12. Biometrické standardy

➔Definice

➔ Standard

Utvořen běžným a opakovaným používáním pravidel, podmínek, směrnic nebo charakteristik produktů či spřízněných procesů a produkčních metod a souvisejících praktik managementu systémů [DeW05].

➔ Technický standard

Definice terminologie; klasifikace komponent; nástin procedur; specifikace dimenze, materiálu, výkonu, designu a funkčnosti; měřítka kvality a kvantity pro popis materiálu, procesů, produktů, systémů, služeb nebo praktik; testovací a vzorkovací metody; popis měřítek přesnosti, velikosti a stability ~ kombinace těchto pojmů tvoří technický standard [DeW05].

➔ **Otevřený standard** – std. plně otevřený veřejnosti

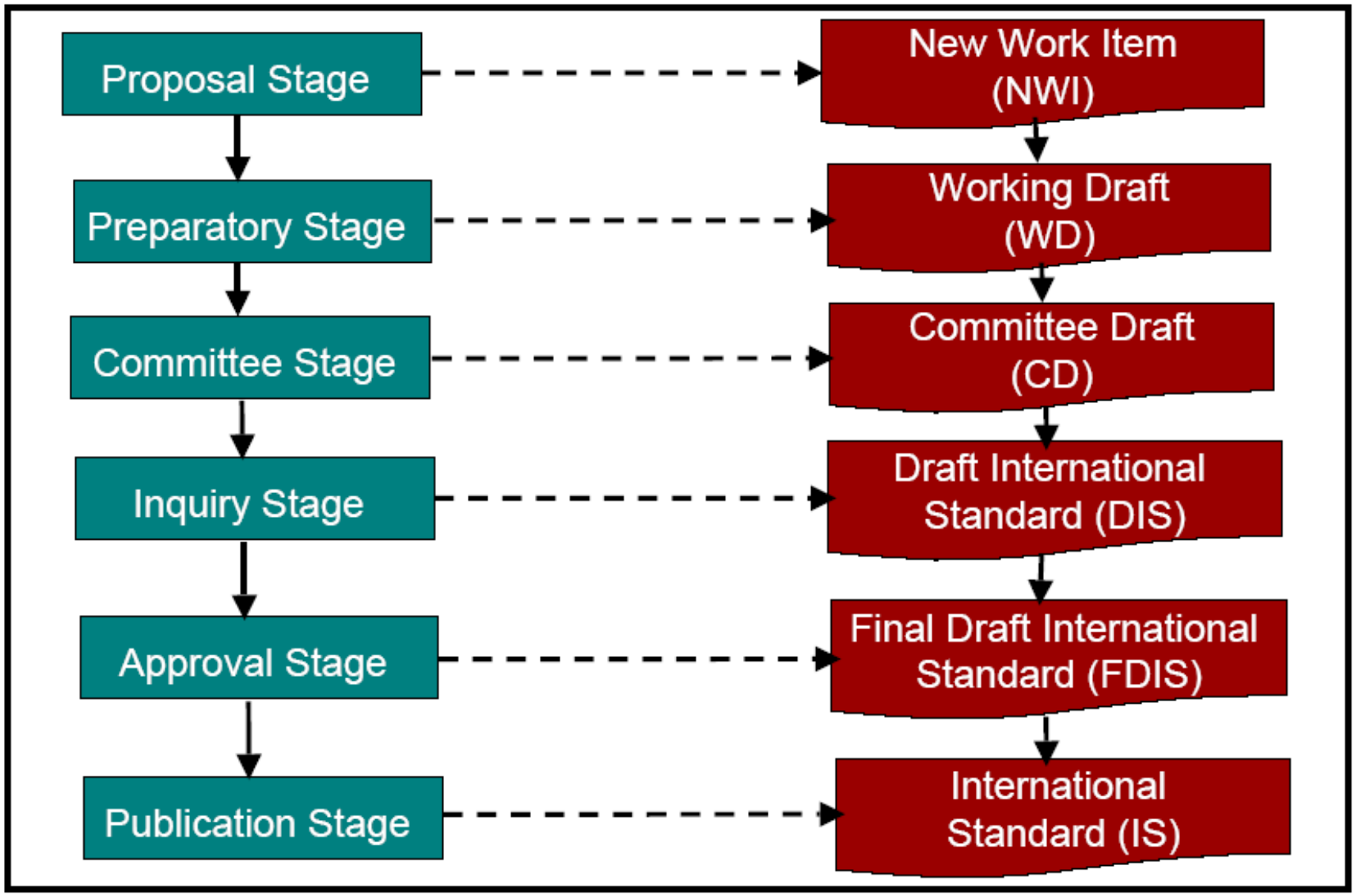
➔Historie

- ➔ Do roku 1996 existoval pouze standard na otisky prstů – daktyloskopické karty a výměna dat pro forenzní medicínu.
- ➔ Listopad 2001 – organizace INCITS (*International Committee for Information Technology Standards*) založila divizi pro biometrii, označenou M1.
- ➔ V červnu 2002 vytvořila organizace *ISO Joint Technical Committee 1* (JTC1) subdivizi pro biometrii, SC37 (*Sub-Committee 37*).
- ➔ V dalších měsících byly vytvořeny subdivize SC17 (*Cards and Personal Identification*) a SC27 (*IT Security Techniques*)

➔Proč standardizaci?

- ➔ V minulosti byla výměna dat z různých biometrických systémů velmi limitovaná až nemožná.
- ➔ Každý výrobce měl vlastní formát, který byl zcela nekompatibilní s ostatními – proprietární formáty.
- ➔ Pro biometrické dokumenty je nutný standard, aby byla data použitelná i u jiného výrobce.
- ➔ NTTAA 104-113 (1996) – *National Technology Transfer and Advancement Act* – donucovací prostředek ke standardizaci, ovšem je nutný dohližitel – v USA např. NIST či DoD.
- ➔ Úspěšný standard musí: být volně dostupný, splňovat požadavky velké skupiny provozovatelů, být flexibilní ke změnám, být konzistentně implementován a být kompatibilní vzhledem ke starším verzím.

