Arhitektura sistema i aplikacije na elektronskoj ličnoj karti BiH V.2.0

mart 2023. godine

Sadržaj

1. Uvod

U nedostatku strateških dokumenta vezanih za razvoj elektronskih dokumenata u Bosni i Hercegovini u pisanju ovog dokumeta korištena je strana literatura. U projektovanju i dizajniranju sistema iskorištene su najbolje prakse kako zemalja u okruženju tako i u Evropskoj uniji. Što zasigurno povećava sigurnost elektronskih ličnih karti, koje ćemo u daljem tekstu skraćeno označavati kao eID (eng. „Electronic Identification Document“).
Funkcije koje eID podržava zasnivaju se na:

1. Zakon o ličnoj karti državljana Bosne i Hercegovine ("Službeni glasnik BiH", broj: 32/01,16/02, 32/07, 53/07, 56/08 i 18/12) – u daljem tekstu Zakon o LK
2. Zakon o Agenciji za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine („Službeni glasnik BiH“, broj 56/08) – u daljem tekstu Zakon o Agenciji
3. Zakon o elektronskom potpisu („Službeni glasnik BiH“, broj 91/06).
4. ICAO standardi - Machine Readable Travel Documents - Part 1: Machine Readable Passport, Specifications for electronically enabled passports with biometric identification capabilities, ICAO Doc 9303, 2006; ICAO, Machine Readable Travel Documents - Part 3: Machine Readable Official Travel Documents, Specifications for electronically enabled official travel documents with biometric identification capabilities, ICAO Doc 9303, 2008; ICAO. Supplemental Access Control for Machine Readable Travel Documents, Technical Report, 2010
5. Iskustvima, zahtjevima i najboljoj praksi Evropske Unije (i njenih članica).

Ugradnja čipa u tijelo lične karte povećava sigurnost dokumenta i smanjuje mogućnost falsifikovanja istog, te istovremeno omogućava upisivanje biometrijskih podataka na ličnu kartu kako bi potvrđivanje identiteta nosioca lične karte bilo još jednostavnije i sigurnije.

Dalje, upotreba elektronske lične karte omogućava sigurno predstavljanje građanina prilikom interakcije sa državnim institucijama i privatnim sektorom kroz komunikaciju baziranu na servisima pojedinih institucija objavljenih na javnoj internet mreži.

Dodatna funkcija lične karte je i aplikacija za digitalno potpisivanje koja omogućava digitalno potpisivanje dokumenata i transakcija u digitalnom svijetu a u skladu sa zakonima Bosne i Hercegovine. U odnosu na prethodnu verziju eID Agencija je zbog tehnoloških razloga promijenila čip, pošto se prethodni prestao proizvoditi, kao i aplikacije upisane u eID čip. Naime, u novoj verziji eID funkciju aplikacije za digitalno predstavljanje preuzima aplikacija za digitalno potpisivanje unutar koje će se upisivati certifikat za digitalno predstavljanje svim podnosiocima zahtjeva za LK.

1. Izmjene u odnosu na verziju 1.2

Zbog tehnoloških razloga Agencija je bila prinuđena promijeniti čip lične karte, jer se prethodni tip čipa prestao proizvoditi. Isto tako postojala je potreba da se tehnički pojednostavi način digitalnog predstavljanja koristeći eID. Imajući u vidu da se ove izmjene nisu mogle odgađati, te promjenu na noviji operativni sistem na čipu, postojeće aplikacije na eID su se morale revidirati. Kako prethodna arhitektura lične karte nije zaživjela u praksi posljednje izmjene nisu imale uticaja na korištenje lične karte. Lista najvažnijih izmjena je sljedeća:

- Promjena na operativni sistem JCOP 3
- Nova verzija ICAO aplikacije
- Nova verzija aplikacije za digitalno potpisivanje zasnovana na GIDS specifikaciji koja objedinjuje i digitalno predstavljanje
- Ukidanje postojeće eID aplikacije za digitalno predstavljanje

2. Proces prikupljanja podataka za eID

Sam proces prikupljanja podataka za eID obavljaju nadležni organi. Način prikupljanja podataka kod nadležnih organa, vođenje i tehničko održavanje podataka za eID su propisani Zakonom o LK, Zakonom o Agenciji te odgovarajućim podzakonskim aktima.

2.1. Nadležni organi u procesu

Agencija za identifikacione dokumente, evidenciju i razmjenu podataka Bosne i Hercegovine je upravna organizacija u sastavu Ministarstva civilnih poslova Bosne i Hercegovine zadužena za oblast identifikacionih dokumenata, skladištenje, personalizaciju i transport dokumenata, te centralno vođenje evidencija i razmjenu podataka između nadležnih organa u Bosni i Hercegovini.

