The Office for Personal Data Protection of the

SLOVAK REPUBLIC

Riadenie identít – technológia riadenia prístupov pomocou biometrického šifrovania

-Biometric Encryption Access Management

Odborárske námestie 3
817 60 Bratislava 15
Tel.:+421 2 502 39 418
Fax: +421 2 502 39 441
STATNY.DOZOR@PDP.GOV.SK
WWW.PDP.GOV.SK

Daniel Valentovič
Tel.: +421 2 50239428
Mob.: +421 903454017
Daniel.Valentovic@pdp.gov.sk

Ochrana osobných údajov patrí medzi ľudské práva a je zaručená ústavou

- **Najviac sa osobné údaje dajú zneužiť vo veľkých aplikáciách, kde sa nachádzajú v hojnej miere:**
  - **eGovernment – všetky osobné údaje občanov od rodných čísiel, bydlísk až po platenie daní a soc. poistného, DB všetkých štátnych orgánov, ministerstiev, polície, samospráv ….**
  - **Systémy E- health** – elektronické zdravotné záznamy
  - **IS finančných inštitúcií a poisťovieň** – ide o peniaze občanov
  - Atď.
- **Najlepšie sa ochránia osobné údaje bezpečným riadením prístupov do systémov, ktoré ich obsahujú a s ktorými občania komunikujú osobne**

Čo rozumieme pod pojmom :

„Ochrana osobných údajov “ ?

- **Definícia Osobných údajov (OU)**

- **§3 zákona 428/2002 Coll. O ochrane OU**

Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu.

Máme osobné údaje, ale aj

OU osobitnej kategórie - ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženskú vieru alebo svetonázor, členstvo v politických stranách alebo politických hnutiach, členstvo v odborových organizáciách a údaje týkajúce sa zdravia alebo pohlavného života (§8)

Niektoré iné právne normy týkajúce sa OU :

- EU:
- **DOHOVOR O OCHRANE JEDNOTLIVCA PRI AUTOMATIZOVANOM SPRACOVANÍ OSOBNÝCH ÚDAJOV** (ETS No. 108)
- **Dodatkový protokol k Dohovoru 108 týkajúci sa orgánov dozoru a cezhraničných tokov údajov** ETS No. 181)
- Smernica 95/46/ES o ochrane OU
- Smernica .2002/58/EC o ochrane súkromia v elektronických komunikáciách

- SR:
- Ústava SR , Article19 and 22
- Zákon 428/2002 Z.z. o ochrane OU
- Zákon 610/2003 Z.z. O elektronických komunikáciách
- Iné špeciálne zákony

EU pohľad na e-systémy EU čl. štátov .:

Po 2009 - EU federatívny e-ID MNGMT , integrované EU riešenia – e- gov , e-health, e- call .....

Interoperabilita e-systémov čl. štátov EU je **KĽÚČ k riešeniu**

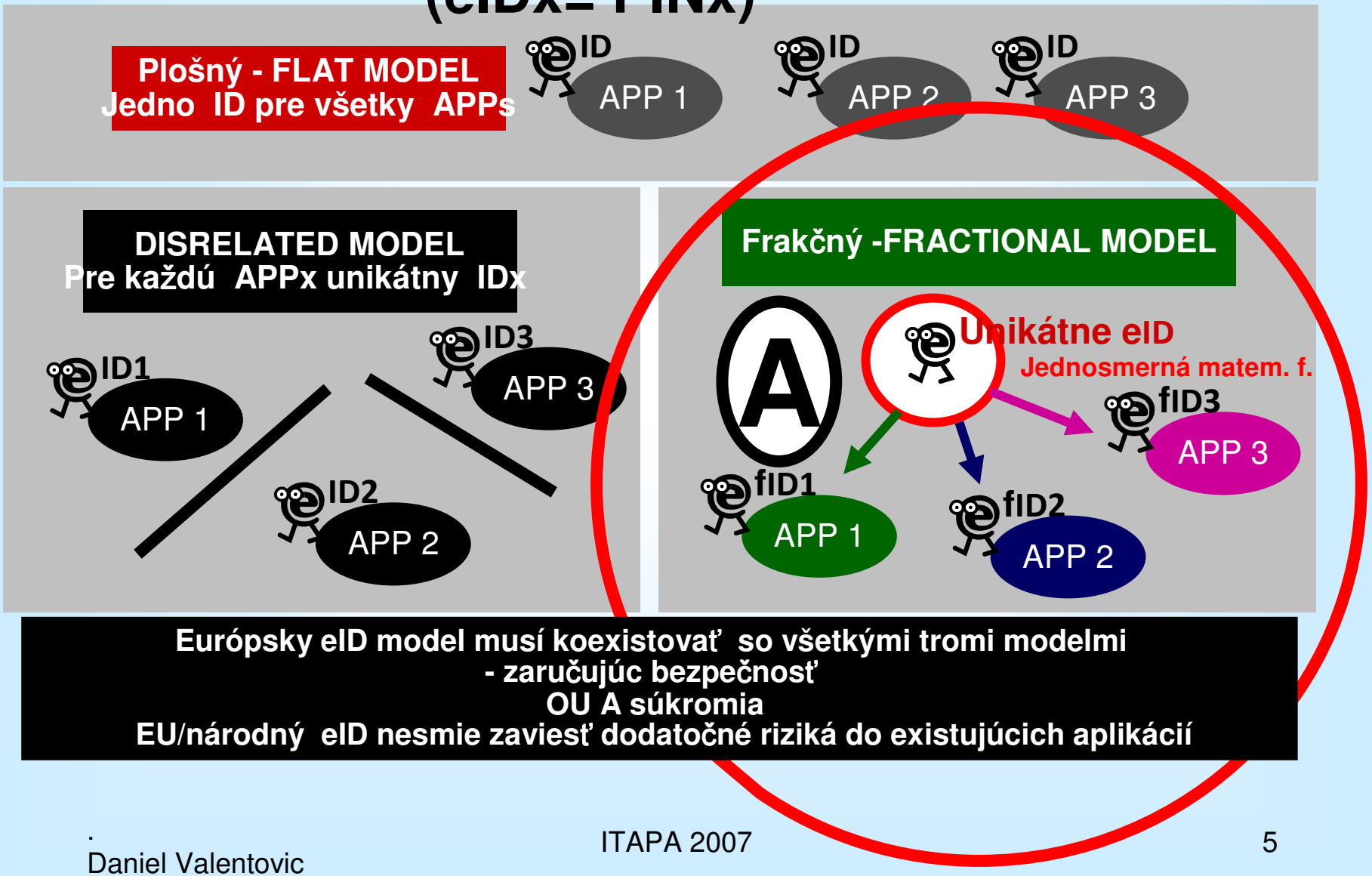
Bezpečnosť e-systémov EU a ochrana osobných údajov a súkromia občanov je **NEVYHNUTNOSŤ**