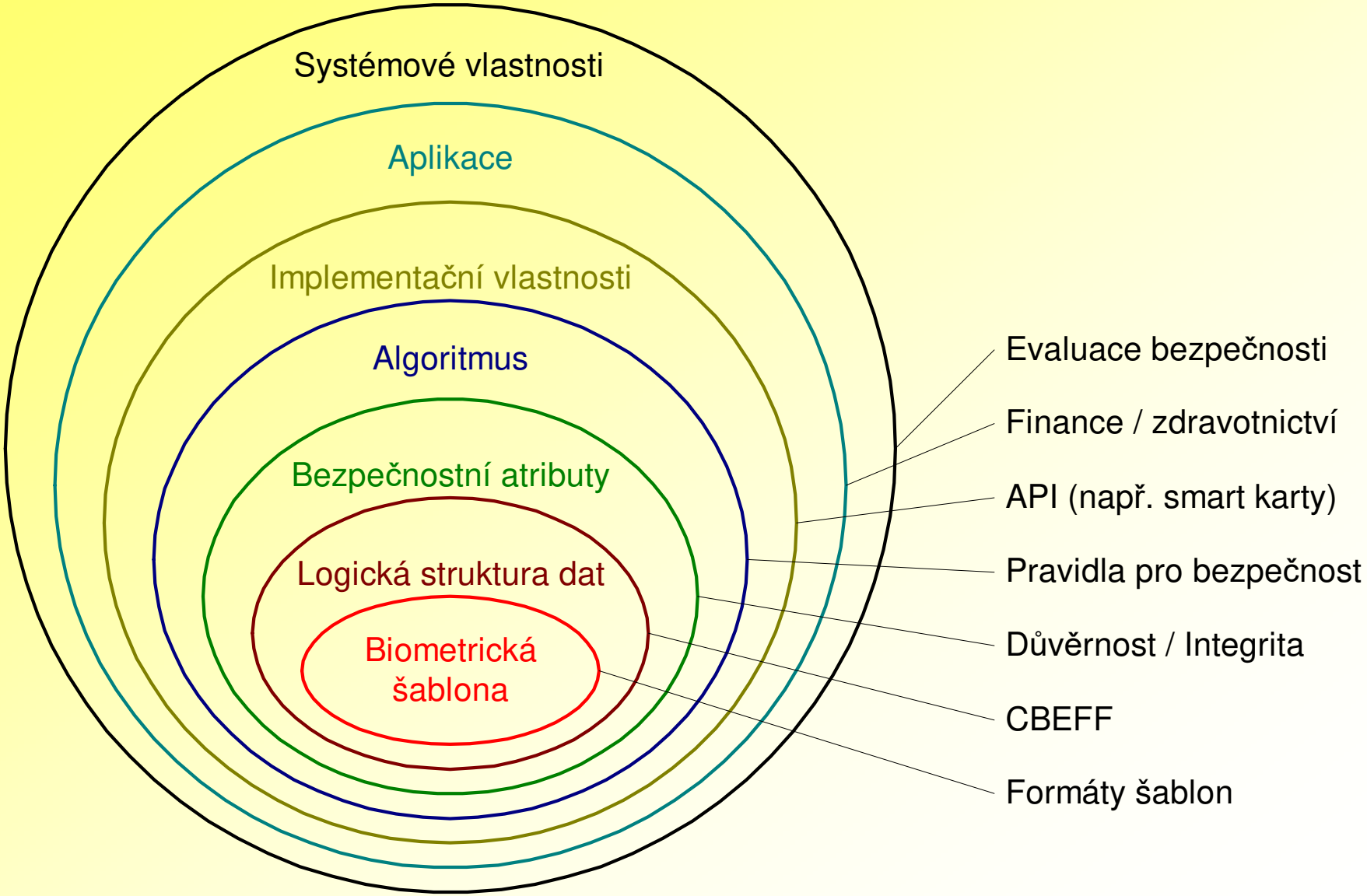
➔Průběh standardizace



➔Typy standardů pro IT-biometrii

- ➔ Standardy k výměně dat
  - ➔ Aplikační struktura
  - ➔ Datové formáty
- ➔ Standardy pro výkonnost biometrických systémů
  - ➔ *Best Practices* pro testování
  - ➔ Standardní databáze (GDPR !)
  - ➔ Praktiky při tvorbě reportů
- ➔ Standardy pro celkovou bezpečnost systémů
  - ➔ Zjišťování zranitelnosti dle std. postupů
  - ➔ Ochrana dat
  - ➔ Zajištění funkčnosti komplexní ochrany

