документа.

Организација *IANA* (*Internet Assigned Numbers Authority*) додијелила је Управи за индиректно опорезивање *OID* 1.3.6.1.4.1.46134. Управа за индиректно опорезивање је на основу тог *OID*-а додијелила Овјериоцу УИО *OID* 1.3.6.1.4.1.46134.10. Идентификациони број овог документа (*OID*) је 1.3.6.1.4.1.46134.10.1.2.1.0.

OID	ОБЈАШЊЕЊЕ
1.3.6.1.4.1.46134	Јединствени идентификациони број додијељен Управи за индиректно опорезивање од стране организације IANA
1.3.6.1.4.1.46134.10	Јединствени идентификациони број Овјериоца УИО додијељен од стране УИО
1.3.6.1.4.1.46134.10.1	Јединствени идентификацијски број додијељен за документе Овјериоца УИО
1.3.6.1.4.1.46134.10.2	Јединствени идентификациони број додијељен за потврде Овјериоца УИО

Табела 7. Јединствени идентификациони бројеви Овјериоца УИО

ДОКУМЕНТИ	ВРСТА ДОКУМЕНТА	ВЕРЗИЈА	ПОДВЕРЗИЈА
1.3.6.1.4.1.46134.10.1	1 за CP	1 за почетну верзију	0 за почетну подверзију
	2 за CPS	1 за почетну верзију	0 за почетну подверзију

Табела 8. Структура јединствених идентификационих бројева докумената Овјериоца УИО

НЕПРОМЈЕЊИВИ ДИО *OID*-А ПОЛИТИКЕ ОВЈЕРАВАЊА	ОВЈЕРИЛАЦ ПОТВРДЕ	ГРУПА ПРОФИЛА ПОТВРДЕ	ПРОФИЛ ПОТВРДЕ	НАЧИН ЧУВАЊА ПРИВАТНОГ КЉУЧА
1.3.6.1.4.1.46134.10.2	0 – *UINO Root CA* 1 – *UINO Issuing CA1* 2 – *UINO Issuing CA2*	Групе потврда су дефинисане према намјени потврда и њиховим корисницима. Ознаке група потврда су сљедеће:	Ознака профила потврде унутар групе потврда. Вриједност ознаке профила потврде почиње од броја 1.	Начин чувања приватног кључа одговара на питање да ли се приватни кључ чува на криптографском уређају. Могуће вриједности су сљедеће:

		10 – потврде за физичка лица 11 – потврде за физичка лица повезана с правним лицима 12 – потврде за електронски печат 13 – потврде за аутентификацију WEB страница и других сервиса 14 – потврде за ИТ опрему 15 – потврде за временски жиг 16 – потврде за OCSP сервис 17 – потврде за потписивање кода		0 – приватни кључ повезан са потврдом се не чува у криптографском уређају 1 – приватни кључ повезан са потврдом се чува у криптографском уређају

Табела 9. Структура јединствених идентификационих бројева потврда Овјериоца УИО

1.3. Учесници *PKI* система

Учесници PKI система су:

- Овјерилац УИО,
- Корисници услуга,
- Трећа лица,
- Остали учесници.

1.3.1. Овјерилац УИО

У Одсјеку за електронске потписе и сертификате у Сектору за информационе технологије постоје следеће организационе јединице:

- Група за одржавање система PKI УИО - *CA*,
- Група за подршку корисницима система PKI УИО - *RA*.

1.3.1.1. Одсјек за електронске потписе и сертификате Група за одржавање система PKI УИО – CA (енг. *Certification Authority*)

Ова организациона јединица у оквиру Овјериоца УИО одговорна је за исправно функционисање опреме и програма, а који су у вези са издавањем електронских потврда. Такође ова једница је задужена и за креирање, потписивање и издавање потврда, управљање животним вијеком потврда завршно са опозивом потврде. Организациона јединица ради у складу са Практичним правилима, при чему су пословни процеси начелно описани у Практичним правилима, а детаљно прописани интерним правилницима Овјериоца УИО.

Серверска инфраструктура CA обухвата:

- ***UINO Root CA*** сервер, као корјенски овјерилац, самопотписани кровни овјерилац,
- ***UINO Issuing CA1*** сервер, као први подређени овјерилац,
- ***UINO Issuing CA2*** сервер, као други подређени овјерилац.

1.3.1.2. Одсјек за електронске потписе и сертификате Група за подршку корисницима система PKI УИО - RA (енг. *Registration Authority*)

Ова организациона јединица у оквиру Овјериоца УИО израђује правила вршења услуга овјеравања, припадајућу документацију и процедуре.

Запослени у Групи за подршку корисницима система PKI УИО који раде у регионалним центрима Управе за индиректно опорезивање овлашћени су за запримање захтјева, провјеравање идентитета корисника и за уношење захтјева за издавање електронских потврда и захтјева за промјену статуса потврда у апликацији Регистрационог тијела Овјериоца УИО.

1.3.2. Корисници

Корисници услуга Овјериоца УИО су:

- Физичко лице, које се идентификује специфичним атрибутима,
- Физичко лице које је запослено у правном лице,
- Правно лице,
- Запослени УИО.

Уколико Овјерилац УИО издаје електронску потврду физичком лицу које је запослено у правном лице, у оквиру атрибута који идентификују корисника налазе се и подаци који означавају назив правног лица.

1.3.2.1. Субјекти овјеравања

Субјект овјеравања је у потврди идентификован као Субјект те је носилац приватног кључа који је повезан с јавним кључем садржаним у потврди.

Субјекти овјеравања у потврдама које издају подређени Овјериоци УИО:

- У личним потврдама за електронски потпис је физичко лице,
- У пословним потврдама за електронски потпис је физичко лице које је повезано са правним лицем,
- У квалификованим потврдама за електронски печат је правно лице,
- У потврдама за аутентификацију *Web* страница је сервер који је идентификован називом домена и којим управља правно лице.

1.3.3. Трећа лица

Трећа лица су лица која се поуздају у електронске потврде издате од Овјериоца УИО, у циљу верификовања електронског потписа и провјере идентитета корисника.

Трећа лица могу провјерити статус опозваности електронских потврда, путем регистра опозваних потврда – *CRL* (енг. *Certificate Revocation List*) или преко *OCSP* (енг. *Online Certificate Status Protocol)* сервиса Овјериоца УИО, који се сваки дан ажурирају.

Трећа лица провјеравају најновије расположиве регистре опозваних потврда, да би имала комплетну и правовремену информацију о опозиву и суспензији потврда.

Ни под којим условима се не треба ослањати на регистар опозваних потврда дуже од максималног рока важења регистра опозваних потврда.

1.3.4. Остали учесници

Остали учесници су правна лица која, на неки начин, доприносе или учествују у обезбјеђивању квалитета рада Овјериоца УИО и давања услуга овјеравања. У ову групу спадају произвођачи и дистрибутери опреме и софтвера, произвођачи и дистрибутери смарт картица, осигуравајуће друштво, и други учесници.

1.4. Употреба потврда

1.4.1. Подручје примјене

UINO Root CA потврда користи се за:

- Издавање потврда њему подређених овјерилаца (*UINO Issuing CA1* и *UINO Issuing CA2*),
- Издавање регистра опозваних потврда (*CRL*),
- Издавање потврде за УИО *OCSP* сервис са којом овај *OCSP* сервис потписује одговоре за статус потврда њему подређених овјерилаца и осталих потврда које издаје овјерилац *UINO Root CA*.

Потврде подређених овјерилаца *UINO Issuing CA1* и *UINO Issuing CA2* се користе за:

- Издавање корисничких потврда,
- Издавање регистра опозваних потврда (*CRL*),
- Издавање потврда за УИО сервис издавања квалификованих електронских жигова,
- Издавање потврда за УИО *OCSP* сервис.

Подручје примјене УИО потврда изданих од стране овјерилаца *UINO Issuing CA1* и *UINO Issuing CA2*:

- Израда електронског потписа и квалификованог електронског потписа,
- Израда квалификованог електронског печата,
- Аутентификација корисника и енкрипција кључа,
- Аутентификација *Web* страница, тј. за аутентификацију *Web* сервера којима се приступа путем *TLS* или *SSL* протокола,
- Израда електронског потписа од стране апликације информационог система,
- Потпис одговора *OCSP* сервиса овјерилаца,
- Потписивање квалификованих временских жигова од стране сервиса за издавање квалификованих временских жигова,
- Доменску аутентификацију запослених,
- Аутентификацију домен контролера,
- Потписивање фајлова информационог система УИО.

Приватни криптографски кључеви који су придружени квалификованим електронским потврдама користе се у процесу квалификованог електронског потписивања електронског документа, који се може користити у општењу органа и општењу органа и странака, у правним пословима и другим правним радњама, као и у управном, судском и другом поступку пред државним органом и другим институцијама, ако је Законом којим се утврђује тај поступак, прописана употреба квалификованог електронског потписа.

Квалификоване електронске потврде потврђују везу између јавног криптографског кључа корисника и идентитета корисника који је извршио квалификовано потписивање електронског документа.

1.4.2. Недозвољене примјене

Свака друга употреба квалификоване електронске потврде која није дефинисана овим документом и није у сагласности са одредбама Закона о електронском потпису и другим документима који регулишу ову област, није дозвољена.

1.5. Политика администрирања документа

1.5.1. Организација управљања документом

Документ Практична правила креира и ажурира Овјерилац УИО:

Адреса:

Управа за индиректно опорезивање
Бана Лазаревића бб
78000 Бања Лука

Контакт:

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

Текућу верзију и претходне верзије документа могуће је преузети са *Web* странице Овјериоца УИО **http://ca.uino.gov.ba,** у дијелу *Документација*.

1.5.2. Лица за контакт

Лица за контакт Овјериоца УИО су шеф Одсјека за електронске потписе и сертификате у Сектору за информационе технологије УИО, запослени који обављају послове техничке подршке и други запослени овлашћени за давање информација у вези примјене Практичних правила и других аката Овјериоца УИО.

Контакт адресе лица из става 1. ове тачке су објављене на званичној *Web* страници Овјериоца УИО.

1.5.3. Лица одређена за усклађивање документа са праксом издавања потврда

Одсјек за електронске потписе и сертификате Сектора за информационе технологије УИО усклађује форму и садржај ових Практичних правила са евентуалним промјенама насталим у пракси издавања електронских потврда.

Такође, Одсјек за електронске потписе и сертификате Сектора за информационе технологије УИО редовно процјењује усклађеност ових Практичних правила са важећим законима.

1.5.4. Процедуре за одобрење Практичних правила

Након измјене законске регулативе, пословног процеса везаног за издавање квалификованих потврда или других измјена које утичу на поступке из обима документа Практична правила, Одсјек за електронске потписе и сертификате Сектора за информационе технологије проводи ревизију овог документа и врши његово усклађивање. Након проведеног процеса усклађивања шеф одсјека за електронске потписе и сертификате одобрава нови документ Практична правила.

Измјене или допуне Практичних правила се морају обавити у складу са одредбама Закона о електронском потпису, подзаконским актима и праксом, те зато могу бити предмет давања одобрења надлежног државног органа.

1.6. Дефиниције и скраћенице

ДЕФИНИЦИЈА	ЗНАЧЕЊЕ ДЕФИНИЦИЈЕ
Аутентификација	Електронски поступак којим се потврђује идентитет лица или изворност и цјеловитост података.
Апликација Овјериоца	Апликација на серверима Овјериоца УИО која генерише и потписује електронске потврде и регистре опозваних потврда помоћу криптографских кључева генерисаних и похрањених у хардверском криптографском модулу.
Апликација Регистрационог тијела	*Web* апликација која служи за регистровање корисника Овјериоца УИО и обраду њихових захтјева за издавање потврда као и захтјева за промјену статуса потврда.
Апликација Централног система	*Web* апликација која омогућава централизовано праћење и управљање животним циклусом криптографских уређаја, креирање налога за издавање криптографских уређаја, издавање софверских потврда и потврда за аутентификацију *Web* страница.
Активациони подаци	Тајни подаци који се користе за активацију криптографских кључева у хардверском криптографском модулу или приступ приватним кључевима софтверских потврда. Активациони податак може бити *PIN*, лозинка или електронски кључ.
Аутор печата	Правно лице које израђује електронски печат.
Desktop апликација за персонализацију криптографских уређаја	*Desktop* апликација намијењена визуелној и електронској персонализацији криптографских уређаја, креирању шаблона за визуелну персонализацију криптографског уређаја, контролу квалитета персонализованих криптографских уређаја, те

	штампању *PIN* и *PUK* кодова криптографског уређаја корисника Овјериоца УИО.
Дешифровање	Криптографски процес којим се шифровани подаци претварају у разумљиве податке (отворени текст), коришћењем кључа за дешифровање и алгоритма за дешифровање.
Електронски дневник	Електронска форма записа о проведеним активностима. Лог датотека.
Електронски документ	Документ у електронском облику који се користи у пословним и другим радњама.
Електронски потпис	Скуп података у електронском облику који су придружени или су логички повезани с другим подацима у електронском облику и који служе за идентификацију потписника и утврђивање вјеродостојности потписаног електронског документа. Електронски потпис креира физичко лице.
Електронски печат	Скуп података у електронском облику који су придружени или су логички повезани с другим подацима у електронском облику или су логички повезани с њима ради осигурања изворности и цјеловитости тих података. Електронски печат креира правно лице.
Електронски временски жиг	Скуп података у електронском облику који повезује тачан датум и вријеме креирања тог скупа података са другим подацима у електронском облику.
Хардверски криптографски модул (енг. *Hardware security module* – HSM)	Уређај одређеног нивоа сигурности који: ▪ Генерише пар криптографских кључева, ▪ Штити криптографске и друге повјерљиве информације, ▪ Извршава криптографске функције.
Инфраструктура јавних кључева (PKI)	Архитектура, организација, хардвер, софтвер, правила, оперативни поступци и процедуре које заједнички подржавају имплементацију и рад криптографског система јавног кључа за управљање животним циклусом електронских потврда.
Јавни кључ (енг. *Public Key*)	Јавно доступан криптографски кључ који одговара упареном приватном кључу. Јавни кључ се може користити за провјеру електронског потписа (ако је јавно објављен као кључ за дешифровање) или за шифровање податка (ако је јавно објављен као кључ за шифровање).
Компромитовање приватног криптографског кључа	Нарушавање сигурности којом се приватни криптографски кључ излаже могућем неовлаштеном приступу, као што су неовлаштено откривање, мијењање или коришћење.

Корисник	Физичко лице које користи електронску потврду издану од стране овјериоца и чији се подаци налазе у потврди.
Квалификована потврда за електронски потпис	Потврда у електронском облику која је издана од стране овлаштеног овјериоца, а која садржи податке предвиђене Законом о електронском потпису и која повезује податке за верификовање електронског потписа са одређеним физичким лицем и потврђује идентитет тог лица.
Квалификовани електронски печат	Скуп података у електронском облику који прате друге податке у електронском облику или су са њима логички повезани. Истим се поуздано гарантује идентитет печатиоца (правно лице), интегритет електронских докумената, и онемогућава накнадно порицање одговорности за њихов садржај који испуњава услове утврђене законом.
Квалификовани електронски потпис	Скуп података у електронском облику који прате друге податке у електронском облику или су са њима логички повезани. Истим се поуздано гарантује идентитет потписника (физичко лице), интегритет електронских докумената, и онемогућава накнадно порицање одговорности за њихов садржај који испуњава услове утврђене законом.
Квалификовани електронски временски жиг	Електронски временски жиг у којем су наведени датум и вријеме засновани на извору тачног времена повезаном с *UTC*-ом и повезани са подацима у електронском облику на начин којим се у разумној мјери искључује могућност незапажене измјене тих података, а који је потписан коришћењем напредног електронског потписа квалификованог пружаоца услуге временског жигосања.
Квалификована средства за формирање квалификованог електронског потписа и печата	Одговарајућа техничка средства (софтвер и хардвер) која се користе за израду квалификованог електронског потписа, односно печата, уз коришћење података за формирање квалификованог електронског потписа, односно печата.
Квалификовани оцјењивач	Физичко или правно лице које задовољава захтјеве прописане eIDAS уредбом Европске уније.
Квалификовани овјерилац	Тијело које пружа једну или више квалификованих услуга повјерења и коме је одговарајуће надзорно тијело одобрило статус квалификованог овјериоца.
Овјерилац	Тијело које издаје и додјељује квалификоване електронске потврде а којем вјерује један или више корисника.
Опозив потврде	Трајни престанак ваљаности потврде прије истека рока важења наведеног у потврди.
Пар кључева	Два математички повезана криптографска кључа (приватни кључ и његов одговарајући јавни кључ) која имају сљедећа својства: ▪ Један кључ из пара кључева може бити коришћен за

	шифровање података, а који се могу дешифровати само коришћењем другог кључа из истог пара кључева, ▪ У случају познавања само једног кључа није могуће (у разумном времену и уз познату технологију) открити други кључ.
Подаци за формирање квалификованог електронског потписа или печата	Јединствени подаци, као што су кодови или приватни криптографски кључеви, које потписник, односно печатилац, користи за израду квалификованог електронског потписа или печата.
Подаци за провјеру квалификованог електронског потписа или печата	Подаци, као што су кодови или јавни криптографски кључеви, који се користе за провјеру квалификованог електронског потписа или печата, чиме се потврђују изворност и цјеловитост података заштићених тим потписом или печатом, те непорецивост креирања потписа или печата од стране одговарајућег аутора.
Потврда	Скуп података у електронском облику који: ▪ Именује и идентификује корисника наведеног у потврди, ▪ Садржи корисников јавни кључ, ▪ Има уписан временски период важења потврде, ▪ Има значење у складу са важећим прописима и нормама, ▪ Идентификује овјериоца који издаје потврде, ▪ Електронски је потписан од стране овјериоца, чиме је заштићен од незапажених промјена.
Потврда овјериоца	Потврда јавног кључа за *CA* којег је издао други *CA* или којег је издао исти *CA*.
Приватни кључ (енг. *Private Key*)	Криптографски кључ којег корисник чува у тајности, а који одговара упареном јавном кључу. Користи се за израду електронског потписа или за дешифровање података шифрованих одговарајућим јавним кључем.
Приватни криптографски кључ апликације овјериоца	Приватни кључ овјериоца, заједно са јавним кључем који је садржан у потврди овјериоца представљају пар кључева овјериоца. Приватни кључ је генерисан приликом иницијализације апликације овјериоца, а користи се за потписивање изданих електронских потврда и регистара опозваних потврда, што се ради помоћу *HSM*-а – хардверског криптографског модула.
Повјерљиве улоге	Улоге од којих зависи сигурност рада пружаоца услуга повјерења.
Потписник	Физичко лице које израђује електронски потпис.
Регистар опозваних потврда – CRL (енг. *Certificate Revocation List - CRL*)	Потписана листа у коју се уписују серијски бројеви и други подаци свих опозваних потврда које је издао овјерилац.