Ochrana OU a ochrana súkromia je občanov EU je zaručená zákonom ...

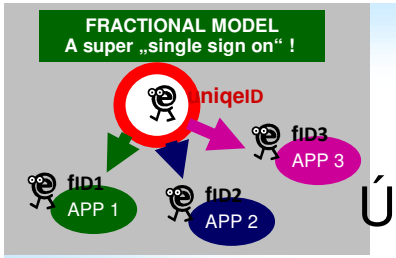
"… to achieve interoperability, both within and across policy areas and, where appropriate, with businesses and citizens, notably on the basis of a European Interoperability Framework". *

***Decision 2004/387/EC**

EU - eID a ochrana OU – existujúce modely (eIDx= PINx)



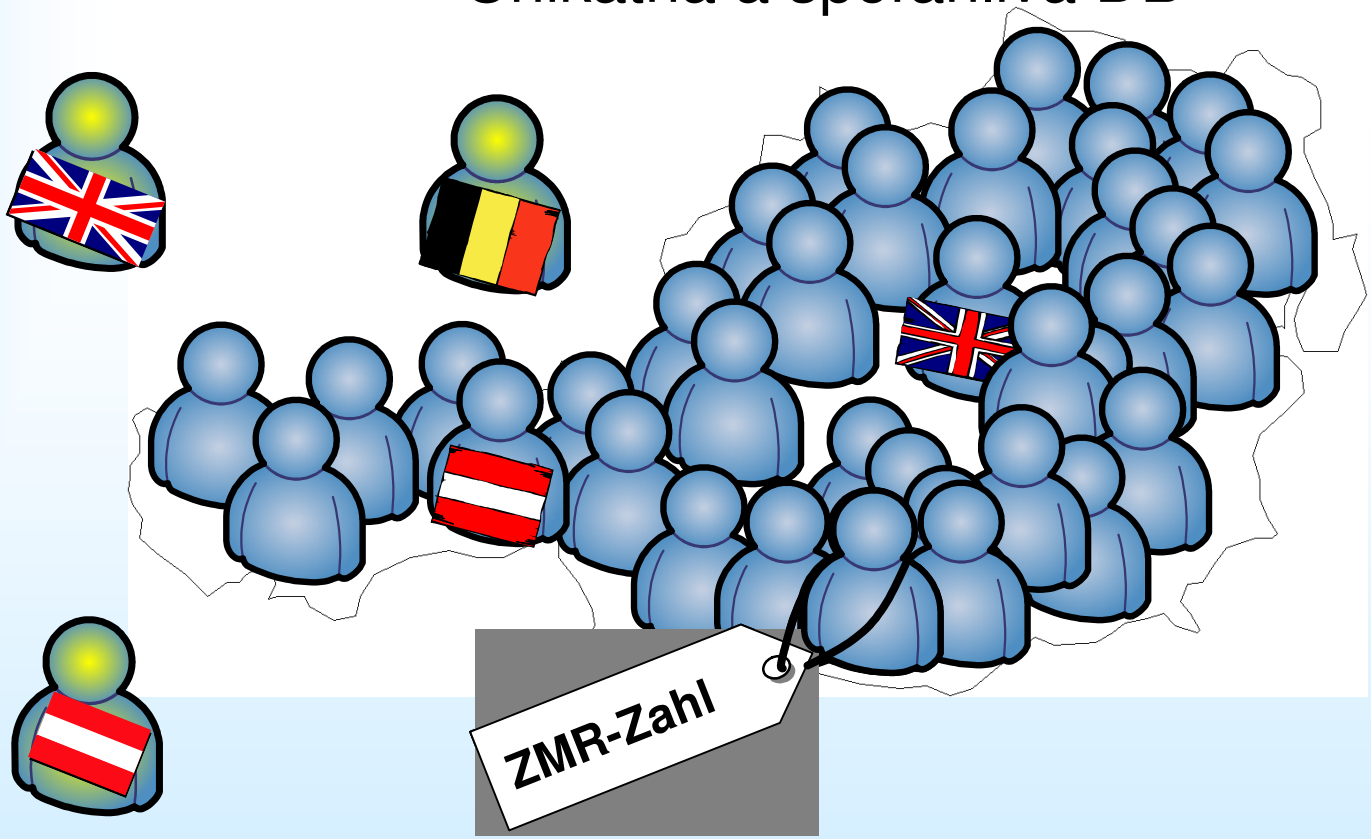
Európsky eID model musí koexistovať so všetkými tromi modelmi
- zaručujúc bezpečnosť
OU A súkromia
EU/národný eID nesmie zaviesť dodatočné riziká do existujúcich aplikácií