Dakle, shodno zakonu, Agencija je nadležna da:

- predlaže i provodi strategiju i politiku razvoja u Bosni i Hercegovini u oblasti identifikacionih dokumenata, a prema ICAO 9303 standardu i drugim relevantnim standardima;
- vrši nabavku, skladištenje, personalizaciju, kontrolu kvalitete i transport identifikacionih dokumenata za potrebe nadležnih organa Bosne i Hercegovine;
- tehnički dizajnira i formira evidencije definirane ovim zakonom;
- održava i upravlja bazama podataka u koje se pohranjuju podaci iz evidencija koje su definirane ovim zakonom i informacionih sistema, putem kojih se pristupa navedenim evidencijama;
- osigurava adekvatnu infrastrukturu, posebne uslove za rad i zaštitu podataka, te druge tehničke preduslove za nesmetano funkcioniranje baza podataka koje su u njenoj nadležnosti i baza podataka koje su u nadležnosti drugih ministarstava, institucija i organa na njihov zahtjev i u skladu sa zakonom;
- izdaje podatke o evidencijama i iz evidencija ovlaštenim institucijama i pravnim licima;
- projektira, razvija i održava softverska rješenja potrebna za vođenje evidencija u nadležnosti Agencije, bilo internim resursima, saradnjom sa izvornim organima ili angažmanom kompanija;
- razvija, održava i unapređuje telekomunikacione mreže za prenos podataka za potrebe Agencije, te drugih organa javne sigurnosti u skladu sa Zakonom o telekomunikacijama, a kako bi se omogućila efikasna razmjena podataka iz registara definiranih ovim zakonom;
- definira standarde za opremu koju de nadležni, prijemni i izvorni organi nabavljati i koristiti u procesu obrade i razmjene podataka u skladu s ovim zakonom;
- definira standarde što je neophodno na lokacijama s kojih se vrši pristup sistemu centralne evidencije i razmjene podataka kako bi se postigla sigurnost i zaštita podataka i sistema;
- provodi upravne postupke koji se tiču djelokruga Agencije u skladu s važedim zakonskim propisima.

Agencija je nadležna za personalizaciju i tehničku obradu sljededih identifikacionih dokumenata:

- ličnih karata,
- ličnih karata za strance,
- vozačkih dozvola,
- putnih isprava,
- dokumenata za registraciju vozila,
- drugih identifikacionih dokumenata uz saglasnost nadležnih organa i posebnu odluku Vijeća ministara.

Agencija vodi evidenciju:

- jedinstvenih matičnih brojeva (JMB);
- prebivališta i boravišta državljana Bosne i Hercegovine;
- ličnih karata državljana Bosne i Hercegovine;
- građanskih, službenih i diplomatskih pasoša;
- vozačkih dozvola;
- registracije motornih vozila i dokumenata za registraciju;
- ličnih karata za strane državljane;
- novčanih kazni i prekršajnu evidenciju;
- i druge evidencije za koje postoji saglasnost izvornih organa, a uz posebnu odluku Vijeća ministara.

Iz svega naprijed navedenog proizilazi da je Agencija nadležna za tehničku podršku u procesu izdavanja dokumenata, tehničko vođenje registara, te personalizaciju dokumenata.

Agencija sarađuje sa nadležnim organima u Bosni i Hercegovini koji su izvorni organi, te drugim organima koji koriste usluge Agencije u skladu sa posebnim propisima.

Kantonalna ministarstva unutrašnjih poslova u Federaciji Bosne i Hercegovine, Ministarstvo unutrašnjih poslova Republike Srpske i u Brčko distriktu nadležni organ koji funkcionalno djeluje kao državna institucija predstavljaju nadležne organe u procesu izdavanja ličnih dokumenata.

Za potrebe izdavanja ličnih dokumenata u sistem Agencije uvezani su svi organi lokalne uprave, odnosno opštine. Matični uredi predstavljaju organizacione jedinice u sastavu opština – gradova i isti su uvezani u sistem.

Neposredno na sistemu izdavanja ličnih dokumenata uvezano je preko 150 organa sa različtih nivoa vlasti, a posebno ističemo činjenicu da preko 600 službenika iz nadležnih opština *vrše provjere upisa u matičnim uredima i dostavljaju podatke nadležnim organima. Sve funkcioniše u realnom vremenu kroz aplikativno i sistemsko rješenje koje pruža IDDEEA.*

2.2. Predaja zahtjeva za ličnu kartu

U procesu podnošenja zahtjeva za izdavanje lične karte, svaki građanin na lokaciji nadležnog organa pored popunjavanja obrasca kroz proces akvizicije biometrijskih podataka predaje iste na čuvanje i postupanje. Pravila akvizicije biometrijskih podataka propisani su Pravilnikom o načinu uzimanja biometrijskih podataka u postupku izdavanja ličnih karata ("Službeni glasnik BiH", broj 102/12, 96/14).