➔Struktura biometrické aplikace



➔Obecné rozdělení biom. standardů

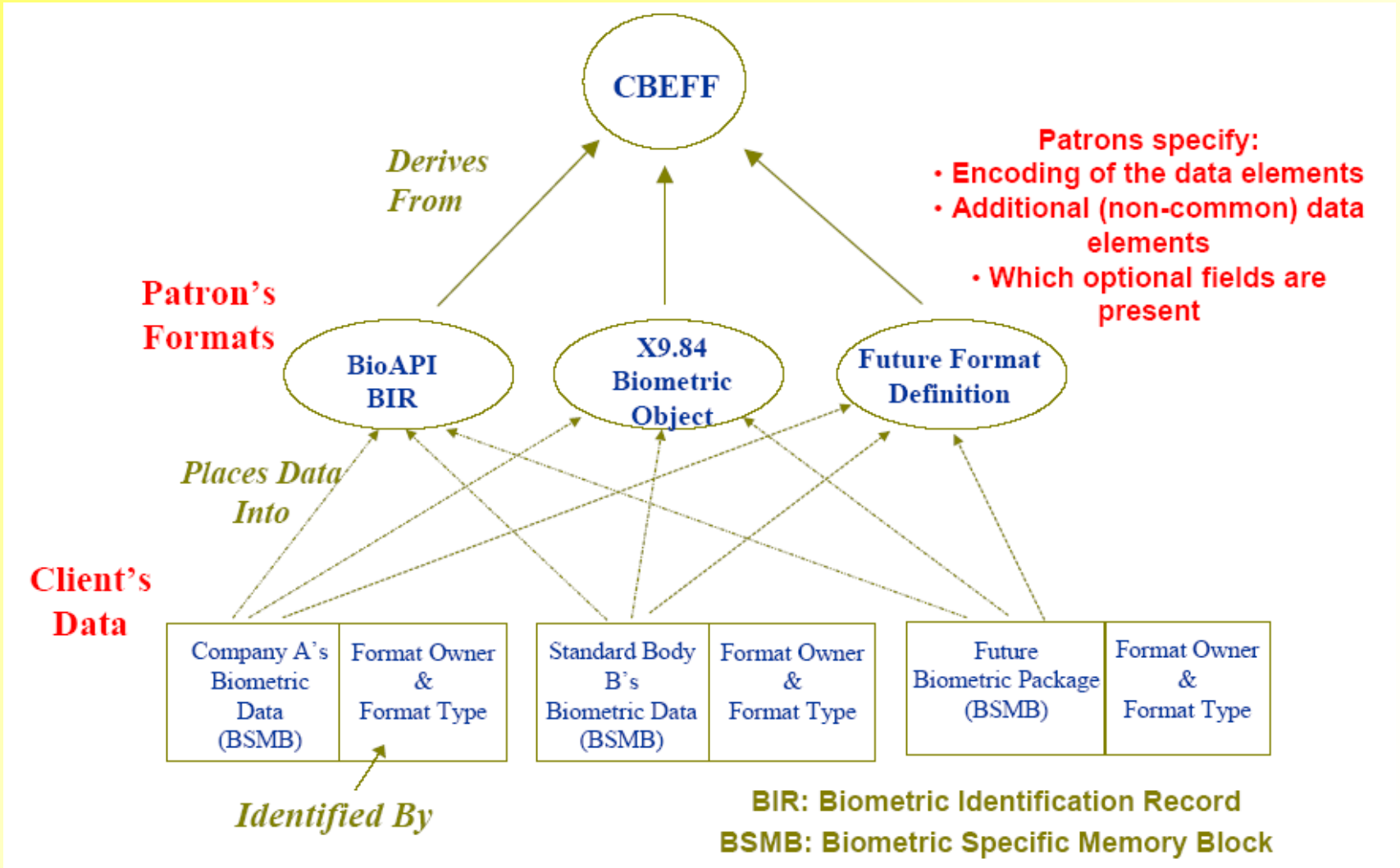
- ➔ Forenzní a identifikační standardy
- ➔ Datové standardy
- ➔ API standardy
- ➔ Bezpečnostní standardy
- ➔ Testovací a certifikační standardy
- ➔ Jiné standardy
  - ➔ COPRAS (*Cooperation Platform for Research & Standards*) – projekt běžící od 02/2004 do 01/2007

