UDC: 57.087:004.8.056 Info M str. 11-16

POBOLJŠANJE FUNKCIONALNOSTI BIOMETRIJSKIH SISTEMA PRIMENOM MEĐUNARODNIH STANDARDA: PREGLED KLJUČNIH ISO STANDARDA
IMPROVING THE FUNCTIONALITY OF BIOMETRIC SYSTEMS BY APPLICATION OF INTERNATIONAL STANDARDS: A REVIEW OF KEY ISO STANDARDS

Milorad Milinković, Univerzitet u Beogradu, Fakultet organizacionih nauka, milorad.milinkovic@mmklab.org

REZIME: U ovom radu prikazani su značaj i povezanost koncepata nekoliko ključnih međunarodnih ISO standarda kao rešenja problema u funkcionisanju biometrijskih sistema. Među suštinski najbitnijim problemima su problem interoperabilnosti u biometrijskim sistemima (BioAPI specifikacija), formatiranje biometrijskih podataka za bezbednu razmenu i skladištenje istih (CBEFF frejmvork), bezbednost transakcija u okviru i između biometrijskih sistema (ACBio formatiranje) i zaštita biometrijskih informacija i privatnosti u biometrijskim sistemima (ISO 24745).

KLJUČNE REČI: Biometrija, Standardi, BioAPI, CBEFF, ACBio, ISO 24745

ABSTRACT: This paper presents the importance and connection of the concepts of several key international ISO standards as the solutions to the problems in the functioning of biometric systems. Among the most crucial problems are the problem of interoperability in biometric systems (BioAPI specification), formatting of biometric data for safe exchange and storage (CBEFF framework), security of transactions within and between biometric systems (ACBio formatting) and protection of biometric information and privacy in biometric systems (ISO 24745).

KEY WORDS: Biometrics, Standards, BioAPI, CBEFF, ISO 24745

1. UVOD

Savremeno poslovanje je danas gotovo nemoguće zamisliti bez pružanja usluga na daljinu putem Interneta (e-bankarstvo, e-obrazovanje, e-zdravstvo, e-prodaja, e-javna uprava itd.). S druge strane razvoj i primena biometrijskih tehnologija i uređaja kao i softverskih aplikacija su poprilično uzeli maha u svakodnevici. To je prema [1] dovelo do problema velikog broja proizvođača hardvera i softvera, odnosno do problema u komunikaciji između softvera i uređaja različitih proizvođača (tzv. „vendor lock-in“). Kako biometrija koristi fizičke i ponašajne karakteristike pojedinaca za jedinstveno identifikovanje korisnika prilikom autentikacije, tokom realizacije gore pomenutih usluga, između subjekata (korisnika usluga i pružaoca usluga), mehanizmi autentikacije postaju sve kritičniji u pogledu bezbednosti i zaštite privatnosti [2].

Tako je prema [2] 1998. godine najpre oformljen BioAPI konzorcijum sa ciljem da razvije Aplikativni Programski Interfejs (API) koji definiše opšti način povezivanja sa različitim biometrijskim tehnologijama koji će biti široko primenjivan i tako obezbediti komunikaciju između aplikacija i biometrijskih tehnologija nezavisno od proizvođača. Nastaje BioAPI specifikacija koja definiše jedinstvenu platformu za komunikaciju između aplikacija i biometrijskih tehnologija različitih proizvođača i ubrzo biva prihvaćena i objavljena kao međunarodni ISO standard (grupa standarda ISO 19784).

S druge strane, bezbednost biometrijskih podataka koji se obrađuju i skladište u biometrijskim sistemima i razmenjuju između istih je suštinski bitna, jer gubitak ili otkrivanje ovih podataka potencijalno vode do mogućih zloupotreba podataka koji predstavljaju deo identiteta pojedinca kao što su krađa identiteta ili bilo koji drugi način ugrožavanja privatnosti. Intenzivan razvoj biometrijskih tehnologija za autentikaciju u aplikacijama u javnom sektoru (pasoši, vize, granična kontrola, lične karte itd.) podstakao je program rada na razvoju međunarodnih standarda čija je uloga bezbednost biometrijskih podataka [3]. Tako je prema [3] nastao ključni standard za skladištenje i razmenu biometrijskih podataka ISO 19785, odnosno CBEFF frejmvork (Common Biometric Exchange Format Framework).

Suština tehničkih standarda je akcenat kako na zaštiti uskladištenih biometrijskih podataka tako i na obezbeđivanju transakcija biometrijskih podataka „s kraja na kraj“ (end-to-end) putem mreže, za šta je potrebna bezbednosna informacija koja je kreirana i procesirana biometrijskim hardverom i softverom na svakom kraju transakcije, uključujući i bezbednost čitave transakcije koja se obavlja putem mreže. Najčešće primenjivan, međunarodno priznat i objavljen standard za transakciju biometrijskih podataka je ACBio, odnosno Autentikacijski kontekst za biometriju sa oznakom ISO 24761 [3].