Lični podaci koji se uzimaju su: ime, prezime, datum rođenja, mjesto rođenja, opšina prebivališta ili boravišta za raseljeno lice, spol, jedinstveni matični broj, fotografija, potpis, otisci prstiju i državljanstvo BiH.
Biometrijski podaci su fotografija lica, otisak prsta i potpis. Fotografija i otisci prstiju se upisuju na čip,a potpis koji se uzima i štampa na dokumentu se ne upisuje na čip.

2.3. Komunikacija između nadležih organa

Sva komunikacija između nadležnih organa u procesu izdavanja ličnih dokumenata se odvija kroz mrežu koju razvija i održava Agencija. Agencija je vlasnik telekomunikacione infrastrukture kojom je izvršeno uvezivanje svih lokacija nadležnih organa širom BiH. Riječ je o radio-relejnoj opremi koja radi na licenciranom opsegu, za što su dobijene sve neophodne dozvole od Regulatorne agencije za komunikacije. Ovaj sistem sastoji se od prenosne (Point-to-Point linkova velikih kapaciteta) i pristupne mreže (Point-to-Multi-Point opreme kojom je izvršeno uvezivanje lokacija nadležnih organa). Sva komunikacija, na kompletnom TK sistemu Agencije, shodno Standardima za opremu i softver, odvija se posredstvom VPN konekcije site-to-site na bazi IPsec. Na ovaj način obezbjeđuje se adekvatna zaštita i kriptovanje saobraćaja. Ovakva arhitektura daje značajne prednosti kao što su: značajno veći kapaciteti u odnosu na ranije korištene, sva administracija, održavanje i nadzor u nadležnosti Agencije, siguran način prenosa informacija, mogućnost jednostavnog proširenja i nadogradnje sistema, korištenje TK sistema Agencije i za sopstvene potrebe korisnika, mogućnost implementacije svih sadašnjih i budućih projekata, nadležni organi nemaju nikakvih dodatnih finansijskih troškova vezanih za uspostavu i održavanje sistema, kao i niz drugih pogodnosti.

2.4. Serijski broj lične karte

Serijski broj lične karte je devetocifreni broj koji se generiše u toku personalizacije dokumenta. Svaka lična karta ima jedinstven serijski broj. Struktura serijskog broja je data u slededoj tabeli.

Pozicija	Dužina	Domen	Opis
1	2 bajta	Hex	Lokacija izdavanja (C i D)
2	2 bajta	Hex	Godina i vrsta dokumenta
3	5 bajta	Hex	Redni broj
HEX: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F			

3. Kartica (obrazac lične karte)

Kartica predstavlja obrazac lične karte definisan Zakonom o LK. Obrazac lične karte služi da se na isti nanose podaci o nosiocu lične karte koji se upisuju u postupku personalizacije i proizvodnje lične karte, te kao medij za nošenje bezkontaktnog memorijskog elementa – čipa.

Osnovu kartice čini tijelo kartice koje je definisano i standardizovano ICAO dokumentima. Tijelo karitce je ID dokument u ID-1 formatu u skladu sa dokumentom ICAO 9303. Definicija sigurnosnih elemenata samog tijela kartice nije predmet ovog dokumenta.

3.1. Elektronski memorijski element (čip)

U tijelo kartice je integrisan beskontaktni čip. Proizvođač čipa je kompanija NXP. Oznaka čipa je J3H145C0X30_9B22B18 (JCOP3 P60). Elektronski memorijski element sadrži operativni sistem JCOP 3. Slobodan prostor za smještanje aplikacija i podataka iznosi 120Kb. Čip ugrađen u tijelo lične karte podržava najnovije kriptografske algoritme (kriptografija eliptičnih krivi) i omogućava niz naprednih funkcija lične karte.

Beskontaknti čip komunicira sa odgovarajućim čitačem (terminalom) koji je i uređaj za čitanje i pisanje po čipu. Komunikacija ove dvije komponente je u skladu sa ISO 14443 a bazirana je na ISO 7816.

3.1.1. Model autentifikcije

Kako bi komunikacija između čipa i čitača bila sigurna koriste se različite kriptografske metode autentikacije:

- BAC – „Basic Access Control“
- PACE – „Password Authenticated Connection Establishment“
- TA – „Terminal Authentication“
- PA – „Passive Authentication“
- CA – „Chip Authentication“

Različite grupe sa podacima štite se na različit način, zavisno od karaktera podataka koji se štite. Naravno, veći nivo zaštite je za grupu u kojoj se nalazi otisak prsta ili fotografija lica nego grupe u kojoj je upisano lično ime.