Root CA	Овјерилац највишег нивоа унутар домена пружаоца услуга повјерења, потписује потврде подређених овјерилаца, властиту потврду, као и административне потврде.
Root потврда овјериоца – Root CA потврда	Потврда коју овјерилац издаје сам себи (енг. *self-signed certificate*), тј. субјект потврде је овјерилац. *Root CA* потврда садржи јавни кључ и назив овјериоца који је издао потврду.
Реактивација потврде	Радња којом се суспендована потврда чини поново ваљаном.
Сигурно средство за израду електронског потписа (енг. *Secure Signature Creation Device* – SSCD)	Средство за израду електронског потписа које осигурава: ▪ Да се подаци за израду сигурног електронског потписа могу појавити само једном, те да је остварена њихова сигурност, ▪ Да се подаци за израду сигурног електронског потписа не могу поновити, те да је потпис заштићен од кривотворења при коришћењу постојеће расположиве технологије, ▪ Да податке за израду сигурног електронског потписа корисника може поуздано заштитити од неовлаштеног коришћења. Средство за израду сигурног електронског потписа не смије при изради сигурног електронског потписа промијенити податке који се потписују или онемогућити кориснику увид у те податке прије процеса израде сигурног електронског потписа.
Средства за провјеру квалификованог електронског потписа и печата	Одговарајућа техничка средства (софтвер и хардвер) која служе за провјеру квалификованог електронског потписа и печата, уз коришћење података за провјеру електронског потписа и печата.
Суспензија потврде	Привремени престанак ваљаности потврде прије истека рока важења наведеног у потврди.
Шифровање	Процес у криптографији којим се подаци мијењају тако да се информације учине неразумљивим за субјекте који не посједују одговарајући кључ за дешифровање. Употребом кључа за дешифровање у поступку дешифровања ове се информације поново могу учинити разумљивим, тј. довести у облик у којем су постојале непосредно прије њиховог шифровања.
Запослени	Лице у радном односу са Управом за индиректно опорезивање.
TSA систем	Систем за пружање услуга издавања временских жигова.

Валидација	Поступак потврђивања да су електронски потпис или печат ваљани.
Валидација потврде	Поступак потврђивања да је потврда ваљана.
Валидација потписа	Процес провјере криптографске вриједности потписа коришћењем података за верификацију потписа.

Табела 10. Дефиниције

Списак скраћеница које се помињу у документу приказан је у оквиру табеле 11.

СКРАЋЕНИЦА	ПУНИ НАЗИВ	ЗНАЧЕЊЕ
AES	*Advanced Encryption Standard*	Алгоритам симетричне криптографије намјењен за шифровање
CA	*Certification Authority*	Овјерилац
CP	*Certification Policy*	Политика овјеравања која указује на примјењивост потврда за одређену групу са захтјевима за сигурност.
CPS	*Certification Practice Statement*	Практична правила пружања услуге овјеравања у којима су побројани оперативни поступци које овјерилац проводи приликом издавања и управљања животним вијеком потврде.
CRL	*Certificate Revocation List*	Регистар опозваних потврда.
CMS	*Certificate Managament System*	Систем за управљање животним вијеком потврда које овјерилац издаје.
DN	*Distinguished Name*	Јединствено име субјекта уписано у потврду којим се идентификује субјект којем је издана потврда.
EAL	*Evaluation Assurance Level*	Тестирани ниво сигурности према стандарду ISO/IEC 15408. Постоји седам (7) нивоа и то од EAL1 до EAL7.

ETSI	*European Telecommunications Standards Institute*	Европски институт за стандарде из области телекомуникација.
HSM	*Hardware Security Module*	Хардверски криптографски модул за криптографске операције.
IETF	*Internet engineering task force*	Радна група за Интернет инжењеринг
ISO	*International organization for standardization*	Међународна организација за стандардизацију
LDAP	*Lightweight Directory Access Protocol*	Протокол за приступ јавном директоријуму
NIST	*National institute of standards and technology*	Национални институт за стандарде и технологију
NTP	*Network Time Protocol*	Протокол мрежног времена
OCSP	*Online Certificate Status Protocol*	Протокол за on-line провјеру статуса потврда, описан у документу RFC 6960.
OID	*Object Identifier*	Идентификатор објекта
PIN	*Personal Identification Number*	Лични тајни број за активацију паметне картице, паметног USB токена или сличног криптографског уређаја.
PKCS#10	*Public Key Cryptography Standard 10*	Стандард за формат захтјева за потврду.
PKI	*Public Key Infrastructure*	Инфраструктура јавних криптографских кључева
QSCD	*Qualified Signature Creation Device*	Квалификовано средство за креирање електронских потписа и печата (паметна картица, паметни USB токен, и слично).
RA	*Registration Authority*	Регистрационо тијело
RFC	*Request for comment*	Документи који дефинишу Internet стандарде и препоруке.
SSCD	*Secure Signature Creation Device*	Средство за формирање квалификованог електронског потписа (паметна картица, паметни *USB* токен, и слично).

UTC	*Coordinated Universal Time*	Координисано универзално вријеме

Табела 11. Списак скраћеница

1.7. Стандарди

- 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. ОБЈАВЉИВАЊЕ И ЛОКАЦИЈА ПОДАТАКА О УСЛУГАМА ОВЈЕРАВАЊА

2.1. Локација за објављивање података о услугама овјеравања

Овјерилац УИО објављује податке и сву документацију која се односи на издавање електронских потврда на *Web* страници **http://ca.uino.gov.ba**. *Web* страница је јавно доступна, као и сви подаци и сва документација која се на њој налази.

2.2. Објављивање података о услугама овјеравања

Овјерилац УИО објављује на својој званичној *Web* страници:

- Политику овјеравања Овјериоца УИО,
- Практична правила пружања услуге овјеравања Овјериоца УИО,
- Претходне верзије Политике овјеравања Овјериоца УИО и Практичних правила пружања услуге овјеравања Овјериоца УИО,
- Образац уговора о обављању услуга овјеравања,
- Образац захтјева за издавање и коришћење електронске потврде,
- Образац захтјева за промјену статуса потврде,
- Дефиниције важећих профила потврда Овјериоца УИО усклађених са eIDAS уредбом Европске уније,
- Корисничка упутства,
- Потврде овјериоца UINO Root CA и подређених овјерилаца *(UINO Issuing CA1* и *UINO Issuing CA2*) са придруженим *hash* вриједностима,
- Регистре опозваних потврда (*CRL* листе) овјерилаца *UINO Root CA, UINO Issuing CA1* и *UINO Issuing CA2*,
- Законску регулативу из подручја електронског потписа и пружања услуга повјерења,
- Цјеновник услуга овјеравања,
- Локације канцеларија Регистрационог тијела,
- Обавјештења корисницима везана за давање услуга овјеравања,
- Друге акте и обавјештења.

Овлаштени запослени задужен за ажурирање садржаја *Web* странице по одобрењу обавља објављивање докумената.

Овјерилац Управе за индиректно опорезивање објављује корисничка упутства и обрасце на *Web* страници, а претходне верзије се замјењују са новим верзијама.

2.3. Учесталост објављивања података о услугама овјеравања

Овјерилац УИО ажурира објављене податке сљедећом динамиком:

- Регистри опозваних потврда (*CRL*) објављују се на свака 24 часа. У случају опозива и/или суспензије потврде, ажурирани регистар опозваних потврда се објављује одмах послије опозива и/или суспензије потврда,
- Промјене на постојећим документима објављују се у најкраћем року послије настале промјене,
- Додатни документи објављују се у најкраћем року по одобравању од стране надлежних органа.

2.4. Контрола приступа подацима о услугама овјеравања

Подаци који су објављени на *Web* страници Овјериоца УИО су јавно доступни. Приступ је ограничен на могућност читања. Сви који приступају овим подацима ради коришћења електронских потврда, дужни су да се упознају са одредбама ових Практичних правила.

Овјерилац УИО има успостављене логичке и физичке сигурносне мјере за заштиту података на *Web* страницама од неовлашћеног брисања и додавања или неовлашћених промјена.

3. ИДЕНТИФИКАЦИЈА И АУТЕНТИФИКАЦИЈА

3.1. Одређивање имена

3.1.1. Врсте имена

Овјерилац UINO Root CA и њему подређени овјериоци УИО у потврду уписују податке о имену, односно називу субјекта за којег се потврда издаје у поље *Subject* потврде. Јединствено име (енг. *Distinguished Name*, *DN*) у пољу *Subject* у потврдама усклађено је с препоруком IETF RFC 5280 и нормом X.520 и оно мора бити јединствено унутар Овјериоца УИО.

У електронским потврдама, које издаје Овјерилац УИО, поље *Issuer* **(**табела 12, табела 13 и табела 14) потврде, које садржи име овјериоца који је издао потврду, и поље *Subject* потврде, које садржи име корисника потврде, су јединствена имена (енг. *Distinguished Name - DN*) у облику *X.509 v3.*

КОМПОНЕНТА ИМЕНА	ВРИЈЕДНОСТ
Назив CA сервера (CN)	*UINO Root CA*
Назив организације (O)	*Uprava za indirektno-neizravno oporezivanje*
Назив државе (C)	*BA*

Табела 12. Структура имена потврде овјериоца *UINO Root CA* Управе за индиректно опорезивање (УИО) у електронским потврдама

КОМПОНЕНТА ИМЕНА	ВРИЈЕДНОСТ
Назив CA сервера (CN)	*UINO Issuing CA1*
Назив организације (O)	*Uprava za indirektno-neizravno oporezivanje*
Назив државе (C)	*BA*

Табела 13. Структура имена потврде подређеног овјериоца *UINO Issuing CA1* Управе за индиректно опорезивање (УИО) у електронским потврдама

КОМПОНЕНТА ИМЕНА	ВРИЈЕДНОСТ
Назив CA сервера (CN)	*UINO Issuing CA2*
Назив организације (O)	*Uprava za indirektno-neizravno oporezivanje*
Назив државе (C)	*BA*

Табела 14. Структура имена потврде подређеног овјериоца *UINO Issuing CA2* Управе за индиректно опорезивање (УИО) у електронским потврдама

Структура имена корисника квалификоване потврде за електронски потпис приказана је у табели 15 и табели 16.

КОМПОНЕНТА ИМЕНА	ВРИЈЕДНОСТ
Назив корисника (*CN*)	Име Презиме (Име и презиме како је наведено у идентификационој исправи)
Серијски број (*SERIALNUMBER*)	*CA:BA*-ЈИП (ЈИП је псеудослучајно генерисани број)
Име (G)	Име (Име потписника како је наведено у идентификационој исправи)
Презиме (SN)	Презиме (Презиме потписника како је наведено у идентификационој исправи)
Мјесто (L)	Мјесто пребивалишта потписника
Назив државе (C)	*BA*

Табела 15. Структура имена за физичко лице у квалификованим електронским потврдама

КОМПОНЕНТА ИМЕНА	ВРИЈЕДНОСТ
Назив корисника (*CN*)	Име Презиме (Име и презиме како је наведено у идентификационој исправи)
Серијски број (*SERIALNUMBER*)	*CA:BA*-ЈИП (ЈИП је псеудослучајно генерисани број потврде)
Име (G)	Име (Име потписника како је наведено у идентификационој исправи)
Презиме (SN)	Презиме (Презиме потписника како је наведено у идентификационој исправи)
Идентификатор организације (2.5.4.97)	*VATBA*-ПИБ (Порески идентификациони број – ПИБ број правног лица)
Назив организације (O)	Регистровани скраћени назив пословног субјекта или назив пословног субјекта ако скраћени назив није регистрован.
Мјесто (L)	Мјесто сједишта правног лица регистрованог у Босни и Херцеговини.
Назив државе (C)	*BA*

Табела 16. Структура имена за корисника у правном лицу у квалификованим електронским потврдама

КОМПОНЕНТА ИМЕНА	ВРИЈЕДНОСТ
Назив правног лица (*CN*)	Назив који правно лице користи за своје представљање
Серијски број (*SERIALNUMBER*)	*CA:BA*-ЈИП (ЈИП је псеудослучајно генерисани број потврде)
Идентификатор организације (2.5.4.97)	*VATBA*-ПИБ (Порески идентификацијски број – ПИБ број правног лица).
Назив организације (O)	Пуни регистровани скраћени назив правног лица или назив правног лица ако скраћени назив није регистрован.
Мјесто (L)	Мјесто сједишта правног лица регистрованог у Босни и Херцеговини.
Назив државе (C)	*BA*

Табела 17. Структура имена правног лица за квалификовани електронски печат

3.1.2. Номенклатура имена

У поље *Subject* квалификоване потврде уписују се подаци о физичком лицу како су наведени у важећем идентификационом документу. Код физичког лица које је повезано са правним лицем у оквиру атрибута који идентификује корисника налазе се и регистровани подаци правног лица.

У сваку потврду уписују се подаци о имену, односно називу субјекта овјеравања, те податак о мјесту пребивалишта и држави физичког лица, односно мјесту и држави сједишта пословног субјекта. Подаци о имену или називу који се уписују у потврду односе се на аутентично име или назив субјекта. Поље *Subject* у потврди усклађено је с документом IETF RFC 5280.

Поље *Subject* у потврдама које се издају за физичка лица садржи име и презиме лица. У пословним потврдама и потврдама за електронски печат поље *Subject* додатно садржи и пуни регистровани назив пословног субјекта и његов идентификатор.

Уколико било који податак који се уноси у поље *Subject* садржи посебне знакове или слова која нису садржана у службеним писмима Босне и Херцеговине, такви знакови се замјењују најближим знаком енглеске абецеде.

Код потврда за аутентификацију *Web* страница поље *Subject* и екстензија *Subject Alternative Name* садрже пуни квалификовани назив сервера (*FQDN*).

Садржај екстензије *Subject Alternative Name* код потврде за физичка лица и физичког лица повезаног са правним лицем може бити *e-mail* адреса субјекта.

3.1.3. Смисленост имена

Имена и називи у атрибутима поља *Subject* који идентификују физичко лице и пословни субјект су смислени. За атрибуте у пољу *Subject* у потврдама које издаје Овјерилац УИО примјењују се сљедећа правила:

- Лично име и презиме морају бити како су наведени у идентификационој исправи, односно у службеним матичним регистрима,
- Назив пословног субјекта мора бити како је наведен у службеним надлежним националним регистрима.