Kako biometrijski sistemi obično povezuju biometrijske reference (otisak prsta, lice, glas, ili neki drugi biometrijski modalitet) sa identifikacionim referencama (ime, prezime, JMBG, broj ličnog dokumenta itd.) razmena ovih informacija u zakonskim okvirima predstavlja problem organizacijama koje ih koriste, jer moraju da zaštite biometrijske informacije i usaglase se za različitim zakonskim regulativama koje se odnose na privatnost. U daljem tekstu biće ukratko predstavljen i međunarodni standard sa oznakom ISO 24745, koje se prema [3] odnosi na tehnike zaštite biometrijskih informacija i predstavlja jedno o mogućih rešenja problema zaštite privatnosti i biometrijskih informacija u okviru biometrijskog sistema.

Uloga, značaj i povezanost ovih standarda opisani su u tekstu koji sledi.

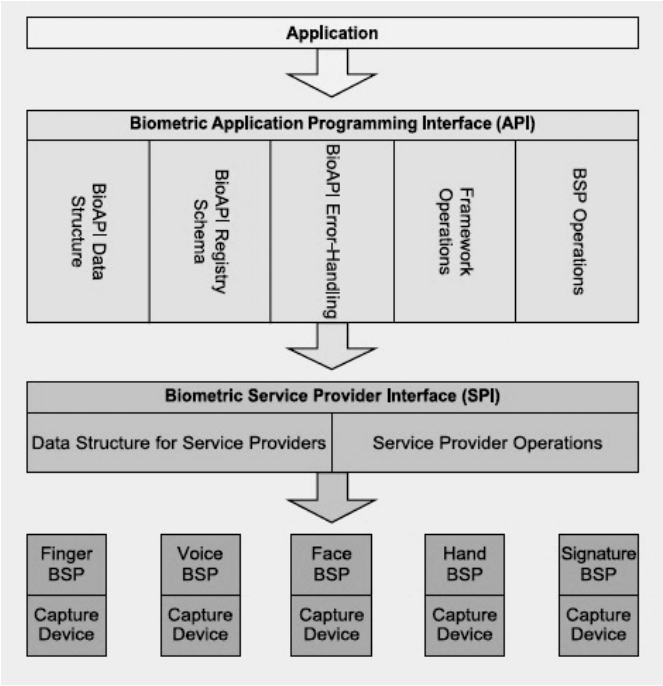
2. ULOGA I ZNAČAJ BIOAPI SPECIFIKACIJE

BioAPI specifikacija je prema [4] standard koji definiše jednostavne interfejse biometrijskih aplikacija, standardni modularni pristup biometrijskim funkcijama, algoritmima i

uređajima, standardne metode za razlikovanje biometrijskih podataka i vrste uređaja, i podršku za biometrijsku identifikaciju u distribuiranim računarskim okruženjima. BioAPI prema [4] obezbeđuje osnovne funkcije biometrijskih sistema kao što su Upisivanje, Verifikacija i Identifikacija i obuhvata interfejs baze podataka koji omogućava BSP-u, softveru koji komunicira sa uređajem za upis i verifikaciju, da upravlja Identifikacijom populacije s ciljem optimalnih performansi.

2.1 *Strukturas BIOAPI platforme*

Osnovna verzija 1.1 koja je po formulisanju uzela maha najpre na Američkom kontinentu sastoji se iz dva suštinska dela (Slika 1): *API*, Aplikativni programski interfejs ili nivo aplikacija, i *SPI* ili nivo definisan kao Interfejs za obezbeđivanje biometrijskih usluga. API je najviši nivo na kome su implementirane osnovne biometrijske funkcije koje svaka softverska aplikacija mora da sadrži kako bi komunicirala sa BioAPI plaformom.



Slika 1. – *Stuktura BioAPI platforme [4]*

Prema [4] API nivo je organizovan u pet kategorija u BioAPI specifikaciji v1.1 koja je osnova daljeg razvoja platforme (Slika 1). Prva kategorija je *Biometric Data Structure* (Struktura biometrijskih podataka) i definiše sve standardne strukture podataka koje se koriste u aplikaciji. BioAPI *Registy Schema* (Registar šema) se koristi za čuvanje informacija za svaku komponentu u BioAPI. BioAPI *Error Handling* (Upravljanje greškama) određuje operacije za upravljanje greškama u BioAPI. *Framework operation*s (Operacije frejmvorka) definiše opšte operacije za pokretanje i deaktiviranje aplikacija. *BSP operations* (BSP operacije) obezbeđuje operacije za razmenu podataka i komunikaciju između aplikacija i BSP-a. Sve biometrijske operacije *Capture* (Slikaj), *Process* (Procesuiraj), *Enroll* (Upiši), *Verify* (Verifikuj), *Identify* (Identifikuj) itd. su definisane u *BSP operations*. Pored ostalog *BSP Operations* obezbeđuje operacije koje omogućavaju aplikacijama da pristupe i upravljaju biometrijskim bazama podataka.