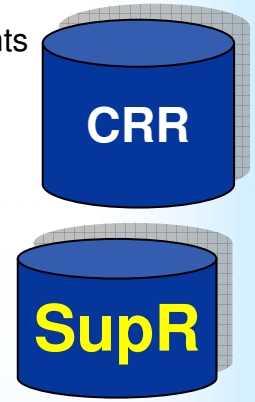


Rakúsko -

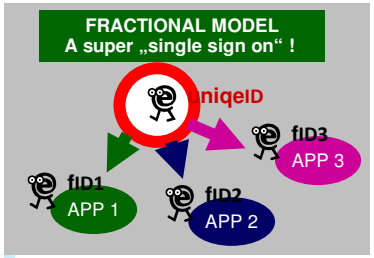
Ústredný register obyvateľstva CRR Central Register of Residents

Unikátna a spoľahlivá DB





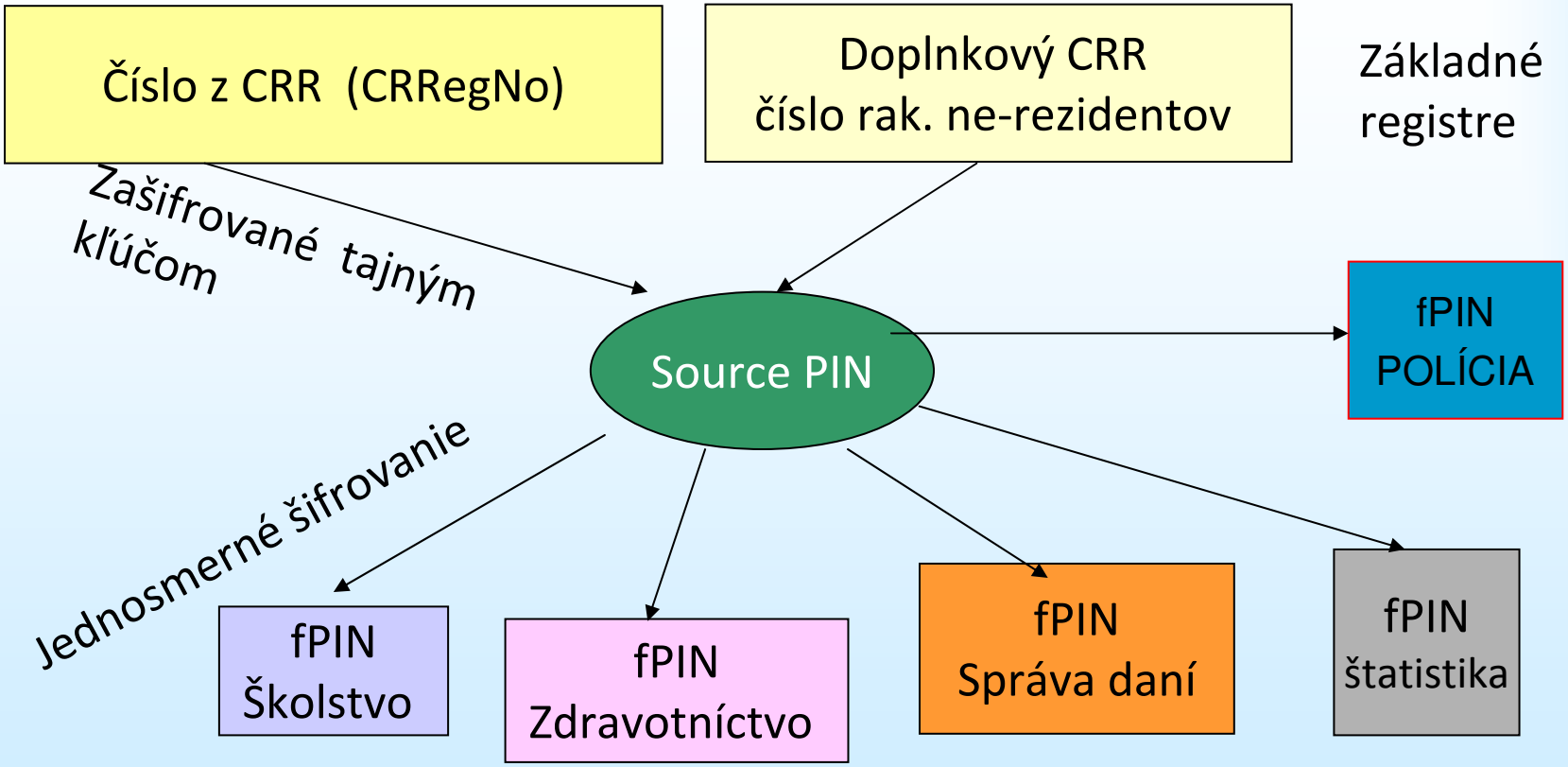
Každý obnčan- rezident má unikátne ID „ZMR-Zahl“ v CRR