ОДРЕЂИВАЊЕ ЕЛЕМЕНАТА ПОЉА SUBJECT У ПОТВРДАМА	
НАЗИВ ПОТВРДЕ	**АТРИБУТИ И ВРИЈЕДНОСТИ ПОЉА SUBJECT**
УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКО ЛИЦЕ	▪ **commonName (CN)**: Име и презиме потписника ▪ **serialNumber**: *CA:BA*-ЈИП ▪ **givenName (G)**: Име потписника ▪ **surname (SN)**: Презиме потписника ▪ **localityName (L)**: Мјесто пребивалишта потписника ▪ **countryName (C)**: *BA*
УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКО ЛИЦЕ ПОВЕЗАНО СА ПРАВНИМ ЛИЦЕМ	▪ **commonName (CN)**: Име и презиме потписника ▪ **serialNumber**: *CA:BA*-ЈИП ▪ **givenName (G)**: Име потписника ▪ **surname (SN)**: Презиме потписника ▪ **organizationIdentifier (2.5.4.97)** : *VATBA*-ПИБ ▪ **organizationName (O)**: Скраћени назив пословног субјекта или пуни регистровани назив пословног субјекта ако скраћени назив није регистрован ▪ **localityName (L)**: Мјесто сједишта пословног субјекта ▪ **countryName (C)**: *BA*

ОДРЕЂИВАЊЕ ЕЛЕМЕНАТА ПОЉА SUBJECT У ПОТВРДАМА	
НАЗИВ ПОТВРДЕ	**АТРИБУТИ И ВРИЈЕДНОСТИ ПОЉА SUBJECT**
УИО КВАЛИФИЦИКОНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ЗАПОСЛЕНЕ	▪ **commonName (CN)**: Име и презиме потписника ▪ **serialNumber**: *CA:BA*-ЈИП ▪ **givenName (G)**: Име потписника ▪ **surname (SN)**: Презиме потписника ▪ **organizationIdentifier (2.5.4.97)** : *VATBA*-ПИБ УИО ▪ **organizationName (O)**: Скраћени назив пословног субјекта или пуни регистровани назив пословног субјекта ако скраћени назив није регистрован ▪ **localityName (L)**: Мјесто сједишта УИО ▪ **countryName (C)**: *BA*
УИО КВАЛИФИЦИКОНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ	▪ **commonName (CN)**: Назив који субјекат користи за своје представљање ▪ **serialNumber**: *CA*:*BA*-ЈИП ▪ **organizationIdentifier (2.5.4.97)** : *VATBA*-ПИБ ▪ **organizationName (O)**: Скраћени назив пословног субјекта или пуни регистровани назив пословног субјекта ако скраћени назив није регистрован ▪ **localityName (L)**: Мјесто сједишта пословног субјекта ▪ **countryName (C)**: *BA*
УИО ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ *WEB* СТРАНИЦА	▪ **commonName**: FQDN сервера ▪ **organizationIdentifier (2.5.4.97)**:*VATBA*-ПИБ ▪ **organizationName**: Назив правног лица ▪ **localityName**: Мјесто сједишта правног лица ▪ **countryName**: *BA*

Табела 18. Одређивање елемената поља *Subject* у потврдама

3.1.4. Правила тумачења разних облика имена

Тумачење облика имена у пољу *Subject* по норми X.520 у Овјериоцу УИО одређено је на сљедећи начин:

- commonName – У потврдама за физичка лица, физичка лица повезана са правним лицима и потврдама за запослене овај атрибут садржи име и презиме физичког лица како је наведено у идентификационој исправи. У потврдама за аутентификацију *Web* страница ставља се само један пуни квалификовани назив сервера (*FQDN*).
- serialNumber – Овај атрибут у пољу *Subject* осигурава јединственост имена субјекта. У потврдама за физичка лица, физичка лица повезана са правним лицима и потврдама за запослене састоји се од скраћенице Овјериоца (CA), двословног ISO кода државе пребивалишта потписника (BA) и псеудослучајно генерисаног броја потврде (ЈИП). У апликацијским потврдама се ово поље не користи.
- givenName – Садржи име физичког лица како је наведено у идентификационој исправи.
- surname – Садржи презиме физичког лица како је наведено у идентификационој исправи.
- organizationIdentifier – У потврдама за физичка лица повезана са правним лицима и потврдама за запослене састоји се од ознаке VAT, двословног ISO кода државе пребивалишта потписника (BA) и пореског идентификационог броја правног лица (ПИБ).
- localityName – У потврдама за физичка лица повезана са правним лицима атрибут *localityName* садржи назив мјеста у којем је сједиште пословног субјекта. У потврдама за физичка лица атрибут *localityName* садржи мјесто пребивалишта потписника. У апликацијским потврдама атрибут *localityName* садржи назив мјеста у којем је сједиште пословног субјекта.
- countryName – Садржи ознаку двословног ISO кода Босне и Херцеговине.

Екстензија *Subject Alternative Name* садржи барем један *FQDN* сервера у потврдама за аутентификацију *Web* страница, односно *e-mail* адресу потписника или *e-mail* адресу повезану с ИТ системом, апликацијом или сервисом у осталим потврдама.

УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА		
АТРИБУТ	**ВРИЈЕДНОСТ**	**ОПИС**
commonName (CN)	Име и презиме	Име и презиме потписника како је наведено у идентификационој исправи
serialNumber	*CA:BA*-ЈИП	ЈИП је псеудослучајно генерисан број потврде
givenName (G)	Име потписника	Име потписника како је наведено у идентификационој исправи
surname (SN)	Презиме потписника	Презиме потписника како је наведено у идентификационој исправи
localityName (L)	Мјесто пребивалишта потписника	Мјесто пребивалишта физичког лица

countryName (C)	Држава потписника	Двословни ISO код државе пребивалишта потписника, BA за Босну и Херцеговину

Табела 19. Тумачење облика имена по X.520 норми за УИО квалификоване потврде за електронски потпис за физичка лица

УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ФИЗИЧКА ЛИЦА ПОВЕЗАНА СА ПРАВНИМ ЛИЦИМА		
АТРИБУТ	**ВРИЈЕДНОСТ**	**ОПИС**
commonName (CN)	Име и презиме	Име и презиме потписника како је наведено у идентификационој исправи
serialNumber	*CA:BA*-ЈИП	ЈИП је псеудослучајно генерисан број потврде
givenName (G)	Име потписника	Име потписника како је наведено у идентификационој исправи
surname (SN)	Презиме потписника	Презиме потписника како је наведено у идентификационој исправи
organizationIdentifier (2.5.4.97)	*VATBA*-ПИБ	ПИБ је порески идентификациони број правног лица
organizationName (O)	Назив пословног субјекта	Скраћени назив пословног субјекта или пуни регистровани назив пословног субјекта ако скраћени назив није регистрован
localityName (L)	Мјесто сједишта пословног субјекта	Мјесто сједишта пословног субјекта
countryName (C)	BA	Двословни ISO код државе Босне и Херцеговине

Табела 20. Тумачење облика имена по X.520 норми за УИО квалификоване потврде за електронски потпис за физичка лица повезана са правним лицима

УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПОТПИС ЗА ЗАПОСЛЕНЕ		
АТРИБУТ	**ВРИЈЕДНОСТ**	**ОПИС**
commonName (CN)	Име и презиме	Име и презиме потписника како је наведено у идентификационој исправи
serialNumber	*CA:BA*-ЈИП	ЈИП је псеудослучајно генерисан број потврде
givenName (G)	Име потписника	Име потписника како је наведено у идентификационој исправи
surname (SN)	Презиме потписника	Презиме потписника како је наведено у идентификационој исправи
organizationIdentifier (2.5.4.97)	*VATBA*-ПИБ УИО	ПИБ УИО је порески идентификациони број Управе за индиректно опорезивање

organizationName (O)	*Uprava za indirektno-neizravno oporezivanje*	Назив пословног субјекта
localityName (L)	Мјесто сједишта УИО или регионалног центра	Мјесто сједишта УИО или регионалног центра
countryName (C)	*BA*	Двословни ISO код државе Босне и Херцеговине

Табела 21. Тумачење облика имена по X.520 норми за УИО квалификоване потврде за електронски потпис за запослене

УИО КВАЛИФИКОВАНА ПОТВРДА ЗА ЕЛЕКТРОНСКИ ПЕЧАТ		
АТРИБУТ	**ВРИЈЕДНОСТ**	**ОПИС**
commonName (CN)	Назив пословног субјекта	Назив који пословни субјекат користи за своје представљање
serialNumber	*CA*:*BA*-ЈИП	ЈИП је псеудослучајно генериран број субјекта
organizationIdentifier (2.5.4.97)	*VATBA*-ПИБ	ПИБ је порески идентификацијски број правног лица
organizationName (O)	Назив пословног субјекта	Скраћени назив пословног субјекта или пуни регистровани назив пословног субјекта ако скраћени назив није регистрован
localityName (L)	Мјесто сједишта пословног субјекта	Мјесто сједишта пословног субјекта
countryName (C)	*BA*	Двословни ISO код државе Босне и Херцеговине

Табела 22. Тумачење облика имена по X.520 норми за УИО квалификоване потврде за електронски печат

УИО ПОТВРДА ЗА АУТЕНТИФИКАЦИЈУ WEB СТРАНИЦА		
АТРИБУТ	**ВРИЈЕДНОСТ**	**ОПИС**
commonName (CN)	Пуни квалификовани назив сервера (FQDN)	Само један пуни квалификовани назив сервера (FQDN)
organizationIdentifier (2.5.4.97)	*VATBA*-ПИБ	ПИБ је порески идентификациони број правног лица
organizationName	Назив пословног субјекта	Пуни регистровани скраћени назив пословног субјекта или назив пословног субјекта ако скраћени назив није регистрован
localityName (L)	Мјесто сједишта пословног субјекта	Мјесто сједишта пословног субјекта
countryName (C)	*BA*	Двословни ISO код државе Босне и Херцеговине

Табела 23. Тумачење облика имена по X.520 норми за УИО потврде за аутентификацију *Web* страница

3.1.5. Јединственост имена

Јединствено име субјекта јединствено је унутар Овјериоца УИО и продукционе хијерархије засноване на серверу *UINO Root CA*. Јединственост имена осигурана је вриједношћу атрибута *serialNumber* у пољу *Subject* потврде.

Овјерилац УИО самостално контролише и додјељује вриједност атрибута *serialNumber* у јединственом имену да би имена различитих субјеката била јединствена.

У апликационим потврдама јединственост имена осигурава се на начин да се у атрибут *commonName* јединственог имена потврде уписује назив апликације који унутар истог пословног субјекта мора бити јединствен.

Јединственост имена у администраторским потврдама осигурана је вриједношћу атрибута *serialNumber* у пољу *Subject* потврде.

3.1.6. Анонимност или псеудоними корисника

Корисници не могу да буду анонимни и не могу да користе псеудониме.

Овјерилац УИО одбија било који захтјев за анонимношћу или за коришћењем псеудонима.

3.1.7. Правила за тумачење различитих врста имена

У квалификованим електронским потврдама имена корисника су вјерно представљена одговарајућим латиничним или ћириличним словима.

Знакови које није дозвољено користити у именима корисника су: " (наводници), ? (упитник), \ (обрнута коса црта), # (тараба), $ (долар), % (проценат), = (једнако), + (плус), | (усправна црта), ; (тачка-зарез), < (мање), > (веће) и , (зарез).

3.1.8. Јединственост имена

Овјерилац УИО гарантује јединственост имена у свом домену. Овјерилац УИО додјељује сваком кориснику јединствено име (*Distinguished Name - DN*), које се уписује у поље *Subject* електронске потврде.

3.1.9. Признавање, аутентификација и улога заштитног знака

Имена којима би се кршила интелектуална или ауторска права других нису дозвољена. Овјерилац УИО није обавезан да верификује да ли је коришћење таквих имена законито. Корисник сноси одговорност за то да обезбиједи законито коришћење одабраног имена.

Овјерилац УИО ће, што је могуће прије, извршити све судске налоге који су издати у складу са законима, а који се тичу правних лијекова за било какво кршење права трећих лица приликом издавања електронских потврда по овим Практичним правилима.

3.2. Почетна провјера ваљаности идентитета

Почетна провјера тачности идентитета је дио процеса захтјева за издавање потврде.

3.2.1. Метод доказивања посједовања приватног кључа

Приватни криптографски кључ корисника квалификованих потврда се генерише у Овјериоцу УИО на *SSCD* уређају.

3.2.2. Аутентификација идентитета физичког лица

Корисник мора бити идентификован у складу са овим Практичним правилима.

Корисник мора бити физички присутан током регистрације.

Током регистрације корисник мора да посједује важећи идентификациони документ са фотографијом (важећа лична карта, пасош или други). Приликом регистрације корисник треба приложити овјерену фотокопију идентификационог документа.

Фотографија у документу за идентификацију се пореди с корисником који је физички присутан (карактеристике лица, старост, пол и сл.).

3.2.3. Аутентификација идентитета правног лица

Квалификована електронска потврда за електронски потпис се може издати само физичком лицу, у складу са Законом о електронском потпису. Физичко лице има право да у име правног лица користи квалификовану електронску потврду, уколико му то дозволи правно лице. Физичко лице може да буде запослено у правном лицу. Квалификована потврда за електронски печат може се издати само правном лицу.

Уколико Овјерилац УИО издаје електронску потврду физичком лицу које је запослено у правном лицу, у оквиру атрибута који идентификују корисника налазе се и подаци који означавају назив правног лица и то пословно име правног лица и идентификатор организације, односно порески идентификациони број.

Уколико је корисник физичко лице која је запослено у правном лицу, неопходно је:

- Утврдити тачан идентитет правног лица и ауторизацију коришћења његовог имена,

- Приложити службене документе о том правном лицу приликом подношења захтјева (Рјешење о регистрацији правног лица – оригинал или овјерена фотокопија), ради потврђивања ваљаности имена правног лица,
- Доказати да је корисник овлаштен од стране правног лица за добијање електронске потврде.

Уколико је корисник физичко лице - странац која је запослена у правном лицу регистрованом у Босни и Херцеговини, неопходно је:

- Утврдити тачан идентитет физичког лица и ауторизацију коришћења његовог имена,
- Потврдити ваљаност имена физичког лица, током чега подносилац захтјева мора осигурати сљедеће службене документе о том физичком лицу:
  - Ваљан идентификациони документ неопходан за улазак у Босну и Херцеговину,
  - Пријаву боравка издату од стране надлежног органа,
  - Потврду о пријави рада издату од стране надлежног органа,
  - Радну дозволу издату од стране надлежног органа,
  - Уговор о раду (издаје правно лице регистровано у Босни и Херцеговини у којој ће радити физичко лице-странац),
- Доказати да је корисник овлаштен од стране правног лица за добијање електронске потврде.

3.2.4. Непровјерени подаци о кориснику

Сви подаци о кориснику које захтијева Закон о електронском потпису морају да буду прописно провјерени.

3.2.5. Провјера тачности података правног лица

Корисник доставља важећу документацију за име правног лица, које ће бити укључено у електронску потврду. Избор ријечи у имену правног лица које треба уписати у потврду мора да буде идентичан ријечима у достављеној документацији.

Коришћење имена правног лица морају дозволити и ауторизовати одговорни представници правног лица, и то:

- Коришћење имена правног лица које је регистровано у судском регистру, морају да ауторизују одговорна лица тог правног лица,
- Коришћење имена правног лица која има једног власника, мора да ауторизује власник,
- Коришћење имена правног лица које је у власништву више партнера, мора да ауторизује партнер који је наведен у уговору о партнерству,
- Коришћење имена правног лица које је власништво неке заједнице, мора да ауторизује надлежна институција.

3.2.6. Критеријуми за међусобну сарадњу

Овјерилац УИО не предвиђа унакрсно овјеравање.

3.3. Идентификација и аутентификација захтјева за обновом кључа

3.3.1. Идентификација и аутентификација за рутинском обновом кључа

Овјерилац УИО не дозвољава обнову кључа. Цијели процес се извршава издавањем нове електронске потврде на претходно описани начин.

3.3.2. Идентификација и аутентификација захтјева за замјеном кључа послије опозива

Овјерилац УИО не дозвољава замјену кључа послије опозива. Цијели процес се извршава издавањем нове електронске потврде.

3.4. Идентификација и аутентификација захтјева за опозивом

Корисник захтијева опозив електронске потврде по једној од сљедећих процедура:

- Корисник се идентификује лично и предаје својеручно потписан захтјев Групи за подршку корисницима система PKI УИО у регионалном центру или сједишту УИО,
- Корисник шаље електронски потписан захтјев електронском поштом (е-маил) Групи за одржавање система PKI УИО, на унапријед одређену адресу електронске поште. Група за одржавање система PKI УИО признаје само електронски потписане захтјеве са важећом квалификованом електронском потврдом издатом од стране Овјериоца УИО. Захтјев се може послати само са *e-mail* адресе која је наведена приликом регистрације корисника у његовом захтјеву и која се налази у издатој потврди.

4. ОПЕРАТИВНИ ЗАХТЈЕВИ У ПРОЦЕСУ ИЗДАВАЊА ПОТВРДА

4.1. Захтјеви за издавање потврда

4.1.1. Ко може да поднесе захтјев за издавање потврде

Захтјев може да поднесе свако физичко лице које испуњава услове наведене у овим Практичним правилима.

4.1.2. Услови за издавање потврде

За издавање квалификоване електронске потврде, корисник је дужан да:

- Попуни и потпише захтјев за издавање и коришћење електронске потврде и уз исти приложи овјерену фотокопију идентификационог документа,
- Испуни захтјеве за идентификацију,
- Испуни финансијске обавезе према цјеновнику,
- Потпише уговор о издавању и коришћењу електронске потврде.

Квалификована електронска потврда за електронски потпис се издаје искључиво физичком лицу.

Квалификована електронска потврда за електронски печат се издаје искључиво правном лицу.

Захтјев за издавање и коришћење електронске потврде садржи податке на основу којих Овјерилац УИО може да ступи у контакт са корисником електронске потврде.

Уговор садржи услове издавања и коришћења потврде, а ступа на снагу када га потпишу уговорне стране.

У случају када се потврда издаје физичком лицу унутар правног лица, прво се потписује уговор са правним лицем, а затим појединачно са сваким физичким лицем унутар правног лица коме се издаје потврда.

Коришћење квалификоване електронске потврде се уговара на рок од пет година и везује се за дан издавања потврде.

4.2. Обрада захтјева за издавање потврда

4.2.1. Обављање функција идентификације и потврђивања аутентичности

Овјерилац УИО идентификује корисника на основу идентификационог документа који корисник подноси (важећа лична карта, пасош или други). Корисник мора лично да поднесе цјелокупну документацију.

4.2.2. Одобрење или одбијање захтјева за издавање потврда

Овјерилац УИО ће одобрити захтјев за издавање квалификоване електронске потврде, уколико су испуњени сљедећи услови:

- Корисник је лично поднио потребну документацију,
- Поднесена документација је провјерена,
- Сви подаци унесени у захтјев сматрају се одговарајућим и комплетним.

Ако корисник не испуни услове из претходног става или ако на било који начин повриједи одредбе ових Практичних правила, Овјерилац УИО ће одбити захтјев за издавање електронске потврде.

4.2.3. Вријеме обраде захтјева за издавање потврде

Овјерилац УИО врши обраду захтјева послије приспјећа захтјева од стране Групе за подршку корисницима система PKI УИО у регионалном центру. Обрада захтјева може да траје најдуже 30 радних дана од дана пријема захтјева.