Prema [4] SPI čine dve kategorije: *Struktura podataka za provajdere usluga* i *Operacije uslužnog provajdera (BSP)*. SPI komunicira jedan na jedan sa BSP-om. API pozivi se usmeravaju na SPI preko koga je odgovarajući BSP priključen na BioAPI. BSP (Biometric Service Provider) bez obzira kog je proizvođača je softver koji komunicira sa biometrijskim uređajem i mora biti kompatibilan sa specifikacijom SPI interfejsa, jer je to jedini način da se uključi u BioAPI radno okruženje i kako bi ga na taj način koristile prehodno navedene aplikacije. BSP prema [4] sadrži jedinstvene aspekte pojedinih biometrijskih tehnologija, tačnije proizvoda i uređaja određenih proizvođača (primera radi postoje BSP lica, šake, zenice oka itd.) Prema [4] BSP može biti *Lokalni* i *Distribuirani*. Lokalni BSP kompletno funkcioniše u okviru pojedinačne platforme, dok distribuirani može biti instanciran i učitan kao odvojene *klijent-server* komponente sa *klijent-server* komunikacijom. Za biometrijske aplikacije klijent-server arhitektura se najčešće primenjuje, jer je sigurnije okruženje za izvršne biometrijske algoritme i kada je u pitanju identifikacija velike populacije ima dovoljno snage za pokretanje biometrijskog algoritma za razliku od lokalnog BSP-a. Pored toga baza podataka može biti na serveru što olakšava rad klijentu.

2.2 *BIOAPI kao međunarodni standard (verzija 2.0)*

Proširivanje osnovne arhitekture BioAPI (v1.1) usledilo je nakon uočavanje mogućnosti primene BioAPI specifikacije kao međunarodnog standarda u oblasti biometrije. Prema [5] nova verzija je pojednostavljena i proširena i u saradnji sa ISO međunarodnom organizacijom za standarde definisana kao multi-standard ISO 19784. Suštinska razlika između stare i nove verzije je prema [5] dodatni sloj ispod BSP-a koga čine *Biometrijski provajderi funkcija (Biometric Function Providers - BFP's)* koji preuzima deo funkcija BSP-a omogućavajući podelu rada između dve komponente. Postoje četiri kategorije BFP-a prema [5]:

- *Sensor BFP* – upravalja senzorima, tj. ulaznim uređajima,
- *Archive BFP* – upravlja pristupom u baze podataka,
- *Processing-algorithm BFP* – procesuira biometrijske uzorke podataka,
- *Matching-algorithm BFP* – upoređuje biometrijski uzorak podatka sa templatom (šablonom) i daje rezultat.

Sve ovo smanjuje potrebu za velikim brojem softvera pojedinačnog proizvođača koji bi inače samo dodatno komplikovali funcionisanje arhitekture i usmeravanje rada proizvođača na stvaranje *BSP-a* i njegovog interfejsa prema BioAPI. Stoga v2.0 pored obavezna dva API interfejsa prema [5] poseduje i *FPI (Function Provider Interface)* interfejs sa funkcijama analognim funkcijama i postojanju svake kategorije BFP-a. U v2.0 koncept *„uređaj (device)"* zamenjen je

konceptom *„jedinica (unit)"* i postoje četiri kategorije jedinica (*sensor, archive, processing-argorithm i matching-algorithm* jedinice) čije su funkcije analogne prethodno navedenim funkcijama BFP provajdera. Stoga kada govorimo o distribuciji biometrijskih sistema i telebiometriji BioAPI postavlja temelje. Takođe ne čudi zašto je BioAPI arhitektura osnova svih međunarodnih standarda u oblasti biometrije koje propisuje ISO organizacija.

3. ULOGA I STRUKTURA CBEFF STANDARDA

CBEFF je višestruki međunarodni standard čiji se Deo 4., pod nazivom *„Specifikacija formata bezbednosnog bloka",* odnosi na zaštitu integriteta i čuvanje poverljivih biometrijskih podataka [6]. CBEFF standard definiše osnovnu strukturu biometrijskog podatka koji se skladišti i razmenjuje u biometrijskom sistemu, odnosno između dva ili više biometrijskih sistema putem mreže, pod nazivom BIR (Biometric Information Record, odnosno *biometrijski informacioni zapis,* u daljem tekstu BIR).

