UDC: 57.097:004.8.056 Info M str. 47-52

UNAPREĐENJE BEZBEDNOSNIH TEHNIKA I ZAŠTITE BIOMETRIJSKIH PODATAKA U BIOMETRIJSKIM SISTEMIMA: PREDSTAVLJANJE MEĐUNARODNOG STANDARDA ISO 24745
IMPROVEMENT OF SECURITY TECHNIQUES AND PROTECTION OF BIOMETRIC DATA IN BIOMETRIC SYSTEMS: PRESENTATION OF INTERNATIONAL STANDARD ISO 24745

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

REZIME: U ovom radu predstavljen je međunarodni standard ISO 24745 kao potencijalni bezbednosni alat za zaštitu biometrijskih informacija, tačnije kao alat za zaštitu privatnosti u biometrijskim sistemima. Ovo je jedan od poslednjih standarda u nizu međunarodno prihvaćenih koji se bave problemom bezbednosti biometrijskih sistema.

KLJUČNE REČI: Biometrija, Privatnost, Bezbednost, Standardi

ABSTRACT: This paper presents the International Standard ISO 24745 as a potential security tool for biometric information protection, more precisely as a tool for privacy protection in biometric systems. This is one of the latest internationally accepted standards that address the security issues of biometric systems.

KEY WORDS: Biometrics, Privacy, Security, Standards

1. UVOD

Savremeno poslovanje je gotovo nemoguće bez pružanja usluga na daljinu putem Interneta (e-bankarstvo, e-obrazovanje, e-zdravstvo, e-prodaja, e-javna uprava itd.). Tokom realizacije ovih usluga, između subjekata (korisnika usluga) i pružaoca usluga, mehanizmi autentikacije postaju sve kritičniji u pogledu bezbednosti i zaštite privatnosti [1].

Među najsavremenijim autentikacijskim mehanizmima su i oni koji koriste biometrijske tehnologije [2]. Ove tehnologije su prema [1] sve prisutnije, što je dovelo do smanjenja njihovih troškova razvoja i korišćenja, dok je sa druge strane dovelo do povećanja njihove primene i razvoja, zbog čega se smatraju prihvatljivim i održivim.

Biometrijske karakteristike pojedinca su idealne za korišćenje u ove svrhe, jer su svojstvene samo tom pojedincu [1]. Međutim, problem je očuvanje privatnosti pojedinca i zaštita biometrijskih informacija (primera radi može doći do krađe identiteta, lažnog predstavljanja itd.) [3]. Stoga, odgovarajuće protivmere, odnosno mere zaštite za očuvanje bezbednosti biometrijskog sistema i privatnosti pojedinaca su suštinsko rešenje problema.

Biometrijski sistemi obično povezuju biometrijske reference (otisak prsta, lice, glas, ili neki drugi biometrijski modalitet) sa drugim informacijama za identifikovanje pojedinaca, pa se zajedno koriste tokom procesa autentikacije [4].

Veza između ovih podataka je bitna da bi se osigurala bezbednost podataka koji sadrže biometrijske informacije. Prema [3] ovaj način povezivanja biometrijskih referenci i identifikacionih referenci (ime, prezime, JMBG, broj ličnog dokumenta itd.) i razmena ovih informacija u zakonskim okvirima predstavljaju 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 međunarodni standard sa oznakom ISO 24745, koje se prema [5] odnosi na tehnike zaštite biometrijskih informacija i predstavlja jedno od mogućih rešenja problema zaštite privatnosti i biometrijskih informacija u okviru biometrijskog sistema.

2. O BIOMETRIJSKIM SISTEMIMA

Biometrijski sistemi prema [1] služe za automatsko prepoznavanje osoba korišćenjem njihovih fizioloških karakteristika (otisak prsta, slika lica, silueta šake, dužica oka - iris itd.) i njihovih ponašajnih karakteristika (potpis, hod, glas).