4.3. Издавање потврда

4.3.1. Активности током издавања потврде

Издавање електронске потврде, врши се на сљедећи начин:

1. Корисник преко *Web* сајта Овјериоца УИО преузима Захтјев за издавање електронске потврде и попуњава га,
2. Корисник, у поступку издавања потврде, идентификује се лично у Групи за подршку корисницима система PKI УИО у регионалном центру,
3. Група за подршку корисницима система PKI УИО у регионалном центру уноси податке о кориснику и креира захтјев у апликацији Регистрационог тијела и прослеђује верификован захтјев Групи за одржавање система PKI УИО,
4. Група за одржавање система PKI УИО на основу верификованог захтјева креира налог за персонализацију криптографског уређаја,
5. Кориснички приватни криптографски кључ се генерише у хардверском криптографском модулу *SSCD* уређаја код Овјериоца УИО,
6. Овјерилац УИО шаље издане корисничке потврде на *SSCD* уређају у регионални центар,
7. Корисник потписује уговор о издавању и коришћењу електронске потврде, преузима електронску потврду на *SSCD* уређају у Групи за подршку корисницима система PKI УИО у регионалном центру и потписује изјаву о преузимању електронске потврде на *SSCD* уређају,
8. Корисник преузима припадајућу лозинку/*PIN* код у затвореној коверти у Групи за подршку корисницима система PKI УИО у регионалном центру**.**

4.3.2. Обавјештавање корисника о издавању потврде

Овјерилац УИО позива корисника да у Групи за подршку корисницима система PKI УИО у регионалном центру преузме електронску потврду на *SSCD* уређају.

4.4. Преузимање потврда

4.4.1. Поступак преузимања потврда

Кориснику се квалификована електронска потврда уручује лично у Групи за подршку корисницима система PKI УИО у регионалном центру.

Првом употребом електронске потврде од стране корисника, потврда се сматра прихваћеном.

Уколико се накнадно утврди да у електронској потврди постоје погрешни подаци, корисник је дужан да се обрати Овјериоцу УИО, ради издавања нове потврде.

4.4.2. Објављивање потврда

Електронска потврда се јавно не објављује од стране Овјериоца УИО.

4.4.3. Обавјештавање о издавању потврда трећих лица

Трећа лица се не обавјештавају о издавању електронске потврде.

4.5. Коришћење пара криптографских кључева и потврде

4.5.1. Коришћење приватног кључа корисника и потврде од стране корисника

Приватни криптографски кључеви потврде *UINO Root CA*, *UINO Issuing CA1* и *UINO Issuing CA2* користе се за потписивање потврда и *CRL*-ова.

Приватни криптографски кључ корисника се користи за креирање квалификованог електронског потписа, а квалификована електронска потврда за верификовање квалификованог електронског потписа.

4.5.2. Коришћење јавног кључа и потврда од стране трећег лица

Треће лице користи јавни кључ и електронску потврду за верификовање електронског потписа.

4.6. Продужетак коришћења потврде

Овјерилац УИО не врши продужење коришћења електронске потврде. Цијели процес се извршава издавањем нове електронске потврде.

4.7. Замјена јавног кључа у потврди

Замјена јавног кључа у електронској потврди се не врши. Цијели процес се извршава издавањем нове електронске потврде.

4.7.1. Околности за замјену јавног кључа у потврди

Не врши се.

4.7.2. Ко може да захтјева замјену јавног кључа у потврди

Не врши се.

4.7.3. Обрада захтјева за замјену јавног кључа у потврди

Не врши се.

4.7.4. Обавјештавање корисника о замјени јавног кључа у потврди

Не врши се.

4.7.5. Поступак прихватања обавјештења о замјени јавног кључа у потврди

Не врши се.

4.7.6. Објављивање потврде код које је извршена замјена јавног кључа

Не врши се.

4.7.7. Обавјештавање трећих лица о издавању потврда

Не врши се.

4.8. Промјена података у потврди

Измјена података у електронској потврди се не врши. Цијели процес се извршава издавањем нове електронске потврде.

4.8.1. Околности за промјену података у потврди

Не врши се.

4.8.2. Ко може да захтјева промјену података у потврди

Не врши се.

4.8.3. Обрада захтјева за промјену података у потврди

Не врши се.

4.8.4. Обавјештење корисника о промјени података у потврди

Не врши се.

4.8.5. Поступак прихватања обавјештења о промјени података у потврди

Не врши се.

4.8.6. Објављивање потврда код кога је извршена промјена података

Не врши се.

4.8.7. Обавјештење трећих лица о издавању потврда

Не врши се.

4.9. Опозив и суспензија потврде

4.9.1. Околности опозива потврде

4.9.1.1. Околности опозива потврда Овјериоца УИО

Овјерилац УИО ће опозвати потврду Овјериоца УИО у року од 5 (пет) дана:

- Ако се заприми доказ да је приватни кључ повезан са јавним кључем у потврди Овјериоца УИО компромитован,
- У случају потребе за промјеном криптографског алгоритма и припадајуће дужине кључа,
- У случају доказа о злоупотреби потврде Овјериоца УИО,
- Ако овлаштено лице Овјериоца УИО поднесе писани захтјев за опозив потврде Овјериоца УИО.

4.9.1.2. Околности опозива корисничких потврда

Овјерилац УИО је дужан да опозове електронску потврду из сљедећих разлога:

- У случају да нека информација садржана у потврди постане нетачна,
- Промјене података у потврди, које захтјевају издавање нове потврде,
- Накнадног утврђивања да подаци које је доставио корисник при идентификацији нису тачни,
- Губитка, оштећења или злоупотребе техничких средстава (хардвера или софтвера) или приватног криптографског кључа, односно компромитовања или сумње у компромитовање приватног криптографског кључа,
- У случају трајне недоступности приватног кључа,
- У случају ако приватни кључ или активациони подаци нису више у посједу потписника, односно печатиоца,
- У случају престанка односа између потписника и пословног субјекта,
- Неиспуњавања обавеза корисника потврде одређених овим Практичним правилима и уговором,
- Уколико опозив електронске потврде захтјева корисник потврде,
- Уколико корисник електронске потврде престане да постоји,
- Уколико корисник изгуби пословну способност или правно лице којем припада корисник престане да постоји,
- У случају да потврда више није у складу са општим правилима,
- Уколико се промијене околности које битно утичу на важење потврде,
- У случају отказа уговора о обављању услуге овјеравања од стране корисника,
- Из других разлога који су утврђени Законом о електронском потпису и другим прописима који регулишу ову област.

4.9.2. Ко може да захтијева опозив потврде

Опозив електронске потврде може да захтјева:

- Корисник електронске потврде – физичко лице,
- Правно лице за запослене у том правном лицу,
- Овјерилац УИО,
- Надлежни државни орган на основу закона.

4.9.3. Процедуре за опозив потврде

4.9.3.1. Опозив потврде због компромитовања приватног криптографског кључа

Опозив електронске потврде због компромитовања или сумње у компромитовање приватног криптографског кључа, врши се на сљедећи начин:

1. Корисник захтјева опозив електронске потврде по једној од сљедећих процедура:

    - Корисник преко *Web* сајта Овјериоца УИО преузима Захтјев за промјену статуса квалификоване електронске потврде и попуњава га. Корисник се идентификује лично у Групи за подршку корисницима система PKI УИО у регионалном центру у којој предаје својеручно потписан захтјев. Послије успјешне идентификације, Група за подршку корисницима система PKI УИО у регионалном центру уноси захтјев у апликацију Регистрационог тијела и прослијеђује га Групи за одржавање система PKI УИО.
    - Корисник шаље захтјев који је електронски потписан квалификованом електронском потврдом електронском поштом (*e-mail*) Групи за одржавање система PKI УИО на унапријед одређену адресу електронске поште. Група за одржавање система PKI УИО признаје само електронски потписане захтјеве са важећом квалификованом електронском потврдом изданом кориснику од стране Овјериоца УИО. Захтјев се може послати само са *e-mail* адресе која је наведена приликом регистрације корисника у његовом захтјеву и која се налази у изданој потврди.

2. Група за одржавање система PKI УИО верификује захтјев корисника (добијен од корисника електронском поштом или добијен од Групе за подршку корисницима система PKI УИО у регионалном центру) и опозива електронску потврду.

Група за одржавање система PKI УИО обавјештава корисника о опозиву електронске потврде електронском поштом. У случају да корисник не посједује адресу електронске поште, обавјештење о опозиву биће му послано поштом на адресу назначену у уговору.

Овјерилац УИО може да се одлучи за опозив квалификоване електронске потврде и без захтјева корисника, уколико установи да је дошло или сумња да је дошло до компромитовања приватног криптографског кључа повезаног с том потврдом.

Послије опозива електронске потврде, корисник може да захтјева издавање нове електронске потврде.

4.9.3.2. Опозив потврде због промјене података у потврди

Опозив електронске потврде због промјене података у потврди, врши се на исти начин како је одређено у тачки 4.9.3.1.

Овјерилац УИО може да се одлучи за опозив електронске потврде и без захтјева корисника, уколико процјени да је дошло до промјене података у потврди, које захтјевају издавање нове електронске потврде.

Послије опозива електронске потврде, корисник може да захтјева издавање нове електронске потврде.

4.9.3.3. Опозив потврде због неиспуњења обавеза корисника

У случају да корисник не испуњава своје обавезе, Група за одржавање система PKI УИО у Овјериоцу УИО врши опозив електронске потврде корисника.

Група за одржавање система PKI УИО обавјештава корисника о опозиву електронске потврде електронском поштом. У случају да корисник не посједује адресу електронске поште, обавјештење о опозиву биће му послато поштом на адресу назначену у уговору.

Послије опозива квалификоване електронске потврде, корисник може да захтјева издавање нове електронске потврде.

4.9.4. Вријеме од пријаве до опозива потврде

Послије подношења захтјева за опозив електронске потврде од стране корисника Овјерилац УИО ће приступити обради захтјева за опозивом потврде, без одлагања.

4.9.5. Временски рок у коме овјерилац спроводи захтјев за опозив потврде

Група за одржавање система PKI УИО, извршава опозив електронске потврде одмах по пријему захтјева за опозив потврде и објављује нови регистар опозваних потврда.

4.9.6. Захтјев за провјеру опозваности потврда од стране трећих лица

Током рада са електронским потврдама издатим од стране Овјериоца УИО, трећа лица имају обавезу да провјеравају опозваност потврда.

4.9.7. Учесталост објављивања регистра опозваних потврда

Регистри опозваних потврда овјериоца *UINO Root CA* објављују се на сваких 6 мјесеци и приликом опозива подређеног овјериоца или потврде за потписивање одговора *OCSP* сервиса овјериоца *UINO Root CA*.

Регистри опозваних потврда овјерилаца *UINO Issuing CA1* и *UINO Issuing CA2* објављују се на свака 24 часа.

У случају да прије редовне објаве дође до опозива или суспензије електронске потврде, Овјерилац УИО одмах објављује нови регистар опозваних потврда и прије истека важења регистра опозваних потврда.

4.9.8. Максимално кашњење у објављивању регистра опозваних потврда

Максимално кашњење објаве *CRL* листе у јавном репозиторијуму јесте један минут. У случају непредвиђених околности које резултују дужим кашњењем објаве *CRL* листе, Овјерилац УИО ће обавијестити кориснике о разлогу кашњења и временском интервалу унутар кога није објављена валидна *CRL* листа.

4.9.9. Расположивост on-line провјере опозваности/статуса потврда

Регистар опозваних потврда и *OCSP* сервис су стално доступни за *on-line* провјеру опозваности електронских потврда.

Путем *OCSP* сервиса Овјериоца УИО доступне су информације о статусу опозваности потврда које су издате од стране Овјериоца УИО.

Адреса УИО *OCSP* сервиса је http://ocsp.uino.gov.ba, а садржана је у екстензији *Authority Information Access* сваке потврде коју издају *UINO Root CA* и подређени *UINO Issuing CA1* и *UINO Issuing CA2*.

Доступност *CRL* и *OCSP* сервиса је 24 часа на дан, 7 дана у седмици.

4.9.10. Захтјеви за on-line провјеру опозваности потврда

Корисници и трећа лица су дужни да провјере статус електронске потврде на основу јавно доступног регистра опозваних потврда Овјериоца УИО.

4.9.11. Друге форме регистра опозваних потврда

Регистар опозваних потврда је расположив и на *Web* страници Овјериоца УИО.

4.9.12. Посебни захтјеви у случају компромитовања кључа

Ако корисник зна или сумња у компромитацију његовог приватног кључа дужан је да одмах престане са његовим коришћењем и поднесе захтјев за опозив електронске потврде.

4.9.13. Околности суспензије и прекида суспензије потврде

Суспензија је привремено деактивирање електронске потврде издане кориснику.

Овјерилац УИО може да суспендује електронске потврде током провјеравања околности у вези са могућим опозивом потврде.

Прекидом (укидањем) суспензије електронска потврда постаје активна (важећа), тако да има све функционалности које је имала и прије суспензије.

4.9.14. Ко може да захтијева суспензију и прекид суспензије потврде

Суспензију електронске потврде може да захтијева:

- Корисник електронске потврде – физичко лице,
- Правно лице за запослене у том правном лицу,
- Овјерилац УИО,
- Надлежни државни орган, на основу закона.

Прекид суспензије може да захтијева:

- Корисник електронске потврде, када установи да су разлози за суспензију престали,
- Правно лице, након престанка разлога суспензије потврде,
- Овјерилац УИО, када установи да су разлози за суспензију престали,
- Надлежни државни орган, на основу закона.

4.9.15. Процедуре за суспензију и прекид суспензије потврде

Суспензија или прекид суспензије квалификоване електронске потврде, врши се на сљедећи начин:

1. Корисник подноси захтјев за суспензију или прекид суспензије електронске потврде по једној од сљедећих процедура:

    - Корисник преко *Web* сајта Овјериоца УИО преузима Захтјев за промјену статуса електронске потврде и попуњава га. Корисник се идентификује лично у Групи за подршку корисницима система PKI УИО у регионалном центру у којем предаје својеручно потписан захтјев. Послије успјешне

идентификације, Група за подршку корисницима система PKI УИО уноси захтјев у апликацију Регистрационог тијела и прослиједјује га Групи за одржавање система PKI.

- Корисник шаље захтјев који је електронски потписан квалификованом електронском потврдом електронском поштом (*e-mail*) Групи за одржавање система PKI УИО на унапријед одређену адресу електронске поште. Група за одржавање система PKI УИО признаје само електронски потписане захтјеве са важећом квалификованом електронском потврдом изданом кориснику од стране Овјериоца УИО. Захтјев се може послати само са *e-mail* адресе која је наведена приликом регистрације корисника у његовом захтјеву.

2. Група за одржавање система PKI УИО верификује захтјев корисника (добијен од корисника електронском поштом или добијен од Групе за подршку корисницима система PKI УИО) и извршава суспензију или прекид суспензије електронске потврде и о томе обавјештава корисника путем електронске поште.

Уколико Овјерилац УИО сумња да је дошло до компромитације приватног криптографског кључа или да је дошло до промјене података у потврди корисника, може да суспендује електронску потврду и без захтјева корисника.

4.9.16. Ограничење периода на који се потврда суспендује

Период суспензије електронске потврде је максимално 30 дана.

4.10. Услуге о статусу потврда

4.10.1. Оперативне карактеристике

Овјерилац УИО пружа услугу провјере статуса опозваности електронске потврде посредством регистра опозваних потврда.

4.10.2. Доступност услуге

Регистар опозваних потврда је стално доступан.

4.10.3. Додатне карактеристике

У регистру опозваних потврда поред података о серијском броју, датуму и времену опозива електронске потврде уписан је и разлог опозива потврде.

4.11. Престанак коришћења потврде

Корисник престаје са коришћењем квалификоване електронске потврде:

- Истеком рока важности електронске потврде,
- Опозивом електронске потврде,
- Током трајања суспензије електронске потврде.

4.12. Откривање и обнова приватног кључа корисника

4.12.1. Политика откривања и обнове приватног кључа корисника

Овјерилац УИО не чува приватне кључеве корисника квалификованих електронских потврда и не може да их открије нити обнови.

4.12.2. Политика енкапсулације кључа сесије и обнове

Не врши се.

5. КОНТРОЛА ФИЗИЧКОГ ПРИСТУПА, ПРОЦЕДУРА И ОВЛАШЋЕНИХ ЛИЦА

Ово поглавље описује контролу физичког окружења, процедура и овлашћених лица, која је имплементирана код Овјериоца УИО да би се заштитило функционисање система.

Процедуре су дефинисане у политици информационе безбједности која се документује, проводи и одржава, а обухвата безбједоносне контроле и оперативне поступке за објекте, системе и информатичку опрему у складу са стандардом ISO/IEC 27001.

УИО дефинише политику информационе безбједности коју одобрава управа УИО и одређује начин управљања својом информационом безбједношћу. О промјенама политике безбједности информација саопштаваће се трећим странама, према потреби. Ово укључује све поуздајуће стране, тијела за оцјењивање, надзорна или друга регулаторна тијела.

Ради се препознавање, анализирање и процјена пословних и техничких ризика на основу стандарда ISO 9001 и ISO/IEC 27001. УИО проводи све безбједоносне захтјеве и оперативне поступке, како су документовани у политици информационе безбједности, на основу одабране мјере смањења ризика.

УИО води попис све информацијске имовине и додјељује класификацију у складу с процјеном ризика.

Политика информационе безбједности и попис информатичке опреме прегледавају се у планираним интервалима (најмање једном сваке године) ради очувања сврхе и учинковитости политике информационе безбједности, те у случају значајних промјена. Све промјене које могу утицати на пружени ниво безбједности одобрава управа УИО.

5.1. Контрола физичког приступа

Овјерилац УИО као вршилац услуга издавања квалификованих електронских потврда примјењује мјере физичке заштите система у складу са овим правилима, важећим законским и подзаконским прописима и међународним препорукама у складу са стандардом ISO/IEC 27001.