BIR je prema [6] skup informacija o biometrijskom podatku (određenom biometrijskom modalitetu određene osobe), struktuiran i podeljen u tri odeljka (bloka): *Standard Block Header (SBH)*, *Biometric Data Block (BDB)* koji sadrži same biometrijske podatke (koji mogu biti šifrovani) i *Security Block (SB)*.

Zaglavlje SBH bloka, odnosno SBH se sastoji od osnovnih polja koja mogu biti zahtevana ili opciona i nose određeni skup podataka neophodan za skladištenje kao i za razmenu biometrijskih podataka u okviru ili između biometrijskih sistema (Tabela 1). Takođe, informacije koje nosi uključuju indikatore bezbednosnih mehanizama koji su korišćeni za zaštitu biometrijskih podataka [6].

Naziv podatka	Zahtevano polje (Z) ili Opciono polje (O)	Opis
SBH bezbednosne opcije	Z	Definiše bezbednost podatka.
Opcije integriteta	Z	Ovo polje definiše koji atribut interiteta ide uz podatak: Potpis ili MAC.
Verzija CBEFF zaglavlja	O	-
Verzija patron zaglavlja	O	Patron format specifikacija ili verzija standarda.
Biometrijski tip	O	Otisak prsta, glas itd.
Biometrijski podtip	O	Dodatno specificiran u okviru tipa.
Biometrijski tip podatka	O	Nivo procesiranja podatka (sirov, poluprocesiran, procesiran).
Biometrijska svrha	O	Svrha korišćenja podatka (upis, verifikacija).
Kvalitet biometrijskog podatka	O	Nivo kvalitet biometrijskog podatka.
Datum kreiranja podatka	O	Datum i vreme kreiranja biometrijskog podatka.
Period validnosti	O	Trajanje "od-do".
Kreator	O	Tekstualni identifikator vlasnika aplikacije.
Indeks	O	Jedinstveni identifikator podatka u okviru zapisa koji koristi aplikacija.
Podzaglavlje/broj osnovnih struktura	O	Broj CBEFF struktura u nivou ispod zaglavlja CBEFF proširene strukture.
Vlanik BDB formata	Z	ID grupe ili proizvođača koji je definisao BDB.
Tip BDB formata	Z	Defiše vlasnik formata.
Identifikator proizvoda (PID)	O	Registrovani identifikator entiteta koji je kreirao biometrijski podataka.
Identifikator patron formata	O	Registrovani identifikator patron formata.
Sekcija biometrijskih podataka	**Z**	**Definiše vlasnik formata. Može biti kodiran.**
Potpis	**Z**	**Digitalni Potpis**

Tabela 1. *Polja standardnog zaglavlja biometrijskih podataka SBH [6]*

BDB odeljak sadrži biometrijske podatke određenog modaliteta (iris, lice itd.) koji se skladište, odnosno razmenjuju [6].

SB bezbednosni blok prema [6] sadrži relevantne bezbednosne informacije, kao što su kriptografske sume (cryptographic checksums), digitalne potvrde (digital certificates) i specifikacije algoritama za enkripciju podataka, koje su korišćene kao garancija integriteta i poverljivosti podataka. Specifikacije u okviru CBEFF bezbednosnog bloka SB prema [7] obuhvataju bezbednosne zahteve koje propagira ACBio (Authentication Context for Biometrics) standard čiji je zadatak da obezbedi sigurnost „end to end" biometrijskih transakcija. U suštini, SB blok sadrži skup ACBio instanci koje sadrže podatke za validaciju integriteta "end-to-end" biometrijske transakcije o kojima će kasnije biti reči.

4. ULOGA I ZNAČAJ ACBIO STANDARDA

ACBio je međunarodni standard objavljen od strane ISO organizacije kao kontekst autentikacije za biometriju pod oznakom ISO 24761. ACBio modelira biometrijsku transakciju kao skup procesa izvršenih od strane Biometrijske Procesorske Jedinice (Biometric Process Unit) ili kraće BPU (npr. senzor, „smart" kartice, uređaj za poređenje, softver koji radi na personalnom računaru itd.) [7]. BPU postavlja relevantne bezbednosne podatke u blok pod nazivom ACBio instanca [7].

BPU prema [7] generiše i prenosi ACBio instance zajedno sa povezanim biometrijskim podacima koji su predmet bilo kog transakcionog procesa podataka. Tehnike bezbednosti koje se koriste u okviru ovog standarda prema [7] mogu da pruže zaštitu od supstitucije ''lažnim'' komponentama biometrijskog sistema i napada reprodukovanim podacima, ali i da uklone opšte pretnje integritetu transakcionih podataka.

