1. Úvod do biometrických systémů

➔Slovo „Biometrie“

➔Původem z řečtiny

➔Složenina ze slov „*bios*“ a „*metron*“

➔Slovo „*bios*“ = život

➔Slovo „*metron*“ = měřítko

➔V IT oblasti = systém či postup k rozpoznávání vzorů

➔V oboru medicíny jiný význam

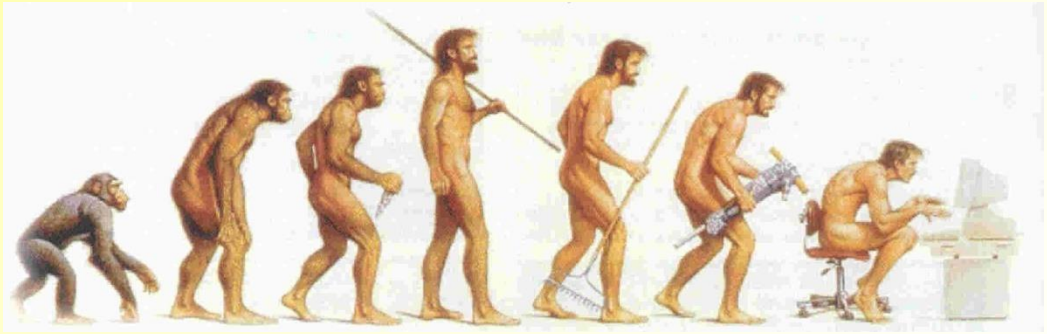
➔Trocha historie

➔Používání biometrických vlastností známo již dávno

➔Dochované informace např. z Číny ze 14. století

➔Denně používáme biometrickou identifikaci:

- ➔Rozpoznávání obličeje
- ➔Rozpoznávání hlasu
- ➔...



➔Biometrické postupy kolem roku 1900 (I.)

➔1858 - **W.J. Herschel** - Koloniální úředník v Indii

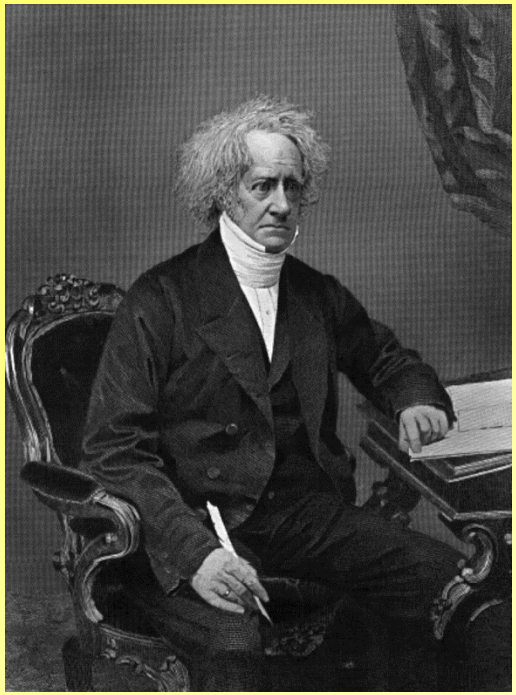
➔1865 - **Francis Galton** - Studie o dědičnosti fyzických vlastností („*Hereditary talent and character*“)

➔1869 - **Francis Galton** - Spoluzakladatel eugeniky (Nauka o dědičných chorobách)

➔1875 - **Francis Galton** - Zakladatel výzkumu dvojčat

➔1880 - **Francis Galton** - Zavedení antropometrie

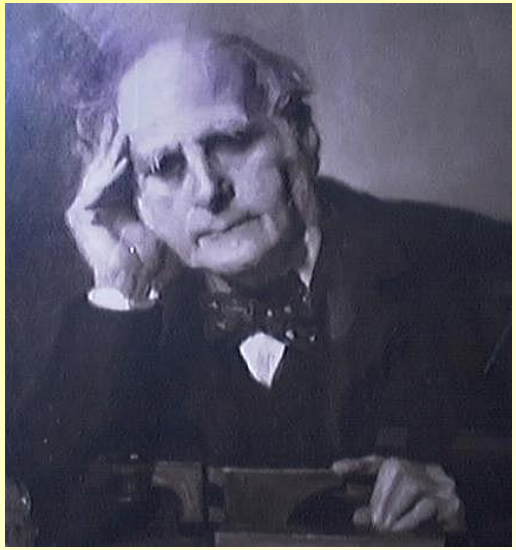
➔Biometrické postupy kolem roku 1900 (II.)



← W.J. Herschel

Otisky prstů ➔

Francise Galtona



← F. Galton

Daktyloskop. ➔

kufřík (1902)

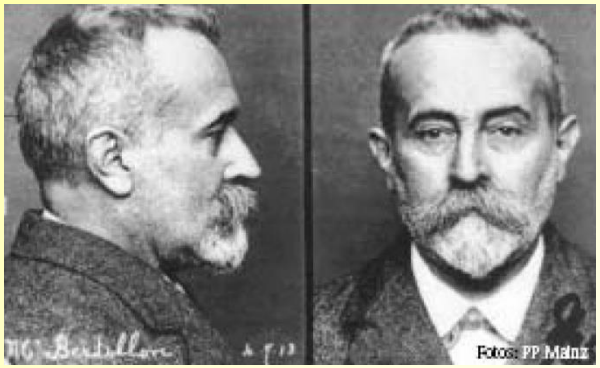
➔Biometrické postupy kolem roku 1900 (III.)

➔1896 - Zavedení daktyloskopie jako identifikačního systému v Argentině

➔1900 - **Francis Galton** - Prosazení daktyloskopie

- ➔Neměnnost a jedinečnost reliéfů kůže na prstech
- ➔1892 - Kniha „*Fingerprints*“
- ➔1893 - Porovnání daktyloskopie s antropometrií
- ➔1894 - Výsledek: Obě metody doporučeny
- ➔Zavedení do policejní služby

➔Biometrické postupy kolem roku 1900 (IV.)



- ➔**Alphonse Bertillon** (1853 - 1914)
  - ➔Zavedl Bertillionáž
  - ➔První použití 1879 - 1882
- ➔Základy antropometrie = Bertillionáž
  - ➔Po 20. roku života zůstávají tělesné rozměry neměnné
  - ➔S vyšším počtem korektně změřených rozměrů těla klesá riziko záměny osob
  - ➔Měřením a registrováním tělesných rozměrů je možné osobu jednoznačně identifikovat
  - ➔Pro měření použito 11 tělesných rozměrů

➔Antropometrie = Bertillionáž (I.)

1. Tělesná výška
2. Délka natažené paže
3. Výška v sedu
4. Délka hlavy
5. Šířka hlavy

6a. Délka pravého ucha

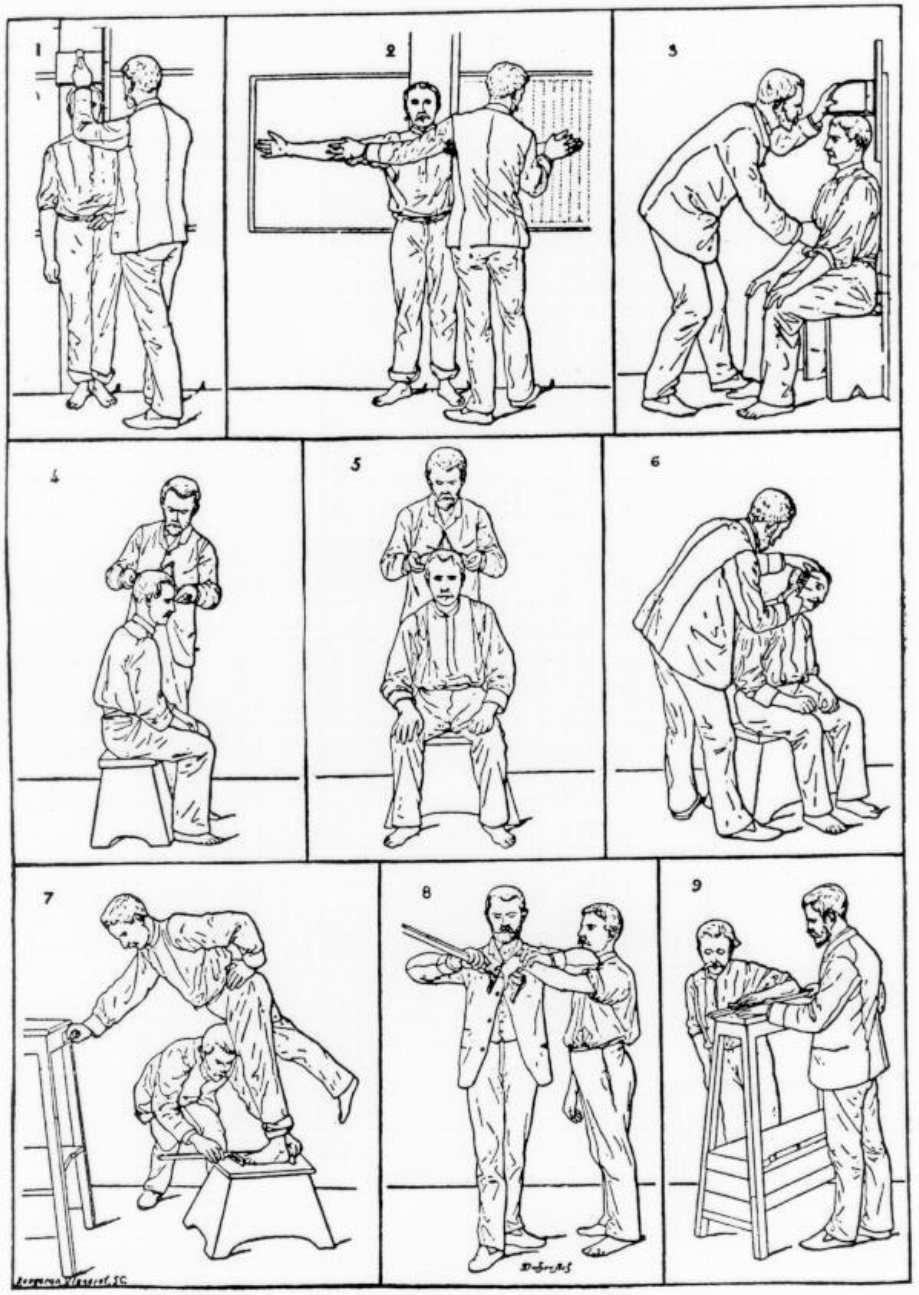
6b. Šířka pravého ucha

7. Délka levé nohy

8a. Délka lev. prostředníčku

8b. Délka levého malíčku

9. Délka levého předloktí



➔Antropometrie = Bertillionáž (II.)