COPRAS
Cooperation Platform for Research & Standards

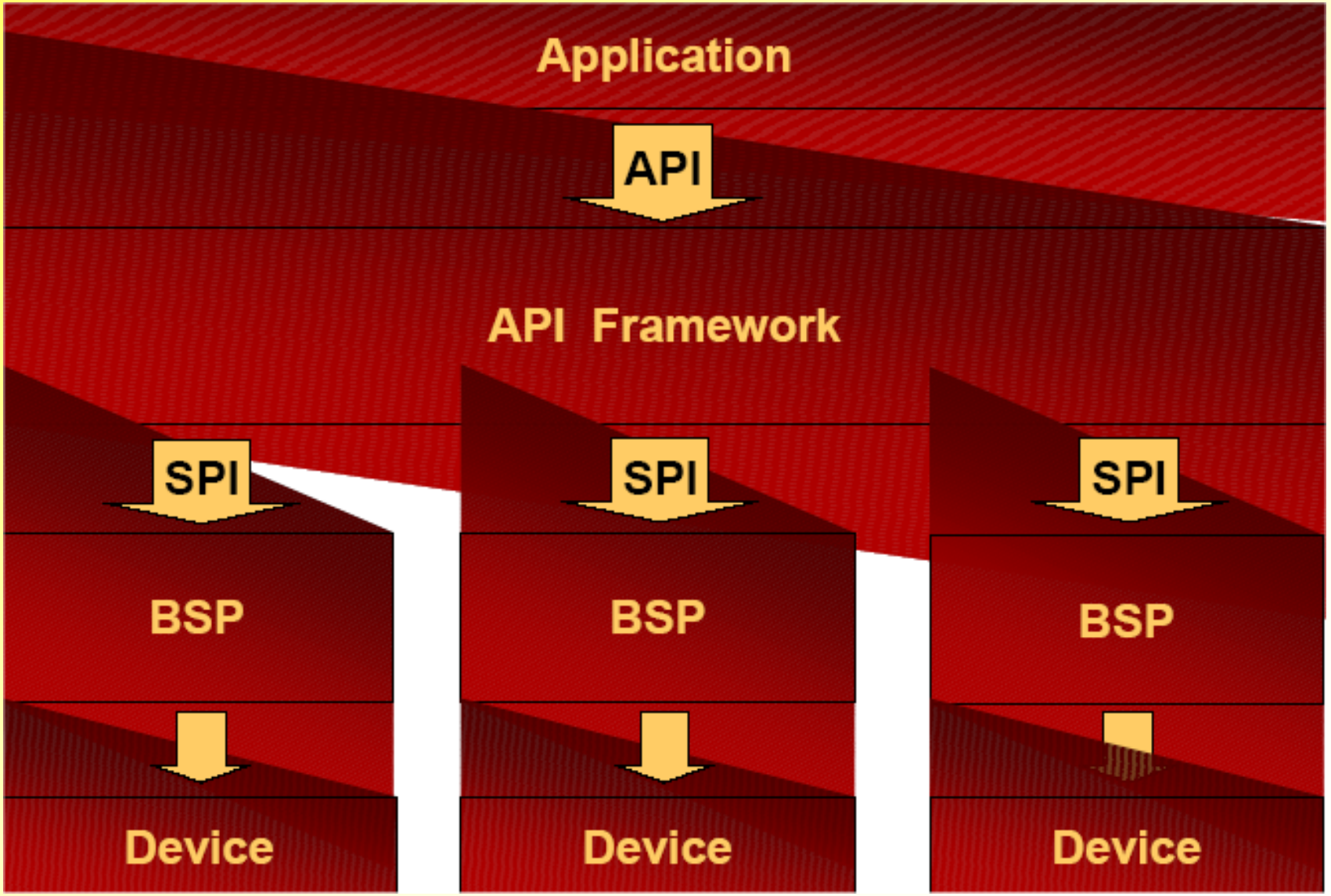
➔Forenzní a identifikační standardy

- ➔ **ANSI / NIST ITL 1-2000** (*Data Format for the Exchange of Fingerprint, Facial and SMT Information*)
- ➔ **CJIS / FBI IAFIS-IC-0110** (*FBI Wavelet Scalar Quantization Standard*)
- ➔ **CJIS-RS-0010 7 FBI** (*Electronic Fingerprint Transmission Standard*)
- ➔ **AAMVA DL / ID-2000** (*National Standard for the Drivers License / Identification Card*)
- ➔ **ANSI / INCITS B10.8** (*Identification Cards Standard*)
- ➔ **ISO JTC1 SC17** (*Cards and Personal Identification*)
- ➔ **EAB Forensic Biometrics Working Group -** https://eab.org/expertise/wg/fbwg.html