Ovi sistemi se prema [6] obično sastoje od pet podsistema:

- *Podsistem za prikupljanje biometrijskih podataka*, koji se sastoji od uređaja za prikupljanje ovih podataka odnosno senzora za prikupljanje signala biometrijske karakteristike i njeno pretvaranje u biometrijski uzorak kao što su slike otiska prsta, lica ili snimak glasa.
- *Podsistem za procesiranje signala*, koji izdvaja biometrijske karakteristike iz uzorka. Izdvojeno svojstvo uzorka tokom procesa upisivanja se skladišti u podsistemu za skladištenje (baza podataka) kao biometrijska referenca za identifikaciju i verifikaciju vlasnika uzorka.
- *Podsistem za skladištenje podataka* je baza za upisivanje gde se identifikacione i biometrijske reference pojedinca povezuju u jedan podatak za identifikaciju. Obično postoje dve baze podataka, za identifikacione i za biometrijske reference, zbog bezbednosti i privatnosti pojedinaca.
- *Podsistem za poređenje (komparaciju)*, određuje sličnost između upisanog biometrijskog uzorka i uskladištene biometrijske reference. Komparacija se vrši jedan-na-jedan ili jedan-na-više.
- *Podsistem za donošenje odluke*, određuje da li upisan biometrijski uzorak i biometrijska referenca pripadaju istom vlasniku i donosi se odluka o potvrdi identiteta.

Biometrijski sistemi prema [6] imaju tri osnova funkcionalna procesa:

- *Proces upisivanja*: predstavlja kreiranje i skladištenje biometrijskih podataka o pojedincu. Biometrijski uzorak

se procesira izdvajanjem njegovih karakteristika, koje se upisuju kao biometrijska referenca u bazu i povezuju sa identifikacionim referencama.
- *Proces identifikacije*: pretraga baze podataka i upoređivanje biometrijskog uzorka sa uskladištenom referencom.
- *Proces verifikacije*: provera da li je osoba koju upisujemo vlasnik uskladištene reference, komparacijom uzorka i reference.

Navedeni podsistemi su osnova svakog biometrijskog sistema koji upisuje, procesira, skladišti, upoređuje i donosi odluku o procesiranom biometrijskom podatku.

3. 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 [5].

ISO 24745 prema [5] precizira sledeće:
- Analizu pretnji i mera zaštite svojstvenih funkcionisanju biometrijskih sistema,
- Bezbednosne zahteve za bezbedno povezivanje biometrijskih i identifikacionih referenci,
- Modele za primenu na biometrijske sisteme sa različitim scenarijima za skladištenje i poređenje biometrijskih referenci, i
- Uputstvo za zaštitu privatnosti pojedinaca prilikom procesiranja biometrijskih informacija.

Ovaj standard ne obuhvata opšte probleme koji se odnose na fizičku bezbednost, bezbednost okoline i upravljanje ključevima za kriptografske tehnike. U ovom radu biće predstavljena analiza pretnji i adekvatnih mera zaštite kao i arhitektura modela biometrijskih sistema sa akcentom na bezbednosti.

4. 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 [7]:

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 autentifikacije zavisi od integriteta biometrijske reference. Ako su biometrijska referenca ili njene određene osobine nepouzdane, biće i rezultat autentifikacije. Nepouzdana biometrijska referenca ili uzorak nastaju:
   - Ako je došlo do slučajnog zakazivanja softvera ili hardvera,
   - Slučajnom ili namernom prepravkom (modifikacijom) pravih biometrijskih referenci od strane neovlašćenih entiteta (korisnik ili vlasnik sistema), bez intervencije spoljnog napadača,
   - Modifikacija (zamena) biometrijske reference od strane spoljnog napadača.