Bertillon Measurements.

Height,	Head length,		L. Foot.
Outer Arms,	Head width,		L. Mid. F.
Trunk,	R. Ear.	Length,	L. L. F.
		Cheek,	L. Fore A.

Name .....
Alias .....
Alias .....
Crime .....
Age ..... Height .....
Weight ..... Build .....
Hair ..... Eyes .....
Born ..... Beard .....
Complexion .....
Occupation .....
Date of arrest .....
Officer .....

REMARKS.

St. L. Detect. Dept. St. Louis, Mo.

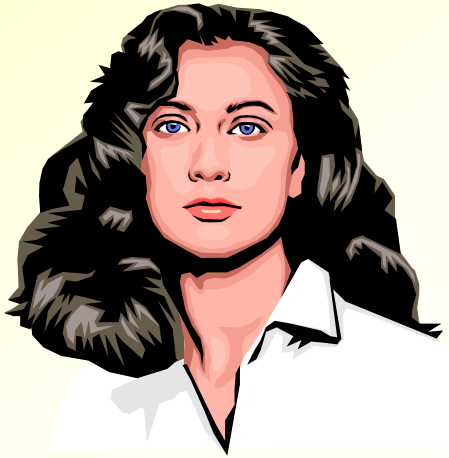
➔Novější éra

- ➔1924 - založení oddělení identifikace otisků u FBI
- ➔1965 - použití systému AFIS s 810 tisíci otisky prstů
- ➔1971 - první článek k rozpoznávání obličeje
- ➔Srpen 2018 - systém AFIS u FBI
  - ➔Celkem 61 miliónů desetic otisků prstů
  - ➔Průměrně 110 tisíc prohledávání denně
  - ➔Reakce na vyhledávání - přibližně 38 minut
- ➔Rok 2022 - systém AFIS u FBI (NGI)
  - ➔Celkem přes 81 miliónů desetic otisků prstů
  - ➔Průměrně 169 tisíc prohledávání denně
  - ➔Reakce na vyhledávání - 18 minut (non urgent)

➔Úvod do problematiky

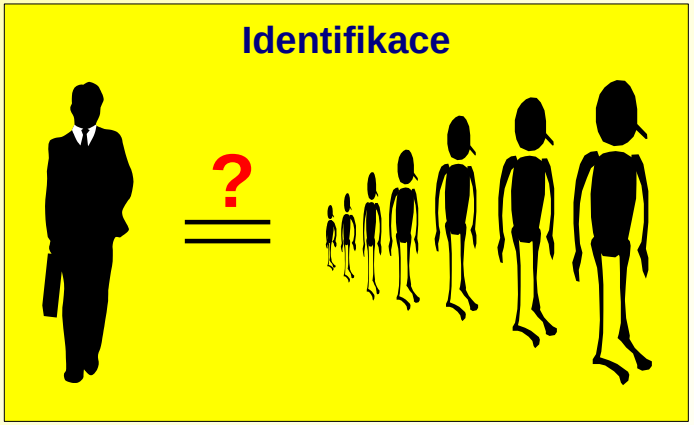
➔Lidé rozpoznávají u jiných automaticky:

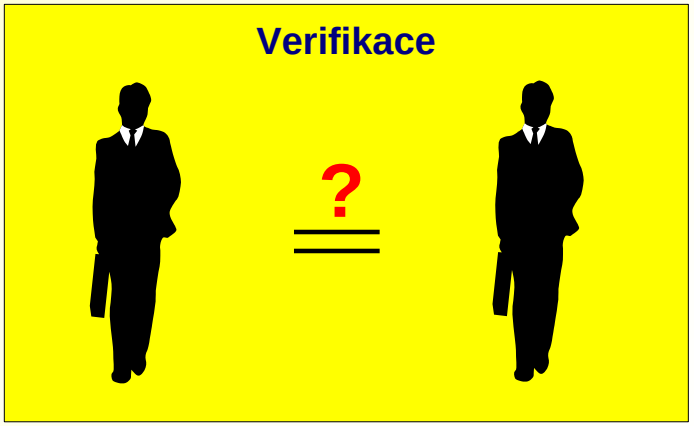
- ➔obličej,
- ➔postavu,
- ➔rty a jejich pohyby,
- ➔hlas a jeho intonaci se zabarvením,
- ➔pohyby, např. chůzi,
- ➔písmo a podpisy,
- ➔...



➔Identifikace vs. Verifikace

- **➔Identita**
  - ➔Rozlišovat fyzickou identitu od elektronické
- **➔Identifikace**
  - ➔Porovnání 1:N
- **➔Verifikace**
  - ➔Porovnání 1:1
- **➔Autentizace**
  - ➔Potvrzení identity
  - ➔Akt porovnání

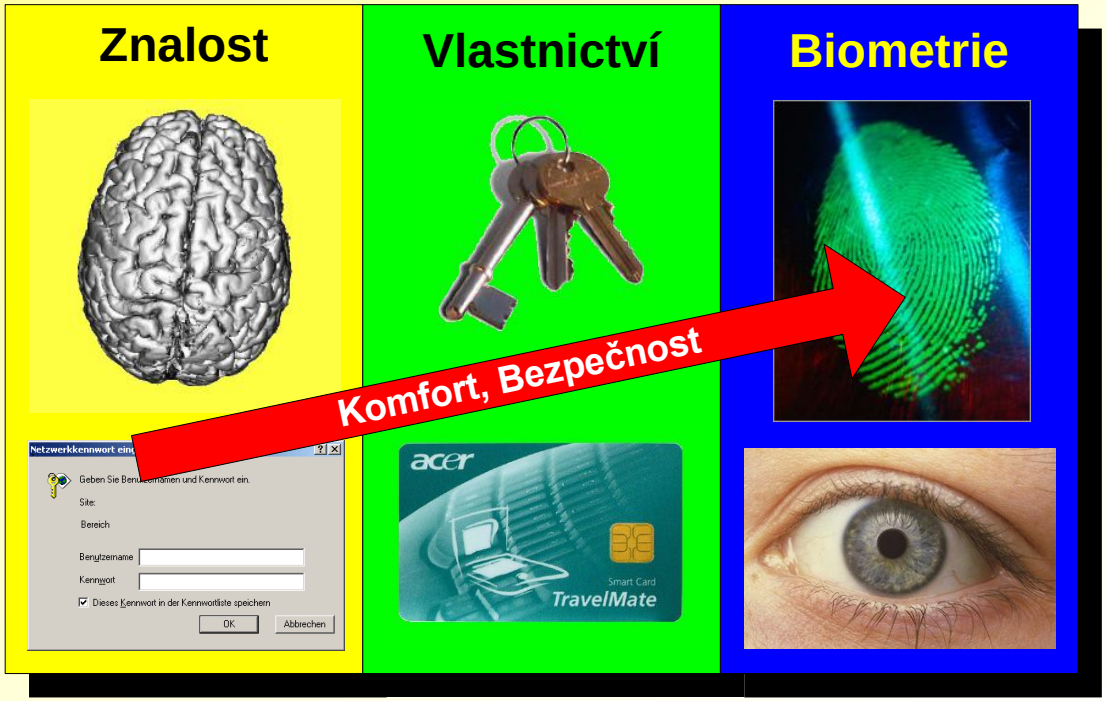




➔Identita (I.)

➔**Identita** je založena na

- ➔něčem co víme („*we know*“)
- ➔něčem co máme („*we have*“)
- ➔něčem co jsme („*we are*“)