➔Datové standardy

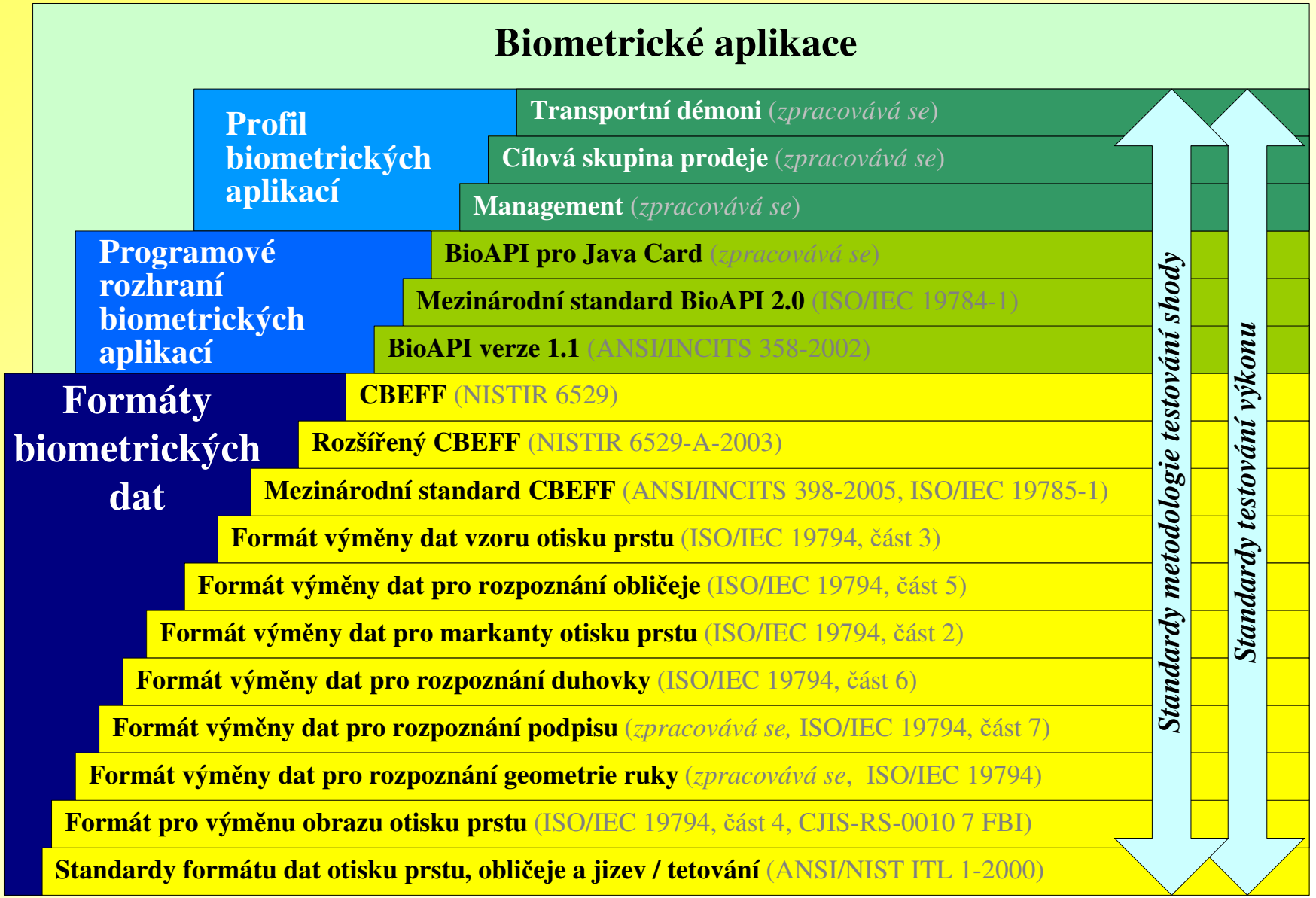


➔API standardy



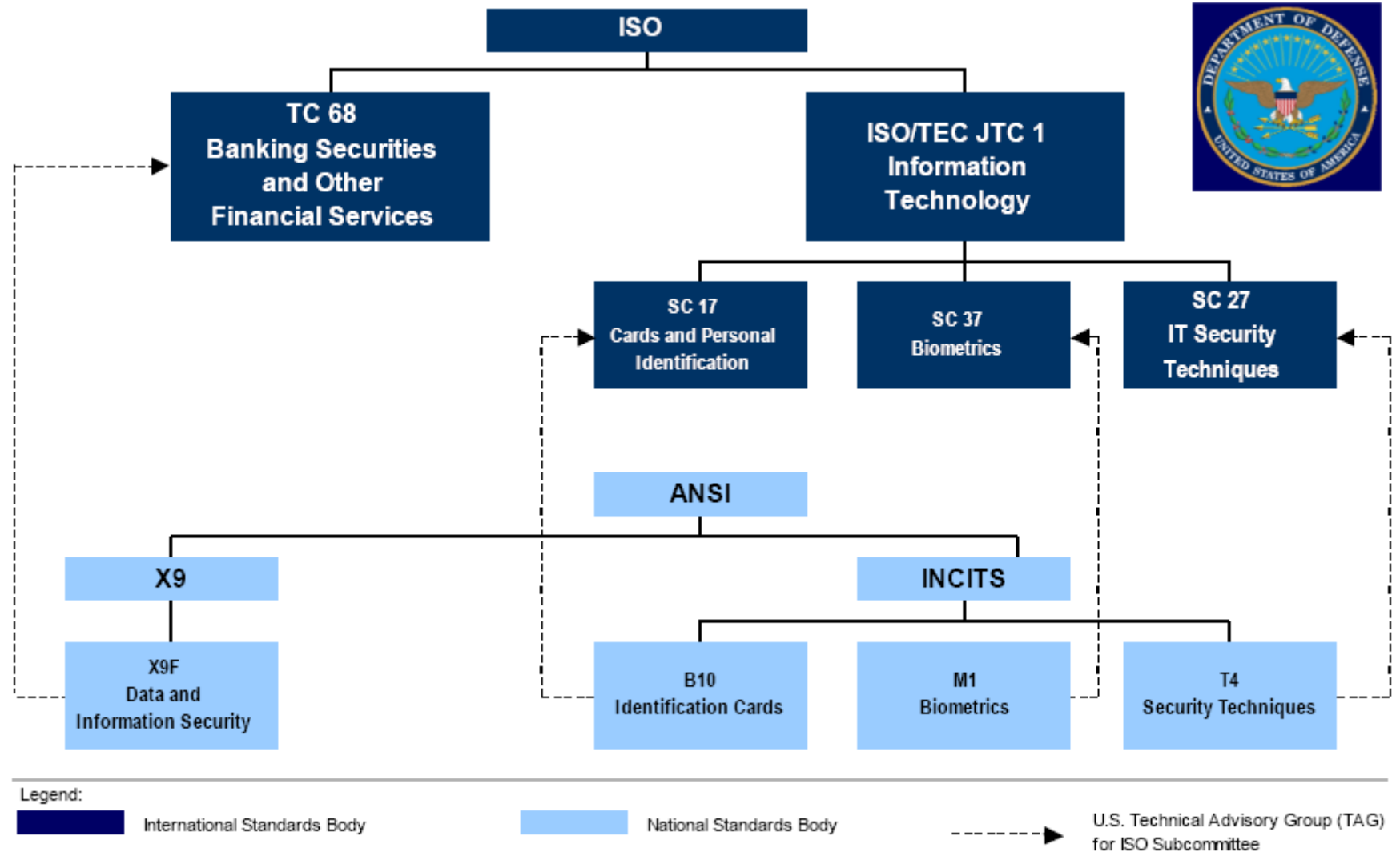
SPI = *Service Provider Interface*; **BSP** = *Biometric Service Provider*