Preventivne i zaštitne mere obuhvataju mehanizme kontrole pristupa i kriptografske tehnike. Zaštita integriteta može se kombinovati sa ostalim tehnikama kao što su upisivanje vremena u referencu (*Time stamping*), MAC (autentikacijski kod poruke), digitalni potpis itd.

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. BEZBEDNOSNE PRETNJE I MERE ZAŠTITE U BIOMETRIJSKIM SISTEMIMA

5.1 *Pretnje i mere zaštite kod biometrijskih komponenti*

Imajući u vidu komponente (podsisteme) biometrijskih sistema, prema ISO 24745 standardu pretnje i mere zaštite su grupisane u Tabeli 1.

Tabela 1: *Pretnje i mere zaštite u komponentama biometrijskog sistema [3]*

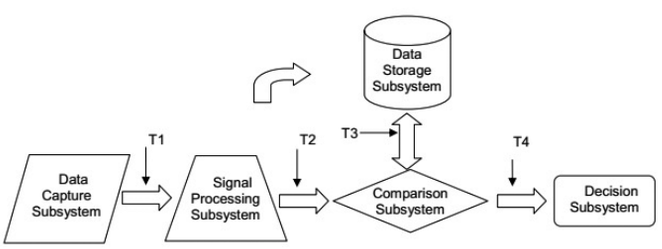
Funkcija biometrijskog (pod)sistema	Pretnje	Mere zaštite
Upisivanje podataka	▪ Prevara senzora ▪ Upis/reprodukcija signala senzora	▪ Trenutna detekcija ▪ Multimodalna biometrija ▪ Izazov/reakcija
Procesiranje signala	▪ Neovlašćena manipulacija podacima tokom procesiranja	▪ Korišćenje proverenih algoritama
Poređenje (komparacija)	▪ Manipulisanje rezultatima poređenja	▪ Bezbedan server i/ili klijent ▪ Provereno OCC poređenje (*On-card comparison*)
Skladištenje	▪ Ugrožavanje baze podataka (neovlašćeno otkrivanje, zamena, modifikacija i brisanje referenci).	▪ Biometrijske reference koje se mogu opozvati/obnoviti ▪ Odvajanje podataka ▪ Kontrola pristupa bazi podataka ▪ Potpis i enkripcija u okviru reference
Odlučivanje	▪ *Hill climbing* napad	▪ Bezbedan kanal ▪ Sakriti rezultat poređenja od subjekta poređenja
	▪ Manipulacije vrednošću praga odluke (*Threshold manipulation*)	▪ Kontrola pristupa podešavanju vrednosti praga odluke ▪ Zaštita vrednosti praga odluke

Sensor spoofing (prevara senzora) je prikazivanje veštačkih biometrijskih karakteristika. Jedna od protivmera je detekcija uživo kojom se prepoznaju psihološke aktivnosti subjekta

uživo ili detekcija i odbijanje poznatih veštačkih biometrijskih modaliteta (primera radi otisak prsta). *Zamena komponenti* podrazumeva uklanjanje i zamenu podsistema (primera radi za poređenje i odlučivanje) biometrijskog sistema i preuzimanje kontrole nad istim. *Hill climbing* je sistematska modifikacija biometrijskog uzorka da bi se dobili znatno viši rezultati poređenja dok se vrednost praga ne dostigne. *Manipulacije pragom vrednosti* poređenja i odluke je promena vrednosti u podsistemu odlučivanja da bi se prihvatio nelegitiman biometrijski uzorak. *Opozive i obnovljive biometrijske reference* nastaju radi diverzifikacije za različite aplikacije, organizacije ili kompanije, ali se odnose na isti subjekat (pojedinca). Pojedinac može imati višestruke biometrijske reference. *Razdvajanje podataka* se odnosi na logičko i fizičko razdvajanje pojedinačnih elemenata podataka (primera radi delimično na tokenu, delimično u bazi). Ovo se može odnositi na identifikacione, biometrijske reference, PI i AD podatke o kojima će kasnije biti reči.