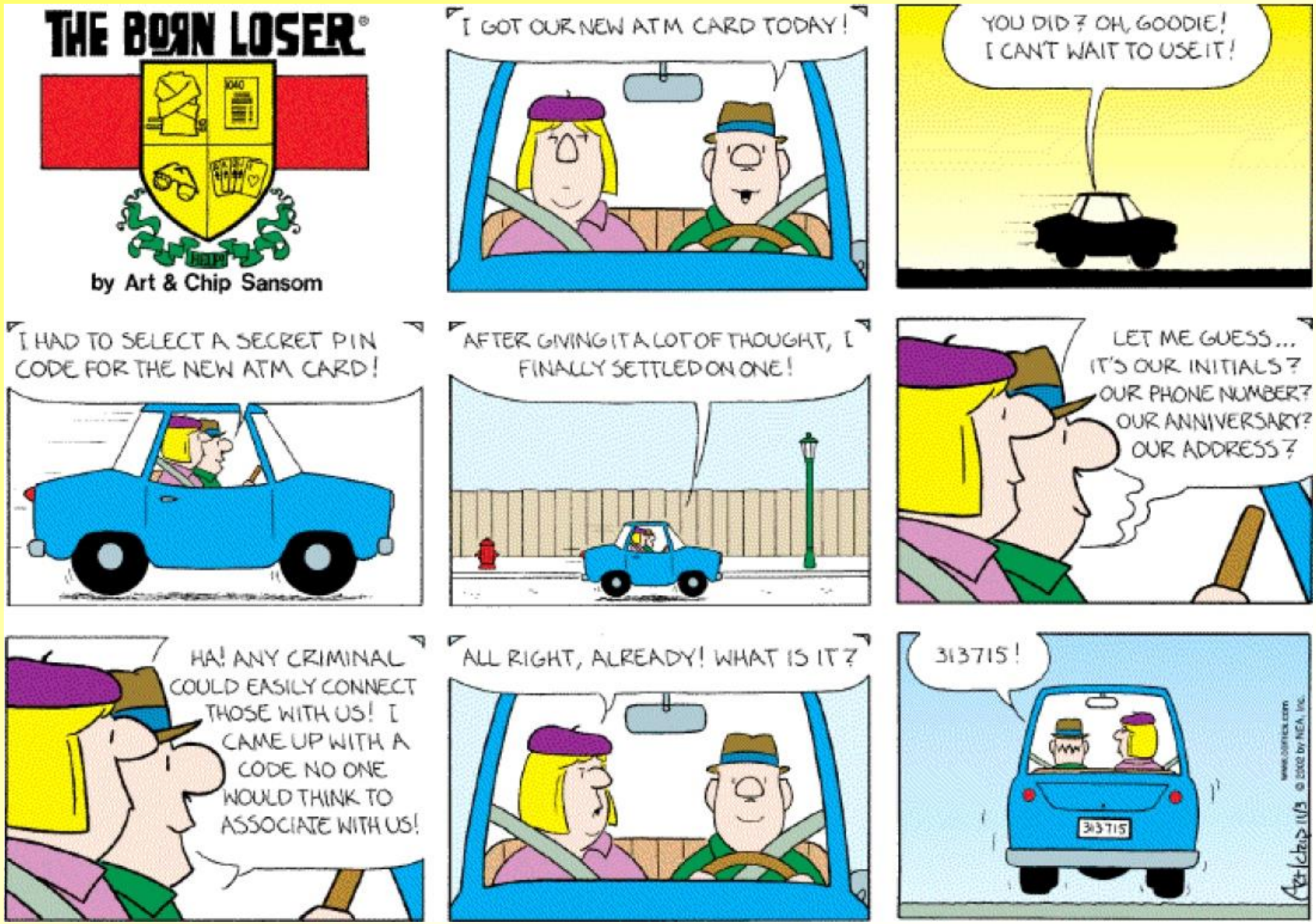
➔Identita (II.) - Něco co víme

- ➔Něco co víme
  - ➔Tajné tlačítko / páčka
  - ➔Předepsaný postup
  - ➔Heslo
  - ➔PIN

"Your logon password is XB#2D940. Write it down and don't lose it again."

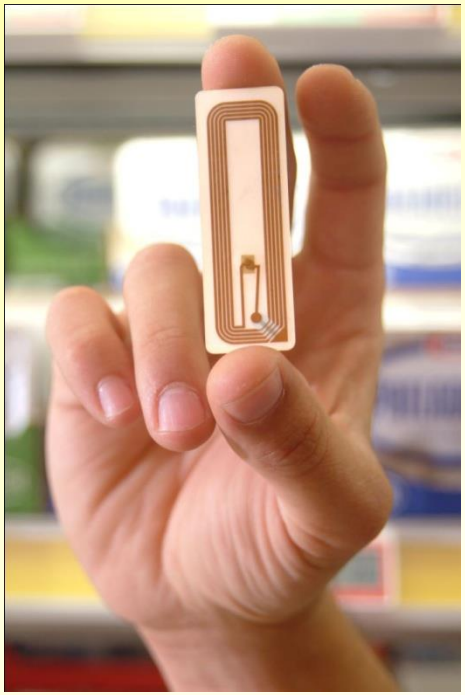
- ➔Idea: Náhodná a lehce zapamatovatelná informace.
- ➔Nebezpečí: Získání této tajné skutečnosti nepovolanou osobou.
  - ➔Slovníkový útok na alfanumerické heslo = 5,5 h.
  - ➔Slovníkový útok na libovolné heslo = 480 h.

➔Identita (III.) - Něco co víme



➔Identita (IV.) - Něco co máme

- ➔Něco co máme
  - ➔Klíč
  - ➔Čipovou (smart) kartu
  - ➔Token
  - ➔RFID-Tag



- ➔Idea: Vlastnictví něčeho, co jiný nemá.
- ➔Nebezpečí: Získání tohoto majetku nepovolanou osobou.
  - ➔Krádež (delší doba ke zjištění skutečnosti)
  - ➔Nelegální kopie / přečtení informací

➔Identita (V.) - Něco co jsme

- ➔Něco co jsme
  - ➔Vzhled
  - ➔Pohyby
  - ➔Chování
  - ➔Projevy v různých situacích

- ➔Idea: Sami jsme nositelem identifikačního klíče.
- ➔Nebezpečí: Použití falešné identity na základě kopie některé biometrické vlastnosti.
  - ➔Kopie otisku prstu ze sklenice v restauraci.
  - ➔Snímek fotografie obličeje z dovolené.

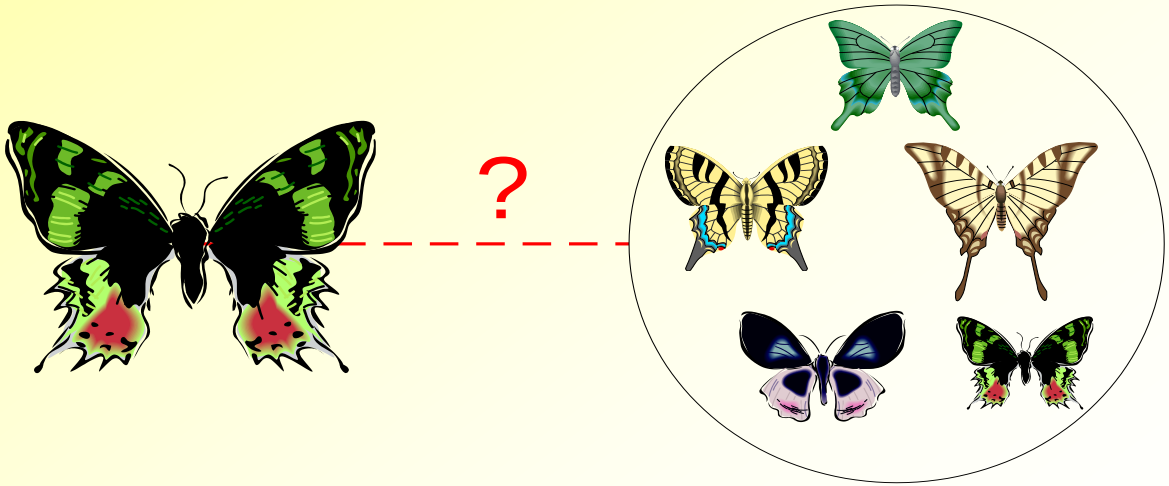
➔Identifikace

➔Porovnání aktuálního vzorku s celou databází referenčních dat (1:N nebo 1:Many).

➔Výsledek: Identita / Nenalezeno.

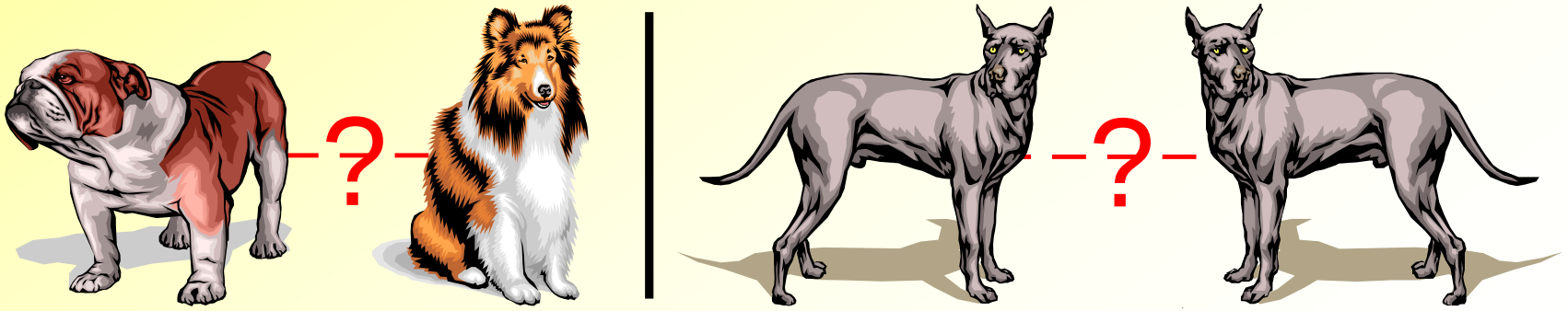
➔Příklady použití:

- ➔Daktyloskopické systémy - AFIS.
- ➔Databáze azylantů.
- ➔Registrace nových uživatelů.



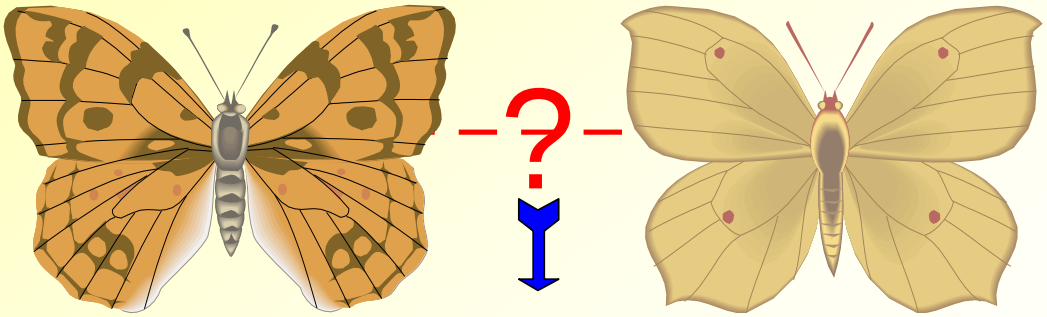
➔Verifikace

- ➔Porovnání aktuálního vzorku s jedním referenčním vzorkem (1:1).
- ➔Výsledek: Potvrzeno / Nepotvrzeno.
- ➔Příklady použití:
  - ➔Přístupové systémy.
  - ➔Databáze azylantů.
  - ➔E-Mailové služby.



➔Autentizace

- ➔Systém může potvrdit autentičnost (hodnověrnost) dané osoby.
- ➔Použití: Identifikace i Verifikace.
- ➔Příklady použití:
  - ➔Přístupové systémy.
  - ➔Daktyloskopické systémy.
- ➔Časté zaměňování verifikace a autentizace.



➔Problematika identity (I.)

- ➔V dřívějších dobách se lidé v menších komunitách znali mezi sebou.
- ➔S růstem populace a nárůstem mobility jsme se začali spoléhat na dokumenty a tajemství, které nám slouží k určení identity.
- ➔Identifikace (verifikace) osob je v současnosti hlavní částí infrastruktury v různých obchodních sektorech, jako např. bankovnictví, hraniční kontrola, právní záležitosti apod.
- ➔Otázky spojené s identitou individua:
  - ➔Je tato osoba skutečnou tou, za kterou se vydává?
  - ➔Byl tento žadatel u nás již někdy dříve?
  - ➔Má mít tento uživatel přístup k našemu systému?