➔Přehled standardů



https://www.iso.org/committee/313770/x/catalogue/

➔Standardy dle DoD



➔Organizace

➔ BioAPI Consortium

➔ http://www.bioapi.com

➔ ANSI X9.F4

➔ http://www.x9.org

➔ BC Working Group

➔ http://www.biometrics.org/html/work_groups.html

➔ DoD-BMO, BEMWG

➔ https://peoiews.army.mil/programs/pm-dod-bio/

➔ U.K. BWG, FVC, FVRT2004, IBG

➔ Např. https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx

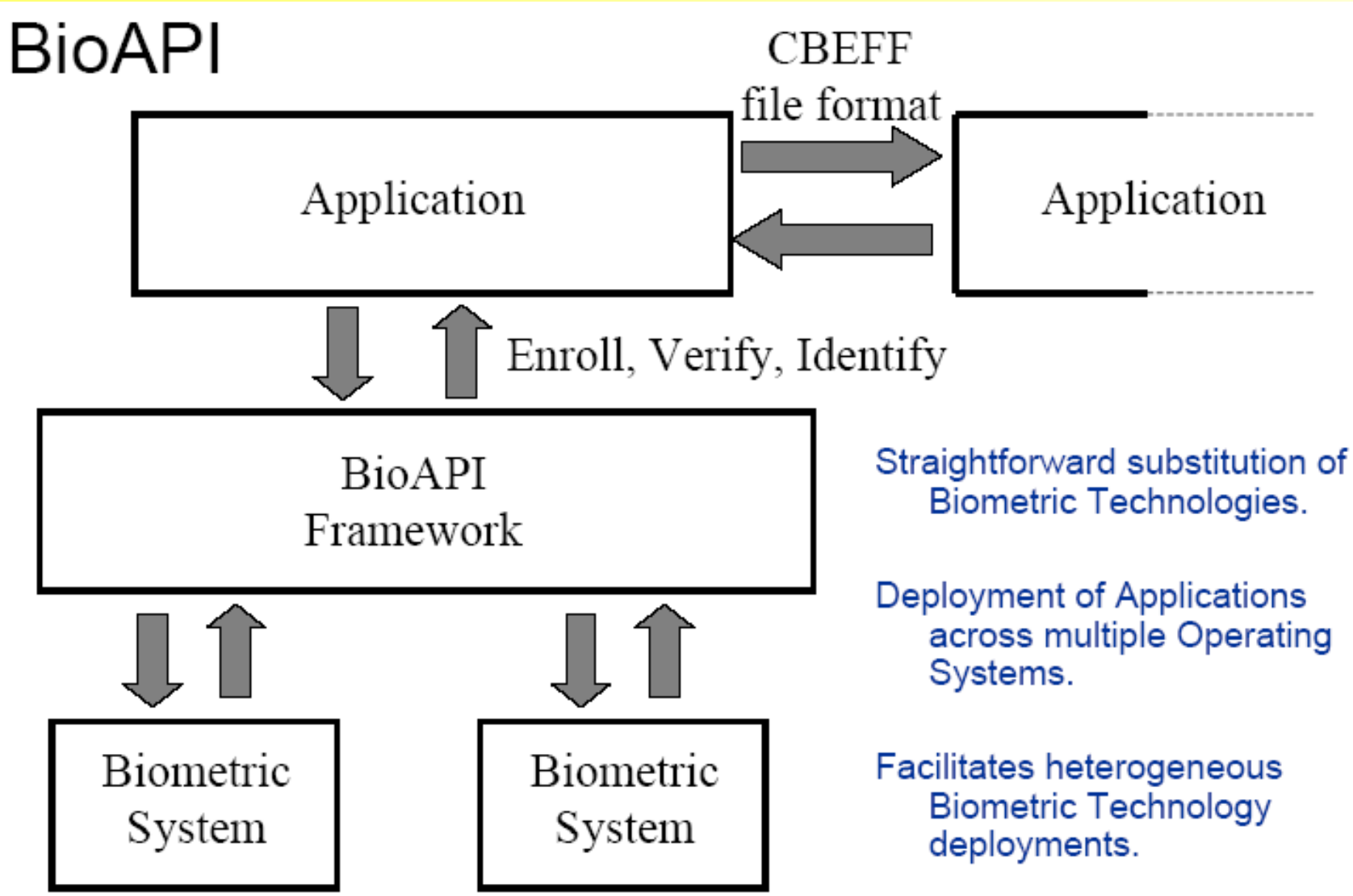
➔Standardy

- ➔ BioAPI – ANSI/INCITS 358 (2002) + ISO/IEC 19784
  - ➔ Programátorské aplikační rozhraní
- ➔ ANSI / X9 – X9.84 (2001)
  - ➔ Finanční aplikace
- ➔ BCWG – CBEFF – NISTIR 6529
  - ➔ Datový formát pro soubory
- ➔ DoD – Common Criteria (CC)
  - ➔ Bezpečnostní evaluace
- ➔ U.K. BWG, FVC, FVRT2004, IBG
  - ➔ Evaluace spolehlivosti a kvality

➔BioAPI Consortium

- ➔ Založeno roku 1998, ale již neexistuje
- ➔ Účel: vývoj standardního API (*Application Programming Interface*) rozhraní k zajištění nezávislosti vývojářů vzhledem k rozhraní aplikace / zařízení (senzor)
- ➔ Sedm zakládajících organizací:
  - ➔ Bioscrypt, Compaq, Iridian, Infineon, NIST, SafLink, Unisys
- ➔ Více jak 90 členů (65% ze severní Ameriky, 25% z Evropy a 10% z Asie); patří sem průmysl, vláda a akademické instituce
- ➔ ISO/IEC 19784 (2018): *Information technology — Biometric application programming interface — Part 1: BioAPI specification*

