Na osnovu člana 61. Zakona o upravi („Službeni glasnik BiH“, br. 32/02, 102/09 i 72/17) i člana 5. Pravilnika o bližim uvjetima za izdavanje kvalificiranih potvrda („Službeni glasnik BiH“, broj: 14/17) direktor Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine donosi

POLITIKU OVJERAVANJA
OVJERIOCA AGENCIJE ZA IDENTIFIKACIONE DOKUMENTE, EVIDENCIJU I RAZMJENU PODATAKA BOSNE I HERCEGOVINE

1. UVOD

Agencija za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (u daljnjem tekstu: IDDEEA) je izgradila infrastrukturu javnih kriptografskih ključeva - Public Key Infrastructure – PKI i kao ovjerilac u smislu Zakona o elektronskom potpisu („Službeni glasnik BiH“, broj: 91/06) prisutna je kao ovjerilac koji pruža usluge izdavanja kvalificiranih elektronskih potvrda, upravljanja životnim ciklusom elektronskih potvrda, pod imenom: Ovjerilac IDDEEA.

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

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

Opća pravila funkcioniranja Ovjerioca IDDEEA sadržana su u dokumentima:

1. Politika ovjeravanja Ovjerioca Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (Certification Policy - CP) (u daljnjem tekstu Politika ovjeravanja),
2. Praktična pravila pružanja usluge ovjeravanja Ovjerioca Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine (Certification Practices Statement - CPS) (u daljnjem tekstu Praktična pravila).

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

Ovjerilac IDDEEA koristi u svojoj infrastrukturi za izdavanje kvalificiranih i nekvalificiranih elektronskih potvrda hijerarhiju više CA (eng. Certification Authority) servera.

Dvorazinsku arhitekturu Infrastrukture Ovjerioca IDDEEA čine dva CA servera:
- Korijenski ovjerilac: "IDDEEA-RootCA-2021":

Podređeni ovjerioci za izdavanje potvrda, potpisani od strane „"IDDEEA-RootCA- 2021":
- „IDDEEA-IssuingCA"

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

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

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

2. OBJAVLJIVANJE I LOKACIJA PODATAKA O USLUGAMA OVJERAVANJA

Ovjerilac IDDEEA objavljuje podatke i svu dokumentaciju koja se odnosi na izdavanje elektronskih potvrda na Web stranici http://iddeea.gov.ba. Web stranica je javno dostupna, kao i svi podaci i sva dokumentacija koji se na njoj nalaze.

Ovjerilac IDDEEA objavljuje na svojoj zvaničnoj Web stranici:

1. Politiku ovjeravanja Ovjerioca IDDEEA,
2. Praktična pravila pružanja usluge ovjeravanja Ovjerioca IDDEEA,
3. Prethodne verzije Politike ovjeravanja Ovjerioca IDDEEA i Praktičnih pravila pružanja usluge ovjeravanja Ovjerioca IDDEEA,
4. Obrazac ugovora o obavljanju usluga ovjeravanja,
5. Obrazac zahtjeva za izdavanje i korištenje elektronske potvrde,
6. Obrazac zahtjeva za promjenu statusa potvrde,
7. Definicije važećih profila potvrda Ovjerioca IDDEEA usklađenih sa eIDAS uredbom Evropske unije,
8. Korisnička uputstva,

9. Potvrde ovjerioca IDDEEA – RootCA-2021 i podređenih ovjerilaca (IDDEEA IssuingCA) sa pridruženim hash vrijednostima,
10. Registre opozvanih potvrda (CRL – eng. Certificate Revocation List) ovjerioca IDDEEA - RootCA-2021, IDDEEA IssuingCA),
11. Zakonsku regulativu iz područja elektronskog potpisa i pružanja usluga povjerenja,
12. Lokacije ureda Registracijskog tijela,
13. Obavještenja korisnicima vezane uz davanje usluga ovjeravanja,
14. Druge akte i obavještenja.

3. IDENTIFIKACIJA I AUTENTIFIKACIJA

Ovjerilac IDDEEA identifikuje korisnika na osnovu identifikacionog dokumenata koje korisnik podnosi (važeća lična karta ili putna isprava). Korisnik mora lično da podnese cjelokupnu dokumentaciju.

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

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

Imena kojima bi se kršila intelektualna ili autorska prava drugih nisu dozvoljena.

Ovjerilac IDDEEA nije obavezan da verificira da li je korištenje takvih imena zakonito.

Korisnik snosi odgovornost za to da osigura zakonito korištenje odabranog imena.