➔Problematika identity (II.)

➔Žijeme nyní v globální společnosti, ve které se vyskytují všehoschopní a nebezpeční jedinci, kterým nemůžeme již věřit na základě předložených osobních dokladů (problematika falešné identity).

➔**Krádež identity** - „*Identity Theft*“

- ➔Zloději identity odcizí kreditní kartu
- ➔Zloději identity zjistí PIN (např. datum narození)
- ➔Zcizeným PINem provedou úspěšně autentizaci
- ➔A vyberou z bankomatu peníze
- ➔V roce 2017 celkem 16,7 mil. krádeží identity (USA) a způsobené škody ve výši 17 mld. USD
- ➔2008 až 2020 přes 11 mld. krádeží identity (USA)

➔Biometrie (I.)

➔Definice biometrie:

Biometrie (IT) je automatické rozpoznávání lidí na základě jejich charakteristických *anatomických rysů* (např. obličej, otisk prstu, duhovka, sítnice) a charakteristického *chování* (např. podpis, chůze).

➔Výhody:

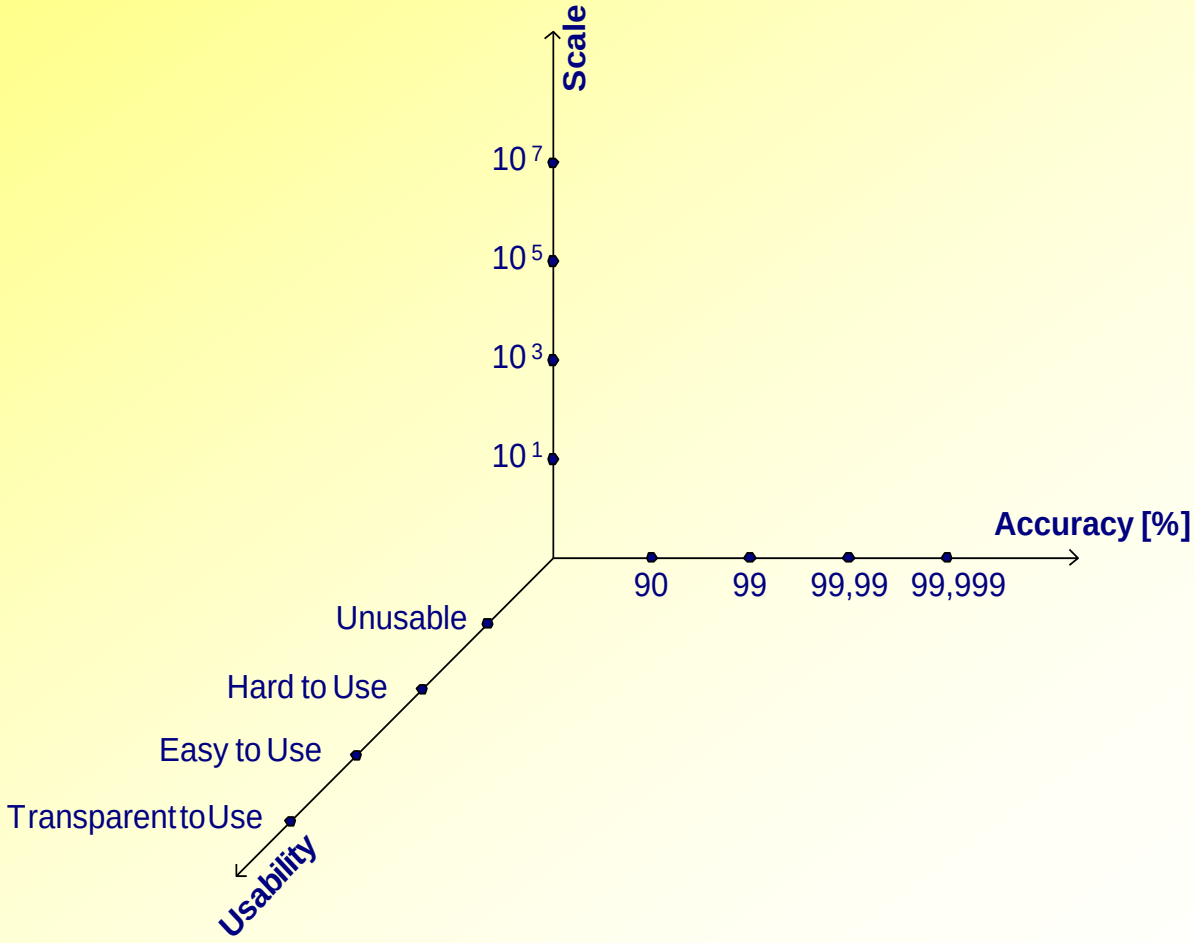
- ➔Odrazuje od podvodů
- ➔Zvyšuje bezpečnost
- ➔Nemůže být lehce přenesena či zapomenuta
- ➔Nemůže být ztracena či zkopírována
- ➔Eliminuje pokusy o popření identity
- ➔Zvyšuje pohodlí

➔Biometrie (II.)

- ➔Nevýhody:
  - ➔Výstupem je skóre porovnání („*matching score*“)
  - ➔Nemůže být anulována v případě prozrazení
  - ➔Samotný biometrický systém je napadnutelný
  - ➔Nezachovává soukromí
  - ➔Nutnost rozpoznávání živosti

➔Výzva pro biometrii

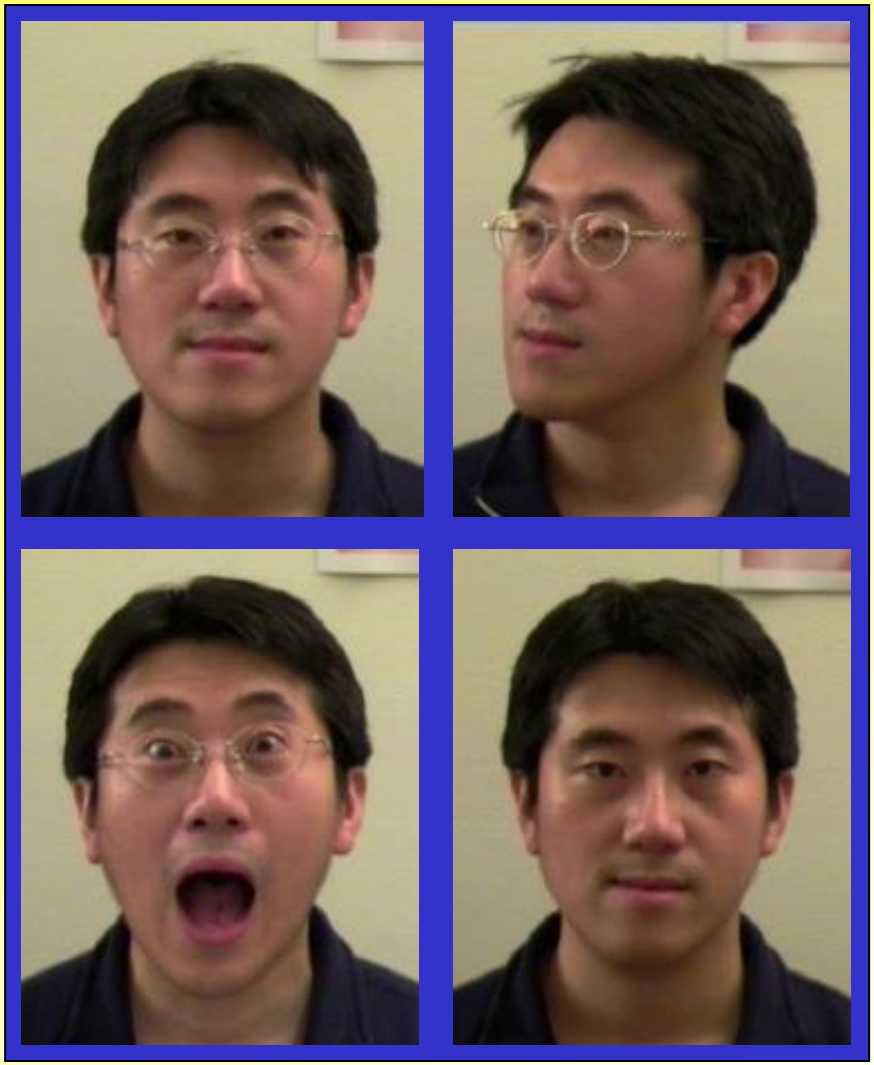
➔Hlavní výzvou pro biometrii je navrhnout biometrický systém, který pracuje souběžně na extrémech všech os níže uvedeného grafu.



➔Proč je biometrie složitá?

- ➔Mezitřídní a vnitrotřídní variabilita
- ➔Segmentace
- ➔Zašuměný vstup
- ➔Výkonnost systému (chyby, rychlost, náklady)
- ➔Jednoznačnost biometrické vlastnosti
- ➔Fúze více biometrických vlastností
- ➔Rozšiřitelnost
- ➔Útoky na biometrický systém
- ➔Otázky privátních dat