3.1.2. Podaci upisani u čip

Podaci koji se nalaze na čipu organizovani su kroz tri aplikacije:

- aplikacija glavne datoteke
- biometrijska ICAO aplikacija (istovjetna kao aplikacija na biometrijskom pasošu)
- aplikacija za digitalno potpisivanje

Pristup podacima zapisanim u aplikacijama je moguć nakon uspješnog predstavljanja čitača korištenjem BAC-a, PACE-a, TA ili CA.

3.1.3. Aplikacija glavne datoteke

Aplikacija glavne datoteke sadrži sistemske podatke neophodne za pristup podacima. Oni su zajednički za sve aplikacije. Pored ličnih podataka i podataka o dokumentu, na čipu moraju biti upisani i sistemski podaci potrebni za pristup podacima. Ova vrsta podataka zapisana je u master datoteci.

Datoteka	Sadržaj	Prava pristupa		
		Čitanje	Pisanje	Interno
EF.ATR	Sadrži opis mogudnosti kartice	Uvijek		
EF.DIR	Sadrži listu kartičnih aplikacija	Uvijek		
EF.CardAccess	▪ PACEInfo ▪ ChipAuthenticationInfo ▪ ChipAuthenticationDomain ▪ ParameterInfo ▪ PrivilegedTerminalInfo ▪ TerminalAuthenticationInfo ▪ CardInfoLocator	Uvijek		
EF.CardSecurity	▪ PACEInfo ▪ ChipAuthenticationInfo ▪ ChipAuthenticationDomainParameterInfo ▪ ChipAuthenticationPublicKeyInfo ▪ TerminalAuthenticationInfo ▪ CardInfoLocator ▪ RestrictedIdentificationInfo ▪ RestrictedIdentificationDomainParameterInfo ▪ signature of this data, including the corresponding DS certificate.	PACE+TA		
EF.ChipSecurity	▪ PACEInfo ▪ ChipAuthenticationInfo ▪ ChipAuthenticationDomainParameterInfo ▪ ChipAuthenticationPublicKeyInfo ▪ PrivilegedTerminalInfo ▪ TerminalAuthenticationInfo ▪ CardInfoLocator ▪ RestrictedIdentificationInfo ▪ RestrictedIdentificationDomainParameterInfo	PACE+TA2 kao IS ili AT sa pravom „Privileged Terminal“		
EF.MRZ	MRZ lozinka			Za PACE
EF.CAN	CAN lozinka			Za PACE
EF.PIN_EID	eID PIN		PACE sa eID PIN; AT + PIN upravljanje	Za PACE
EF.PUK	PUK			Za PACE
EF.CVCA_LINK	Link certifikat za TA	Tokom PACE	Pri importu	
EF.PrKCA1	Privatni ključ za CA čiji je javni ključ upisan u EF.CardSecurity			Za CA nakon PACE + TA2
EF.PrKCA2	Privatni ključ za CA čiji je javni ključ upisan u EF.ChipSecurity			Za CA nakon PACE + TA2 kao IS ili AT sa pravom „Privileged Terminal“
AT: „Authenticated Authentication Terminal“ (PACE sa eID-PIN ili CAN (sa CAN datim pravima), TA2, CA2);				

Da bi se spriječilo prepoznavanje kartice korištenjem javnog ključa za CA zapisanog u EF.CardSecurity, ovaj ključ nije zavisan od čipa. Svi čipovi iste generacije sadrže isti ključ tako da je na osnovu javnog

ključa moguće prepoznati samo generaciju kartica a nikako konkretnu karticu. Isto tako i potpis za EF.CardSecurity je nepromjenjiv za jednu generaciju čipova.

3.1.4. Lozinke

Za potrebe BAC/PACE protokola koristi se različite lozinke zavisno od vrste aplikacije:

- 6 znakova iz prvog reda mašinski čitljive zone,
- Hash vrijednost serijskog broja dokumenta, datuma rođenja i datuma isteka iz mašinski čitljive zone,
- eID PIN je dostavljen vlasniku u momentu podnošenja zahtjeva koji ujedno predstavlja i transportni ključ
- 8-o cifreni PUK dostavljen vlasniku u momentu podnošenja zahtjeva i predstavlja i aktivacijski broj

3.1.5. Pristupni broj kartice („CAN“ – Card Access Number)

CAN je šestocifreni broj upisan u prvi red mašinski čitljive zone na pozicijama nakon serijskog broja dokumenta. Ovo je prostor u MRZ namjenjen upisu proizvoljnh podataka. Lozinka se koristi za BAC/PACE. Ovu lozinku nije moguće izračunati na osnovu vidljivih podataka sa lične karte. Upotrebljava se za uspostavljanje sigurnog kanala između kartice i terminala u slučajevima kada se ne zahtjeva bilo kakav unos od vlasnika kartice. Ova lozinka nema brojač neuspjelih pokušaja.