4.1 *Struktura acbio standarda*

ACBio je sastavljen iz tri osnovna bloka informacija [8]:

- *BPU blok informacija* sadrži statičke informacije o BPU, određene unapred i nezavisne od izvršenja u realnom vremenu: njegova funkcija, nivo bezbednosti i/ili otpornost na kvar, kvalitet implementiranih funkcija itd.
- *Verifikatorski kontrolni blok* je namenjen za informaciju koja treba da ukaže na to da li je ACBio instanca generisana na zahtev verifikatora ili ne.
- *Biometrijski procesni blok* je namenjen za informacije koje se odnose na izvršenje podprocesa BPU u realnom vremenu. Sadrži informacije o ulaznim i izlaznim podacima procesiranim u BPU. Ako BPU primi podatak od druge BPU ili pošalje podatak drugoj BPU, onda je taj podatak obavezan element u ovom bloku.

4.2 *Uloga standarda u bezbednosti biometrijskih podataka*

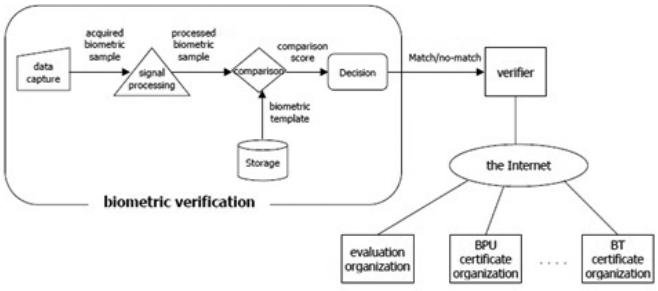
ACBio je dizajniran sa akcentom na problemu privatnosti. Definisan je tako da verifikator (biometrijska aplikacija za donošenje odluke o uspešnosti verifikacije) može da proveri validnost biometrijskog procesa verifikacije bez korišćenja privatnih podataka poput biometrijskog uzorka i biometrijskog šablona koji se prenose u okviru ACBio instance [7].

Ovaj standard ne definiše protokole interne komunikacije između BPU jedinica, korisnika i verifikatora [8]. Neophodno je istaći da je suštinski element ACBio standarda ACBio instanca koja prema [8] obuhvata informacije za potvrdu validnosti tokom procesa verifikacije primenom sledećih principa:

- ACBio instancu je kreirao BPU po nalogu verifikatora,
- ACBio instance koje se odnose na određeni proces biometrijske verifikacije su korektno međusobno povezane,
- ACBio instanca zadržava svoj integritet,
- Za svaki BPU, ACBio instanca je generisana i poslata verifikatoru da bi isti mogao da verifikuje validnost podprocesa izvršenih na BPU,
- ACBio zahteva da svaka BPU ima mogućnost da generiše digitalni potpis kojim verifikator može verifikovati integritet ACBio instance.

ACBio instance obezbeđuju integritet podataka korišćenjem bezbednosnih tehnika, kao što su digitalni potpisi i kriptografske kontrolne sume [8]. ACBio instanca može da sadrži i podatke za obezbeđivanje drugih aspekata transakcije, kao što su validacija biometrijskog hardvera i potvrda sposobnosti učinka biometrijskih procesa verifikacije. Integritet biometrijskog hardvera kao i performanse i bezbednost biometrijskih tehnologija prema [8] obezbeđeni su putem eksternih šema za evaluaciju, dok će rezultati biti ugrađeni u mašinski čitljivim formatima podataka koji mogu biti potvrđeni putem validacije biometrijskih procesa verifikacije prema potrebi.

Na kraju, verifikator prema [8] potvrđuje proces biometrijske verifikacije proverom informacija koje nosi ACBio instanca. Na slici 2. prikazana je relacija između verifikatora i sajtova relevantnih organizacija. Verifikacija se vrši putem Interneta.



Slika 2. *Proces verifikacije u ACBio [8]*

5. O STANDARDU ISO 24745

Ovaj međunarodni standard predstavlja skup zahteva i smernica koje treba primeniti radi bezbednog i sa zahtevima privatnosti usklađenog upravljanja i procesiranja biometrijskih informacija [9].

ISO 24745 prema [9] pored ostalog precizira sledeće:

- Bezbednosne zahteve za bezbedno povezivanje biometrijskih i identifikacionih referenci,
- Modele za primenu na biometrijske sisteme sa različitim scenarijima za skladištenje i poređenje biometrijskih referenci.

Ovaj standard ne obuhvata opšte probleme koji se odnose na fizičku bezbednost, bezbednost okoline i upravljanje ključevima za kriptografske tehnike.