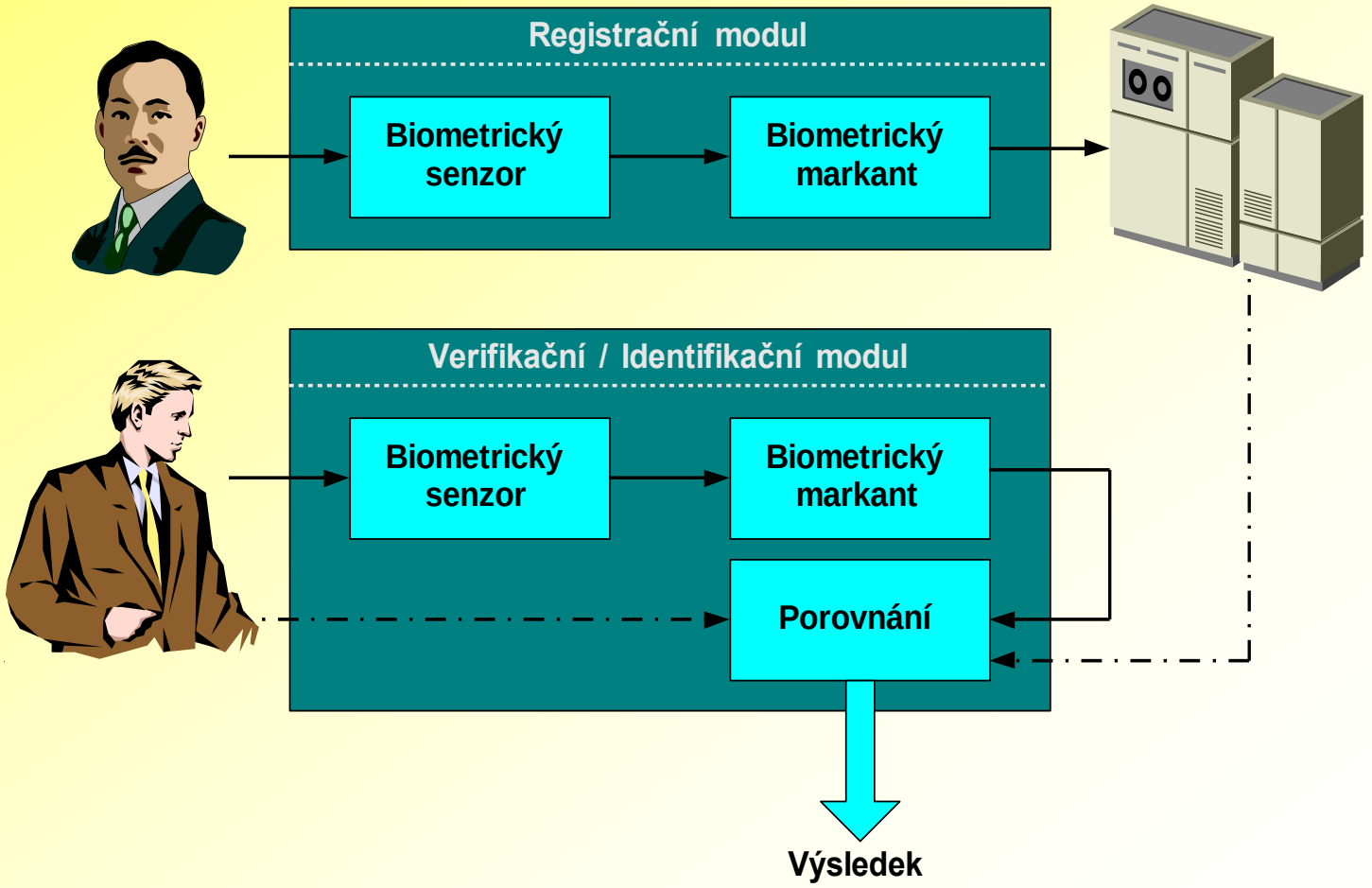
➔Mezitřídní a vnitrotřídní variabilita



➔Biometrický systém

➔Registrační modul - vložení identity uživatele

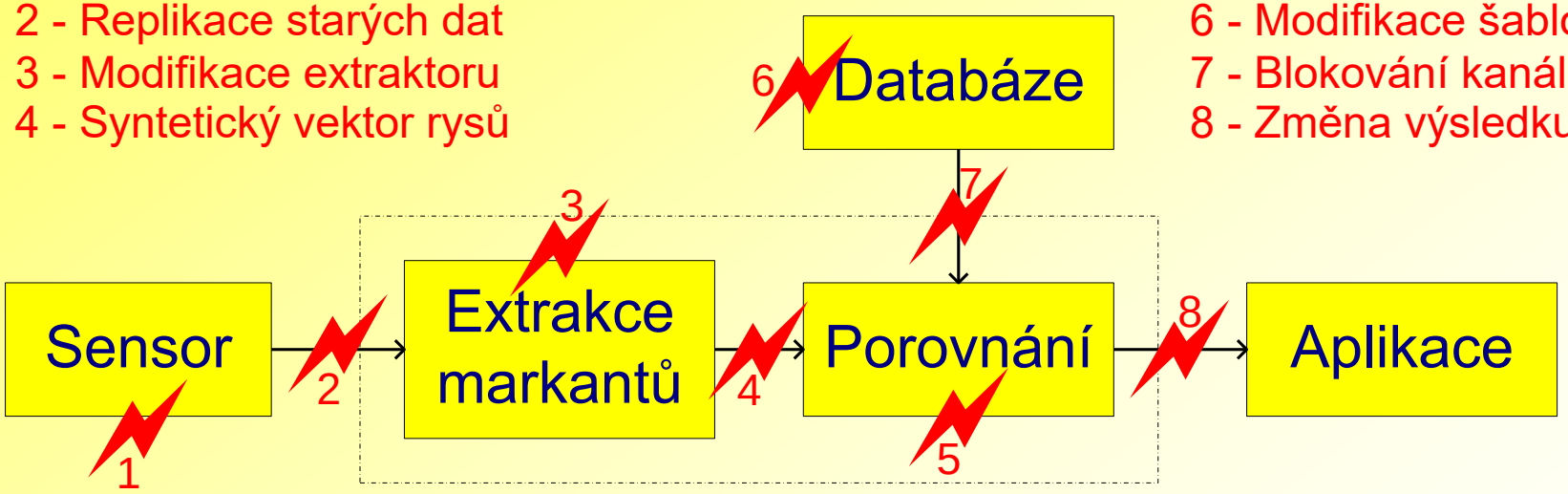
➔Verifikační / Identifikační modul



➔Slabá místa biometrického systému

1 - Podvrh biom. vlastnosti
2 - Replikace starých dat
3 - Modifikace extraktoru
4 - Syntetický vektor rysů

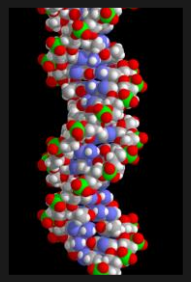
5 - Změna porovnání
6 - Modifikace šablony
7 - Blokování kanálu
8 - Změna výsledku



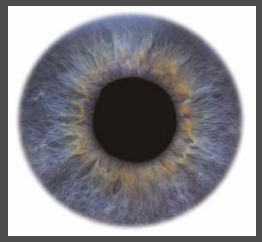
➔Příklad umělého otisku prstu

➔Detekce živosti „*Liveness Recognition*“

➔Biometrické vlastnosti (I.)


DNA

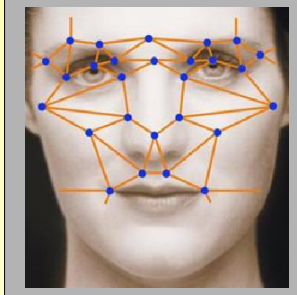
Otisk prstu


Duhovka

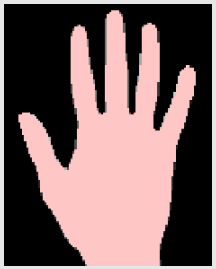
Sítnice

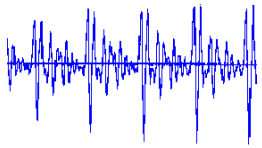
Termogram obličeje

Žíly ruky


Obličej

Podpis


Geometrie ruky


Hlas

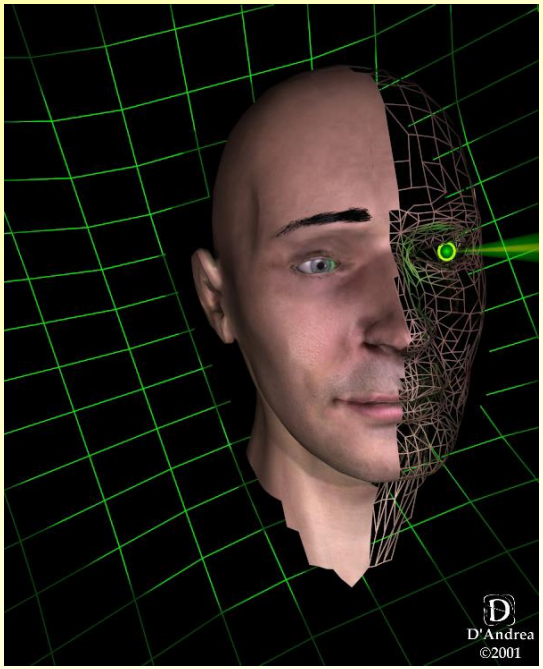
➔Biometrické vlastnosti (II.)

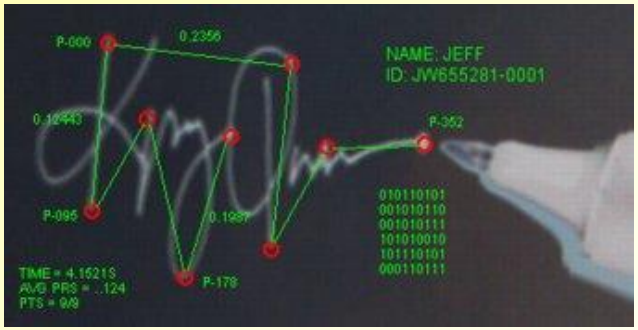
➔Anatomické (fyzické) vlastnosti:

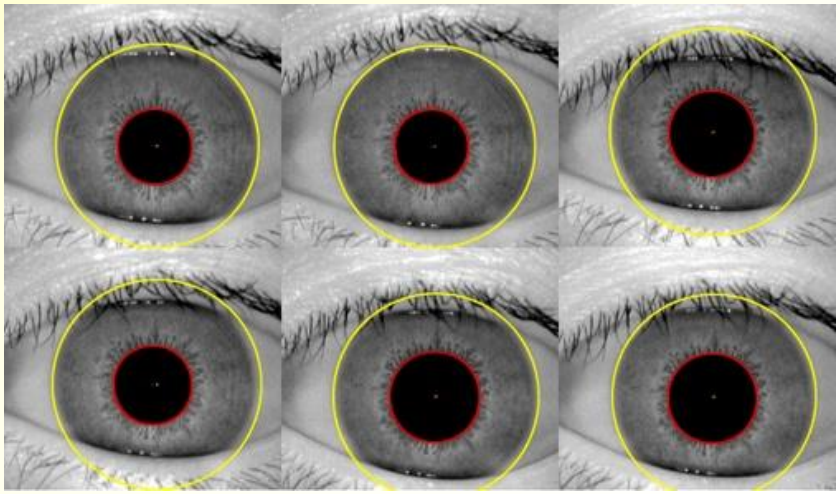
- ➔Otisk prstu
- ➔Obličej
- ➔Duhovka oka
- ➔Sítnice oka
- ➔Geometrie ruky
- ➔Dlaň
- ➔Termogram obličeje
- ➔Termogram ruky
- ➔Dentální obraz
- ➔Podpis
- ➔Tvar ucha
- ➔Snímek nehtu
- ➔DNA

➔Biometrické vlastnosti (III.)