Kvalificirana elektronska potvrda za elektronski potpis se može izdati samo fizičkom licu, u skladu sa Zakonom o elektronskom potpisu.

Korisnik mora biti fizički prisutan u toku registracije.

4. OPERATIVNI ZAHTJEVI U PROCESU IZDAVANJA POTVRDA

Za izdavanje elektronske potvrde, korisnik je dužan da:

1. Popuni i potpiše zahtjev za izdavanje i korištenje elektronske potvrde i uz isti priloži na uvid identifikacioni dokument,
2. Ispuni zahtjeve za identifikaciju,
3. Potpiše ugovor o izdavanju i korištenju elektronske potvrde.

Zahtjev za izdavanje i korištenje elektronske potvrde sadrži podatke na osnovu kojih Ovjerilac IDDEEA može da stupi u kontakt s korisnikom elektronske potvrde.
Ugovor sadrži uvjete izdavanja i korištenja potvrde, a stupa na snagu kada ga potpišu ugovorne strane.

Korištenje kvalifikovane elektronske potvrde se ugovara na rok od pet godina i vezuje se za dan izdavanja potvrde, odnosno rok valjanosti lične karte odnosno pasoša punoljetnog državljanina BiH, ukoliko se zahtjev za izdavanje elektronske potvrde podnosi putem ovlaštenog Registracionog tijela diplomatsko konzularnog predstavništva Bosne i Hercegovine.

Ovjerilac IDDEEA će odobriti zahtjev za izdavanje elektronske potvrde, ukoliko su ispunjeni sljedeći uvjeti:

1. Korisnik je lično podnio potrebnu dokumentaciju,
2. Podnesena dokumentacija je provjerena,
3. Svi podaci unijeti u zahtjev smatraju se odgovarajućim i kompletnim.

Ako korisnik ne ispuni uvjete iz prethodnog stava ili ako na bilo koji način povrijedi odredbe ovih Politika ili Praktičnih pravila, Ovjerilac IDDEEA će odbiti zahtjev za izdavanje elektronske potvrde.

Izdavanje elektronske potvrde vrši se na sljedeći način:

1. Korisnik, u postupku izdavanja potvrde, identificira se lično u Registracionom uredu,
2. Po izvršenoj identifikaciji neposrednim putem u saradnji s ovlaštenim službenikom popunjava/daje podatke neophodne za Zahtjev za izdavanje kvalifikovane digitalne potvrde.
3. U Zahtjev se unose traženi podaci koje ovlašteni službenik ovjerioca IDDEEA elektronskim putem evidentira u aplikaciju IDDEEA RA. Nakon uspješno popunjenog Zahtjeva za izdavanje kvalifikovane digitalne potvrde, ovlašteni službenik Ovjerioca IDDEEA štampa u papirnoj formi obrazac Zahtjeva u koji su uneseni potrebni podaci i isti predaje na uvid podnosiocu. Podnosilac je dužan da provjeri tačnost unesenih podataka i svojim potpisom potvrđuje iste, čime se formalno smatra da je Zahtjev podnesen.
4. Ovlašteni službenik u Registracionom uredu unosi podatke o korisniku i kreira zahtjev u aplikaciji Registracijskog tijela i prosljeđuje verificiran zahtjev operativnom tijelu PKI IDDEEA,
5. Korisnik potpisuje ugovor o izdavanju i korištenju elektronske potvrde,
6. Operativno tijelo PKI IDDEEA na osnovu verificiranog zahtjeva kreira nalog za izdavanje elektronske potvrde,

Postupak i proces za izdavanje elektronske potvrde zavisi od vrste elektronske potvrde:

1. Digitalne kvalifikovane elektronske potvrde na ličnoj karti državljana Bosne i Hercegovine;

Proces izdavanja za elektronske potvrde i za dva para ključeva sastoji se od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebnim podsistemima:

a) pred-predstavljanje QSCD-a (generisanje ključeva na kartici, postavljanje lozinke za osiguranje certifikata)
b) dobijanje obrasca zahtjeva za izdavanje elektronske potvrde,
c) pregled obrasca zahtjeva za izdavanje elektronske potvrde,
d) priprema elektronske potvrde,
e) kreiranje QSCD-a (izdavanje i pohranjivanje elektronske potvrde, ispis podataka o subjektu)
f) distribucija elektronske potvrde i privatne lozinke (PIN koda) i obavještenja subjektu.

