UDC: 57.087:004 Info M: str. 44-47

REŠAVANJE PROBLEMA INTEROPERABILNOSTI BIOMETRIJSKIH SISTEMA I BEZBEDNOSTI BIOMETRIJSKIH PODATAKA PRIMENOM TEHNIČKIH STANDARDA
TROUBLESHOOTING INTEROPERABILITY OF BIOMETRIC SYSTEMS AND SECURITY OF BIOMETRIC DATA USING TECHNICAL STANDARDS

Milorad Milinković

REZIME: U ovom radu prikazana su dva najčešća problema u funkcionisanju biometrijskih sistema, problem interoperabilnosti kako između komponenti sistema tako i između različitih sistema, i problem bezbednosti biometrijskih podataka i zaštite privatnosti kako prilikom skladištenja i razmene, tako i prilikom biometrijske transakcije u okviru biometrijskog sistema ili između različitih biometrijskih sistema korišćenjem Interneta. Prikazivanjem strukture BioAPI platforme, CBEFF frejmvorka i ACBio autentikacijskog konteksta za biometriju i njihove povezanosti istaknute su prednosti primene pomenutih standarda kao rešenja ovih problema.

KLJUČNE REČI: Biometrija, standardi, BioAPI, CBEFF, ACBio

ABSTRACT: This paper indicates two the most common problems in functioning of biometric systems, problem of interoperability between system's components as well as between different biometric systems and problem of biometric data security and privacy protection, both in storage and exchange, and in biometric transaction within a biometric system as well as between different biometric systems using the Internet. Presenting the structure of BioAPI platform, CBEFF framework and ACBio (Authentication Context for Biometrics) and their relationship, highlights the benefits of the application of these standards as a solution to the aforementioned problems.

KEY WORDS: Biometrics, Standards, BioAPI, CBEFF, ACBio

1. UVOD

Biometrija se veoma brzo razvija i sve šire primenjuje (primera radi kontrola pristupa, e-trgovina, internet bankarstvo i druge oblasti). S obzirom na činjenicu da je razvoj biometrijskih tehnologija i uređaja kao i softverskih aplikacija uzeo maha, prema [1] pojavio se problem velikog broja proizvođača samim tim i problem u komunikaciji između softvera i uređaja različitih proizvođača (tzv. „vendor lock-in"). S druge strane, kako prema [2] biometrija koristi fizičke i ponašajne karakteristike pojedinaca za jedinstveno identifikovanje korisnika prilikom autentifikacije, bezbednost ovih podataka mora biti na najvišem nivou.

Stoga je prema [3] ne tako davne 1998. godine BioAPI konzorcijum formiran 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. Tako nastaje BioAPI specifikacija koja definisanjem jedinstvene platforme za komunikaciju između aplikacija i biometrijskih tehnologija i statusom standarda ubrzava prihvatanje biometrijskih tehnologija i velikog broja komercijalnih aplikacija.

S druge strane, bezbednost biometrijskih podataka koji se obrađuju i skladište u biometrijskim sistemima i razmenjuju između istih je veoma bitna, jer gubitak ili otkrivanje ovih podataka potencijalno vode do ugrožavanja integriteta sistema prilikom autentifikacije i mogućih zloupotreba podataka koji predstavljaju deo identiteta pojedinca kao što su krađa identiteta ili bilo koji drugi način ugrožavanja privatnosti. Da bi se predupredile ovakve situacije, postoje preventivne mere, a jedna od njih je primena tehničkih standarda. Intenzivan razvoj biometrijskih tehnologija za autentifikaciju 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 [2].

Suština tehničkih standarda je akcenat kako na zaštiti uskladištenih biometrijskih podataka, uključujući biometrijske uzorke i reference, korišćenjem kriptografskih tehnika kao što su digitalni potpisi i šifrovanje (enkripcija), 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.