- ➔Dynamické vlastnosti (chování):
  - ➔Hlas / Řeč
  - ➔Gestikulace obličeje
  - ➔Podpis (dynamika)
  - ➔Dynamika stisku kláves
  - ➔Pohyby rtů
  - ➔Chůze
  - ➔*Zužování duhovky*

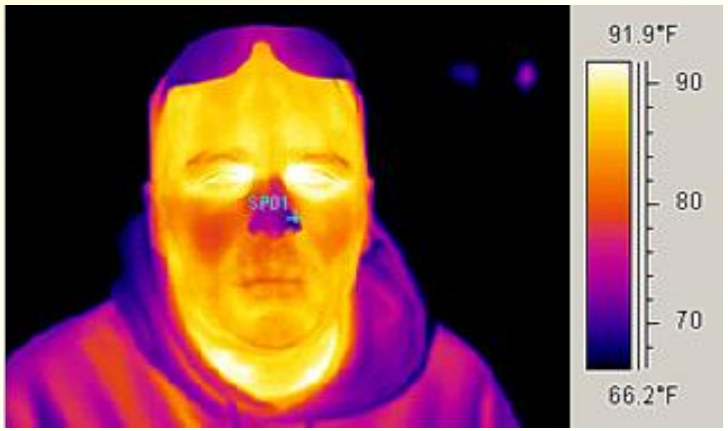






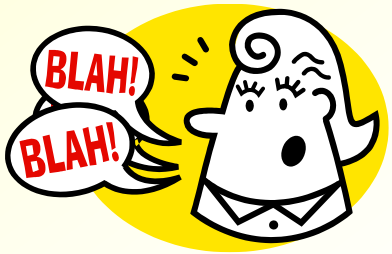
➔Anatomické (fyzické) vlastnosti

- ➔Jeden pevný rys = biometrická vlastnost
- ➔Vlastnost vždy přítomna, nezávisle na akci uživatele
- ➔Biometrická metoda se nazývá „*Statická metoda*“
- ➔Příklady:
  - ➔Otisk prstu
  - ➔Obraz obličeje
  - ➔Měření geometrie ruky
  - ➔Obraz duhovky oka
  - ➔Termogram obličeje
  - ➔Obraz sítnice oka
  - ➔DNA



➔Dynamické vlastnosti

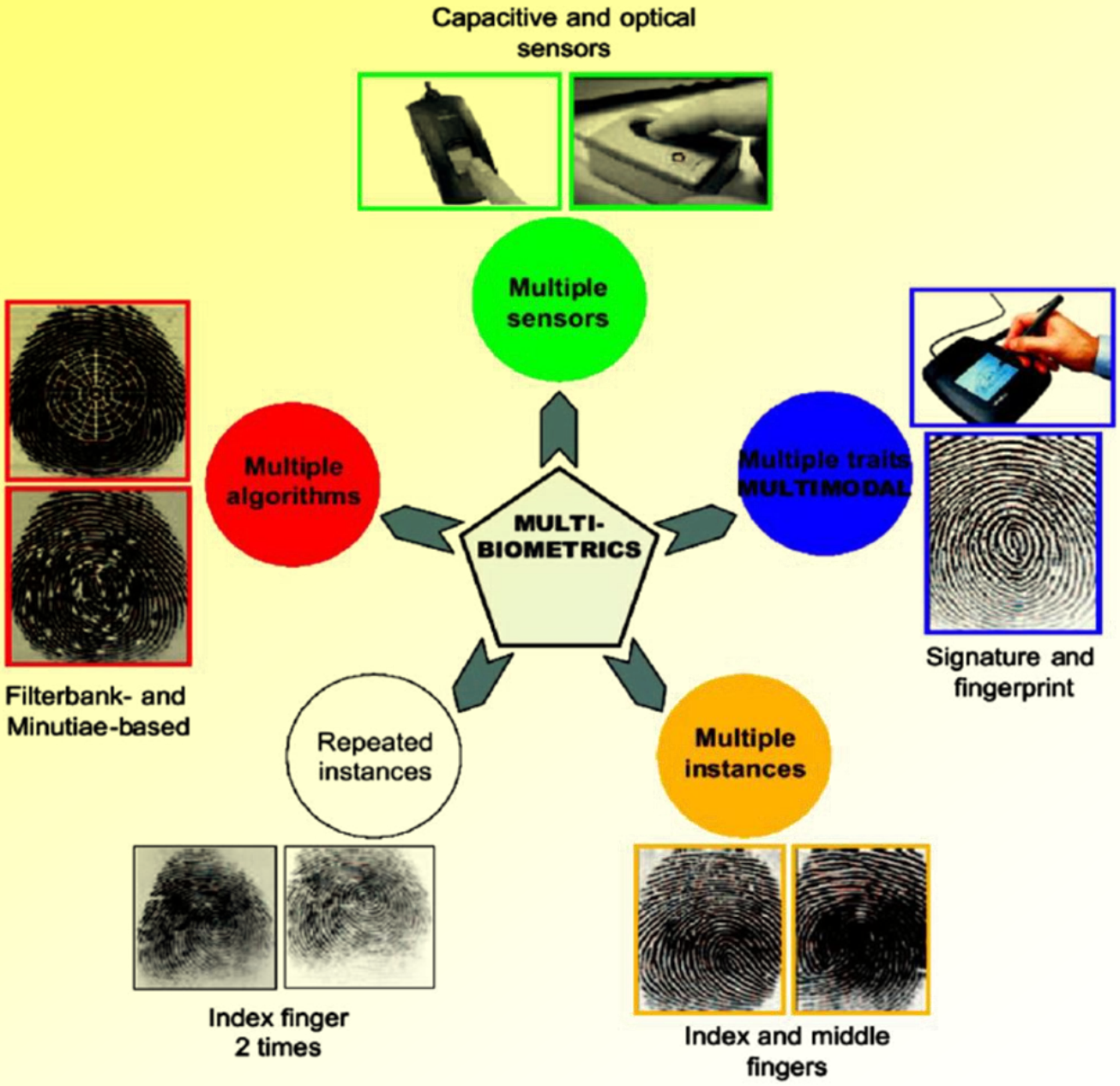
- ➔Pouze ve spojení s nějakou akcí uživatele
- ➔Nazývané též „*vlastnosti chování*“
- ➔Biometrická metoda se nazývá „*Dynamická metoda*“
- ➔Každé nasnímání může vést k naprosto odlišné sadě biometrických vzorků
- ➔Příklady:
  - ➔Rozpoznání mluvčího
  - ➔Dynamika podpisu
  - ➔Dynamika stisku kláves
  - ➔Pohyby rtů
  - ➔Chůze



➔Kombinování biometrických vlastností (I.)

- ➔Unimodální biometrický systém
  - ➔Používá pouze 1 biometrickou vlastnost
  - ➔Nižší spolehlivost
- ➔Multimodální biometrický systém
  - ➔Použití buď více příznaků jedné vlastnosti
    - ➔Statické a dynamické vlastnosti podpisu
  - ➔Použití více biometrických vlastností
    - ➔Rozpoznávání obličeje v kombinaci s duhovkou
  - ➔Zvýšení spolehlivosti rozpoznání
  - ➔Více robustní vůči falšování a pokusům o útok
  - ➔Vyšší časové nároky a nároky na systém

➔Kombinování biometrických vlastností (II.)



➔Biometrické aplikace

Forenzní	Vládní	Komerční
Identifikace mrtvol	Národní ID karty	ATM – bankomaty
Krim. vyšetřování	Řidičský průkaz Registrace voličů	Kontrola přístupu Počítačový login
Určení rodičovství	Sociální dávky	Mobilní telefony
Ztracené děti	Hraniční kontroly	e-Komerce Smart karty