3.1.6. Lozinka iz mašinski čitljive zone (MRZ)

Inspekcijski sistemi mogu koristiti lozinku iz MRZ-a umjesto CAN lozinke za potrebe BAC/PACE protokola. MRZ lozinka je u stvari SHA-1 hash vrijednost broja dokumenta, datuma rođenja i datuma isteka dokumenta. Na ovaj način postojeći inspekcijski sistemi mogu koristiti elektronsku ličnu kartu umjesto pasoša za kontrolu prelaska državne granice.

3.1.7. Pin (Personal Identification Number) broj

eID PIN je alfanumerički niz minimalne dužine šest znakova poznat samo vlasniku kartice. Koristi se za otključavanje kartice odnosno dozvolu pristupa. Poznavanje ovog broja povezuje vlasnika kartice sa karticom. U terminologiji dvofazne autentikacije lična karta (kartica) je nešto „što građanin ima“ a eID PIN broj nešto „što građanin zna“.

Koristi se načešće prilikom digitalnog potpisivanja i digitalnog predstavljanja. U eID BIH koristimo isti PIN broj za autentifikaciju prilikom digitalnog predstavljanja i digitalnog potpisivanja.
U toku predaje zahtjeva za izdavanje eID generiše se transportni ključ ili jednostavnije rečeno početni identifikacioni broj koji se treba promijeniti. Transportni ključ služi za promjenu i generisanje novog trajnog i samo vlasniku kartice poznatog eID PIN broja.

Čip sadrži brojač pokušaja koji se uvećava nakon svakog neuspjelog unosa eID PIN-a. eID PIN se može promijeniti samo na način da građanin korištenjem odgovarajućeg softvera Agencije unese prvo postojeći PIN a zatim novi PIN.

3.1.8. PUK (Pin Unblocking Key) – ključ za deblokiranje kartice

Nakon što se kartica blokira, deblokiranje je moguće korištenjem 8-cifrenog PUK broja. Čip vodi računa o broju deblokiranja kartice. PUK je slučajno generisan broj koji se dostavlja građaninu u momentu podnošenja zahtjeva za izdavanje lične karte.

3.2. Pravila pristupa podacima na čipu

3.2.1. Standardna/Napredna inspekcijska procedura za ICAO aplikaciju

Pristup biometrijskoj aplikaciji odnosno podacima zapisanim u njoj dodatno je moguć korištenjem standardne inspekcijske procedure i napredne inspekcijske procedure u skladu sa dokumentom TR-01110.

U sljedećoj tabeli su dati tipovi terminala sa vrstom BAC/PACE lozinke i mogućim pravima.

Tip terminala	BAC/PACE lozinka	Moguda prava
Inspekcijski terminali	MRZ lozinka	Pravo čitanja na DG1 i DG2 biometrijske aplikacije i data grupa eID aplikacije. Pravo čitanja DG3 biometrijske aplikacije nakon uspješne TA i postojanja prava u CV certifikatu.
Čitač/terminal koji se predstavlja kartici	EID lozinka	Pravo čitanja/pisanja data grupa aplikacije za digitalno potpisivanje/ predstavljanje Posebna prava: • Import certifikata za digitalno potpisivanje • Promjena eID pina • Deblokiranje eID pina

3.3. Inspekcijski sistem

Inspekcijski sistem jeste čitač/terminal agencije za sprovođenje zakona (policija, granična policija). Ovakav sistem ima pravo pristupa DG1 (mašinski čitljiva zona) i DG2 (fotografija lica) grupi sa podacima. Ako u toku terminal autentikacije dokaže da ima pravo čitanja onda može pristupiti i DG3 (otisci prstiju) grupi sa podacima.

Inspekcijski sistem nikada nema pravo pisanja po čipu niti pravo pristupa aplikaciji za digitalno potpisivanje.

3.4. Čitač/terminal koji se predstavlja kartici

Terminal koji izvrši autentikaciju (predstavljanje) ima pravo pristupa eID čipu. Prava dodijeljena tokom autentikacije određuje koji podaci se mogu čitati odnosno koje funkcije se mogu prozivati. Autentikacijski terminal može promijeniti neke podatke na čipu uz dobijanje odgovarajućih prava.