5.2 *Pretnje i mere zaštite prilikom prenosa biometrijskih informacija*

Komunikacioni kanali između različitih komponenti biometrijskog sistema mogu biti ugroženi i tako uticati na bezbednost čitavog sistema. Rizik je veći kod distribuiranih arhitektura. Situacije u kojima se prenose podaci nalaze se na Slici 1 i sumirane su u Tabeli 2. U Tabeli 2, ako mreža interveniše između podsistema za poređenje i odlučivanje, pretnje i odgovarajuće mere za T1, T2 i T3 su primenjive i za T4.



Slika 1: *Arhitektura biometrijskog sistema i moguće pretnje [8]*

Tabela 2: *Pretnje i mere zaštite tokom prenosa biometrijskih informacija [4]*

Funkcija biometrijskog (pod)sistema	Podaci	Pretnje	Mere zaštite
Upis podataka – Procesiranje signala (T1) **Procesiranje signala - Poređenje (T2)**	Biometrijski uzorak i karakteristika	▪ Prisluškivanje	▪ Enkriptovan/bezbedan kanal
		▪ Reprodukcija	▪ Izazov/reakcija
		▪ Fizička sila	▪ Uredba o isteku vremena
Skladište - Poređenje (T3)	Biometrijska referenca	▪ Prisluškivanje	▪ Enkriptovan/bezbedan kanal
		▪ Reprodukcija	▪ Izazov/reakcija
		▪ Čovek u sredini (*Man in the middle*)	▪ Enkriptovan/bezbedan kanal ▪ Provera integriteta biometrijskog podatka sa digitalnim potpisom ili MAC kodom
		▪ *Hill climbing*	▪ Bezbedan kanal
Poređenje - Odluka (T4)	Rezultat poređenja	▪ Manipulacija rezultatom poređenja	▪ Bezbedan kanal

Prisluškivanje je presretanje osetljivih informacija tokom prenosa između komponenti biometrijskog sistema. *Man in the middle* je napad u kome napadač može da čita, ubaci i modifikuje biometrijske podatke koji se prenose između dva podsistema iako se zna da je uspostavljena veza bila ugrožena.

5.3 *Obnovljive biometrijske reference kao tehnologija mere zaštite*

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).

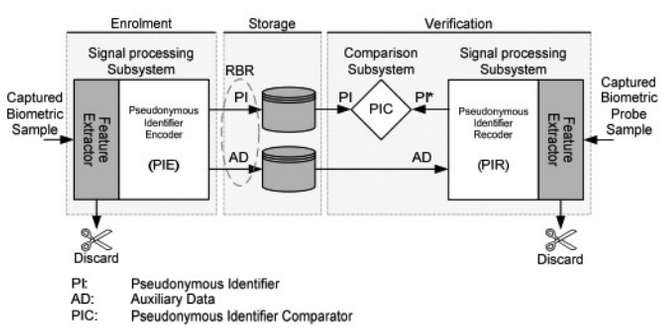
Diverzifikacija uključuje generisanje višestrukih, nezavisnih referenci proisteklih iz istih biometrijskih karakteristika koje se mogu primeniti za obnovu biometrijske reference ili za obezbeđivanje nezavisne reference koja se koristi u različitim aplikacijama [5].

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 [5] sastoje od dva elementa podataka:

1. „Indentifikatori pod pseudonimom“ (*Pseudonymous identifiers*, odnosno PI u daljem tekstu), i
2. 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 2. 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 2: *Arhitektura za kreiranje RBR [8]*

6. PRIMENA MODELA BIOMETRIJSKIH SISTEMA I NJIHOVA BEZBEDNOST

U okviru ovog standarda prema [7] predlaže se 8 modela biometrijskih sistema koji su klasifikovani prema lokaciji za skladištenje i upoređivanje biometrijskih informacija (Tabela 3) imajući u vidu bezbednosni aspekt. Svaki model ima svoje prednosti i mane kada je u pitanju upravljanje biometrijskim informacijama u okviru sistema.