Elektronická identita fyzických osôb

The Office for Personal Data Protection of the SLOVAK REPUBLIC

Fractional PIN = Sektor specific PIN (fPIN) je **≥128 ASCII ZN.**



Kde je bezpečnosť ?

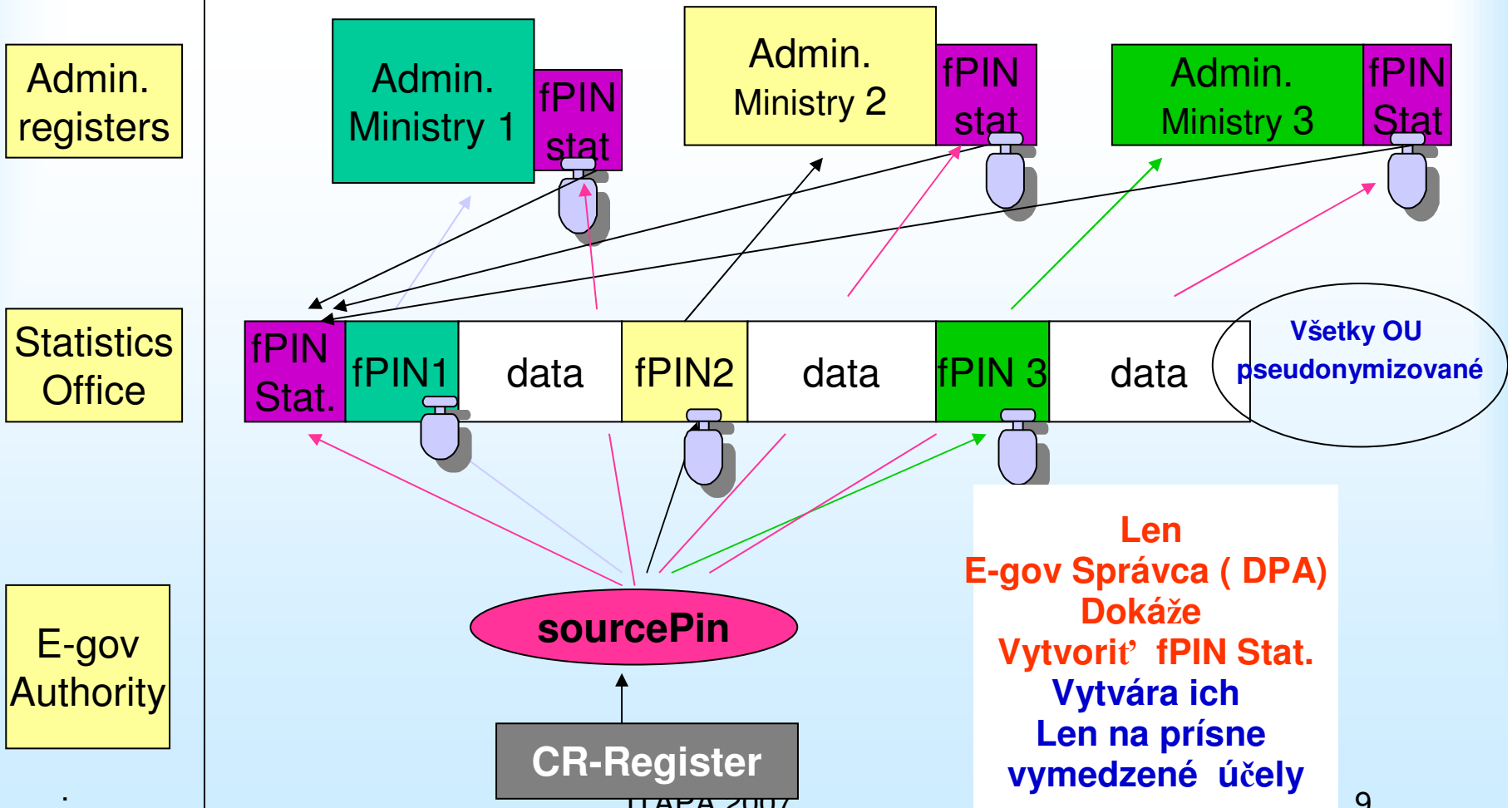
- Každý občan má unikátny systém PINov :
  - 1Source PIN + veľa fPINs + SV-number + (pssPINs) + e-signature (+ PIN občianskej karty- napr. 7854)