Razlikujemo dvije vrste ovakvih terminala: službeni terminal nadležnog organa i terminal korisnika, odnosno vlasnika eID. Terminal korisnika mora koristiti eID pin kako bi obezbjedio pristup podacima u čipu. Primjer ovakvog terminala je komunikacije preko mreže gdje identitet lica koje koristi uslugu se određuje preko digitalnog predstavljanja. Zato se od lica traži da unese eID PIN kako bi dokazao svoj identitet.

3.5. Resetovanje brojača pokušaja unosa eID PIN-a korištenjem PUK broja

Ako je kartica blokirana ili je korisnik tri puta promašio eID PIN broj, korištenjem PUK broja može vratiti brojač pokušaja na nulu. Za ovu operaciju takođe nije potrebna TA ili CA, već je dovoljno da se korisnik predstavi korištenjem PUK broja.

4. Sistemi koji pružaju podršku

U okviru ovog poglavlja opisani su pozadinski sistemi, odnosno sistemi koji pružaju podršku.

4.1. PKI za dokumente

Dio podataka zapisanih na čipu su potpisani tokom personalizacije od strane IDDEEA-e. Autentičnost potpisa se provjerava kroz PKI za dokumente.

PKI za dokumente se sastoji od:

- središnjeg CA (root CA, CSCA – Country Signing Certificate Authority)
- potpisnika ili DS-a (DS - Document Signer)

Potvrda sa javnim ključem potpisnika je smještena u datoteci EF.CardSecurity na čipu. Javni dio – odnosno certifikat središnjeg CA, te odgovarajući link certifikat je javno dostupan preko sajta Agencije, na sljedećem url adresama
https://www.iddeea.gov.ba/csca/
https://www.iddeea.gov.ba/egradjanin/r/eid/a101/csca-certificates1

Potvrde PKI za dokumenta su tipa X.509. Profile potvrde je propisan Politikom potvrda a u skladu je sa ICAO 9303.

Javni ključ središnjeg CA kao i liste opozvanih potvrda su dostupne na web stranici IDDEEA na linku:
https://www.iddeea.gov.ba/csca/csca_crl

IDDEEA osigurava javnu dostupnost korisnicima usluga navedenim informacijama.

4.2. PKI terminala/čitača za predstavljanje

Tokom TA procedure lanac potvrda se šalje prema čipu. Ovaj lanac potvrda određuje tip terminala kao i efektivna prava. Lanac je generisan od strane PKI terminala/čitača za predstavljanje.

PKI terminala/čitača za predstavljanje se sastoji od tri sloja:

- središnjeg CA (root CA, CVCA – Country Verifying Certification Authority)

- više provjerilaca validnosti dokumenta (DVs – Document Verifiers)
- inspekcijskih sistema i terminala koji se predstavljaju kartici

Postoji više provjerilaca validnosti dokumenata (DVs) jer svaki od njih obavlja različitu ulogu:

- kontrola kvalitete tokom personalizacije kartice
- primjene kod nadležnih organa
- provjere primjene zakona – policija i granična policija

Potvrde koje izdaje PKI terminala/čitača za predstavljanje su tipa CVC (Card Verifiable Certificates) u skladu sa ISO 7816 dio 6 i TR-03110. Pošto čip nije u stanju provjeravati liste opozvanih certifikata, ovaj tip certifikata se izdaje na kratko vrijeme.

Pošto čip nema vlastito napajanje on u sebi ne sadrži sat. Kako bi imao podatak o datumu i na taj način mogao da provjeri važnost potvrda, čip vrši aproksimaciju stvarnog datuma kroz prepisivanje datuma izdavanja certifikata koje prima tokom TA. Kako su ovi certikati kratkog trajanja maksimalna greška jeste period trajanja tih certifkata. Osim TA potvrda koriste se i datumi izdavanja iz CVCA i DV certikata.

4.3. PKI za certifikate za digitalno potpisivanje i predstavljanje

IDDEEA je u septembru 2020. godine uspješno završila proces certifikacije po eIDAS direktivi EU, čime je ispunila jedan od glavnih uslova za upis u registar ovjeritalja u BiH pri Ministarstvu komunikacija i prometa BiH. Poslije provedenih dodatnih procedura IDDEEA je upisana u registar ovjeritelja u BiH 15.04.2022. godine. Registar je javno dostupan na sljedećoj url adresi:

http://www.mkt.gov.ba/data/Slike/Dokumenti/Registar_ovjeritelja_u_Bosni_i_Hercegovini_15.04.2022-potpisano.pdf

Ovim su se stekli svi zakonski preduslovi da IDDEEA započne sa upisom certifikata za digitalno predstavljanje i digitalno potpisivanje u odgovarajuće aplikacije na eID. (Uz napomenu da u vrijeme pisanja ovog dokumenta Vijeće Ministara nije donijelo odluku o cijeni koštanja certifikata za digitalno potpisivanje čime bi bio i praktično omogućen i započet upis certifkata za digitalno potpisivanje od strane IDDEEA-e u čip lične karte. Prijedlog IDDEEA-e je da certifikat za digitalno potpisivanje bude besplatan, odnosno bude uključen u postojeću cijenu LK)