Tabela 3. *Klasifikacija modela biometrijskih sistema [5]*

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

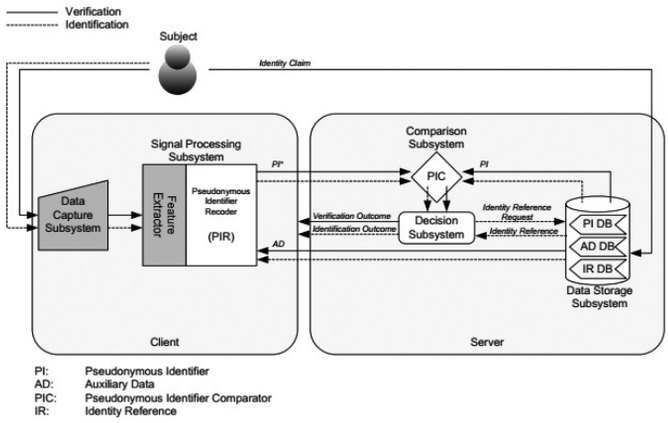
Da bismo razumeli modele, najpre treba razjasniti pojmove servera, klijenta i tokena u ovom standardu [7]:

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.). Neki od najvažnijih i najčešće primenjivanih modela prikazani su u tekstu koji sledi.

6.1 *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 3).

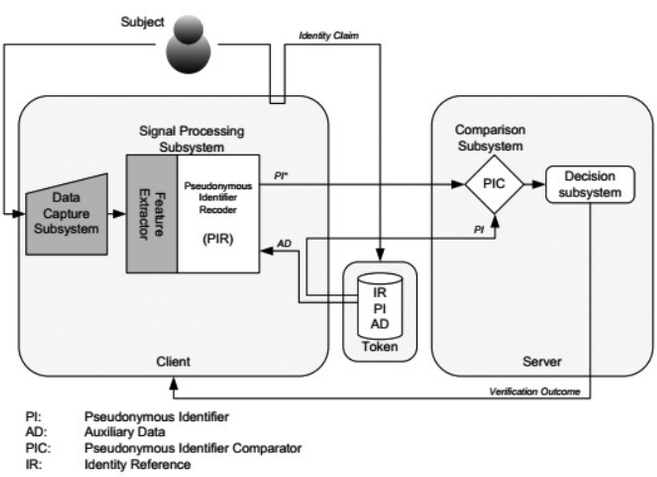
U ovom modelu se zahteva da server veruje podacima sa klijenta. Može se koristiti za identifikaciju i verifikaciju. S obzirom na to da su osetljive PII (Personal Identification Information - primera radi biometrijske reference i reference identiteta, u daljem tekstu PII) raspoložive na serveru, odgovarajuća 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 [7]. 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 3: *Model A [7]*

6.2 *Model B - Skladištenje na tokenu i upoređivanje na serveru*

U ovom modelu token se koristi za skladištenje biometrijskih referenci i zahteva se da se uslikani biometrijski podaci šalju na upoređivanje serveru (Slika 4). Osoba povezuje svoje biometrijske reference sa identifikacionim referencama na tokenu tokom procesa upisivanja u sistem. Osoba koja želi da potvrdi svoj identitet treba da poseduje token i da ga poveže sa klijentom, i takođe da prinese svoje biometrijske karakteristike (konkretan modalitet(e) koji se koristi(e) u sistemu). Tada klijent šalje uskladištene i uslikane biometrijske podatke serveru na upoređivanje. Kao i u prethodnom modelu, zbog privatnosti predlaže se korišćenje RBR, PI* i PI se šalju serveru, dok AD ostaju na klijentu.