- Každý ssPINs sa vymaže po ukončení transakcie (nie je nikdy uchovaný v otvorenej forme ale iba v zašifrovanej forme ffPIN daného Sektora „s“)
- Každý občan má viac ako 20 úplne rôznych a e-IDS = fPINov v e- governmente ktoré sú odvodené z jediného Source PIN :
  - Kto dokáže „kraknúť“ v SR viac ako 100 miliónov úplne odlišných eIDs aby sa dostal ku kompletným OU v celom e- goverment systéme ? Keď krakne 1 fPIN , dostane sa k údajom jedinej osoby prislúchajúcim jedinému ministerstvu

- Ako používať tak veľa eID=ssPINov? Je vôbec možné manažovať ich? – ÁNO – a celkom jednoducho
  - Netreba ich uchovávať všetky , sektor uchováva len svoje v zašifrovabnej forme, možno ich kedykoľvek vypočítať z Source PIN keď treba avšak iba autorizovaným subjektom
  - Vždy sa uchovávajú len v zašifrovanej forme ffPIN
- Ak nesmú byť fPINy uchované v odkrytej forme, iba zašifrovanej forme ffPINov aj keď ich niekto ukradne, nič z nich nemá!

- Je vôbec možné využívať informáciu z viacerých rôznych subsystémov rakúskeho e-gov pri tak obrovskom počte ssPINov? ÁNO – a celkom jednoducho =>

Spájanie databáz na sčítanie ľudu/štatistiky v Rakúsku



Biometrické šifrovanie
Biometric Encryption – BE

Môže byť riadenie prístupov ešte bezpečnejšie?

Áno – pomocou technológie biometrického šifrovania riadenia prístupov - dodatočnej BE verifikácie užívateľa

Základná charakteristika užitočnej biometrie

- Ak biologická , psychologická, alebo iná neopakovateľná charakteristika jednotlivca má nasledovné vlastnosti...
  - Má ju každá osoba
  - Je pre každého unikátna -
  - Je stála – nemí sa s časom -
  - Je čitateľná – lacné čítačky

….Potom môže slúžiť ako spoľahlivý biometrický údaj pre danú aplikáciu.

ALE – akékoľvek reálne biometrické údaje sa môžu odcudziť , alebo zneužiť , a pritom dotknutá osoba nemôže zmeniť svoj biometrický údaj, ak treba, podobne ako PIN

Príklady využitia biometrie :

- Hraničná kontrola
- Prevencia podvodov a závažnej kriminality , detektívne služby a súdne lekárstvo
- Záznam kontroly vstupov
- Platobné systémy
- **Riadenie vstupov :**

ALE – akékoľvek reálne biometrické údaje sa môžu odcudziť , alebo zneužiť , a pritom dotknutá osoba nemôže zmeniť svoj biometrický údaj, ak treba, podobne ako PIN

Prečo biometrické šifrovanie BE?

Je všeobecne známe, že priame použitie biometrických údajov, alebo ich priamych vzorov (templates) je extrémne zraniteľné

- Napríklad v r. 2006, Európsky splnomocnenec pre ochranu osobných údajov (EDPS) Peter Hustinx varoval, vo svojom oficiálnom stanovisku, o rizikách vzhľadom na ochranu súkromia pre priame použitie biometrických údajov, alebo ich vzorov na účel indexov, alebo kľúčov k vzájomne interoperabilným databázam
- **atď.**

Odpoveď : Technológia biometrického šifrovania (Biometric Encryption – BE Technology) nepoužíva priame obrazy biometrických údajov , alebo ich priame vzory (templates) – ani pre prístupové systémy a ani verifikáciu osôb. Tieto nie sú ani nikde zaznamenané a je tiež skoro nemožné ich spätne vypočítať z údajov, ktoré sa skutočne používajú a uchovávajú

Základná informácia o technológii biometrického šifrovania vrátane citácií študijnej literatúry je dostupná v nasledovnej práci :

http://www.eubiometricsforum.com/dmdocuments2/WhitePaperBiometricEncryptionOntario.pdf

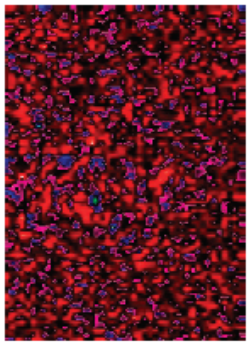
.