Овјерилац УИО примјењује мјере физичке заштите система издавања електронских потврда ради ограничавања приступа хардверским и софтверским компонентама система као што су сервери, радне станице, криптографски модули, мрежни уређаји и припадајући софтвер и архиви.

5.1.1. Локација и размјештај просторија (безбједност околине)

Проводе се контроле како би се избјегао губитак, оштећење или угрожавање имовине и прекид пословне активности. Опрема Овјериоца УИО се налази у сигурној просторији која је осигурана двонивовском електронском бравом у згради сједишта УИО.

Контрола физичког приступа Овјериоцу УИО је имплементирана у складу са Законом о електронском потпису и подзаконским актима, и то на сљедећи начин:

- Приступ у просторије, безбједну зону, електронски се биљежи и уноси у електронски дневник за приступ просторијама, и исти се прегледа,
- Браве, електронски системи заштите и системи противпожарне заштите су у складу са важећим стандардима,
- Простор и систем надгледани су 24 часа, 7 дана у седмици од стране овлаштених лица Овјериоца УИО,
- Приступ се може проводити искључиво уз присуство најмање два овлаштена лица која имају право приступа,
- Приступ због одржавања система мора бити унапријед најављен, осим у случају сметњи у раду система за које Група за одржавање система PKI УИО утврди да захтијевају хитну интервенцију,
- Сваки приступ заштићеној просторији евидентира се унутар електронске евиденције.

5.1.2. Контрола физичког приступа за појединце

Овјерилац УИО обезбјеђује да је приступ систему овјеравања ограничен искључиво на овлашћене запослене.

Запослени у Овјериоцу УИО мора се придржавати сљедећих обвеза:

- Извршавати своје администраторске дужности у безбједној зони. Улазак у безбједну зону је могућ искључиво уз идентификацију бесконтактном картицом. Отварање ормара у коме је смјештена опрема Овјериоца УИО је могућ искључиво уз идентификацију са посебном бесконтактном картицом, чији је носилац друга овлашћено лице,
- Штитити бесконтактну картицу за улазак у безбједну зону и за отварање ормара са опремом,
- Смјештати картице *HSM* администратора и *HSM* оператора и друге медије који садрже криптографске кључеве, приступне параметре корисничких налога или друге повјерљиве податке у сигурну касу-контејнер. За отварање касе-контејнера потребан је пар кључева,
- Штитити лозинке које омогућавају приступ приватним криптографским кључевима,
- Смјештати резервне копије приватног кључа у сигурну касу-контејнер,
- Запослени са одговарајућом улогом у систему штите своју смарт картицу за приступ Централном систему *CMS*-а, који омогућава централизовано праћење и управљање животним циклусом криптографских уређаја,
- Запослени са одговарајућом улогом у систему штите своју смарт картицу за приступ *Desktop* апликацији која служи за визуелну и електронску персонализацију криптографских уређаја,
- Запослени по завршетку рада са апликацијама Централног система и *Desktop* апликације за персонализацију криптографских уређаја одлажу смарт картице којима приступају апликацијама на безбједно мјесто,
- Запослени са одговарајућом улогом у систему штите *PIN* код смарт картице коју користе за пријаву на апликацију Централног система *CMS*-а и *Desktop*

апликацију *CMS*-а за персонализацију криптографских уређаја, у зависности од улоге која им је додијељена,
- Одјављивати се са свих апликација у случају да напушта рачунар, а рачунар остаје без надзора.

Запослени који обавља послове пријема захтјева за издавање електронске потврде и пријема захтјева за промјену статуса потврде у регионалном центру, дужан је да се придржава сљедећих обвеза:

- Извршавати своје дужности у зони пријема,
- Штитити своју смарт картицу коју користи за пријављивање на апликацију Регистрационог тијела,
- Штитити *PIN* код смарт картица које омогућавају пријављивање на апликацију Регистрационог тијела,
- Одјављивати се са свих апликација у случају да напушта рачунар, а рачунар остаје без надзора,
- Након престанка са радом са апликацијом Регистрационог тијела одлагати своју смарт картицу на безбједно мјесто.

5.1.3. Напајање и климатизација

Просторије у којима се налази инфраструктура Овјериоца УИО у главној канцеларији УИО су опремљене:

- Системом за непрекидни извор напајања електричном енергијом и стабилизацију напона за рачунарску и комуникациону опрему, који је повезан са агрегатом,
- Независним системом за климатизацију који омогућава контролу температуре и влажности ваздуха унутар просторија Овјериоца УИО.

5.1.4. Заштита од поплаве

Опрема Овјериоца УИО смјештена је на мјесту које је осигурано од поплаве.

5.1.5. Заштита од ватре

Опрема Овјериоца УИО заштићена је аутоматским системом противпожарне заштите у складу са прописаном и важећом законском регулативом.

5.1.6. Смјештање медија

Сви рачунарски медији који садрже податке о пословима Овјериоца УИО, укључујући и медије са резервним копијама података, смјештају се у ватроотпорне безбједне касе-контејнере, од којих се једна налази на централној локацији Овјериоца УИО, а друга на удаљеној, безбједној локацији.

5.1.7. Одлагање непотребних података

Непотребна папирна документација и рачунарски медији за смјештај података се комисијски сијеку на комадиће и физички уништавају.

Подаци са медија, као што су криптографски кључеви, подаци за активирање или електронски дневници, неповратно се бришу, прије него што се медији пошаљу на уништавање.

Уништавање медија на којима се налазе повјерљиви подаци, те уништавање података и кључева повезаних с *HSM* модулима проводи се у складу са интерним процедурама УИО.
Брисање и уништавање података *HSM* модула проводи се и прије њиховог евентуалног слања на сервис или поправак, као и приликом сваког њиховог уклањања из безбједне зоне Овјериоца УИО и њиховог транспортовања на друге локације УИО.

5.1.8. Смјештај резервних копија података на удаљеној локацији

Овјерилац УИО користи безбједну удаљену локацију за смјештај медија са подацима. Медији се смјештају у касу-контејнер. Просторију у којој је смјештена ватроотпорна безбједна каса-контејнер на поменутој удаљеној локацији надзиру овлашћена лица Овјериоца УИО.

5.2. Контрола процедура

5.2.1. Повјерљиве улоге овлашћених лица

Овјерилац УИО гарантује да све послове који се обављају у оквиру прописане дјелатности обављају лица од повјерења са тачно прописаним обавезама и овлашћењима. Рад ових лица је подложан сталним провјерама.

Овлашћена лица Овјериоца УИО зависно од додјељене улоге могу да обављају послове на:

- HSM модулу,
- Серверима Овјериоца УИО,
- Апликацијама овјериоца,
- Апликацији Регистрационог тијела CMS-а,
- Апликацији Централног система CMS-а,
- Desktop апликацији CMS-а за персонализацију криптографских уређаја,
- Мрежним уређајима и приступним листама.

Привилегије одређених корисничких налога на оперативним системима рачунара и корисничких налога у апликацијама, ограничавају приступ овлашћеним лицима Овјериоца УИО на радње које су им потребне у обављању њихових дужности.

Унутар Овјериоца УИО постоје сљедеће безбједоносне функције:

- Главни администратор безбједности - администрира и имплементира безбједоносне функције и процедуре, управља активностима на додатном унапређењу послова издавања, опозива и суспензије електронских потврда,
- Систем администратор – одговоран је за инсталацију, конфигурацију и одржавање сигурних система овјериоца за регистрацију корисника, издавање електронских потврда и дистрибуисање тачног времена. Обезбјеђује средства за формирање сигурног електронског потписа за кориснике и управљање опозивом електронских потврда,
- Систем оператор – одговоран је за рад сигурних система на дневном нивоу и има ауторизовану одговорност за имплементацију система за формирање резервних копија и процедуре опоравка,
- Систем евидентичар - одговоран је за прегледање и одржавање архива и лог фајлова сигурних система овјериоца.

5.2.2. Потребан број овлашћених лица за оперативне послове

Овјерилац УИО има имплементирану двоструку ауторизацију за кључне оперативне послове у апликацији овјериоца и то на начин описан у овом поглављу.

Двије ауторизације Администратора овјериоца су потребне да би се извршили сљедећи послови, и то:

- Промјена лозинке Администратора овјериоца,
- Подешавање броја ауторизација Администратора овјериоца на једну ауторизацију,
- Генерисање приватног криптографског кључа апликације овјериоца, односно обнова профила овјериоца,
- Конфигурисање потврда апликације овјериоца,
- Опозив потврда апликације овјериоца,
- Подешавање броја ауторизација за *Security Officer*-е на једну ауторизацију,
- Креирање и обнова профила *Security Officer*-а,
- Промјена *hash* алгоритма за потврде.

Двије *Security Officer* ауторизације потребне су да би се извршили сљедећи послови, и то:

- Регистровање корисника у апликацији Овјериоца УИО,
- Провођење операција за промјену статуса потврде,
- Подешавање или промјена рока важности потврде,
- Подешавање или промјена правила у вези коришћења потврде,
- Подешавање или промјена администраторских правила,
- Креирање, промјена или брисање корисничких налога са улогом *Security Officer*.

Двије ауторизације се користе и за сљедеће послове:

- Приступ безбједним касама,
- Генерисање криптографског кључа апликације овјериоца,

- Креирање и обнова профила *HSM* администратора и *HSM* оператора,
- Промјена заборављене лозинке *HSM* администратора и *HSM* оператора.

Остали послови који нису наведени у овој тачки, извршавају се уз ауторизацију једног овлашћеног лица Овјериоца УИО.

5.2.3. Идентификација и аутентификација овлашћених лица

Овјерилац УИО врши провјеру својих запослених, прије него што им додијели одређене привилегије које могу да буду:

- Упис у одговарајућу приступну листу за улазак у заштићене просторије Овјериоца УИО,
- Идентификациона бесконтактна картица за улазак у безбједну зону,
- Идентификациона бесконтактна картица за приступ серверском ормару,
- Кориснички налог на оперативном систему сервера и радних станица Овјериоца УИО,
- Администраторске и операторске картице за *HSM*,
- Кориснички налог на апликацији Овјериоца УИО,
- Кориснички налог на апликацији Регистрационог тијела *CMS*-а и смарт картица са електронском потврдом за приступ апликацији Регистрационог тијела,
- Кориснички налог на апликацији Централног система *CMS*-а за управљање и издавање криптографског уређаја у главној канцеларији и смарт картица са електронском потврдом за приступ апликацији Централног система *CMS*-а,
- Кориснички налог на *Desktop* апликацији *CMS*-а за персонализацију криптографских уређаја и смарт картица са електронском потврдом за приступ *Desktop* апликацији CMS-а.

Кориснички налози, картице и потврде из става 1. ове тачке, креирају се посебно за свако овлашћено лице Овјериоца УИО.

Забрањено је заједничко коришћење корисничких налога, картица или потврда између овлашћених лица Овјериоца УИО.

5.2.4. Разграничење овлашћења овлашћених лица

Активности запослених унутар Овјериоца УИО ограничене су овлашћењима дефинисаним на нивоу:

- Хардверског криптографског уређаја (*HSM*),
- Оперативног система сервера и радних станица,
- Апликације Овјериоца УИО,
- Апликације за управљање и издавање потврда,
- Апликације за персонализацију криптографских уређаја,
- Апликације регистрационог тијела.

5.3. Контрола овлашћених лица

Послове Овјериоца УИО, у смислу Практичних правила, обављају запослени који су у радном односу у УИО. Запослени Овјериоца УИО морају бити квалификовани за обављање послова из ових Практичних правила и подлијежу провјери стручне способности.

Запослени Овјериоца УИО не смију објављивати, односно саопштавати неовлашћеним лицима, повјерљиве информације везане за безбједност Овјериоца УИО или информације о корисницима електронских потврда.

Запосленима Овјериоца УИО не додјељују се послови изван дјелокруга послова за које су ангажовани, а који би могли да доведу до сукоба интереса са овим пословима.

Запослени Овјериоца УИО добијају од шефа Одсјека за електронске потписе и сертификате документацију са детаљним описом процедура којих су дужни да се придржавају.

5.3.1. Захтјеви у вези са квалификацијама, искуством и безбједносна провјера овлашћених лица

Запослени Овјериоца УИО морају да задовоље одређене захтјеве у погледу стручне квалификације за свако радно место на које се ангажују, као и у погледу радног искуства и искуства на сличним радним дужностима.

Приликом запошљавања узима се у обзир да лице које се ангажује није било осуђивано за радње које су у вези са пословима које обавља код овјериоца.

5.3.2. Поступци за провјеру претходног радног ангажовања

Провјера претходног радног ангажовања лица за рад код Овјериоца УИО врши се у складу са законом и прописима из ове области.

5.3.3. Обука

Обука запослених у Овјериоцу УИО обухвата:

- Упознавање са инфраструктуром Овјериоца УИО,
- Упознавање са поступцима заштите инфраструктуре и података,
- Оспособљавање за коришћење апликација Овјериоца УИО, у складу са додијељеном улогом,
- Оспособљавање за креирање резервних копија података,
- Предузимање поступака за опоравак система послије штете,
- Упознавање са другим дужностима везаним за рад Овјериоца УИО.

За запослене који запримају захтјеве у регионалним центрима, обука укључује:

- Упознавање са дјелатношћу Овјериоца УИО, врстама потврда и захтјевима за промјену статуса потврда,
- Оспособљавање за коришћење апликације Регистрационог тијела,
- Упознавање са другим дужностима везаним за рад Овјериоца УИО.

Лицима која похађају обуку, обезбјеђује се одговарајућа литература, у складу са темом обуке.

5.3.4. Учесталост поновних обука

Запослени код Овјериоца УИО похађају обуке за обнављање и усавршавање знања најмање једном годишње, а ванредно када се изврше промјене техничких средстава (хардвера и софтвера) Овјериоца УИО и начина обављања дјелатности.

5.3.5. Учесталост и редослијед ротације послова овлашћених лица

Овјерилац УИО није установио правила ротације послова, како не би дошло до нарушавања правила вршења различитих овлашћења и дужности, у вези са различитим повјерљивим улогама запослених у Овјериоцу УИО.

5.3.6. Санкције за неауторизоване активности

У случају извршене или сумње на извршене неауторизоване активности од стране овлашћеног лица Овјериоца УИО, истом ће бити онемогућен даљи приступ техничким средствима (хардверу и софтверу) Овјериоца УИО, а Овјерилац УИО ће суспендовати или опозвати електронске потврде које су издате том лицу.

Извршене неауторизоване активности, пријављују се надлежним организационим јединицама УИО, државним органима и институцијама, у складу са важећим законским и интерним прописима.

5.3.7. Захтјеви за спољне сараднике

У случају да се додијели повјерљива улога спољном сараднику за то лице важе исти услови као за стално запослена лица Овјериоца УИО.

5.3.8. Документација за потребе запослених

Запосленима се даје одговарајућа документација са детаљним описом процедура којих морају да се придржавају.

5.4. Процедуре надгледања рада система

Догађаји који се односе на обављање дјелатности Овјериоца УИО записују се у електронске дневнике (*audit log*) и евиденције које се ручно воде, са датумом и временом догађања.

5.4.1. Врсте догађаја који се евидентирају

Догађаји који се евидентирају су у вези са:

- Издавањем потврде овјериоца *UINO Root CA* и потврда њему подређених овјерилаца,
- Издавањем потврда за потпис одговора *OCSP* сервиса,
- Управљањем животним циклусом кључева овјериоца *UINO Root CA* и кључева повезаних с потврдом за *OCSP* сервис,
- Управљањем животним циклусом хардерског криптографског уређаја,
- Опозивањем потврда које издаје овјерилац *UINO Root CA*,
- Корисничким криптографским кључевима и електронским потврдама: издавање, преузимање, опозив, суспензија, прекид суспензије, деактивирање, архивирање и други,
- Криптографским кључевима апликације овјериоца,
- Техничким средствима (хардвер и софтвер) Овјериоца УИО,
- Администрирањем, креирањем резервних копија, безбједоносним правилима и коришћењем апликација овјериоца,
- Физичким приступом систему Овјериоца УИО, успјешни и неуспјешни приступ систему Овјериоца УИО,
- Покретањем и заустављањем сервиса Овјериоца УИО,
- Подизањем и спуштањем система, квар хардвера,
- Кадровским промјенама у оквиру Овјериоца УИО.

5.4.2. Учесталост прегледа електронских дневника и ручних евиденција

Овлашћени администратори Овјериоца УИО прегледају електронске дневнике и ручне евиденције једанпут недјељно.

Под прегледом, подразумијева се:

- Прикупљање свих електронских дневника и ручних евиденција од посљедњег прегледа,
- Преглед и анализа записа у електронским дневницима и ручним евиденцијама,
- Разрјешавање евентуалних проблема или пријава шефу Одсјека за електронксе потписе и сертификате, који преузима даље кораке у циљу рјешавања проблема.

5.4.3. Вријеме чувања евиденција

Копије електронских дневника и ручних евиденција се чувају најмање 10 година.

5.4.4. Заштита електронских дневника

Електронски дневници и ручне евиденције штите се механизмима и поступцима који обезбјеђују повјерљивост и интегритет дневника.

Нови записи електронских дневника и ручних евиденција система не смију се аутоматски записивати преко постојећих записа.

Тако заштићени електронски дневници и ручне евиденције система су на захтјев расположиви само овлашћеним лицима.

5.4.5. Креирање резервних копија електронских дневника

Електронски дневници свакодневно се ажурирају. За креирање резервних копија задужена су овлашћена лица Овјериоца УИО. Резервне копије електронских дневника, чувају се у главној канцеларији УИО.