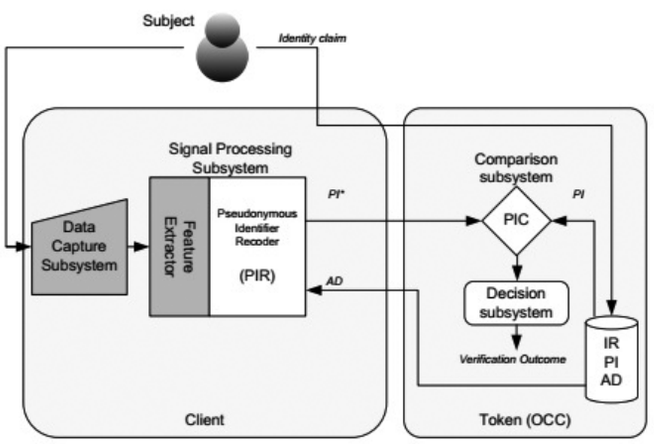


Slika 4: *Model B [7]*

U ovom modelu se kao i u prethodnom podrazumeva da server veruje podacima sa klijenta. Obično se koristi za verifikaciju, s obzirom na to da se token koristi za identifikaciju. Ne zahteva obezbeđivanje baze podataka, jer su podaci za identifikaciju na tokenu, ali zahteva bezbednost mreže prilikom prenosa podataka na server [7]. Akcenat ovog modela je po svemu sudeći na privatnosti pojedinaca.

6.3 *Model F - Skladištenje i poređenje na tokenu*

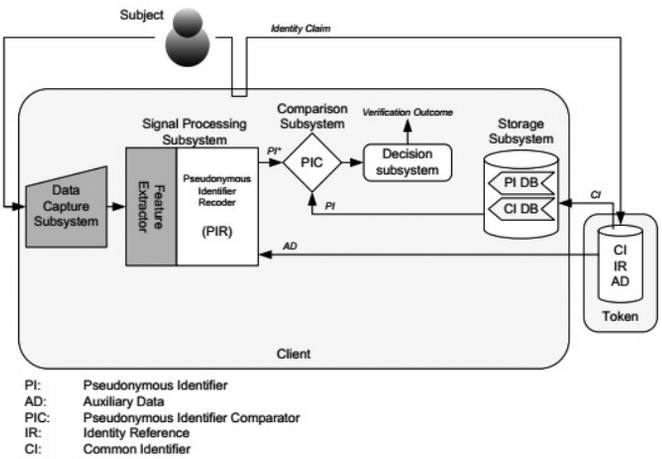
U ovom modelu skladištenje i upoređivanje biometrijskih podataka vrši se na tokenu (Slika 5). Osoba povezuje svoje biometrijske reference i identifikacione reference na tokenu prilikom upisa. Osoba koja želi da potvrdi svoj identitet mora da prikaže biometrijski uzorak klijentu pomoću tokena. Token mora biti opremljen algoritmom za poređenje/odlučivanje. Klijent može primera radi biti bankomat. Ovaj model se obično koristi kod bankarskih transakcija korišćenjem OCC (On-Card Comparison - poređenje na kartici, u daljem tekstu OCC). Ovaj tip OCC modela je najjači mehanizam za zaštitu ličnih informacija [4]. Token skladišti BR i IR, i poređenje se izvršava na kartici. Klijent prikuplja biometrijski uzorak osobe kao i njene IR podatke i šalje ih na token za upoređivanje sa već uskladištenim. Rezultat poređenja se šalje serveru banke. Token može da sadrži podsistem za procesiranje signala, što privatnost i bezbednost pojedica podiže na znatno viši nivo. Kao i kod ranijih modela korišćenje RBR se preporučuje. U tom slučaju AD podaci se šalju klijentu, dok PI podaci ostaju na tokenu. Ovde je privatnost na prvom mestu i u rukama pojedinca koji je vlasnik. Modaliteti i ceo sistem za poređenje standardizovani su ISO 24787 standardom koji je prema [5] usko specijalizovan za poređenje na kartici.