Digitalna elektronska potvrda za QSCD i PIN dostavlja se RA-u i preuzima ga lično korisnik ili se šalju korisniku e-poštom i/ili SMS-om na registrovanu e-adresu i/ili registrovani broj telefona.

2. Kvalifikovana digitalna elektronska potvrda za elektronsko potpisivanje na daljinu;

Proces izdavanja za elektronske potvrde i za jedan par ključeva se sastoji od jasno razdvojenih dijelova (ili funkcija), sa svojim zasebnim podsistemima:

a) pregled obrasca zahtjeva za izdavanje elektronske potvrde,
b) priprema elektronske potvrde, registracije i aktivacijskog koda,
c) slanje registracije i aktivacijskog koda i obavještenja korisniku,
d) generisanje ključeva na sigurnoj pohrani i izdavanje elektronske potvrde.

Registracijski kod se korisniku šalje putem dva odvojena kanala, jedan putem e-pošte, a drugi putem drugog sigurnog kanala (siguran web portal kojem se može pristupiti kvalifikovanom elektronskom potvrdom, preporučenom poštom ili putem posebne web stranice na kojoj se imaoc identificira posebnim kodom primljenim putem SMS-a i drugim podacima koji su mu poznati (npr. Jedinstveni matični broj korisnika, broj važeće lične karte ili pasoša i slično). Iznimno, jedan od gore navedenih kodova može korisniku predati i ovlaštena osoba Ovjerioca IDDEEA RA lično.

Procedure su osmišljene na način da ih ne može provoditi samostalno jedna osoba.

Ovjerilac IDDEEA može ovlastiti provjerene vanjske izvođače za određene poslove (npr. ispis podataka o vlasniku, printanje PIN-a, isporuku itd.) na temelju pisanog ugovora, što redovito prati i za koje je odgovoran kao da obavlja same zadatke.

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

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

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

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

1. U slučaju da neka informacija sadržana u potvrdi postane netačna,
2. Promjene podataka u potvrdi, koje zahtjevaju izdavanje nove potvrde,
3. Naknadnog utvrđivanja da podaci koje je dostavio korisnik pri identifikaciji nisu tačni,
4. Gubitka, oštećenja ili zloupotrebe tehničkih sredstava (hardvera ili softvera) ili privatnog kriptografskog ključa, odnosno kompromitiranja ili sumnje u kompromitiranje privatnog kriptografskog ključa,
5. U slučaju trajne nedostupnosti privatnog ključa,
6. U slučaju ako privatni ključ ili aktivacijski podaci nisu više u posjedu potpisnika, odnosno pečatioca,
7. U slučaju prestanka odnosa između potpisnika i poslovnog subjekta,
8. Neispunjavanja obaveza korisnika potvrde određenih ovim Politikama, Praktičnim pravilima i ugovorom,
9. Ukoliko opoziv elektronske potvrde zahtjeva korisnik potvrde,
10. Ukoliko korisnik elektronske potvrde prestane da postoji,
11. U slučaju da potvrda više ne ispunjava formalne zahtjeve definisane Politikom i Praktičnim pravilima,
12. Ukoliko se promijene okolnosti koje bitno utiču na važenje potvrde,
13. U slučaju otkaza ugovora o obavljanju usluge ovjeravanja od strane korisnika,
14. Iz drugih razloga koji su utvrđeni Zakonom o elektronskom potpisu i drugim propisima koji reguliraju ovu oblast.

Opoziv elektronske potvrde može da zahtijeva:

1. Korisnik elektronske potvrde – fizičko lice,
2. Ovjerilac IDDEEA,
3. Nadležni državni organ na osnovu zakona.

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

Registri opozvanih potvrda ovjerioca objavljuju se na svaka 24 sata.

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

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

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

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

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

Ovjerilac IDDEEA može da suspendira elektronske potvrde i privremeno onemogući upotrebu, tokom provjere i razjašnjenja okolnosti u vezi s mogućim opozivom potvrde.

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

Korisnik prestaje s korištenjem elektronske potvrde:

1. Istekom roka važnosti elektronske potvrde,
2. Opozivom elektronske potvrde,
3. Tijekom trajanja suspenzije elektronske potvrde.