5.4.6. Систем прикупљања података за електронске дневнике и ручне евиденције

Систем прикупљања података за електронске дневнике и ручне евиденције свих система у Овјериоцу УИО је интерни систем који је комбинација аутоматских и ручних процеса који се изводе на серверима Овјериоца УИО и које покреће, односно надгледа запослене Овјериоца УИО с повјерљивим улогама.

ДОГАЂАЈИ КОЈИ СЕ ЗАПИСУЈУ У ЕЛЕКТРОНСКЕ ДНЕВНИКЕ И РУЧНЕ ЕВИДЕНЦИЈЕ	НАЧИН ПРИКУПЉАЊА ПОДАТАКА	ОДГОВОРНО ЛИЦЕ ИЛИ СИСТЕМ
Догађаји повезани са електронским потврдама	аутоматско	апликација Овјериоца УИО
Регистар изданих електронских потврда	аутоматско, ручно	апликација Овјериоца УИО, запослени Овјериоца УИО
Догађаји повезани са апликацијама Овјериоца УИО	аутоматско	апликације Овјериоца УИО
Догађаји на оперативном систему	аутоматско	оперативни систем
Догађаји на рачунарској мрежи	аутоматско	*firewall*-и, оперативни систем

Креирање резервних копија и обнова базе корисника електронских потврда	аутоматско, ручно	оперативни систем, апликација Овјериоца УИО, запослени Овјериоца УИО
Креирање резервних копија конфигурације и обнова логова PKI инфраструктуре Овјериоца УИО	аутоматско, ручно	оперативни систем, апликација Овјериоца УИО
Физички приступ до PKI инфраструктуре Овјериоца УИО	ручно, аутоматско	запослени Овјериоца УИО, систем за контролу приступа
Приступ сефу у коме су смјештене администраторске и операторске картице HSM уређаја	ручно	запослени Овјериоца УИО
Приступ сефу у коме су смјештене лозинке администраторских налога сервера PKI окружења, лозинке администраторских и операторских картица HSM уређаја, лозинке за приступ апликацијама УИО Овјериоца	ручно	запослени Овјериоца УИО
Промјене хардвера и софтвера на систему	ручно	запослени Овјериоца УИО
Одржавање рада на систему и простору	ручно	запослени Овјериоца УИО
Кадровске промјене	ручно	запослени Овјериоца УИО

Табела 24. Догађаји који се записују у електронске дневнике и ручне евиденције и начини прикупљања записа о тим догађајима

5.4.7. Обавјештавање о инцидентном догађају

О инцидентном догађају се обавјештава шеф Одсјека за електронске потписе и сертификате. Лице које је изазвало догађај се не обавјештава.

Овјерилац УИО дјелује правовремено и координисано како би брзо реаговао на инциденте и ограничио утицај кршења безбједности.

Дефинисани су запослени чија улога је да прате упозорења о потенцијално критичним безбједоносним догађајима и које треба обезбједити да се пријављују релевантни инциденти у складу с процедурама стандарда ISO/IEC 27001.

Овјерилац УИО извјештава надлежно тијело у складу с примјењивим регулаторским правилима о било којем кршењу безбједности или губитку интегритета у року од 24 часа од утврђивања кршења.

Ако повреда безбједности или губитак интегритета може негативно утицати на физичко или правно лице коме је пружена поуздана услуга, такође се обавјештава и физичко или правно лице о кршењу безбједности или губитку интегритета без непотребног одгађања.

Свака критична рањивост коју Овјерилац УИО претходно није ријешио рјешава се у року од 48 часова након откриħа.

5.4.8. Процјена рањивости система

Процјена рањивости система се врши у склопу свакодневних активности које се спроводе на систему, анализама ризика, размјеном искустава са овјериоцима из окружења и прегледом електронских дневника и ручних евиденција.

5.5. Архивирање података

5.5.1. Врсте података који се архивирају

Овјерилац УИО архивира сљедеће податке и документа:

- Електронске дневнике,
- Уговоре и документацију корисника,
- Захтјеве за издавање и коришћење електронске потврде,
- Захтјеве за промјену статуса електронске потврде (опозив, суспензија, прекид суспензије и друго),
- Електронске потврде,
- Регистре опозваних потврда,
- Интерна акта Овјериоца УИО везана за обављање дјелатности Овјериоца УИО.

5.5.2. Период чувања података у архиви

Овјерилац обезбјеђује трајно чување свих релевантних података који се тичу електронских потврда, у складу са важећим прописима.

5.5.3. Заштита архиве

Архива докумената се чува на централној локацији Овјериоца УИО (Главна канцеларија УИО) и у канцеларијама Регистрационог тијела.

Архива је заштићена са одговарајућим сигурносним механизмима Овјериоца УИО (физичко-техничком заштитом и надзором, ограниченим приступом, шифрама и кључевима). Приступ архивама дозвољен је само овлашћеним лицима.

Овјерилац УИО обезбјеђује тајност текућих и архивираних записа о електронским потврдама.

5.5.4. Процедуре архивирања

Папирни документи архивирају се на централној локацији Овјериоца УИО (Главна канцеларија УИО) и у канцеларијама Регистрационог тијела.

Овјерилац УИО свакодневно ради архивирања израђује копије електронских дневника и података.

5.5.5. Временска ознака архивираних података

Архивирани подаци носе временску ознаку са сервера који је синхронизован са извором тачног времена.

5.5.6. Систем архивирања (интерни или екстерни)

Овјерилац УИО користи комбиновани систем архивирања (интерни и екстерни). Архивирање електронских података извршава запослени у Овјериоцу УИО, техничким средствима за архивирање, која су у власништву Овјериоца УИО.

5.5.7. Процедуре контроле приступа архивираним подацима

Архивирани електронски подаци чувају се у касама-контејнерима за чије отварање су потребна два кључа. Касе-контејнери се налазе у заштићеним просторијама. Просторије су са рестриктивним и ауторизованим приступом.

5.6. Генерисање нових кључева овјериоца

Генерисање нових кључева Овјериоца УИО врши се пет година прије истека рока важности постојећих кључева. Генерисање кључева могуће је спровести и раније, из сљедећих разлога:

- Потребно је промијенити криптографски алгоритам којим овјерилац потписује потврде и регистре опозваних потврда,
- Потребно је промијенити дужину кључева овјериоца,
- Потребно је промијенити рок важности кључева овјериоца,
- Потребно је промијенити *hash* алгоритам овјериоца, примјеном кога се израчунава *hash* вриједност потврде и регистра опозваних потврда,
- Потребно је промијенити садржај постојећих поља или екстензија потврде овјериоца или додати нове екстензије потврди овјериоца,
- Приватни кључ овјериоца је оштећен или је компромитован.

5.7. Опоравак система послије катастрофе

Одржава се план континуитета рада за реаговање у случају катастрофе, укључујући компромитацију приватног кључа за потпис или неку другу компромитацију.

Процедуре се обнављају у складу с планом континуитета након рјешавања било којег узрока катастрофе који се може поновити (нпр. безбједоносна рањивост) и одговарајућим мјерама санације у складу са стандардом ISO 22301.

5.7.1. Процедуре рада у случају катастрофе или приликом компромитовања система

Овјерилац УИО има планове за очување и опоравак система овјеравања након катастрофе. Интерним плановима обухваћени су поступци очувања и опоравка система за случај катастрофе узроковане кваром опреме, људском грешком, отуђењем или компромитовањем опреме и података, пожаром, природном катастрофом, терористички чином и сл.

Интерним плановима обухваћени су и поступци које треба предузети у циљу опоравка и успоставе првобитних безбједоносних прилика система овјериоца.

5.7.2. Оштећења у рачунарским ресурсима, програмима и/или подацима

У случају штете настале на техничким средствима (хардверу и софтверу) или подацима, при чему приватни криптографски кључ апликације овјериоца није уништен или оштећен, сервиси апликације овјериоца биће поново успостављени у најкраћем могућем року.

У случају уништења или оштећења приватног криптографског кључа апликације овјериоца, послије отклањања узрока уништења или оштећења, спроводи се поступак реконструисања кључа.

5.7.3. Компромитовање приватног криптографског кључа апликације овјериоца

Овјерилац УИО ће, у случају компромитовања приватног криптографског кључа апликације овјериоца, одмах:

- Опозвати издате електронске потврде,
- Опозвати потврду апликације овјериоца,
- Објавити регистар опозваних потврда,
- Обавијести кориснике издатих електронских потврда.

Овјерилац УИО ће, у случају компромитовања приватног криптографског кључа апликације овјериоца, послије отклањања узрока компромитовања:

- Генерисати нове криптографске кључеве апликације овјериоца,

- Издати корисницима нове електронске потврде.

5.7.4. Наставак рада послије катастрофе

Послије престанка катастрофе и отклањања њеног узрока, Овјерилац УИО ће у најкраћем могућем року да доведе систем у продукционо стање и настави са радом.

5.8. Престанак рада овјериоца

Овјерилац УИО, у случају престанка рада, има обавезу:

- Обавијестити све заинтересоване стране (надлежни орган и своје кориснике) о престанку рада,
- Пренијети своје обавезе другом овјериоцу, уколико постоје могућности за то,
- Опозвати све издате електронске потврде, којима није истекао рок важности, уколико не успије да пренесе своје обавезе на другог овјериоца,
- Уништити или потпуно онемогућити коришћење својих приватних кључева, који су коришћени за креирање потврда и регистра опозваних потврда, тако да се исти не могу реконструисати.

Овјерилац УИО ће о планираном престанку обављања послова везаних за електронски потпис и овјеравање обавијестити своје кориснике и надлежни државни орган у складу са важећим прописима.

Овјерилац УИО ће предузети све што могућности у датом тренутку буду дозвољавале, како би обезбиједио наставак обављања услуге код другог овјериоца за своје кориснике.

Овјерилац УИО има обавезу да овјериоцу, код кога је обезбиједио наставак пружања услуге према својим корисницима, достави сву постојећу документацију и архиву, која се односи на обављање услуге везане за електронски потпис и овјеравање.

Ако се не постигне пренос обавеза на другог овјериоца, Овјерилац УИО има обавезу да сву постојећу документацију и архиву, која се односи на обављање услуга везаних за електронски потпис и овјеравање достави надлежном државном органу.

Уколико нема могућности за пренос обавеза пружања услуге везане за електронски потпис и овјеравање на другог овјериоца, Овјерилац УИО ће раскинути уговоре о издавању и коришћењу електронских потврда са својим корисницма и опозвати све важеће електронске потврде, о чему ће обавијестити кориснике и надлежни државни орган.

Овјерилац УИО ће електронском поштом да обавијести кориснике електронских потврда и овјериоце признате од стране Овјериоца УИО, односно овјериоце који признају Овјериоца УИО као овјериоца о престанку рада у складу са важећим прописима.

Корисници издатих квалификованих електронских потврда биће обавијештени о престанку рада, преко званичне *Web* странице Овјериоца УИО или на други начин, посредством средстава јавног информисања или електронском поштом.

6. КОНТРОЛЕ ТЕХНИЧКЕ ЗАШТИТЕ

6.1. Генерисање пара криптографских кључева и инсталација

6.1.1. Генерисање пара криптографских кључева

Овјерилац УИО одржава апликације овјериоца које извршавају *UINO Root CA*, *UINO Issuing CA1* и *UINO Issuing CA2*, а парови њихових криптографских кључева су генерисани током процеса церемоније генерисања кључева (енг. *Key Generation Ceremony*) по прецизно дефинираној процедури. Током церемоније генерисања пара криптографских кључева користи се заштита која важи за просторије Овјериоца УИО, заштита коју пружа хардверски криптографски модул (енг. *Hardware Security Module – HSM*), оперативни систем, апликација овјериоца и вишеструка аутентификација овлашћених лица.

У Церемонији генерисања кључева учествовале су овлашћена лица Овјериоца УИО са повјерљивим улогама и ревизор који свједочи да је Церемонија генерисања парова кључева извршена у складу са документом Управе за индиректно опорезивање Церемонија генерисања криптографских кључева УИО која служи као протокол за генерисање кључева у коме су документирани кораци који се изводе приликом поменуте церемоније.

Ревизор потписује овај документ на крају церемоније и тиме свједочи да је поступак генерисања парова кључева спроведен у складу са протоколом.

У документ се потписују сва лица која су учестовала у церемонији генерисања кључева.

Пар криптографских кључева корисника за потписивање и верификовање квалификованог електронског потписа генерише се на *SSCD* уређају, који представља средство за формирање квалификованог електронског потписа. Пар криптографских кључева повезан са корисничком потврдом за креирање квалификованог електронског потписа се никада не смјешта на хардверску или софтверску опрему Овјериоца УИО.

6.1.2. Уручење приватног криптографског кључа кориснику

Уручење приватног кључа кориснику врши се уручивањем *SSCD* уређаја у просторијама Овјериоца УИО, у сједишту или у регионалном центру УИО.

6.1.3. Достављање јавног криптографског кључа корисника овјериоцу

Кориснички криптографски јавни кључ потврде за израду квалификованог електронског потписа се заједно са приватним кључем генерише у Овјериоцу УИО на *SSCD* уређају и нема потребе да корисник доставља јавни криптографски кључ овјериоцу.

Кориснички криптографски јавни кључ потврде у облику датотеке PKCS#12 формата се заједно са приватним кључем генерише у Овјериоцу УИО и нема потребе да корисник доставља јавни криптографски кључ овјериоцу.

Криптографски јавни кључ потврде за аутентификацију *Web* страница се доставља Овјериоцу УИО у облику датотеке PKCS#10 формата и подвргава се темељној провјери прије издавања одговарајуће потврде.

6.1.4. Уручење јавног криптографског кључа трећим лицима

Јавни криптографски кључ апликације овјериоца у форми потврде је јавно доступан и на *Web* страници Овјериоца УИО.

Корисничке јавне криптографске кључеве и потврде Овјерилац УИО јавно не објављује нити уручује трећим лицима.

6.1.5. Дужине криптографских кључева

Дужине криптографских кључева за које Овјерилац УИО издаје електронске потврде су:

- Криптографски кључеви апликације овјериоца: *RSA* кључеви најмање дужине 4096 бита,
- Кориснички кључеви: *RSA* кључеви најмање дужине 2048 бита.

6.1.6. Генерисање параметара јавног криптографског кључа и провјера квалитета

Генерисање параметара јавног криптографског кључа апликације овјериоца врши се у хардверским криптографским модулима Овјериоца УИО, а параметри јавних криптографских кључева корисника генеришу се у криптографским *SSCD* уређајима и софтверу Овјериоца УИО, у зависности од профила потврде по којем се издаје потврда.

Одговорно лице Овјериоца УИО задаје параметре јавних кључева апликације овјериоца и корисника, као што је наведено у дефиницијама профила потврда.

6.1.7. Намјена кључа

За потписивање електронских потврда, потврда за сервис Овјериоца УИО за издавање временских жигова, припадајућег регистра опозваних потврда и потпис одговора *OCSP* сервиса употребљава се искључиво приватни криптографски кључ апликације овјериоца којег одржава Овјерилац УИО.

Јавни криптографски кључ апликације овјериоца употребљава се за валидацију електронског потписа електронске потврде и регистра опозваних потврда (*Key Usage = Certificate Signing, Off-line CRL Signing, CRL Signing*).

Приватни кључеви потврде УИО *OCSP* сервиса намијењени су само за потписивање одговора УИО *OCSP* сервиса (*Key Usage = digitalSignature, nonRepudiation, extKeyUsage = OCSPSigning).*

Намјена јавног криптографског кључа квалификоване електронске потврде или печата корисника је верификовање квалификованог електронског потписа или печата и осигуравање непорецивости.

Врста потврда	Садржај екстензије *Key Usage*
Квалификоване електронске потврде Овјериоца УИО	*Certificate Signing, Off-line CRL Signing, CRL Signing*
Квалификована електронска потврда за електронски потпис на смарт картици	*Non-Repudiation*
Квалификована електронска потврда за електронски печат на смарт картици	*Digital Signature*
Потврда за УИО OCSP сервис	*Key Usage = digitalSignature, nonRepudiation, extKeyUsage = OCSPSigning*
Квалификована електронска потврда за електронски временски жиг	*Key Usage = digitalSignature, nonRepudiation, extKeyUsage = timeStamping*

Табела 25. Садржај екстензије *Key Usage* у квалификованим електронским потврдама које издаје Овјерилац УИО

6.2. Заштита приватног криптографског кључа

6.2.1. Стандарди за хардверски криптографски модул

Све операције за генерисање криптографских кључева и потписивање потврда Овјериоца УИО врше се на хардверском криптографском модулу, који задовољава безбједоносне стандарде ISO/IEC 15408 (Common Criteria) EAL4+.

Квалификовано средство за креирање електронског потписа и печата корисника задовољава стандард EAL4+.

6.2.2. Контрола приступа приватном кључу од стране n од m овлашћених лица

Овјерилац УИО има имплементирану вишеструку ауторизацију за приступ приватном криптографском кључу апликација овјерилаца *UINO Root CA, UINO Issuing CA1* и *UINO Issuing CA2* Овјериоца УИО.

Приступ корисничком приватном крипптографском кључу ограничен је само на корисника.

6.2.3. Откривање приватног криптографског кључа

Овјерилац УИО не нуди могућност откривања приватног криптографског кључа.

6.2.4. Креирање копије приватног криптографског кључа

Послије генерисања криптографских кључева апликације овјериоца, уз присуство овлашћених лица Овјериоца УИО, креира се копија приватног криптографског кључа апликације овјериоца. Приватни криптографски кључ апликације овјериоца је шифрован *AES* (*Rijndael*) алгоритмом и никад се не налази изван хардверског криптографског модула у дешифрованом облику. Дешифровање приватног криптографског кључа је могуће само у хардверском криптографском модулу, на основу копије приватног криптографског кључа, уз помоћ двије администраторске смарт картице за приступ хардверском криптографском модулу и њихових лозинки.