Daniel Valentovic

12 November 2007

Biometric Encryption:

A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy

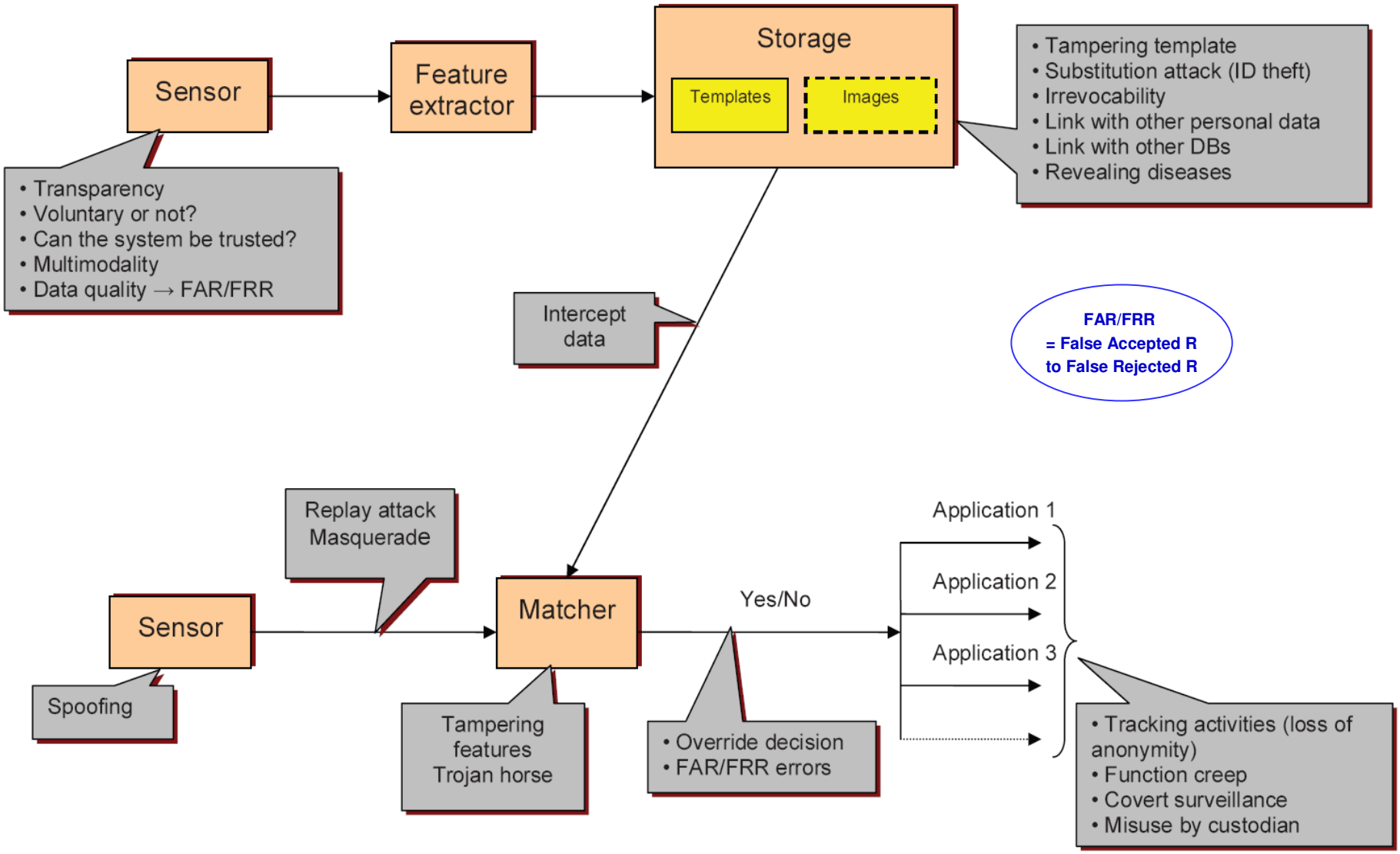


Ann Cavoukian, Ph.D.
Information and Privacy Commissioner/Ontario

Alex Stoianov, Ph.D.
Biometrics Scientist

March 2007

Riadenie prístupu do systémov
Klasická biometria



Bezpečnostná zraniteľnosť klasického biometrického systému používajúceho originálne biometrické údaje , alebo ich priame vzory

- **Spoofing:** falošné modely odtlačkov prstov, tváre, alebo obrazu dúhovky , atď .
- **Replay attacks**: napr. vstup pripraveného sfalšovaného obrazu
- **Substitution attack:** prepísanie vzoru autorizovanej osoby biometrickým vzorom útočníka – ukradnutie identity .
- **Tampering:** vzory môžu byť pozmenené tak, že sa obdržia vysoké overovacie skóre zhody bez ohľadu na to , aký obrázok sa predloží systému.
- **Masquerade attack:** digitálny "artefact" obrazu vytvorený z „ukradnutého" vzoru odtlačku prstu, tak, aby artefakt vyprodukoval zhodu overovacieho skóre.
- **Trojan horse attacks:** Niektoré časti systému , napríklad overovač „matcher" , sa nahradia trójskym koňom, ktorý vždy vyrobí zhodu overovacieho skóre
- **Overriding Yes/No response:** obídenie biometrickej časti a generovanie odpovedi „áno = zhoda"
- **Nedostatočná presnosť** : FRR aj FAR. Vysoké FRR spôsobia nepohodu užívateľov a systém sa často nastaví na nízky prah kvality
- Atď.