➔Standard BioAPI

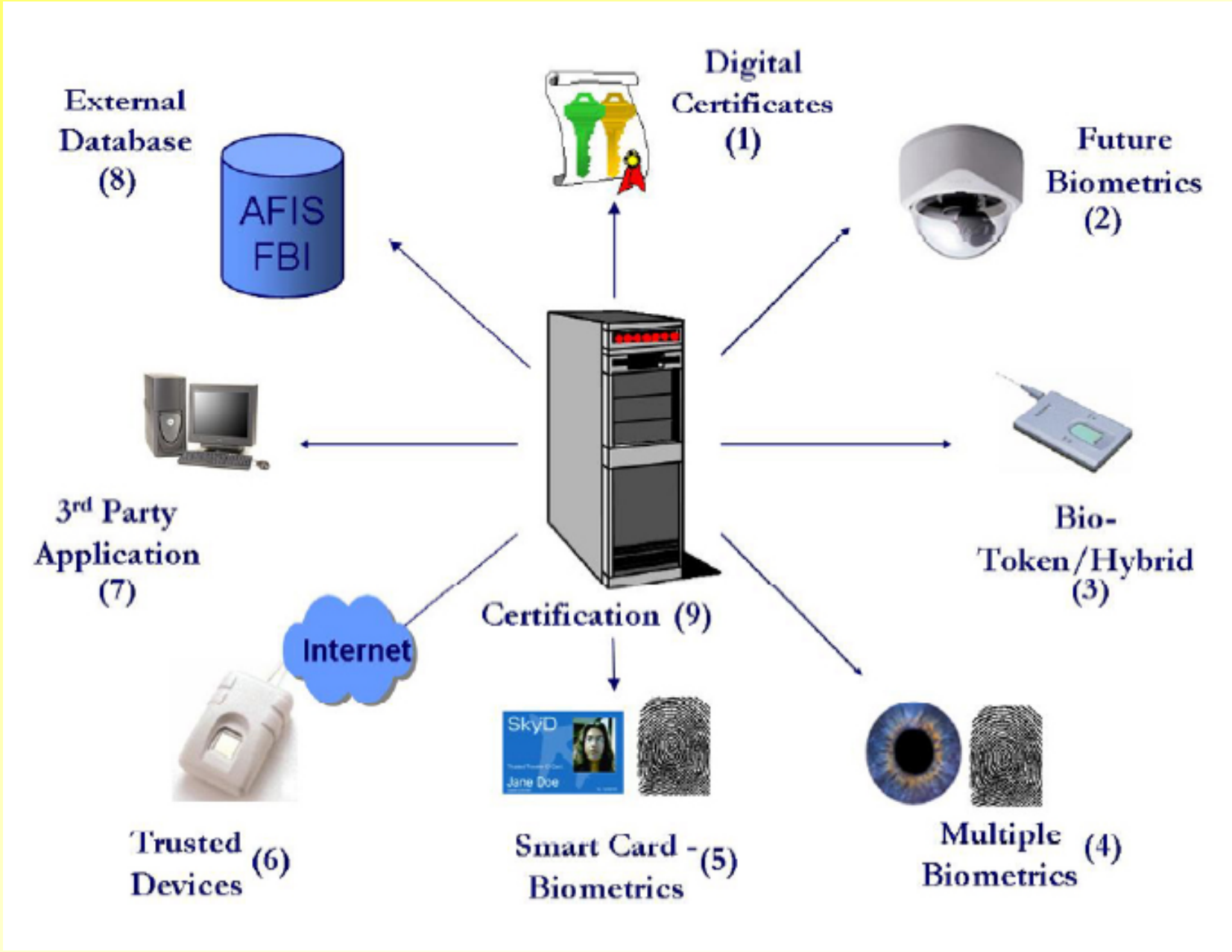


Straightforward substitution of Biometric Technologies.

Deployment of Applications across multiple Operating Systems.

Facilitates heterogeneous Biometric Technology deployments.

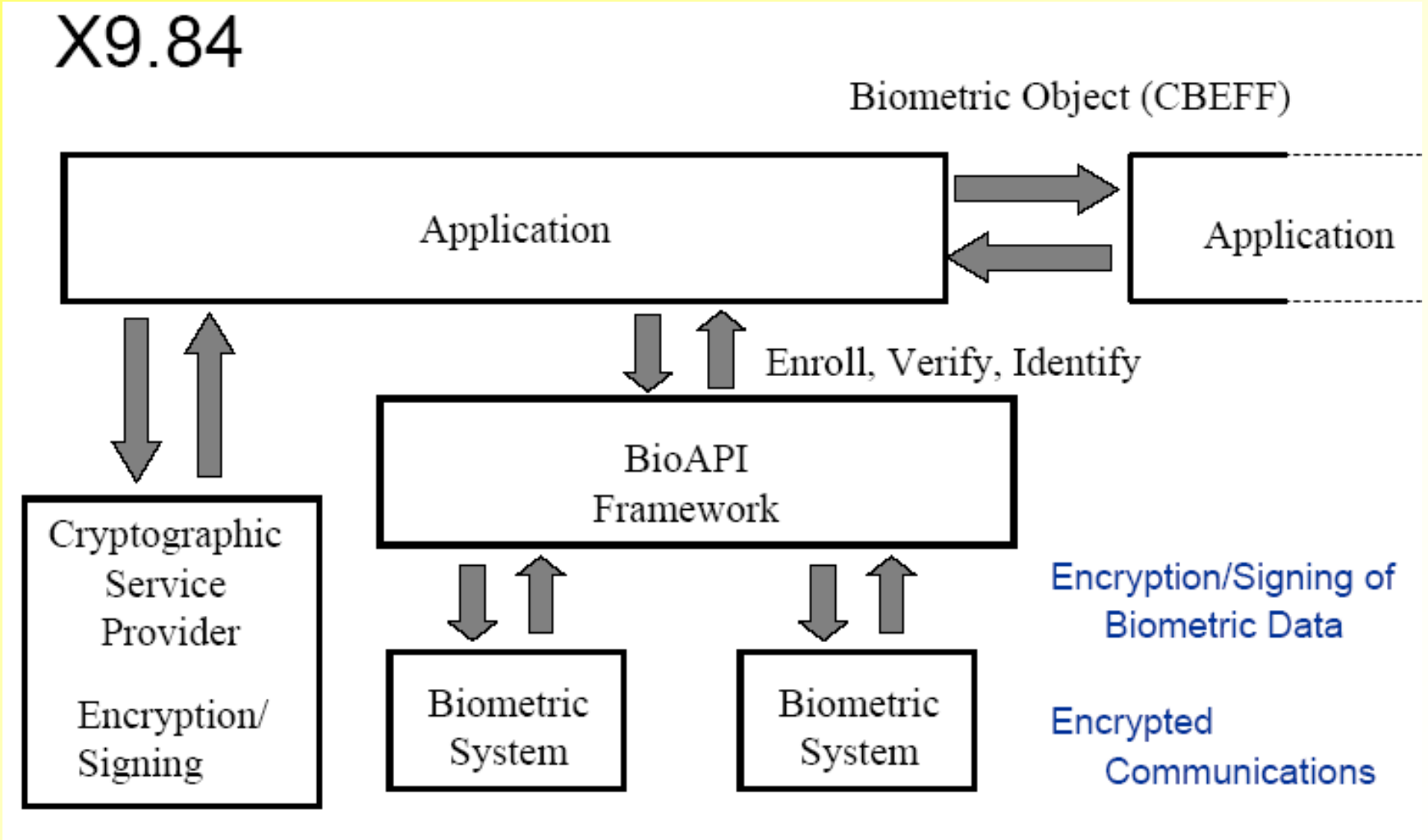
➔Standard BAPI (již dávno neexistuje)