Креирање копија приватних криптографских кључева повезаних са квалификованим електронским потврдама корисника се не ради.

6.2.5. Архивирање приватног криптографског кључа

Овјерилац УИО архивира копију приватног криптографског кључа апликације овјериоца послије његовог креирања, на локацији Овјериоца УИО и другој удаљеној локацији, у заштићеним просторијама у касама-контејнерима за дуготрајно чување.

Архивирање приватних криптографских кључева повезаних са квалификованим електронским потврдама корисника се не ради.

6.2.6. Пребацивање приватног кључа у криптографски модул или из њега

Приватни криптографски кључ апликације овјериоца је генерисан у хардверском криптографском модулу. Само уколико наступи хардверски квар хардверског криптографског модула апликације овјериоца, он ће бити замијењен новим модулом, а приватни кључ пребачен (импортован) у тај модул, уз писану одлуку одговорног лица Овјериоца УИО и уз вишеструку ауторизацију запослених Овјериоца УИО.

Приватни криптографски кључ повезан са квалификованом електронском потврдом корисника је генерисан у хардверском криптографском *SSCD* уређају и не експортује се.

6.2.7. Чување приватног криптографског кључа у криптографском модулу

Криптографски кључеви се чувају у криптографским модулима и могу да се користе само уколико су на правилан начин активирани.

6.2.8. Поступак за активирање приватног криптографског кључа

За реконструкцију и активирање приватног криптографског кључа апликације овјериоца потребна је ауторизација два *HSM* администратора са својим картицама и лозинкама и два *HSM* оператера са својом картицом и лозинком. Приватни криптографски кључ апликације овјериоца се активира послије стартовања апликације овјериоца.

Кориснички приватни криптографски кључеви се активирају послије успјешне аутентификације корисника са лозинком у корисничкој апликацији приликом електронског потписивања или печатирања.

6.2.9. Поступак за деактивирање приватног криптографског кључа

Приватни криптографски кључ апликације овјериоца се деактивира заустављањем апликације овјериоца и деактивирањем *HSM*-а.

Корисничке апликације деактивирају приватни криптографски кључ послије електронског потписивања и извлачења смарт катрице из читача картица, или истеком времена корисничке сесије.

6.2.10. Поступак за уништавање приватног криптографског кључа

Приватни криптографски кључ апликације овјериоца се уништава само у случају планираног престанка рада овјериоца, а што се спроводи само уз писану одлуку одговорног лица Овјериоца УИО.

Приватни криптографски кључ корисника се уништава уколико га корисник обрише са смарт картице, физички оштети смарт картицу.

6.2.11. Класификовање криптографских модула

Стандард за криптографске модуле према којима може да се врши њихово класификовање је ISO/IEC 15408 EAL, и наведени је у тачки 6.2.1.

6.3. Остали аспекти администрирања над паром криптографских кључева

6.3.1. Архивирање јавног криптографског кључа

Овјерилац УИО архивира јавни криптографски кључ апликације овјериоца и јавне криптографске кључеве корисника.

6.3.2. Рок важности потврда и криптографских кључева

Рокови важности потврда Овјериоца УИО су:

- Потврде апликације овјериоца: двадесет (20) година,
- Квалификоване електронске потврде корисника: пет (5) година,
- Потврда за потпис одговора *OCSP* сервиса: једна (1) година,
- Квалификована потврда за електронски печат: пет (5) година,
- Потврда за аутентификацију *Web* страница за правна лица: 398 дана,
- Потврда за аутентификацију *Web* страница и *Kerberos* потврда за домен контролер: двије (2) године,
- Потврда за потписивање кода: три (3) године.

6.4. Подаци за активирање

6.4.1. Генерисање и употреба података за активирање

Подаци за активирање приватног кључа апликације овјериоца генеришу се приликом генерисања криптографских кључева и могу да их користе искључиво овлашћена лица Овјериоца УИО.

Лозинку за активирање приватног кључа (*PIN* код) корисника генерише генератор лозинке. Лозинка има четири или више нумеричких карактера. Корисник има могућност промјене лозинке и њене дужине.

Уколико корисник узастопно пет пута унесе погрешну лозинку (*PIN* код) долази до закључавања смарт картице. Смарт картицу је могуће откључати са *PUK* кодом који се кориснику доставља заједно са лозинком (*PIN* кодом) у затвореној коверти.

6.4.2. Заштита података за активирање

Овлашћена лица овјериоца УИО су дужна да чувају лозинке које се користе за активирање кључева.

Сваки корисник квалификоване електронске потврде је одговоран за чување лозинке свог *SSCD* уређаја.

6.4.3. Остали видови података за активирање

Не постоје.

6.5. Безбједоносни захтјеви за рад

Осјетљиви подаци морају бити заштићени од откривања поновним коришћењем објеката за чување (нпр. избрисаних датотека) доступним неовлашћеним корисницима.

Интегритет свих система и информација заштићен је од вируса, злонамјерног и неовлашћеног софтвера.

6.6. Безбједносни захтјеви за рачунаре

6.6.1. Специфични рачунарски техничко-безбједносни захтјеви

На систему Овјериоца УИО имплементиране су техничко-безбједносне контроле и механизми, и то:

- Контрола приступа до системских сервиса апликације Овјериоца УИО,
- Контрола приступа функцијама апликације Овјериоца УИО,
- Строга подјела улога између овлашћених лица Овјериоца УИО,
- Употреба криптографских модула за смјештање криптографских кључева овлашћених лица Овјериоца УИО,
- Безбједно архивирање података апликације Овјериоца УИО и електронских дневника,
- Заштита електронских дневника, односно података у истима о свим догађајима који се односе на безбједност,
- Успостављање механизама обнове система, криптографских кључева и базе података апликације Овјериоца УИО.

Да би се открили, забиљежили и спријечили покушаји недозвољеног приступа ресурсима система, Овјерилац УИО континуирано прати систем.

6.6.2. Ниво заштите рачунара

Оперативни систем на серверима Овјериоца УИО је у складу са стандардом заштите ISO/IEC 15408 EAL4+, како би се омогућио сигуран рад апликације овјериоца.

6.7. Технички надзор у току обављања дјелатности

6.7.1. Развој система

Овјерилац УИО користи и ослања се на апликацију овјериоца, која је развијена по строгим критеријумима стандарда ISO/IEC 15408 и сертификована према нивоу EAL4+. Додатни софтвер (CMS) који се користи приликом пружања услуге издавања електронске потврде је од поуздане фирме и све новије верзије софтвера се тестирају на тестном окружењу прије него што се имплементирају на продукционом окружењу.

6.7.2. Управљање безбједношћу

Овјерилац УИО има механизме и процедуре које примјењује у контроли и надзору свих техничких система. У случају нарушавања безбједности система Овјериоца УИО или

губитка интегритета, Овјерилац УИО ће у року од 24 часа о томе обавијестити надлежни орган.

6.7.3. Надзор безбједности током употребе система

Безбједносна контрола се периодично извршава провјеравањем рада компоненти Овјериоца УИО.

6.8. Надзор безбједности рачунарске мреже

Овјерилац УИО штити мрежу и системе од напада, сегментира своје системе у мреже или зоне базиране на процјени ризика узимајући у обзир функционални, логички и физички (укључујући локацију) однос између поузданих система и услуга. Исте безбједоносне контроле примјењују се на све системе у истој зони.

Рачунарску мрежу Овјериоца УИО чине повезани мрежни сегменти, на којима се налазе сервери и радне станице. Сегменти су међусобно повезани мрежним уређајима и *firewall*-има. Безбједносна правила на *firewall*-има и мрежним уређајима дозвољавају саобраћај само између сервера и радних станица по протоколима који су потребни за обављање дјелатности Овјериоца УИО и за приступ сервисима Овјериоца УИО.

Раздваја се намјенска мрежа за администрирање ИТ система и оперативна мрежа Овјериоца УИО.

Раздвајају се продукциони системи за услуге од система који се користе у развоју и испитивању (нпр. Системи за развој, тестирање и поступно постављање).

Успоставља се комуникација између различитих поузданих система само путем поузданих канала који се логично разликују од осталих комуникацијских канала и пружају сигурност идентификације његових крајњих тачака и заштита података канала од модификације или откривања. Ако је потребан висок ниво доступности ванјског приступа повјерљивој услузи, ванјска мрежна веза биће редудантна како би се осигурала доступност услуга у случају квара једне мрежне везе.

Проводи се редовито скенирање (сваких 90 дана) рањивости на јавним и приватним IP адресама и биљеже докази да је свако скенирање рањивости извршило лице или ентитет који посједује вјештине, алате, стручност, етички кодекс и независност потребне за пружање поузданог извјештаја.

Проводи се редовни (једанпут сваке године или при постављању и након надоградње/измјене инфраструктуре или апликације за које Овјерилац УИО утврђује да су значајне) тест пенетрације (*Penetration test*). Биљеже се докази да је сваки тест пенетрације провело лице или субјект с вјештинама, алатима, познавањем, етичким кодексом и независношћу потребним за пружање поузданог извјештаја.

6.9. Временска ознака

Електронске потврде и регистри опозваних потврда имају временску ознаку датума и времена издавања, датума и времена престанка важења потврде и датума и времена издавања сљедећег регистра опозваних потврда. Временска ознака није криптографски временски жиг. Систем тачног времена је путем *NTP* протокола (енг. *Network Time Protocol*) усклађен са спољним *UTC* (*Coordinated Universal Time*) извором тачног времена који у складу са законском регулативом обезбјеђује Институт за метрологију БиХ.

7. САДРЖАЈ ПОТВРДЕ, РЕГИСТРА ОПОЗВАНИХ ПОТВРДА И OCSP ПРОФИЛИ

7.1. Профил потврде

7.1.1. Верзија потврде

Овјерилац УИО издаје потврде у складу са спецификацијом *X.509* верзије 3. Профил квалификоване електронске потврде у складу је са стандардима наведеним на почетку овог документа.

Документ с описом профила потврда Овјериоца УИО доступан је на *Web* страници Овјериоца УИО под називом „УИО профили потврда“.

Потврде Овјериоца УИО садрже основна поља *X.509* потврде (табела 26).

НАЗИВ ПОЉА	ОПИС ПОЉА
Version	Верзија спецификације *X.509* потврде.
Serial Number	Јединствен серијски број електронске потврде.
Signature Algorithm	*Hash* алгоритам и асиметрични криптографски алгоритам коришћени за потписивање потврде од стране апликације овјериоца.
Issuer	Јединствено име овјериоца.
Valid From	Датум и вријеме почетка важења електронске потврде.
Valid To	Датум и вријеме престанка важења електронске потврде.
Subject	Јединствено име корисника потврде.
Public Key	Назив алгоритма јавног кључа и параметри јавног криптографског кључа корисника потврде.

Табела 26. Основна поља *X.509* потврде

7.1.2. Екстензије потврде

Називи екстензија *X.509* потврда које апликација овјериоца уписује у квалификоване електронске потврде и њихов опис дати су у сљедећој табели (табела 27).

НАЗИВ ПОЉА - ЕКСТЕНЗИЈЕ	ОПИС ПОЉА - ЕКСТЕНЗИЈЕ
Enhanced Key Usage (EKU)	Показује да се јавни кључ може користити за једну или више сврха (проширена могућност коришћења кључа).
Authority Information Access	Адреса потврде „UNO IssuingCA1“ или „UNO IssuingCA2“ сервера и URI OCSP сервиса.
Certificate Policies	Идентификација CPS-а и адреса *Web* странице на којој се налазе ова Практична правила.
Subject Alternative Name	Алтернативна имена корисника (*e-mail*, итд).
CRL Distribution Points	Локација на којој се налазе регистри опозваних потврда.
Authority Key Identifier	Идентификатор јавног криптографског кључа овјериоца.
Subject Key Identifier	Идентификатор јавног криптографског кључа корисника потврде.
Key Usage	Намјена јавног криптографског кључа корисника квалификоване електронске потврде.
Basic Constraints	Ознака која указује на врсту потврде (потврда овјериоца или корисничка потврда).
Qualified Certificate Statements	Ознака да је потврда издана као квалификована електронска потврда.

Табела 27. Екстензије *X.509* потврде

7.1.3. Идентификациона ознака алгоритма

Овјерилац УИО потписује квалификоване електронске потврде и регистре опозваних потврда примјеном алгоритма *SHA512RSA* (*OID* 1.2.840.113549.1.1.13) у складу са документима *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* и *RFC* 6931 – *Additional XML Security Uniform Resource Identifiers (URIs)*.

7.1.4. Форме имена

Потврде *UINO Root CA* и потврде њему подређених овјерилаца (*UINO Issuing CA1* и *UINO Issuing CA2*) у пољима *Issuer* и *Subject* садрже пуно јединствено име (енг. *Distinguished Name*) издаваоца потврде.

У електронским потврдама које издаје Овјерилац УИО, име Овјериоца УИО које је наведено у пољу *Issuer* и име корисника потврде које је наведено у пољу *Subject* су

јединствена имена (енг. *Distinguished Name – DN*). На име корисника (енг. *Common Name – CN*) у електронској потврди се примјењује *UTF8 String* кодирање.

7.1.5. Ограничења у именима

Специјални знаци чије коришћење у именима није дозвољено су: ? (упитник), \ (*backslash*), # (тараба), $ (долар), % (проценат), = (једнако), + (плус), | (усправна црта), ; (тачка-зарез), < (мање), > (веће) и , (зарез). Исте је потребно замијенити другим знацима.

7.1.6. Идентификациона ознака политике овјеравања

Све потврде издате од стране Овјериоца УИО садрже *OID* политике овјеравања на основу које је издата потврда. *OID* за сваку политику овјеравања дефинисан је у поглављима 1.1.1 и 1.2.

7.1.7. Употреба екстензије за раздвајање политика

Не користи се.

7.1.8. Квалификатори политике овјеравања

Овјерилац УИО користи потпоље *Policy Qualifier=CPS* екстензије *Certificate Policies* потврде, у коме објављује адресу *Web* странице на којој се налазе ова Практична правила и друга акта Овјериоца УИО.

7.1.9. Процесуирање критичних екстензија потврда

Корисничке апликације морају да процесуирају екстензије потврда које су означене као критичне (енг. *critical*).

7.2. Профил регистра опозваних потврда

7.2.1. Верзија регистра опозваних потврда

Овјерилац УИО издаје *X.509* регистре опозваних потврда (енг. *Certificate Revocation List – CRL*) верзије 2. Профил регистра опозваних потврда је у складу са документом *RFC* 5280 – *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. Регистри опозваних потврда Овјериоца УИО садрже основна поља *X.509* регистра (табела 28) и екстензије *X.509* регистра (табела 29).

НАЗИВ ПОЉА	ОПИС ПОЉА
Version	Верзија спецификације *X.509* регистра опозваних потврда.
Signature Algorithm	*Hash* алгоритам и асиметрични криптографски алгоритам коришћени за потписивање регистра опозваних потврда од стране апликације овјериоца.
Issuer	Јединствено име овјериоца.
Effective Date (This Update)	Датум и вријеме издавања регистра опозваних потврда.
Next Update	Датум и вријеме сљедећег издавања регистра опозваних потврда.
Revoked Certificates	Списак серијских бројева опозваних потврда (енг. *serial number*) и датума и времена њиховог опозивања (енг. *revocation date*).

Табела 28. Основна поља *X.509* регистра опозваних потврда

7.2.2. Екстензије регистра опозваних потврда

Називи екстензија *X.509* регистра опозваних потврда које апликација овјериоца уписује у регистре и њихов опис дати су у сљедећој табели (табела 29).

НАЗИВ ЕКСТЕНЗИЈЕ	ОПИС ЕКСТЕНЗИЈЕ
Authority Key Identifier	Идентификатор јавног криптографског кључа овјериоца.
CRL Number	Редни број регистра опозваних потврда (*OID* 2.5.29.20).
Reason Code	Разлог опозива потврде. Могући разлози опозива потврда (према документу *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* која садржи ову екстензију укључиваће информације о статусу опозива за потврде које су већ истекле.
Invalidity Date	Датум компромитовања или сумње у компромитовање приватног криптографског кључа или датум када је електронска потврда на неки други начин престала да буде важећа (*OID* 2.5.29.24).

Табела 29. Екстензије *X.509* регистра опозваних потврда

7.3. OCSP профил

Овјерилац УИО омогућава интернетску провјеру статуса опозива изданих потврда путем *OCSP* сервиса чији је рад у складу с документом IETF RFC 6960.

Подаци о статусу опозива потврда путем *OCSP* сервиса доступни су у стварном времену.

7.3.1. Верзија OCSP-а

Профил одговора *OCSP* сервиса Овјериоца УИО у складу је са верзијом 1 према документу IETF RFC 6960.

7.3.2. OCSP екстензије

Екстензије одговора OCSP сервиса Овјериоца УИО приказане су у табели 30.

НАЗИВ ЕКСТЕНЗИЈЕ	КРИТИЧНО	ОПИС
Nonce	НЕ	Вриједност nonce-а из захтјева за статусом потврде.
Extended Revoked Definition	НЕ	Код разлога опозива потврде (енг. *reason code*).

Tabela 30. Екстензије одговора OCSP сервиса Овјериоца УИО

8. РЕВИЗИЈА УСКЛАЂЕНОСТИ РАДА ОВЈЕРИОЦА УИО И ДРУГЕ ПРОЦЈЕНЕ

Овјерилац УИО извршава редовне унутрашње ревизије рада (*internal audit*).

Надлежни орган има право извршити ревизију, у складу са законом и подзаконским актима.
Надлежни орган је Министарство комуникација и транспорта Босне и Херцеговине.