Ako funguje biometrické šifrovanie (Biometric Encryption BE)

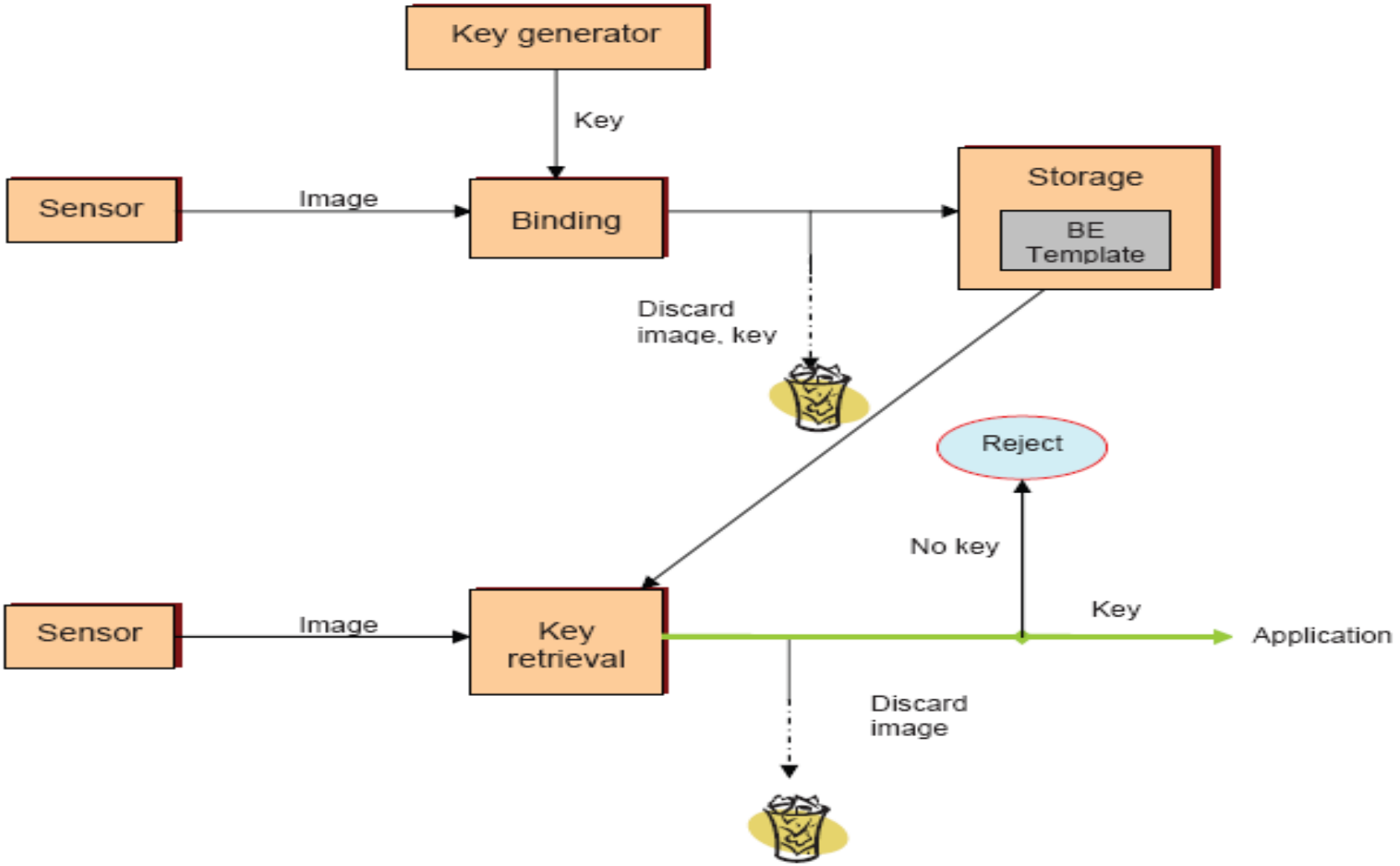
PRINCÍP riadenia prístupov

- Biometric Encryption BE je proces , ktorý bezpečne zviaže PIN , alebo kryptovací/digitálny kľúč s biometrickým údajom tak ,aby
  - Ani kľúč, ani biometrický údaj nemohli byť obnovené z uloženého biometricky zašifrovaného obrazu (BE template)
  - Kľúč môže byť znovu obnovený len po predložení príslušnej biometrickej vzorky v procese verifikácie užívateľa.
  - Digitálny kľúč (password, PIN, kraptovací kľúč, atď.) je náhodne generovaný pri zápise (enrolment) , tak, že užívateľ (ani ktokoľvek iný) ho nepozná.
  - V princípe je digitálny kľúč zašifrovaný biometrickým údajom.
  - Kľúč samotný je úplne nezávislý od biometrického údaja, preto môže byť vždy zmenený, alebo aktualizovaný
  - Po obdržaní biometrického vzoru BE algoritmus bezpečne a konzistentne priviaže kľúč k biometrickému údaju , aby vytvoril chránený BE vzor (BE template) , tiež zvaný (privátny vzor - private template)
  - BE template sa môže uchovať v DB, alebo aj lokálne (smart card, token, laptop, mob. telefón, atď.).
  - **Na konci zápisu (enrolment) sa biometrický údaj aj digitálny kľúč zničia (vymažú).**
- **Pri verifikácii,** užívateľ poskytne svoju čerstvú biometrickú vzorku, ktorá:
  - Keď sa aplikuje na BE template, umožní BE algoritmu znovu získať správny- ten istý kľúč key/password. Teda Biometrický údaj slúži ako *dešifrovací kľúč.*
  - **Na konci verifikácie, sa biometrická vzorka znovu zničí (vymaže)**
- Samozrejme je technologickou výzvou urobiť taký systém - niektorí dodávatelia dodávajú systém riadenia prístupov typu - **Biometric Encryption BE**