5.1 *Bezbednosni zahtevi za zaštitu biometrijskih informacija u biometrijskim sistemima*

Prema standardu ISO 24745 tri osnovna bezbednosna zahteva (karakteristike) koje svaki biometrijski sistem mora da ispunjava (sadrži) su prema [10]:

1. **Poverljivost** je osobina biomerijskih sistema koja štiti informaciju od neovlašćenih pristupa ili otkrivanja. Biometrijska referenca (u daljem tekstu BR) uskladištena u bazi podataka tokom upisivanja se prenosi u podsistem za komparaciju tokom procesa verifikacije i identifikacije. Tokom ovih procesa, biometrijskoj referenci može da pristupi neovlašćeno lice i tako ugrozi identitet pojedinca. Identifikacione reference (u daljem tekstu IR) mogu biti otkrivene i time može biti ugrožena privatnost. Ove situacije se mogu izbeći preventivno primenom mehanizama kontrole pristupa i različitih formi tehnika za enkripciju.
2. **Integritet** je osobina koja se odnosi za očuvanje tačnosti i kompletnosti imovine. Integritet biometrijskih referenci je veoma bitna osobina za očuvanje bezbednosti kompletnog biometrijskog sistema. Integritet procesa autentikacije zavisi od integriteta biometrijske reference. Ako su biometrijska referenca ili njene određene osobine nepouzdane, biće i rezultat autentikacije. Nepouzdana biometrijska referenca ili uzorak nastaju:
   a. Ako je došlo do slučajnog zakazivanja softvera ili hardvera,
   b. Slučajnom ili namernom prepravkom (modifikacijom) pravih biometrijskih referenci od strane neovlašćenih entiteta (korisnik ili vlasnik sistema), bez intervencije spoljnog napadača,
   c. Modifikacija (zamena) biometrijske reference od strane spoljnog napadača.
   d. Preventivne i zaštitne mere obuhvataju mehanizme kontrole pristupa i kriptografske tehnike.
3. **Obnovljivost/Opozivost;** Mnogo je načina koji mogu ugroziti biometrijsku referencu, recimo napadač može doći u posed tokena sa istom, može koristiti lažne reference za pristup sistemu itd. Ako dođe do ugrožavanja reference, iste treba opozvati (revocation) da bi se izbegli mogući scenariji ugrožavanja sistema i privatnosti učesnika. Treba kreirati novu referencu i povezati je kao i opozvanu sa identifikacionim referencama. Kod određenog vremena validnosti reference (slično kao kod promene lozinke), ukoliko se referenca traži i nakon isteka validnosti, istu treba obnoviti, ili opozvati i zameniti.

5.2 *Obnovljive biometrijske reference kao mehanizam zaštite podataka*

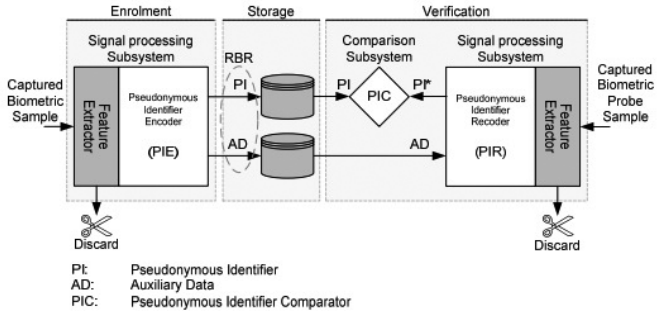
Obnovljivost biometrijskih referenci je mera zaštite protiv pretnji tokom skladištenja i prenosa. Da bi opoziv ili obnova

biometrijskih referenci bili izvodljivi, proces kreiranja istih treba da podržava proces diverzifikacije (razdvajanja) [9].

Diverzifikacija uključuje generisanje višestrukih, nezavisnih referenci proisteklih iz istih biometrijskih karakteristika koje se mogu primeniti za obnovu biometrijske reference ili za obezbeđivanje nezavisne reference koja se koristi u različitim aplikacijama [9].

Proces diverzifikacije treba da je nepovratan (neizmenjiv). Između transformisanih biometrijskih referenci ne treba da postoji jedinstvena veza. Obnovljive biometrijske reference (*renewable biometric references*, odnosno RBR u daljem tekstu) se prema [9] sastoje od dva elementa podataka: „Indentifikatori pod pseudonimom“ (*Pseudonymous identifiers*, odnosno PI u daljem tekstu), i Odgovarajući pomoćni podaci (*Auxiliary data*, odnosno u daljem tekstu AD). Oba elementa podataka su generisana tokom upisa i oba moraju biti uskladištena s obzirom na to da se obavezno koriste tokom verifikacije ili identifikacije.