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

5. KONTROLA FIZIČKOG PRISTUPA, PROCEDURA I OVLAŠTENIH OSOBA

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

1. Pristup u prostorije, sigurnu zonu, elektronski se bilježi i unosi u elektronski dnevnik za pristup prostorijama, i isti se pregleda,
2. Brave, elektronski sistemi zaštite i sistemi protupožarne zaštite su u skladu sa važećim standardima,
3. Prostor i sistem nadgledani su 24 sata, 7 dana u sedmici od strane ovlaštenih lica Ovjerioca

IDDEEA,

4. Pristup se može provoditi isključivo uz prisutnost najmanje dva ovlaštena lica koja imaju pravo pristupa,
5. Pristup zbog održavanja sistema mora biti unaprijed najavljen, osim u slučaju smetnji u radu sistema za koje operativno tijelo PKI IDDEEA utvrdi da zahtijevaju hitnu intervenciju,
6. Svaki pristup zaštićenoj prostoriji evidentira se unutar elektronske evidencije.

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

Prostorije u kojima se nalazi infrastruktura Ovjerioca IDDEEA u sjedištu IDDEEA su opremljene:

1. Sistemom za neprekidni izvor napajanja električnom energijom i stabilizaciju napona za računarsku i komunikacijsku opremu, koji je povezan sa agregatom,
2. Neovisnim sistemom za klimatizaciju koji omogućava kontrolu temperature i vlažnosti vazduha unutar prostorija Ovjerioca IDDEEA.

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

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

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

Ovjerilac IDDEEA garantira da sve poslove koji se obavljaju u okviru propisane djelatnosti obavljaju lica od povjerenja s tačno propisanim obavezama i ovlaštenjima. Rad ovih lica je podložan stalnim provjerama. Zaposleni Ovjerioca IDDEEA moraju biti kvalificirani za obavljanje poslova iz Praktičnih pravila i podliježu provjeri stručne sposobnosti.

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

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

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

ponovno uspostavljeni u najkraćem mogućem roku.

Ovjerilac IDDEEA će u slučaju kompromitiranja privatnog kriptografskog ključa aplikacije ovjerioca odmah:

1. Opozvati izdane elektronske potvrde,
2. Opozvati potvrdu aplikacije ovjerioca,
3. Objaviti registar opozvanih potvrda,
4. Obavijestiti korisnike izdanih elektronskih potvrda.

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

Ovjerilac IDDEEA u slučaju prestanka rada ima obavezu:

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

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

6. KONTROLE TEHNIČKE ZAŠTITE

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

Par kriptografskih ključeva korisnika za potpisivanje i verificiranje kvalificiranog elektronskog potpisa generira se na SSCD uređaju ili sistemima namjenjenim za izdavanje elektronske potvrde za udaljeni elektronski potpis, koji predstavljaju sredstvo za formiranje kvalificiranog elektronskog potpisa.

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

1. Kriptografski ključevi aplikacije ovjerioca: RSA ključevi najmanje dužine 4096 bita,
2. Korisnički ključevi: RSA ključevi najmanje dužine 2048 bita.

Generiranje parametara javnog kriptografskog ključa aplikacije ovjerioca vrši se u hardverskim

kriptografskim modulima Ovjerioca IDDEEA, a parametri javnih kriptografskih ključeva korisnika generiraju se u kriptografskim SSCD uređajima i softveru Ovjerioca IDDEEA, ovisno od profila potvrde po kojem se izdaje potvrda.

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

Ovjerilac IDDEEA ima implementiranu višestruku autorizaciju za pristup privatnom kriptografskom ključu aplikacija ovjerioca IDDEEA – RootCA-2021 i IDDEEA IssuingCA Ovjerioca IDDEEA.

Ovjerilac IDDEEA ne nudi mogućnost otkrivanja privatnog kriptografskog ključa.
Kreiranje kopija privatnih kriptografskih ključeva povezanih sa kvalificiranim elektronskim potvrdama korisnika se ne radi.

Rokovi važnosti potvrda Ovjerioca IDDEEA su:

Period važenja javnih i privatnih kriptografskih ključeva u potvrdama koje izdaje Ovjerilac IDDEEA je:

1. Root javni verifikacijski ključ i elektronska potvrda TSP-a: 20 godina.
2. Root privatni ključ za potpisivanje TSP-a: 20 godina.
3. Javni verifikacijski ključ i elektronska potvrda izdavaoca TSP-a: 10 godina.
4. Privatni ključ izdavaoca TSP-a: 10 godina.
5. Javni verifikacijski ključ i elektronska potvrda korisnika: do 10 godina.
6. Privatni ključ korisnika: do 10 godina.
7. OCSP javni verifikacijski ključ i elektronska potvrda: do 3 godine.
8. OCSP privatni ključ za potpisivanje: do 3 godine.
9. Ovjerilac IDDEEA može prilagoditi period važenja nekih kriptografskih ključeva korisnika na osnovu posebnih zahtjeva i zahtjeva javne nabavke u skladu sa propisima i vrstom elektronske potvrde.