PKI za certifikate za digitalno predstavljanje i potpisivanje se sastoji od:

- središnjeg root CA tijela i potpisujućeg CA tijela koje izdaje certifikate za podnosioce zahtjeva za eID. (**CN=IDDEEA-RootCA-2021**)

te dva potpisujuća CA tijela koje je potpisalo središnje root CA tijelo :

- Potpisujuće CA tijelo za certifikate za digitalno potpisivanje – koje certifikovano po eIDAS direktivi EU (**CN = IDDEEA-IssuingCA**)
- Potpisujuće CA tijelo za digitalno ptredstavljanje koje nije certifikovano po eIDAS direktivi EU (**CN= IDDEEA-IssuingAuthCA**)

Cerifikati za digitalno potpisavanje koje izdaje potpisujuće CA tijelo IDDEEA-e će važiti 5 godina, a proces zanavljanja certifikata dok traje važnost LK (obično 10 godina) će biti omogućen kroz softversko middleware rješenje IDDEEA-e, bez potrebe da korisnik ide na lokaciju nadležnog organa.
Zanavljanje certifikata korisnika u slučaju isteka LK se obavlja kroz redovnu proceduru zamjene i izdavanja LK na lokaciji nadležnog organa.
Certifikati za digitalno predstavljanje koje izdaje odgovarajuće potpisujuće CA tijelo će važiti 10 godina i biće upisani u svaku eID karticu, odnosno LK.

4.3.1. Lista opozvanih LK

Lista opozvanih kartica LK se objavljuje na web sajtu Agencije www.iddeea.gov.ba, što je u suštini spisak izgubljenih i ukradenih LK.
Opozivom kartice, odnosno proglašenjem iste ukradenom ili izgubljenom u evidenciji LK koju vodi i održava IDDEEA automatski se opozivaju i svi certifikati koji su upisani u tu karticu od strane IDDEEA-e. Prilikom opozivanja, a u skladu rada IDDDEEA-inog CA tijela opozovani certifikati se upisuju na CRL listu agencije, koja je javno objavljena i dostupna na web sajtu agencije:

- CRL lista za potpisujuće CA tijelo za certifikate za digitalno potpisivanje

https://www.iddeea.gov.ba/PKI/CRL/certdist?cmd=crl&issuer=CN=IDDEEA-IssuingCA

- CRL lista za potpisujeće CA tijelo za certifikate za digitalno predstavljanje

https://www.iddeea.gov.ba/PKI/CRL/certdist?cmd=crl&issuer=CN=DIDDEEA-IssuingAuthCA

URL adresa OCSP (Online Certificate Status Protocol) respondera za PKI za certificate je:

https://www.iddeea.gov.ba/PKI/OCSP/status/ocsp

Politika certifikacije je javno objavljena na web sajtu Agencije na url adresi

https://www.iddeea.gov.ba/PKI/CPS

5. Osnovne funkcionisanja eID Sign i MW

U ovom poglavlju ćemo detaljnije opisati način funkcionisanja aplikacije za digitalno potpisivanje i odgovarajućeg middleware softvera.
Certifikati za digitalno predstavljanje će se upisivati u eID svim građanima, dok će se certifikati za digitalno potpisivanje upisivati samo onim građanima koji to žele i koji se izjasne u toku procesu podnošenja zahtjeva za eID.

5.1. Korištenje aplikacije za digitalno potpisivanje

Aplikacija za digitalno potpisivanje ima funkcionalnost i digitalnog predstavljanja. Koja operacija će se vršiti zavisti od odabranog certifikata.
Zasnovana je na GIDS specifikaciji aplikacija i za korištenje na MS Windows operativnim sistemima ne zahtjeva nikakvu instalaciju midlever softvera.
Pod korištenjem u ovom smislu podrazumjevamo redovan rad kao što je digitalno potpisivanje dokumenta ili digitalno predstavljanje korištenjem npr. MS Edge preglednika ili Google Chrome preglednika na aplikacije, sisteme ili web prezentacije javnih ili privatnih organizacija koje omoguće proces digitalnog predstavljanja (odnosno autentifikacije) sa eID certifikatima za digitalno predstavljanje.
Za korištenje na ostalim operativniim sistemima (Linux, macOS) potrebo je instalirati odgovarajući midlver koji je javno dostupan OpenSC, a uputstva su na sljedećoj url adresi:
https://github.com/OpenSC/OpenSC/wiki

Napominjemo da je za korištenje eID u Firefox web pregledniku neophodna instalacija gore navedenog midlever softvera nezavisno na kojem operativnom sistemu se isti pokreće. Tehnička uputstva vezano za korištenje i druge funkionalnosti eID će biti dostupna na web stranici Agencije.