Ključni standard za skladištenje i razmenu biometrijskih podataka prema [2] je ISO 19785, odnosno CBEFF frejmvork (Common Biometric Exchange Format Framework), dok je najčešće primenjivan, međunarodno priznat i objavljen standard za transakciju biometrijskih podataka ACBio, odnosno Autentikacijski kontekst za biometriju, sa oznakom ISO 24761.

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

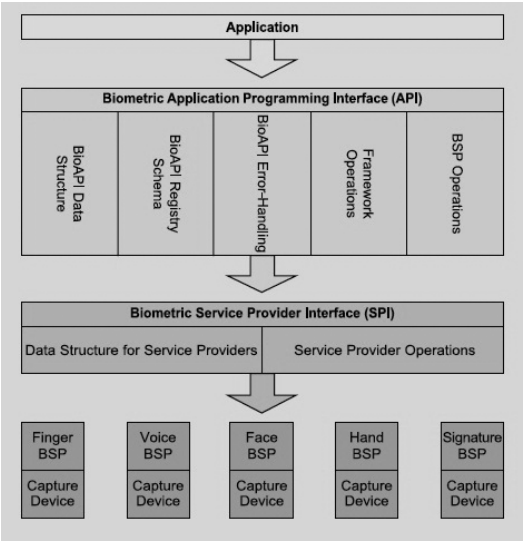
2. BIOAPI SPECIFIKACIJA (VERZIJA 1.1)

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. Takođe, prema [4] definiše API (Application Program Inteface) za aplikativne programere i SPI (Service Provider Interface) za programere u oblasti biometrijskih tehnologija koji predstavljaju dva osnovna nivoa BioAPI platforme.

2.1 *STRUKTURA 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. 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* – upravlja 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 biometrijskih sistema i međunarodnih standarda 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].

Tabela 1. *Polja standardnog zaglavlja biometrijskih podataka SBH [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 kvaliteta 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.
Vlasnik BDB formata	Z	ID grupe ili proizvođača koji je definisao BDB.
Tip BDB formata	Z	Definiše vlasnik formata.
Identifikator proizvoda (PID)	O	Registrovani identifikator entiteta koji je kreirao biometrijski podatak.
Identifikator patron formata	O	Registrovani identifikator patron formata.
Sekcija biometrijskih podataka	**Z**	**Definiše vlasnik formata. Može biti kodiran.**
Potpis	**Z**	**Digitalni Potpis**

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. ACBIO

ACBio je međunarodni standard objavljen od strane ISO organizacije kao kontekst autentifikacije za biometriju pod oznakom ISO 24761:2011. 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*

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 ACBIO STANDARDA U BEZBEDNOSTI BIOMETRIJSKIH PODATAKA*

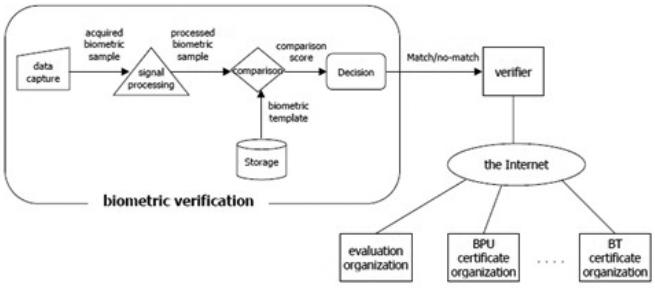
ACBio je dizajniran sa akcentom na problemu privatnosti. Definisan je tako da verifikator (biometrijska aplikacija za donošenje odluke o uspešnosti verifikacije) može da proveri validnost biometrijskog procesa verifikacije bez korišćenja privatnih podataka poput biometrijskog uzorka i biometrijskog šablona 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. ZAKLJUČAK

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

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] Zvanična web stranica BioAPI konzorcijuma: http://www.bioapi.org/
[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.

Milorad Milinković, dipl.inž, Univerzitet u Beogradu, Fakultet organizacionih nauka
Kontakt: milorad.milinkovic@mmklab.org
Oblasti interesovanja: menadžment, menadžment kvalitetom, internet marketing, e-poslovanje