Slika 5: *Model F [7]*

6.4 *Model H – Skladištenje na tokenu i klijentu, poređenje na klijentu*

U ovom modelu AD, IR i CI se nalaze na tokenu, i PI i CI (Common Identifier – podatak koji povezuje biometrijske i identifikacione reference kada su u odvojenim bazama, u daljem tekstu CI) se nalaze na klijentu. Tokom verifikacije, token prikazuje CI i AD klijentu. PI koji je povezan sa CI klijent povlači iz svog podsistema za skladištenje i šalje AD PIR-u. PIR generiše PI* zasnovan na biometrijskom uzorku pojedinca nastalog tokom upisivanja. PI* se poredi sa PI koji je uskladišten na klijentu i rezultat poređenja se šalje podsistemu odlučivanja za donošenje odluke o verifikaciji (da li je potvrđen identitet ili ne).



Slika 6: *Model H [7]*

U ovom modelu, klijent može biti kiosk, koji prema [2] možemo naći na aerodromima i u javnim zgradama za potrebe personalne autentikacije. Model je primenjiv i na graničnim prelazima korišćenjem e-pasoša u registrovanoj aplikaciji za identifikaciju putnika [2].

Na kraju, kako se većina biometrijskih sistema sastoji se od servera i nekoliko klijenata koji su opremljeni senzorima, odnosno uređajima za upisivanje biometrijskih podataka, i kako se većina operacija i procesa u okviru sistema obavlja putem mreže, potrebno je obezbediti prenos podataka.

Imajući sve ovo u vidu prema [6] paralelna primena *AC-Bio - konteksta autentikacije za biometriju*, koji je usvojen kao međunarodni standard ISO 24761 i u okviru koga se predlažu posebni bezbednosni mehanizmi za nesmetan prenos podataka, uticala bi na podizanje bezbednosti biometrijskih podataka kao i kompletnog biometrijskog sistema na znatno viši nivo.

7. ZAKLJUČAK

U okviru ovog standarda velika pažnja je posvećena analizi pretnji koje mogu ugroziti privatnost korisnika i dovesti do zloupotrebe biometrijskih informacija koje se razmenjuju u okviru jednog ili između više biometrijskih sistema. Da bi autentikacija bila uspešna predložen je čitav niz mera zaštite kao protivmera, odnosno odgovora na pomenute pretnje. Navedene tri karakteristike biometrijskih sistema: *poverljivost, integritet i obnovljivost/opozivost* koje se propagiraju u ovom standardu 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 biometrijskih sistema.

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 detaljno opisanima u [6], a imajući u vidi 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 njegova šira i brža primena u praksi s obzirom na činjenicu da se njegovo uvođenje zasniva na dobrovoljnoj bazi. Kada bi brže zaživeo u praksi, šira primena dovela bi do daljeg unapređenja postojećeg i razvoja novih standarda koji se bave rešavanjem problema biometrijskih sistema.

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] S. Z. Li, A. Jain, *Encyclopedia of Biometrics*, Springer US, SAD, 2015.
[2] V. Cantoni et al., *Biometric Authentication*, Springer, 2014.
[3] Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, Springer, 2013.
[4] P. Campisi, *Security and Privacy in Biometrics*, Springer London, UK, 2013.
[5] F. Deravi, *Biometric Standards,* In N. K. Ratha & V. Govindaraju (Eds.), *Advances in Biometrics*, Springer London, UK, 2011.
[6] M. Milinković, *Rešavanje problema interoperabilnosti biometrijskih sistema i bezbednosti biometrijskih podataka primenom tehničkih standarda*, Info M, br 53, FON, Beograd, 2015.
[7] *Information technology — Security techniques — Biometric information protection, ISO 24745*, ISO, 2011.
[8] Zvanična Internet prezentacija ISO organizacije: *www.iso.org*

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