Pregled arhitekture RBR prikazan je na slici 3. Strelica predstavlja tok informacije. Tokom upisa, faza izdvajanja karakteristika generiše podatke o biometrijskim karakteristikama biometrijskog uzorka koji se upisuje. Zatim, koder PI elemenata (PIE - *Pseudonymous identifier encoder*) generiše RBR koja sadrži PI i AD. Kada je RBR generisana, upisan uzorak i ekstrahovane karakteristike mogu se bezbedno ukloniti. RBR je uskladištena na odgovarajućem medijumu (primera radi smart kartica, elektronska baza podataka). PI i AD mogu biti logički ili fizički odvojeni. Tokom verifikacije, faza ekstrakcije karakteristika obrađuje probni biometrijski uzorak (uzorak koji se ispituje). Zatim, PI snimač (PIR - *pseudonymous identifier recoder*) konstruiše PI* zasnovan na obezbeđenim AD elementima i izdvojenim karakteristikama. Nakon toga, podsistem za upoređivanje upoređuje PI nastao nakon upisa sa PI*, i dobijeni rezultat šalje podsistemu za odlučivanje koji donosi odluku.



Slika 3: *Arhitektura za kreiranje RBR [10]*

5.3 *Primena modela biometrijskih sistema i njihova bezbednost*

U okviru ovog standarda prema [10] predlaže se 8 modela biometrijskih sistema koji su klasifikovani prema lokaciji za skladištenje i upoređivanje biometrijskih informacija (Tabela 2) imajući u vidu bezbednosni aspekt. Svaki model ima svoje prednosti i mane kada je u pitanju upravljanje biometrijskim informacijama u okviru sistema.

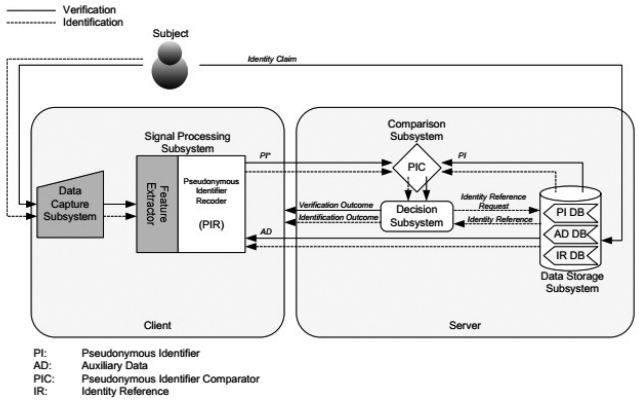
		Skladištenje			
		Server	Klijent	Token	Distribuirano
Poređenje	Server	A		B	G
	Klijent	C	D	E	H
	Token			F	

Tabela 2. *Klasifikacija modela biometrijskih sistema [9]*

Da bismo razumeli modele, najpre treba razjasniti pojmove servera, klijenta i tokena u ovom standardu [10]: *Server* je računar koji je putem mreže povezan sa klijentom. Klijent je PC, odnosno računar u formi kioska (primera radi bankomat itd.) na kome je smešten odgovarajući operativni sistem. *Klijent* obezbeđuje *front-end* servise za biometrijski sistem i interfejs za komunikaciju sa serverom i/ili tokenom. Biometrijski senzor je obično povezan sa klijentom. PDA uređaji i određeni pametni telefoni smatraju se klijentima u ovom standardu. *Token* je prenosni uređaj za skladištenje i upoređivanje biometrijskih podataka (Smart kartice, e-pasoši itd.). Kao primer biće prikazan Model A.

5.3.1 Model A - Skladištenje na serveru i poređenje na serveru

U ovom modelu biometrijske reference su skladištene na serveru i ekstrahovani biometrijski podaci se upoređuju na serveru (Slika 4). Zahteva se da server veruje podacima sa klijenta. Može se koristiti za identifikaciju i verifikaciju. S obzirom na to da su osetljive PII (Personal Identification Information - primera radi biometrijske reference i reference identiteta, u daljem tekstu PII) raspoložive na serveru, odgovarajuća bezbednost baze podataka i bezbednost mreže se podrazumevaju. Ovaj standard predlaže korišćenje AFIS-a (komercijalni automatski sistem za identifikaciju otisaka prstiju), dok sa aspekta privatnosti, ovaj model podrazumeva korišćenje RBR zbog osetljivih PII [10]. Proces upisivanja i kreiranja PI i AD se obavlja na klijentu, dok se skladištenje i verifikacija obavljaju na serveru. Informacija o potvrdi identiteta se nakon poređenja na serveru vraća klijentu.



Slika 4: *Model A [10]*

ZAKLJUČAK

Standardizacija biometrijskih sistema se čini jednim od ključnih faktora njihove uspešne primene i funkcionisanja, jer uspostavljanjem jedinstvenog radnog okruženja, radnog pro-

tokola, tehničkih interfejsa i svega ostalog što čini jednu nezavisnu funkcionalnu platformu kao što je BioAPI, biometrijski sistemi dobijaju dve osnovne karakteristike – *interoperability* (interoperabilnost) *i interchangeability* (interčejndžibilnost ili uzajamna razmena dva ili više sistema) koje ih čine jedinstvenim i omogućavaju funkcionisanje sistema nezavisno od porekla komponenti. Komponente postaju zamenljive, sistemi funkcionalniji i usklađeniji, olakšana je komunikacija u okviru sistema i, što nije ni malo zanemarljivo, troškovi razvoja i eksploatacije komponenti i sistema postaju niži.