Biometrické šifrovanie
Biometric Encryption – BE

- Iné pojmy používané na BE:
  - biometric cryptosystem,
  - private template,
  - fuzzy commitment scheme,
  - fuzzy vault,
  - fuzzy extractor,
  - secure sketch,
  - biometric locking,
  - biometric key binding,
  - biometric key generation,
  - virtual PIN,
  - Biometrically hardened passwords,
  - biometric signature,
  - BioHashing.

Riadenie prístupu do systémov
Biometrické šifrovanie BE



	Klasická biometria : **Bezpečnosť a ochrana osobných údajov**	**Biometrické šifrovanie :** **Bezpečnosť a ochrana osobných údajov**
1	Uchovaný biometrický vzor je unikátny identifikátor pre danú osobu	Neexistuje tu tradičný biometrický vzor, preto z neho nemôže byť priradený identifikátor pre konkrétnu osobu (str 16, 17, kniha : A. Cavoukian a A. Stojanov : **Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy**)
2	Následné použitie biometrického vzoru (unikátny identifikátor) je možné na prístup (logovanie)k transakciám, ak sa biometria stane široko rozšírenou.	Bez unikátneho identifikátora sa transakcie nemôžu zbierať ani priradiť konkrétnej osobe (str. 17, 25)
3	Prezradená databáza osôb a ich biometrických údajov, alebo ich vzorov ovplyvní kvalitu ochrany súkromia ich všetkých	Žiadne veľké DB biometrických údajov sa netvoria, tvoria sa len databázy biometricky zašifrovaných kľúčov. Ak sa jedná o vyzradenie tak len jediného kľúča naraz. (str. 23)
4	Ochrana súkromia a bezpečnosť sa nedá zaručiť .	Ochrana súkromia a bezpečnosť (vrátane osobných údajov) sa ľahko dosiahne .(str. 17-20, 26-28)
5	Klasická biometria nemôže dosiahnuť vysokú úroveň bezpečnosti procesov „výzva-odpoveď“	Bezpečnosť procesov „výzva-odpoveď“ je ľahko dosiahnuteľnou voľbou . (str. 26-28)

	Klasická biometria : **Bezpečnosť a ochrana osobných údajov**	**Biometrické šifrovanie (BE) :** **Bezpečnosť a ochrana osobných údajov**
6	Biometrické údaje len nepriamo chrániť súkromie osôb (osobných informácií a údajov) vo veľkých súkromných , alebo štátnych databázach.	BE môže umožniť vytvorenie privátnych a vysoko bezpečných databázových štruktúr akronymov pre profesionálne IS založené na privátnych alebo štátnych databázach. (str. 19, 20, 27)
7	*1:veľa* identifikačné systémy trpia vážnymi dopadmi na ochranu súkromia, ak je databáza prezradená.	*1:veľa* Identifikačné systémy sú aj privátne (cudzí sa nedostane k osobným informáciám) aj bezpečné. (str. 17, 20)
8	Biometrické údaje ,alebo ich vzory užívateľa môžu byť ľahko nahradené falošnými ak dôjde k prelomeniu ochrany systému, ukradnutiu účtu, alebo jeho zneužitiu	Biometricky zašifrované identifikátory sa môžu zrušiť a nové vytvoriť v prípade že dôjde k prelomeniu ochrany systému, ukradnutiu účtu, alebo jeho zneužitiu. (str. 17)
9	Biometrický systém je zraniteľný potenciálnymi útokmi.	BE systém je odolný (obnoviteľný) voči mnohým známym útokom. (str. 18)
10	Agregovanie údajov	Minimalizácia údajov (str. 17)

Záver

- BE technológia (biometrického šifrovania) prístupového manažmentu je spoľahlivá a bezpečná a môže výrazným spôsobom zvýšiť bezpečnosť prístupu k E- gov , e- health ...
  - Môže sa zavádzať po krokoch:
    - Zvýšenie bezpečnosti pre prístup do veľkých systémov – napr. e- gov pre chránené osoby (napr. členov vlád, osoby čo si priplatia za bezpečnosť...)
    - Prístup cez štátne úradovne napr. magistráty, políciu , atď. do niektorých podsystémov (napr. registra trestov, cez lekárske ambulancie do e-health)
    - Povinné použitie, ak tak bude požadovať zákon a budú zdroje na realizáciu
- Technológia biometrického šifrovania BE je podporovaná úradmi na ochranu osobných údajov , lebo môže výrazne zvýšiť ochranu osobných údajov občanov.

Ďakujem za pozornosť