„Chytrá zbraň“

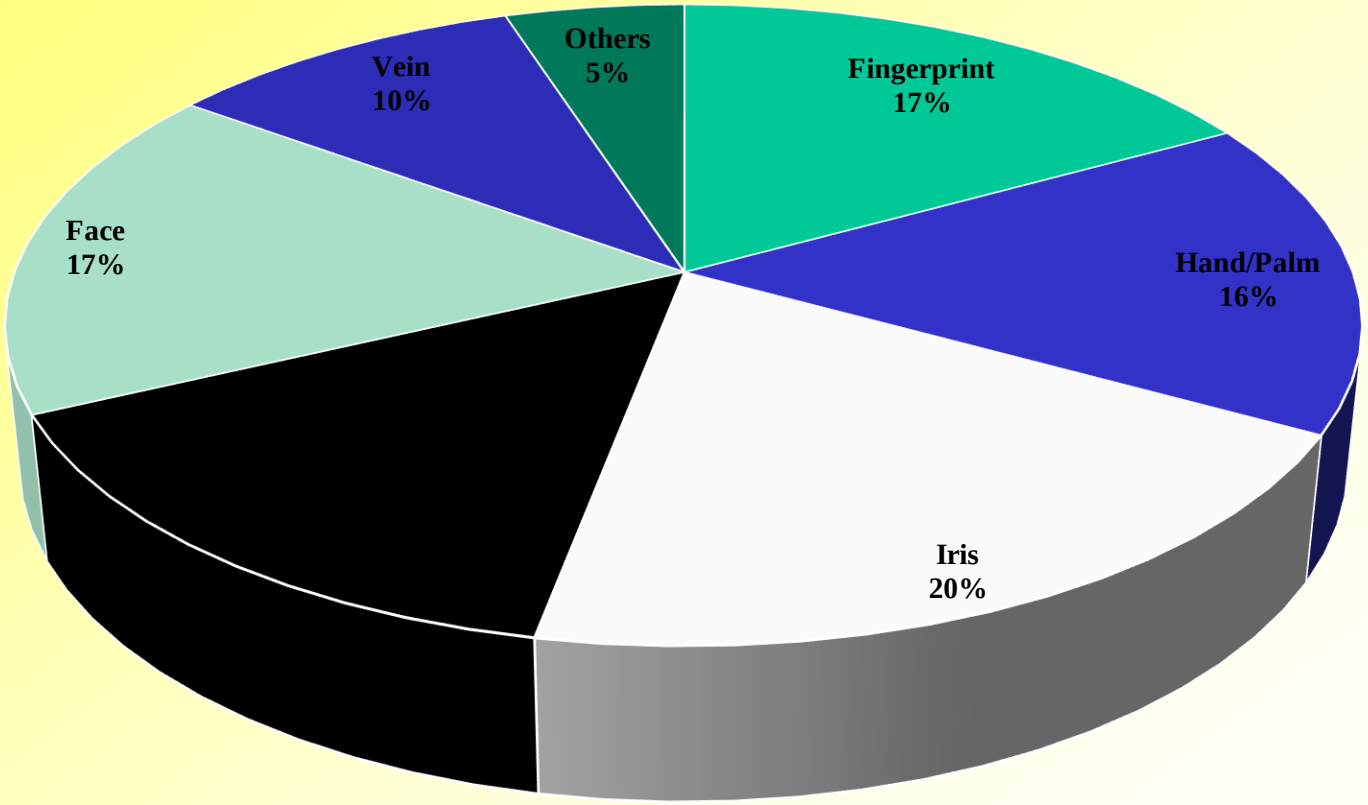
Mobil

Letiště Frankfurt

Letiště Ben Gurion

➔Vývoj biometrických aplikací (I.)

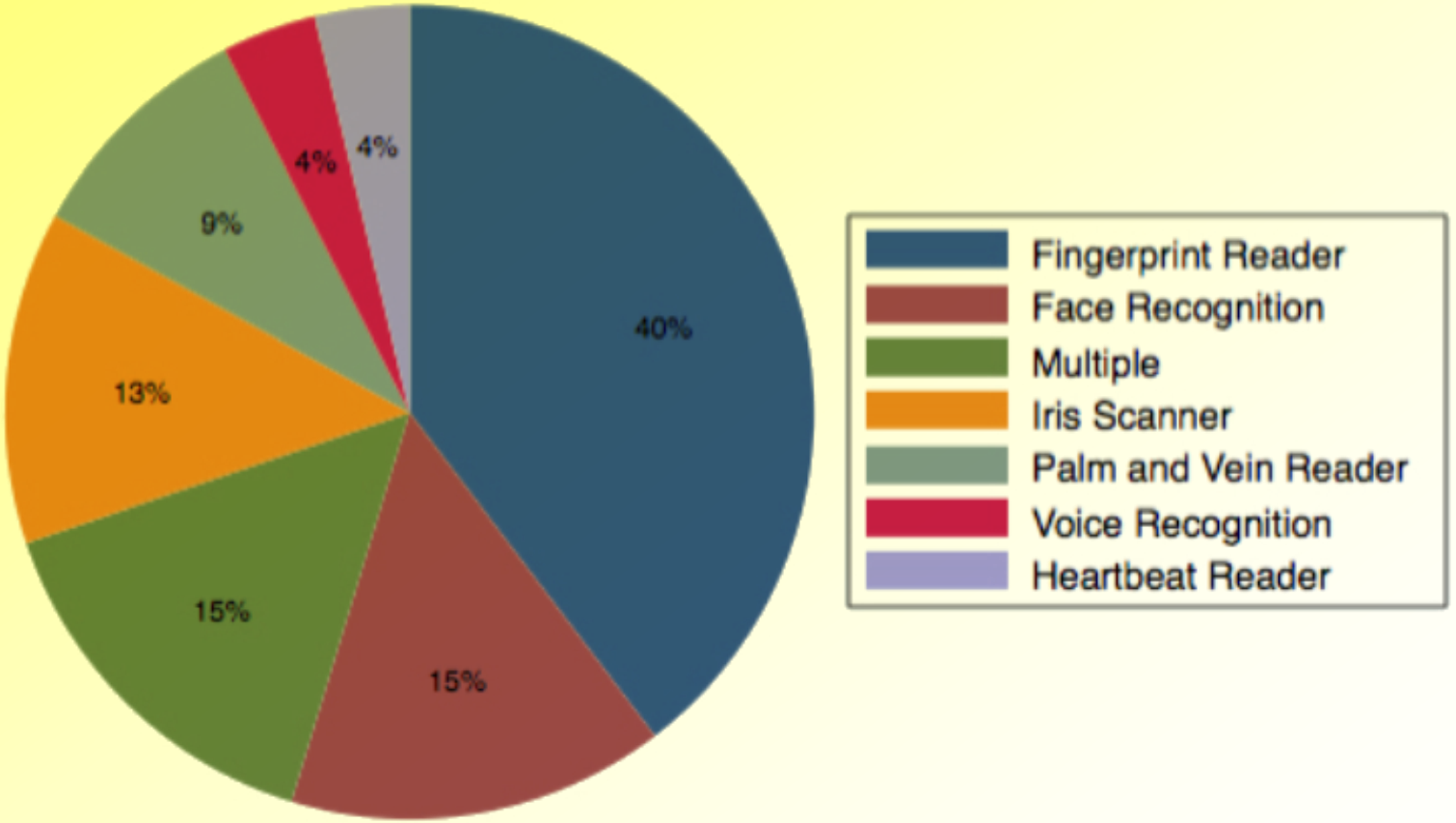
➔Aktualizace je složitá (cena průzkumů)



Zdroj: Global Biometrics Market by Type, 2004

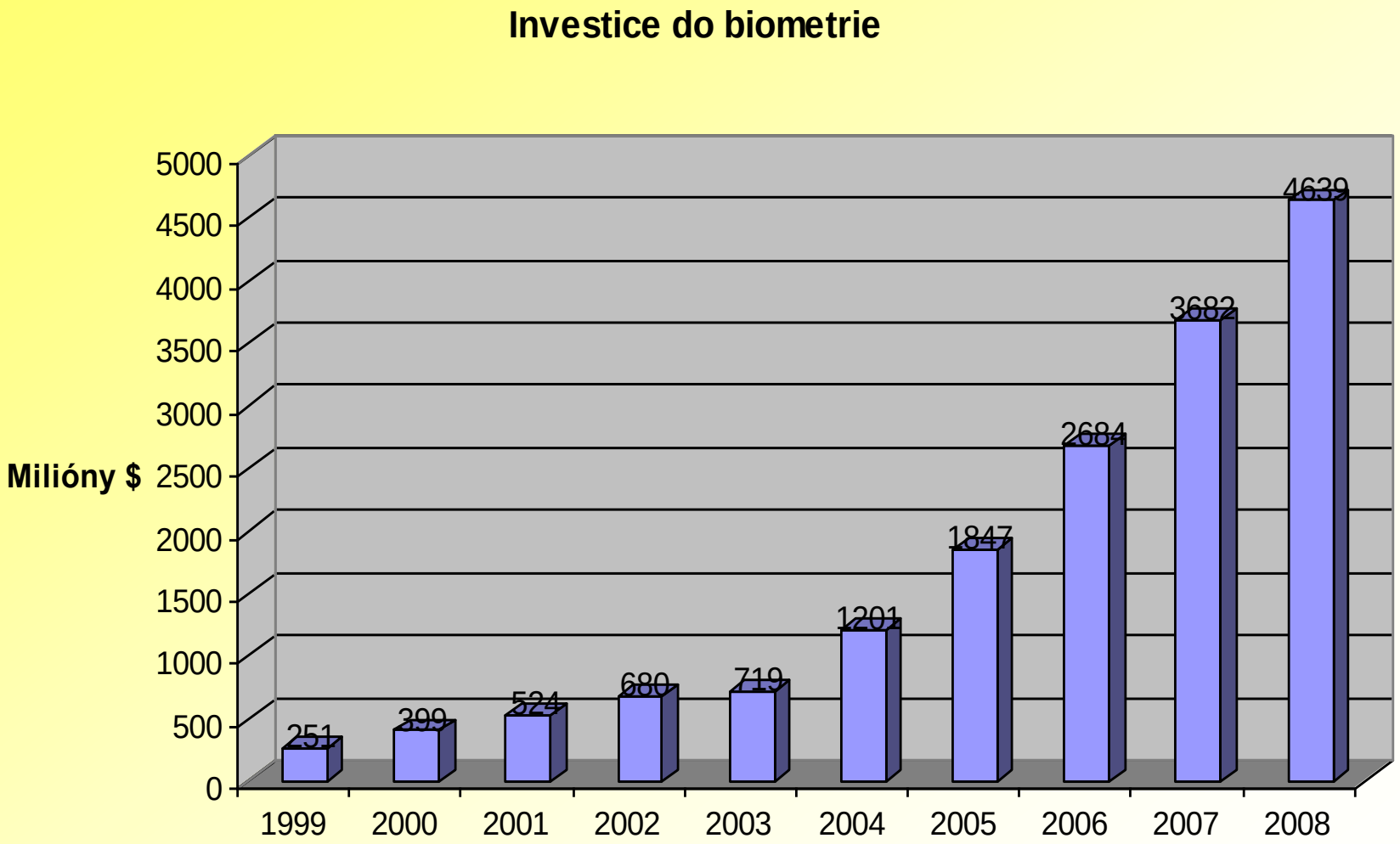
➔Vývoj biometrických aplikací (II.)