S druge strane, ako analiziramo strukturu BIR zapisa i ACBio instance, prirodu i količinu informacija koju nose uz biometrijski podatak, mehanizme zaštite samog podatka bez potrebe uvida u isti, kao i povezanost i usklađenost ove dve strukture itd., može se reći da CBEFF i ACBio standardi opravdano nose nazive „dobrih praksi" kada govorimo o tehničkim bezbednosnim standardima. Međutim, kako biometrijske tehnologije svakodnevno napreduju i imaju sve širu primenu u praksi, za skladištenje biometrijskih podataka kao i za njihovu razmenu potrebno je održavati nivo bezbednosti istih redovnim ažuriranjem standarda.

U okviru ISO 24745 navedene tri karakteristike biometrijskih sistema: *poverljivost, integritet i obnovljivost/opozivost* utiču na poboljšanje performansi biometrijskih sistema sa akcentom na zaštiti privatnosti i biometrijskih informacija. *Koncept obnovljive i zamenjive biometrijske reference (RBR)* predstavlja nacrt jednog potencijalno veoma efikasnog mehanizma zaštite biometrijskih informacija uzimajući u obzir detaljan pristup rešenju problema privatnosti. Na kraju, u okviru standarda predlaže se arhitektura ukupno 8 primenjivih modela biometrijskih sistema, u zavisnosti od lokacije skladištenja i upoređivanja podataka u sistemu, sa akcentom na bezbednosti. Prednost ovog standarda je ta što je usvojen kao međunarodni, pa se na taj način povećava informisanost zainteresovanih entiteta i njegova dostupnost u praksi. Dalje, paralelna primena ovog standarda sa BioAPI platformom, CBEFF radnim okvirom i ACBio standardom, imajući u vidu kompatibilnost pomenutih standarda, učinila bi svaki biometrijski sistem znantno bezbednijim i funkcionalnijim.

Problem koji se ovde javlja isti je kao i kod svih standarda, a to je njihova šira i brža primena u praksi s obzirom na činjenicu da se njihovo uvođenje zasniva na dobrovoljnoj bazi. Kada bi brže zaživeli u praksi, šira primena dovela bi do daljeg unapređenja postojećih i razvoja novih standarda koji se bave rešavanjem problema biometrijskih sistema.

Stoga je zadatak korisnika biometrijskih tehnologija da standarde primenjuju kako bi uočili njihove eventualne nedostatke, dok je zadatak tela za standardizaciju (organizacija, instituta, konzorcijuma itd.) da prate rast i razvoj biometrijskih tehnologija i unapređuju postojeće i razvijaju nove i savremenije tehničke standarde.

PRIZNANJA

Ovaj rad je deo projekta „Primena multimodalne biometrije u menadžmentu identiteta", finansiranog od strane Ministarstva Prosvete i Nauke Republike Srbije, pod zavodnim brojem TR 32013.

REFERENCE

[1] Zvanična web stranica o biometriji: http://www.biometrics.org/
[2] S. Z. Li, A. Jain, „*Encyclopedia of Biometrics*", Springer US, SAD, 2009.
[3] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, Springer, 2013
[4] BioAPI konzorcijum, *BioAPI Specifikacija Verzija 1.1*, http://www.bioapi.org, 2002.
[5] BioAPI konzorcijum, *BioAPI Specifikacija Verzija 2.0*, http://www.bioapi.org, 2008.
[6] Izveštaj o CBEFF-u na web stranici NIST instituta: http://csrc.nist.gov/publications/nistir/NISTIR6529A.pdf
[7] N. Clarke, „*Transparent User Authentication*", Springer, London, 2011.
[8] Izveštaj o ACBio standardu, *„Information technology - Security techniques - Authentication context for biometrics (ACBio)"*, ISO, 2011.
[9] F. Deravi, *Biometric Standards,* In N. K. Ratha & V. Govindaraju (Eds.), *Advances in Biometrics*, Springer London, UK, 2011.
[10] Izveštaj o ISO 24745 standardu: *„Information technology — Security techniques — Biometric information protection", ISO 24745*, ISO, 2011.

Milorad Milinković, dipl.inž, Univerzitet u Beogradu, Fakultet organizacionih nauka, Stručni saradnik u MMKLAB (Istraživač pripravnik na projektu TR 32013)
Kontakt: milorad.milinkovic@mmklab.org
Oblasti interesovanja: menadžment, menadžment kvalitetom, internet marketing, e-poslovanje