8.1. Учесталост ревизије и анализа ризика

Овјерилац УИО врши анализу ризика којом идентификује критичне сервисе који захтјевају коришћење безбједних система и високе нивое безбједности:

- Прије почетка обављања услуга овјеравања,
- Током оперативног рада по потреби, а најмање сваких 6 мјесеци.

Овјерилац УИО извршава редовне унутрашње ревизије рада два пута годишње.

Могуће је извршити и више од двије ревизије годишње уколико је то захтијевано од надлежног органа или је то посљедица незадовољавајућих резултата претходне ревизије.

8.2. Квалификација лица које врши ревизију

Шеф Одсјека за електронске потписе и сертификате у Сектору за информационе технологије УИО одговоран је за спровођење унутрашњих ревизија и одређивање лица која их спроводе.

Унутрашња ревизија се спроводи ангажовањем стручног лица из или ван Овјериоца УИО које мора да има искуства на подручју:

- Технологије инфраструктуре јавних криптографских кључева,
- Вршења дјелатности овјериоца,
- Спровођења ревизије овјериоца или другог информационо-комуникационог система.

8.3. Однос лица које врши ревизију према предмету ревизије

Лице које врши ревизију поступа у складу са важећим прописима и међународним стандардима. Ревизију може вршити лице запослено у Овјериоцу УИО или спољно стручно лице.

8.4. Садржај ревизије

У оквиру унутрашње ревизије провјеравају се:

- Садржај Политике овјеравања,
- Садржај Практичних правила,
- Да ли Овјерилац УИО обавља дјелатност у складу са важећим прописима, Политиком овјеравања, Практичним правилима и интерним актима (везаним за процедуре приступа просторијама Овјериоца УИО, управљања апликацијом Овјериоца УИО, објављивања регистра опозваних потврда, креирања резервних копија и другим интерним актима),
- Технички процеси и процедуре,
- Физичка безбједност,
- Примјењене мјере информационе безбједности.

8.5. Предузете активности као резултат утврђених недостатака

У случају утврђених недостатака, спроводе се активности на отклањању истих у што краћем року.

8.6. Објављивање извјештаја ревизије

Извештај ревизије представља интерни документ Овјериоца УИО и не објављује се јавно. Намијењен је искључиво овлашћеним лицима Овјериоца УИО за потребе отклањања евентуално пронађених недостатака.

9. ОСТАЛИ ПОСЛОВИ И ПРАВНА ПИТАЊА

9.1. Цјеновник

Овјерилац УИО објављује цјеновник за издавање електронских потврда на својој *Web* страници.

Свака промјена цијена издавања квалификованих електронских потврда објављује се на *Web* страници Овјериоца УИО и биће доступна свим заинтересованим лицима.

9.1.1. Надокнада за издавање потврда

Овјерилац УИО наплаћује издавање електронске потврде на основу цјеновника, који је објављен на *Web* страници Овјериоца УИО.

9.1.2. Надокнада за приступ потврдама

Овјерилац УИО не објављује електронске потврде, тако да оне нису јавно доступне, па не може ни да наплаћује приступ електронској потврди.

9.1.3. Надокнада за провјеру опозваности и статуса потврда

Провјера опозваности електронске потврде и добијање информација о статусу потврде коришћењем регистра опозваних сертификата (*Certificate Revocation List - CRL*) или *OCSP* сервиса се не наплаћује.

9.1.4. Надокнада за друге услуге

Овјерилац УИО задржава право да наплаћује различите услуге у зависности од пружених услуга у сваком конкретном случају.

9.1.5. Повратак уплаћених средстава

У случају да Овјерилац УИО раскине уговор, а претходно не изда електронску потврду кориснику, корисник може да тражи повратак уплаћених средстава на износ цијене потврде.

9.2. Финансијска одговорност

Овјерилац УИО сноси финансијску одговорност за обављање своје дјелатности у складу са важећим законским прописима.

9.2.1. Осигурање

Овјерилац УИО је дужан да обезбиједи најнижи износ осигурања од одговорности за могућу штету насталу вршењем услуга издавања квалификоване електронске потврде у складу са важећим прописима, тако да:

1) Осигурана сума на коју мора бити уговорено осигурање по једном штетном догађају не може износити мање од 50.000,00 КМ, подразумијевајући при том као штетни догађај појединачну штету насталу употребом једне квалификоване електронске потврде у једном акту у правном промету;
2) Укупна осигурана сума на коју мора бити уговорено осигурање од одговорности овјериоца кумулативно на годишњем нивоу, по свим штетним догађајима, не може бити нижа од 1.500.000,00 КМ.

9.2.2. Други фондови

Није примјењено.

9.2.3. Осигурање или гаранција за крајње кориснике

Осигурање или гаранција за крајње кориснике описани су у оквиру тачке 9.2.1.

9.3. Тајност пословних података

9.3.1. Обим тајних података

Тајни подаци су сви подаци које Овјерилац УИО прибави и креира у обављању своје дјелатности као овјерилац.

Приступ подацима, који се сматрају тајним, може бити одобрен овлашћеним лицима Овјериоца УИО и надлежним државним органима, ако су испуњени законом прописани услови.

9.3.2. Подаци који се не сматрају тајним

Подаци који се не сматрају тајним су:

- Регистри опозваних сертификата, као и подаци које они садрже,
- Политика овјеравања,
- Практична правила,
- Подаци и документи која су објављена на званичној *Web* страници Овјериоца УИО, за које постоји писмена сагласност за јавно објављивање.

9.3.3. Одговорност за заштиту тајних података

Запослени Овјериоца УИО и корисници обавезују се:

- Да чувају тајност података примјеном мјера које користе за заштиту својих тајних података и да ће их користити само за потребе због којих су били прикупљени или формирани у односу на одредбе Практичних правила,
- Да неће неовлашћено откривати тајне податке, без претходног одобрења у писаној форми, које даје корисник или надлежни орган.

9.4. Чување података о личности

Овјерилац УИО је дужан да се у свом пословању придржава одредби Закона о заштити личних података.

9.4.1. План чувања личних података

Лични подаци се чувају у складу са Законом о заштити личних података и подзаконским актима за провођење истог.

9.4.2. Подаци о личности који се сматрају тајним

Сви подаци о корисницима који су заштићени законом сматрају се повјерљивим подацима о личности.

9.4.3. Подаци о личности који се не сматрају тајним

Сви подаци, који су јавно доступни.

9.4.4. Одговорност за заштиту личних података

Овјерилац УИО је одговоран за личне податке и заштиту тих података, у складу са тачком 9.3.3.

9.4.5. Упозорење и сагласност за коришћење личних података

Овјерилац УИО ће користити за потребе пружања услуге овјеравања личне податке само ако корисник да сагласност током процеса регистрације. Сматра се да је корисник дао сагласност уколико је потписао Уговор о издавању и коришћењу квалификоване електронске потврде.

9.4.6. Откривање личних података у складу са судским или административним поступком

Овјерилац УИО ће открити или доставити личне податке на захтјев надлежног органа и у другим случајевима када је то у складу са законом.

9.4.7. Друге околности за откривање личних података

Овјерилац УИО ће открити личне податке заштићене законом уз претходну сагласност корисника или на захтјев надлежног органа и у другим случајевима предвиђеним законом.

9.5. Заштита права интелектуалне својине

Сва права интелектуалне својине Овјериоца УИО укључујући заштитне знаке и ауторска права остају искључиво власништво Овјериоца УИО.

Софтвер треће стране Овјерилац УИО користи у складу с одредбама важеће лиценце.

9.6. Права и обавезе

9.6.1. Права и обавезе овјериоца

Овјерилац УИО гарантује пружање услуге овјеравања, у складу са законом, другим прописима, овим Практичним правилима и другим актима Управе за индиректно опорезивање који су у складу са важећим прописима Босне и Херцеговине.

Овјерилац УИО има обавезу да:

- Изврши провјеру идентитета корисника у поступку издавања или промјене статуса електронске потврде, као и тачност података у захтјеву за издавање и коришћење електронске потврде, односно захтјеву за промјену статуса електронске потврде,
- Изда квалификовану електронску потврду, у складу са законом,
- Обезбиједи да квалификована електронска потврда садржи све потребне податке, у складу са законом,
- Унесе у квалификовану електронску потврду основне податке о свом идентитету и о идентитету корисника, као и јавни криптографски кључ корисника који је пар његовом приватном криптографском кључу,
- Обезбиједи видљив податак у електронској потврди о тачном датуму и времену (час и минут) издавања потврде,
- Усвоји или одбије извршавање захтјева за промјену статуса квалификоване електронске потврде, у складу са законом,
- Води ажуран, тачан и безбједним мјерама заштићен регистар опозваних потврда и да исти буде јавно доступан,

- Обезбиједи видљив податак у регистру опозваних потврда о тачном датуму и времену (час и минут) опозива електронске потврде,
- Врши надзор над радом организационих јединица у саставу овјериоца.

Овјерилац УИО пружа услуге у складу са важећим прописима и интерним актима.

9.6.2. Права и обавезе Групе за подршку корисницима система PKI УИО

Група за подршку корисницима система PKI УИО, има права и обавезе да:

- Провјери идентитет корисника у поступку издавања електронске потврде и тачност података у захтјеву за издавање и коришћење електронске потврде,
- Провјери идентитет корисника и тачност података у захтјеву за промјену статуса електронске потврде,
- Прослиједи податке за издавање и промјену статуса електронске потврде, као и сву документацију Групи за одржавање система PKI УИО.

9.6.3. Права и обавезе корисника

Овјерилац УИО обезбјеђује поштовање и остваривање свих права и обавеза корисника, која су утврђена прописима, а односе се на квалификовану електронску потврду укључујући и ова правила.

Корисник је обавезан да:

- Чува средства и податке за формирање квалификованог електронског потписа од неовлашћеног приступа и употребе,
- Достави све потребне податке и информације о свом идентитету и о промјенама које утичу или могу утицати на тачност утврђивања његовог идентитета одмах, а најкасније у року од 24 (двадесетчетири) часа од тренутка настанка промјене,
- Одмах затражи опозив своје квалификоване електронске потврде у свим случајевима губитка или оштећења средстава или података за формирање квалификованог електронског потписа,
- Намјенски користи квалификовану електронску потврду,
- Испуњава друге обавезе у складу са законом и закљученим уговором који је сачињен у складу са важећим прописима.

9.6.4. Права и обавезе трећих лица

Трећим лицима се гарантује да Овјерилац УИО услуге овјеравања пружа у складу са законом, овим Практичним правилима и другим важећим прописима.

Обавезе трећих лица, прије него што се поуздају у квалификовану електронску потврду издату од стране Овјериоца УИО су:

- Провјеравање статуса потврде,
- Упознавање се са одговорностима и ограничењима Овјериоца УИО дефинисаним у овим Практичним правилима и другим актима објављеним на званичној *Web* страници Овјериоца УИО.

9.6.5. Права и обавезе других учесника

Сваком учеснику гарантује се да Овјерилац УИО услуге овјеравања пружа у складу са законом, овим Практичним правилима и другим важећим прописима Овјериоца УИО.

9.7. Изузеће од одговорности

Овјерилац УИО не одговара за штету насталу због непоштовања права и обавеза прописаних законом, важећим подзаконским прописима и овим Практичним правилима.

9.8. Одговорност и ограничења од одговорности

9.8.1. Одговорност и ограничења од одговорности овјериоца

Овјерилац УИО је дужан да на прописан начин издаје квалификоване електронске потврде и одговоран је за штету причињену лицу које се поуздало у ту потврду, у складу са законом, актима овјериоца и уговором закљученим између Овјериоца УИО и корисника.

Овјерилац УИО је дужан да чува доказе о томе да је поступао у складу са важећим прописима.

9.8.2. Престанак рада

У случају престанка рада, Овјерилац УИО ће:

- Обавијестити све кориснике путем *Web* странице и надлежног тијела државне управе најмање шест мјесеци прије планираног прекида рада,
- Осигурати наставак пружања услуга повјерења код другог пружаоца услуга повјерења свим корисницима којима је већ издао потврде и доставити сву документацију везану за пружање услуга повјерења том пружаоцу услуга повјерења,
- Опозвати све издане потврде у најкраћем могућем року, а најкасније у року од 48 часова, обавијестити надлежно тијело државне управе и доставити сву документацију везану за извршене услуге, у случају да не обезбиједи наставак пружања услуга повјерења преко другог даваоца услуга повјерења,

- Осигурати доступност пописа опозваних потврда у року од године дана након опозива свих потврда,
- Архивирати све податке у складу с периодом прописаним релевантним законом од посљедњег дана рада овјериоца.

9.8.3. Одговорност и ограничења од одговорности корисника квалификоване електронске потврде

Корисник је одговоран за штету која је настала његовом кривицом, односно због неиспуњавања обавеза утврђених у тачки 9.6.3. ових Практичних правила.

Корисник је одговоран ако с намјером или из нехата обрише потврду и/или припадајући приватни кључ са смарт картице. Смарт картица са које је обрисана потврда и/или припадајући приватни кључ не подлијеже рекламацији, ни гаранцији.

Корисник није одговоран за штету, ако докаже да је поступао у складу са законом, подзаконским актима и закљученим уговором.

9.9. Надокнаде

За пружање услуга Овјериоца УИО, корисник плаћа надокнаде у складу са тачком 9.1. ових Практичних правила.

9.10. Ступање на снагу и престанак важења правних аката

9.10.1. Ступање на снагу правних аката

Правна акта Овјериоца УИО ступају на снагу у року утврђеном у сваком од тих аката у складу са законом.

Политика овјеравања Овјериоца УИО и ова Практична правила објављују се и јавно су доступна свим заинтересованим лицима на *Web* страници Овјериоца УИО.

9.10.2. Период важења

Примјена ових Практичних правила није временски ограничена и иста ће бити на снази до објављивања нових правила.

9.10.3. Ефекат трајања

Овјерилац УИО ће и послије престанка важења електронске потврде штитити повјерљивост личних и других података корисника, као и послије престанка важења својих аката.

9.11. Појединачна обавјештења и комуникација са корисницима

Овјерилац УИО комуницира са корисницима путем електронске поште, писаним путем и *Web* странице, осим ако није другачије одређено овим Практичним правилима.

9.12. Допуне Практичних правила

9.12.1. Поступак за допуну

Овјерилац УИО ће, у случају промјене законске регулативе и процедуре рада извршити усклађивање својих важећих аката са истим.

Измјене и допуне Практичних правила, које се односе на рад Овјериоца УИО и издавање електронских потврда по правилу се усвајају тридесет дана прије почетка примјене. Измјене и допуне Практичних правила, које по процјени Овјериоца УИО не утичу битно на кориснике усвајају се осам дана прије почетка примјене.

9.12.2. Механизам и период обавјештавања

О измјенама и допунама Практичних правила и осталих докумената везаних за Практична правила, Овјерилац УИО обавјештава Министарство комуникација и транспорта БиХ и исте објављује на *Web* страници Овјериоца УИО.

9.12.3. Околности под којима *OID* мора да се промијени

Промјена *OID*-а ће се извршити уколико Овјерилац УИО одлучи да изврши измјене у Политици овјеравања и Практичним правилима, а које захтијевају промјену *OID*-а.

9.13. Рјешавања у случају спора

Уколико дође до спора између УИО и корисника квалификоване електронске потврде, односно трећих лица у вези међусобних права и обавеза и тумачења уговора и ових Практичних правила, УИО ће настојати да спор ријеши мирним путем, споразумно, а уколико до споразума не дође, спор ће рјешавати надлежни суд у Бањој Луци.

9.14. Мјеродавно право

За тумачење и примјену ових Практичних правила мјеродавно је законодавство Босне и Херцеговине.

9.15. Усклађеност са важећим законодавством

Правни акти Овјериоца УИО су у складу са законом и другим прописима Босне и Херцеговине који регулишу ову област.

9.16. Остале одредбе

9.16.1. Уговор са корисницима

Пружање услуга овјеравања (издавање и коришћење електронске потврде) регулише се посебним уговором између Овјериоца УИО и корисника, у складу са законом и другим прописима.

9.16.2. Преношење права

Корисник електронске потврде не може права из закљученог уговора са Овјериоцем УИО у цјелини или дјелимично преносити на трећа лица.

Овјерилац УИО права и обавезе из уговора закљученог са корисником, може у потпуности или дјелимично, без сагласности корисника, пренијети на другог регистрованог овјериоца у БиХ или надлежни орган.

9.16.3. Измјена ових Практичних правила

Измјене или допуне појединих одредби ових Практичних правила или аката донесених на основу ових Практичних правила не утичу на важење осталих одредби ових Практичних правила.

9.16.4. Примјењивост за адвокатске накнаде и одрицање од права

Није примјењиво.

9.16.5. Виша сила

Овјерилац УИО се ослобађа одговорности за било коју штету причињену кориснику, другом учеснику или трећем лицу, приликом пружања услуге овјеравања, уколико је до штете дошло усљед разлога, који су ван контроле Овјериоца УИО, односно усљед више силе.

Вишу силу представљају ванредне околности и непредвидљиве ситуације као што су природне катастрофе, тероризам, недостатак напајања или прекид телекомуникационих веза, пожар, непредвидљиви инциденти као што су вируси или напади са циљем онемогућавања сервиса, грешке у криптографским алгоритмима и сл.

9.17. Ступање на снагу

Ова Практична правила ступају на снагу даном доношења а почињу са примјеном осмог дана од дана објављивања на *Web* страници Овјериоца УИО.

Број: 01-02-2-160-8/21
Датум: 12.03.2021.

Директор
Управе за индиректно опорезивање

_____

др. Миро Џакула