Svaki korisnik kvalificirane elektronske potvrde je odgovoran za čuvanje lozinke svog SSCD uređaja, odnosno pristupnih kodova i lozinki za pristup servisima korištenja elektronskog potpisa za udaljeno potpisivanje.

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

1. Kontrola pristupa do sistemskih servisa aplikacije Ovjerioca IDDEEA,
2. Kontrola pristupa funkcijama aplikacije Ovjerioca IDDEEA,
3. Stroga podjela uloga između ovlaštenih lica Ovjerioca IDDEEA,
4. Upotreba kriptografskih modula za smještanje kriptografskih ključeva ovlaštenih lica Ovjerioca IDDEEA,

5. Sigurno arhiviranje podataka aplikacije Ovjerioca IDDEEA i elektronskih dnevnika,
6. Zaštita elektronskih dnevnika, odnosno podataka u istima o svim događajima koji se odnose na sigurnost,
7. Uspostavljanje mehanizama obnove sistema, kriptografskih ključeva i baze podataka aplikacije Ovjerioca IDDEEA.

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

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

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

7. SADRŽAJ POTVRDE, REGISTRA OPOZVANIH POTVRDA I OCSP PROFILI

Ovjerilac IDDEEA izdaje potvrde sukladne specifikaciji X.509 verzije 3.

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

Ovjerilac IDDEEA potpisuje kvalificirane elektroničke potvrde i registre opozvanih potvrda primjenom algoritma SHA512RSA sukladno dokumentima RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 4055 – Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile i RFC 6931 – Additional XML Security Uniform Resource Identifiers (URIs).

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

8. REVIZIJA USKLAĐENOSTI RADA IDDEEA OVJERIOCA I DRUGE PROCJENE

Ovjerilac IDDEEA vrši analizu rizika provodeći testove ranjivosti sistema kojom identifikuje kritične servise koji zahtijevaju korištenje sigurnih sistema i visok nivo sigurnosti:

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

Ovjerilac IDDEEA izvršava redovne unutarnje revizije rada provođenjem testova ranjivosti sistema dva puta godišnje.

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

Rukovodilac Tehničkog sektora IDDEEA ili drugo lice po posebnom ovlaštenju direktora, odgovoran je za provođenje unutarnjih revizija i određivanje lica koja ih provode.

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

1. Tehnologije infrastrukture javnih kriptografskih ključeva,
2. Vršenja djelatnosti ovjerioca,
3. Provođenja revizije ovjerioca ili drugog informacijsko-komunikacijskog sistema.

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

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

9. USKLAĐENOST SA eIDAS 2.0

IDDEEA u okviru priprema za nadolazeći regulatorni okvir eIDAS 2.0 primjenjuje najnovije verzije tehničkih standarda navedenih u Prilogu 1 ovog dokumenta, a radi lakše akreditacije i poređenja sa EU standardima. U cilju osiguranja dugoročne regulatorne relevantnosti, predviđena je integracija infrastrukture IDDEEA s evropskim sistemima za digitalni identitet, uključujući EU Digital Identity Wallet (EUDI).

Ova usklađenost omogućiti će interoperabilnost kvalificirane elektronske potvrde na nivou EU, te osigurati pravovremenu adaptaciju na zahtjeve eIDAS 2.0 regulative.

10. OSTALI POSLOVI I PRAVNA PITANJA

Ovjerilac IDDEEA može da naplaćuje izdavanje elektronske potvrde na osnovu posebnih odluka Vijeća ministara Bosne i Hercegovine koje će u slučaju donošenja biti objavljene na Web stranici Ovjerioca IDDEEA.

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

Ovjerilac IDDEEA je dužan da osigura najniži iznos osiguranja od odgovornosti za moguću štetu nastalu vršenjem usluga izdavanja kvalificirane elektronske potvrde u skladu sa važećim propisima, tako da:

1. Osigurana suma na koju mora biti ugovoreno osiguranje po jednom štetnom događaju ne može iznositi manje od 50.000,00 KM, podrazumijevajući pri tom kao štetni događaj pojedinačnu štetu nastalu upotrebom jedne kvalificirane elektronske potvrde u jednom aktu u pravnom prometu,
2. Ukupna osigurana suma na koju mora biti ugovoreno osiguranje od odgovornosti ovjerioca kumulativno na godišnjem nivou, po svim štetnim događajima, ne može biti niža od 1.500.000,00 KM.