Tehnički preduslovi za korištenje eID za funkcije digitalnog predstavljanja i potpisivanja su:

- Posjedovanje računara (Desktop ili LapTop) sa modernim operativnim sistemom.
    - MS Windows 10 ili noviji
    - Linux (npr Ubuntu 20.04 ili noviji kao i ekvivalntne druge novije distribucije, a zavisno od OpenSC midlvera)
    - MACOS zavisno od OpenSC midlevera
- Posjedovanje beskontaktnog čitača/pisača za pametne kartice (npr: Omnikey 5x21 CL ili ekvivalentni)
- Instalacija eID MW softvera za ostale funkcionalnosti (promjena PIN koda, otključavanje PIN koda pomoću PUK koda, zanavljanje certifikata za digitalno potpisivanje dok važi LK)

5.2. Korištenje eID MW softvera

Osnovne funkcionalnosti eID MW softvera su sljedeće:

1. Izbor čitača pametnih kartica
2. Prepoznavanje eID BiH kao odgovarjuće pametne kartice spojene na čitač, čime se omogućavaju ostale funkcionalnosti
3. Promjena PIN koda za eID karticu
4. Deblokiranje PIN koda za eID karticu
5. Upis certifikata u eID

5.3. Izbor čitača pametnih kartica i prepoznavanje kartice

Podržani čitači pametnih kartica trebaju imati odgovarajuće karakteristike. Moraju biti bezkontakni pošto je i eID beskontakna pametna kartica. Takođe , čitači pametnih kartica moraju ispunjavati odgovarajuće kriterijume za rad sa eID pametnim karticama. Testirana i podržana je opcija korištenja Omnikey 5x21 beskonaktnog pisača/čitača.
Kako Agencija bude testirala druge modele čitača pametnih kartica ažuriraće listu podržanog hardvera na svojoj web stranici.
eID MW softver prikazuje sve čitače pametnih kartica spojenihna računar. Korisnik treba odbrati onaj čitač na koji je prislonio eID karticu.
Ukoliko je odabrana pametna kartica eID BiH sa verzijom aplikacija i operativnog sistema opisanog ovim dokumentom, omogućuje se druge funkcionalnosti eID MW softvera.

5.4. Promjena PIN koda eID kartice

Promjena PIN koda na eID MW softveru je moguća samo ako se unese postojeći PIN kod.
Ukoliko se radi o prvoj izmjeni PIN koda nakon uručenja eID potrebno je unijeti incijalni PIN kod, odnosno transportni ključ, kako bi se omogućila promjena PIN koda na kartici. eID MW softver vraća poruku o uspješnosti ove operacije.

5.5. Deblokiranje eID kartice

Deblokiranje eID kartice je u stvari proces resetovanja PIN koda kad se on zaključa ili zaboravi. Za proces deblokiranja koristi se PUK kod koji korisnik dobija u procesu podnošenja zahtjeva ze eID.
Korisnik unosi navedeni PUK kod , a eID MW softver računa administratorski ključ (admin key) na osnovu unesenog PUK koda i kriptografskih operacija poznatih Agenciji.
Dužina admin key-a za eID je 48 hex znakova. Dobijeni admin ključ se koristi za postavljanje novog PIN koda.
eID MW prikazuje rezultat ove operacije korisniku.

5.6. Import certifikata

Korištenjem eID MW softvera je moguće zanoviti certifikat za digitalno potpisivanje , korištenjem funkcionalnosti importa certifikata. Zavisno od načina implementacije, zanavljanja i dobijanja certifikata proces se sastoji od unosa PIN koda eID, te odgovarajuće lozinke kojom se otključava dobijeni certifikat.

Proces zanavljanja certifikata za digitalno potpisivanje se realizuje na siguran način, korištenjem kriptografskih operacija zasnovanih na infrastrukturi javnog ključa i certifikatu za digitalno predstavljanje koji je važeći dok važi eID kartica.

Kako je certifikat za digitalno predstavljanje upisan eID neophodna je dodatna autentifikacija unosom PIN koda korisnika eID, da bi se ostavrila sigurna komunikacija između eID MW i resursa Agencije kao preduslov za početak procesa zanavaljanja certifikata za digitlalno potpisivanje.

Detaljne tehničke informacije o eID MW softveru će biti dostupne kroz tehnička uputstava za korištenje softvera i javno dostupna na www.iddeea.gov.ba