➔Průzkum 53 praktických aplikací v USA za 2004-2016



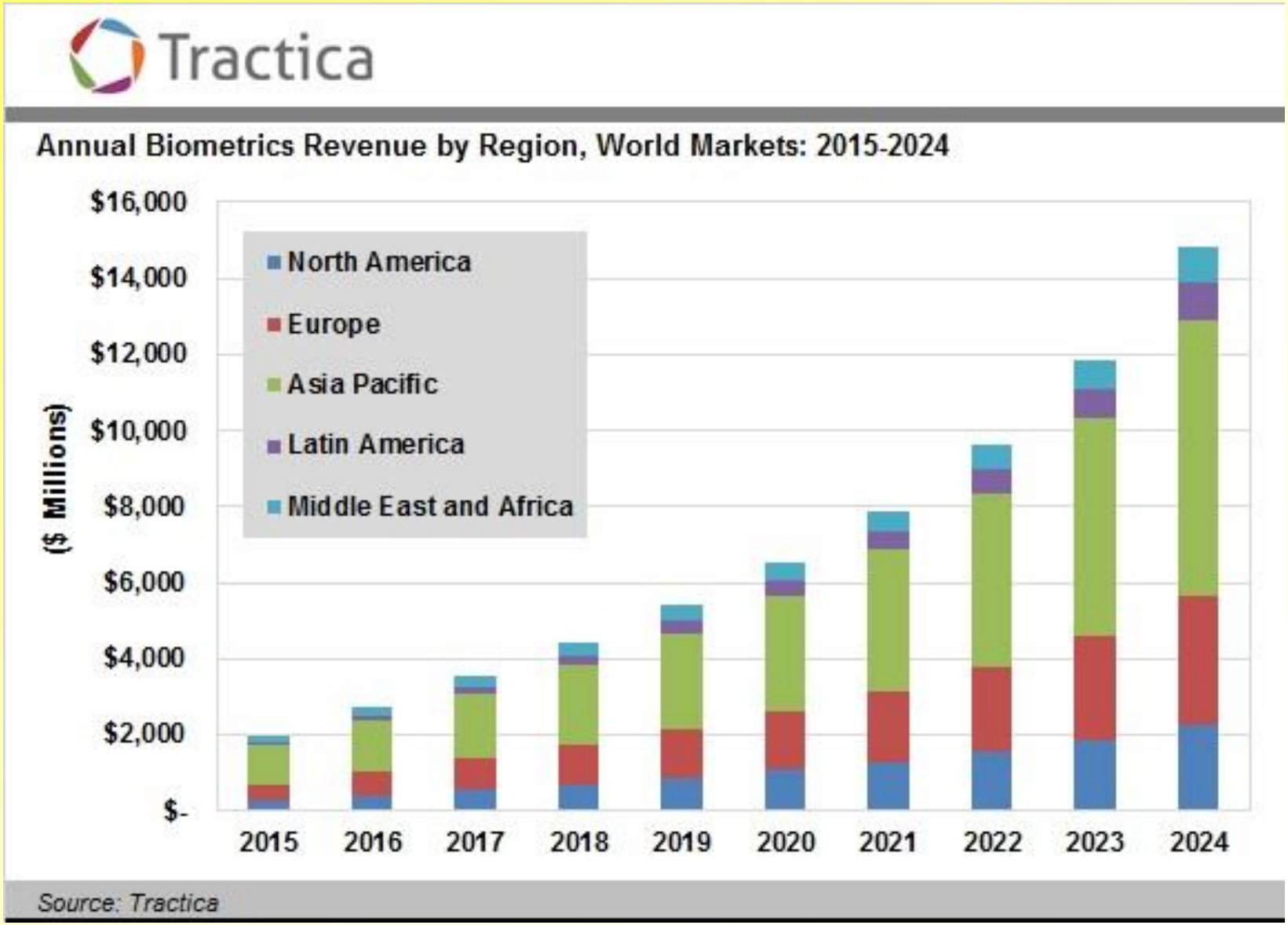
Zdroj: Current Biometric Adoption and Trends

➔Vývoj biometrických aplikací (III.)



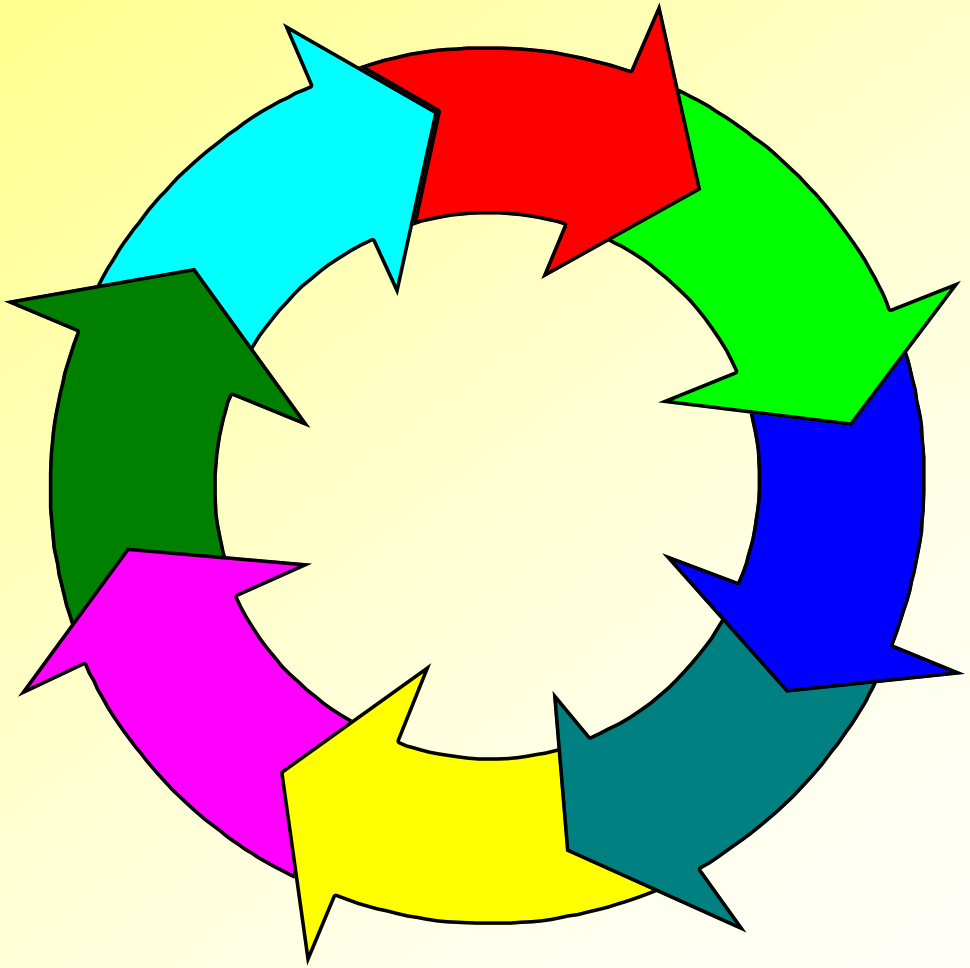
Zdroj: IBG, 2004

➔Vývoj biometrických aplikací (IV.)



➔Vlastnosti biometrických rysů (I.)

- ➔Univerzalita
- ➔Jedinečnost
- ➔Konstantnost
- ➔Získatelnost
- ➔Výkonnost
- ➔Akceptace
- ➔Bezpečnost proti falšování
- ➔Finanční náklady na pořízení



Popis - viz násl. slide

➔Vlastnosti biometrických rysů (II.)

	Univerzalita	Jedinečnost	Konstantnost	Získatelnost	Výkonnost	Akceptace	Bezpečnost	Finance
Obličej	vysoká	nízká	střední	vysoká	nízká	vysoká	nízká	nízké
Otisk prstu	střední	vysoká	vysoká	střední	vysoká	střední	vysoká	nízké
Geometrie ruky	střední	střední	střední	vysoká	střední	střední	střední	střední
Žíly ruky	střední	střední	střední	střední	střední	střední	vysoká	střední
Duhovka	vysoká	vysoká	vysoká	střední	vysoká	nízká	vysoká	vysoké
Sítnice	vysoká	vysoká	střední	nízká	vysoká	nízká	vysoká	vysoké
Podpis	nízká	nízká	nízká	vysoká	nízká	vysoká	nízká	nízké
Hlas	střední	nízká	nízká	střední	nízká	vysoká	nízká	nízké
Termogram	vysoká	vysoká	nízká	vysoká	střední	vysoká	vysoká	vysoké

➔**Univerzalita** = ∀ osoba by měla mít tuto vl.

➔**Jedinečnost** = !∀ dvě osoby nesmí vlastnit stejnou vl.

➔**Konstantnost** = daná vl. zůstává s časem neměnná

➔**Získatelnost** = vl. je kvantitativně měřitelná

➔**Výkonnost** = vl. se dá přesně a snadno porovnat

➔**Akceptace** = ochotnost lidí pro nasnímání dané vl.

➔**Bezpečnost** = snadnost vytvoření falsifikátu dané vl.

➔**Finance** = cenové náklady na pořízení systému

➔Vlastnosti biometrických rysů (III.)

- ➔Další aspekty:
  - ➔Použitelnost
  - ➔Údržba
  - ➔Dostupnost
  - ➔Provedení
  - ➔Anonymita
  - ➔Distribuovatelnost
- ➔Spolehlivost?
  - ➔Osvětlení / Teplota
  - ➔Make-up
  - ➔Zranění / Operace
  - ➔Čepice / Brýle
  - ➔Sestřih / Vousy
  - ➔Stárnutí

- ➔Typy útoků:
  - ➔„*Low-Force-Attack*“ - napodobení podpisu, hlasu
  - ➔„*Brute-Force-Attack*“ - použití speciálních technik

➔Souhrn (I.)

➔Spolehlivá a automatická identifikace / verifikace osob se stává nutností; Příklady: národní identifikační karty, hraniční kontrola, přístupové systémy, e-Shopping ...

➔Neexistuje žádná náhrada za biometrii, ve smyslu spolehlivé identifikace / verifikace osob.

➔Biometrické senzory jsou laciné a některé z nich jsou i velmi kompaktní (pro mobilní telefony a laptopy).

➔Některé biometrické systémy nejsou úplně dostatečně přesné, spolehlivé nebo bezpečné pro některé využití.

➔Je třeba testování biometrických systémů na rozsáhlých databázích.

➔Biometrie může vylepšit ochranu našeho soukromí, ale jsou nutné vládní předpisy a směrnice.

➔Souhrn (II.)

- ➔Nutný výzkum především v následujících oblastech:
  - ➔Nové reprezentace
  - ➔Porovnávací algoritmy
  - ➔Efektivní indexování v databázi
  - ➔Multimodální biometrické systémy
  - ➔Detekce živosti
  - ➔Ochrana šablon
  - ➔Vylepšení chybových hranic
- ➔Nutné další investice a mnoho práce

➔Konec

➔Děkuji za pozornost!

➔Použitá literatura: [Dit04], [Dra01], [Hau04], [Jai03], [Jai04], [Kar03]