Ovlaštena lica Ovjerioca IDDEEA i korisnici obavezuju se:

1. Da čuvaju tajnost podataka primjenom mjera koje koriste za zaštitu svojih tajnih podataka i da će ih koristiti samo za potrebe zbog kojih su bili prikupljeni ili formirani u odnosu na odredbe Praktičnih pravila,
2. Da neće neovlašteno otkrivati tajne podatke, bez prethodnog odobrenja u pisanoj formi koje daje korisnik ili nadležni organ.

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

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

Ovjerilac IDDEEA garantira pružanje usluge ovjeravanja, u skladu sa zakonom, drugim propisima, Praktičnim pravilima i drugim aktima Agencije za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine koji su usklađeni s važećim propisima Bosne i Hercegovine.

Ovjerilac IDDEEA ima obavezu:

1. Izvršiti provjeru identiteta korisnika u postupku izdavanja ili promjene statusa elektronske potvrde, kao i tačnost podataka u zahtjevu za izdavanje i korištenje elektronske potvrde,

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

Ovjerilac IDDEEA pruža usluge u skladu sa važećim propisima i internim aktima.

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

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

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

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

U slučaju prestanka rada, Ovjerilac IDDEEA će:

1. Obavjestiti Ured za nadzor i akreditaciju ovjerilaca i sve aktuelne korisnike najmanje devedeset (90) dana prije namjere prestanka rada;
2. U dogovoru sa Uredom za nadzor i akreditaciju ovjerilaca prebaciti svoje aktivnosti na drugog pružaoca usluga povjerenja ili opozvati sve važeće certifikate na dan ili nakon isteka otkaznog roka;
3. U slučaju da prebacivanje usluga drugom pružaocu usluga nije moguće, Ovjerilac IDDEEA će dostaviti svu dokumentaciju, podatke i opremu Ministarstvu transporta i komunikacija Bosne i Hercegovine u skladu sa Zakonom o elektronskom potpisu;
4. Obezbijediti da se sva dokumentacija i arhiva prebaci na drugog pružaoca usluga povjerenja ili na Ministarstvo transporta i komunikacija Bosne i Hercegovine ili da se čuva najmanje deset (10) godina od posljednjeg dana rada;
5. Obezbijediti dostupnost i pristup relevantnim spiskovima opozvanih certifikata i OSCP-u u periodu od 6 mjeseci nakon opoziva svih certifikata.

Prije prestanka pružanja usluga, Ovjerilac IDDEEA će uništiti privatne ključeve CA, uključujući i rezervne kopije ili ih povući iz upotrebe, na način da se privatni ključevi ne mogu ponovo preuzeti.

Na web-sajtu IDDEEA-e izdati obavijest o prekidu pružanja usluga.

Korisnik je odgovoran za štetu koja je nastala njegovom krivicom.

Korisnik je odgovoran ako s namjerom ili iz nehata obriše potvrdu i/ili pripadajući privatni ključ sa lične karte. Obrisana potvrda i/ili pripadajući privatni ključ ne podliježe reklamaciji, ni garanciji. Korisnik je odgovoran za čuvanje pristupnih kodova i lozinki neophodnih za upotrebu elektronskog potpisa za udaljeno potpisivanje.

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

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

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

Ovom Politikom ovjeravanja Ovjerioca Agencije za identifikacione dokumente, evidenciju i

razmjenu podataka stavlja se van snage Politika broj: 15-02-30-31-1041-17/2025 od 29.01.2026. godine.

Usklađivanje sa najnovijim verzijama tehničkih standarda, vrši se izmjenom Priloga 1.

Ova Politika ovjeravanja stupa na snagu danom donošenja.

Direktor
prof.dr. Almir Badnjević

дигитално потписано / digitalno potpisano / digitally signed

Broj: 15-02-30-31-1041-20/2025
Datum: 16.06.2026. godine

Prilog 1

Tehnički standardi:

ETSI EN 319 401	V3.2.1	2026-01
ETSI EN 319 411-1	V1.5.1	2025-04
ETSI EN 319 411-2	V2.6.1	2025-06
ETSI EN 319 412-1	V1.7.1	2026-05
ETSI EN 319 412-2	V2.5.0	2026-05
ETSI EN 319 412-3	V1.4.1	2025-11
ETSI EN 319 412-5	V2.6.1	2026-05
ETSI EN 319 421	V1.3.1	2025-07