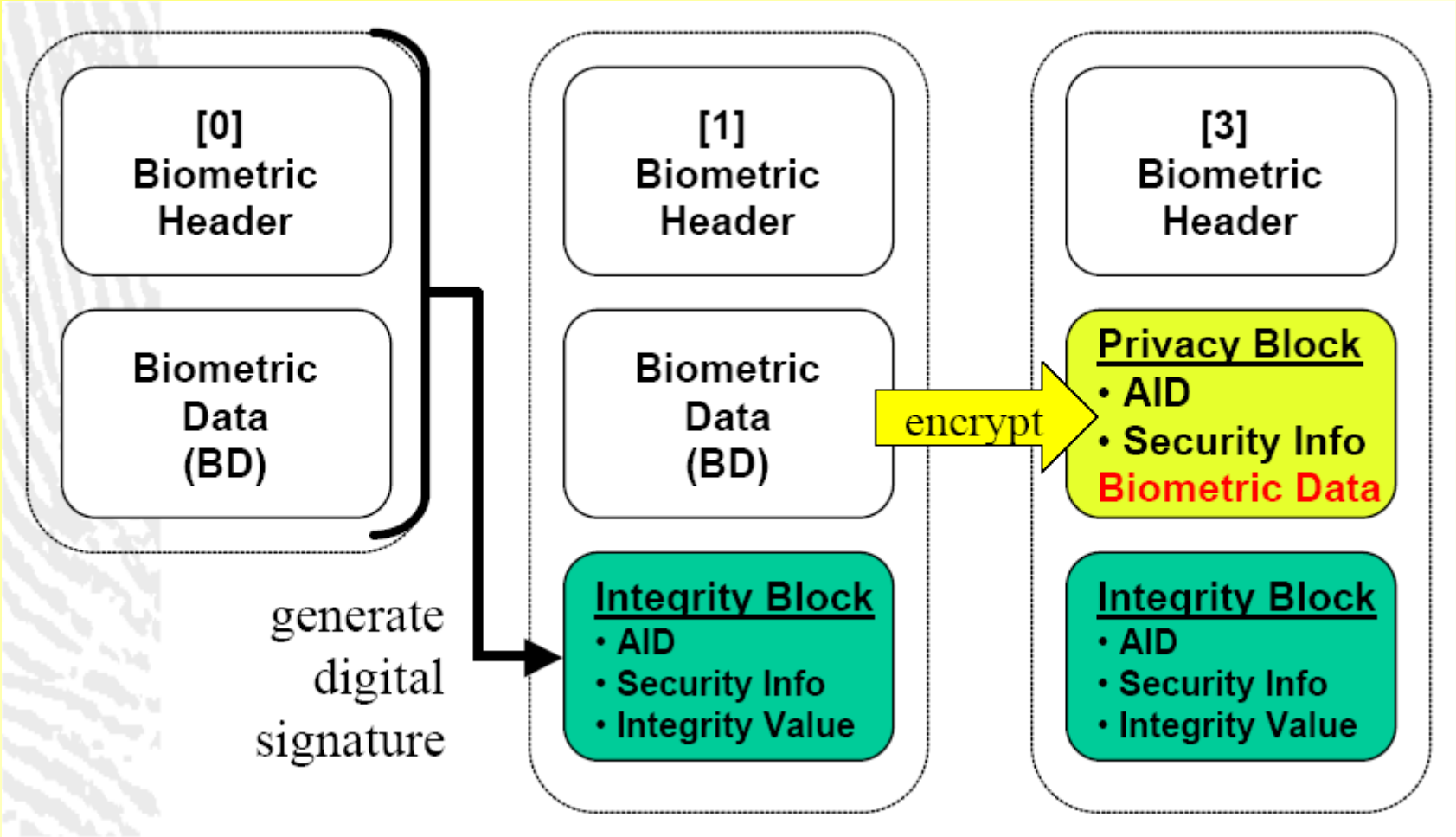
➔Standard X9.84 (I.)

- ➔ Organizace založena roku 2001, stále funguje
- ➔ Účel:
  - ➔ Bezpečnostní požadavky na registraci, verifikaci / identifikaci, uložení a přenos…
  - ➔ Formát šablony kompatibilní s CBEFF
- ➔ Členové:
  - ➔ *Committee on Financial Services X9*
  - ➔ *Subcommittee on Information Security X9F*
- ➔ Požadavky:
  - ➔ Chybovost menší než 10^{-4} (verif. / identif.)
  - ➔ *False Match* by mělo odpovídat použití PINu

➔Standard X9.84 (II.)



➔Standard X9.84 (III.)



➔Standard CBEFF (I.)

- ➔ **CBEFF** = *Common Biometric Exchange File Format*
- ➔ Definuje základní pole pro biometrická data
- ➔ Registrace biometrických dat (IBIA)
- ➔ Umožňuje nové adaptace
- ➔ Publikován jako NISTIR 6529 roku 2001
- ➔ Nová verze se jmenuje NISTIR 6529-C
- ➔ Spolupracovníci: BioAPI, ANSI X9.84, TOG CDSA HRS, NIST, AAMVA, XCBEFF (XML), ISO SC17 7816-11
- ➔ ISO/IEC 19785-1:2015: *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

➔Standard CBEFF (II.)

Hlavička	Specifický datový blok	Podpis

- ➔ Bezpečnostní nastavení (např. šifrovaný, otevřený, …)
- ➔ Integritní nastavení (např. podepsaný)
- ➔ Verze CBEFF hlavičky
- ➔ Vydavatel (např. *BioAPI Header Version*)
- ➔ Typ biometriky (např. obličej, otisk prstu, …)
- ➔ Typ datového záznamu (např. zpracovaný)
- ➔ Účel záznamu (např. registrace)
- ➔ Kvalita záznamu
- ➔ Datum vytvoření
- ➔ … a další údaje

➔Standard INCITS M1

- ➔ Formát pro výměnu dat
- ➔ Zaměřen na otisk prstu, obličej a duhovku oka, tedy na biometrické charakteristiky využitelné v kriminalistice.
- ➔ Tvořen organizací NIJ (*National Institute of Justice, Office of Science and Technology, USA*).
- ➔ V rámci tohoto projektu byl vytvořen katalog biometrie (*Biometrics Catalogue*), který obsahuje nejen různé typy biometrie (včetně návrhů na datový formát), ale i různé kategorie produktů, v nichž může být biometrie využita.
- ➔ http://www.biometricscatalog.org/

➔Standard „*Best Practices*“

- ➔ Účel: Popis nejlepších metod pro testování biometrických systémů.
- ➔ Použití na jakoukoliv biometriku a aplikaci!
- ➔ ISO/IEC 19795: *Biometric performance testing and reporting*
- ➔ Rysy:
  - ➔ Experimentální evaluace
  - ➔ Evaluace technologie / scénáře / operační
  - ➔ Definice experimentálních podmínek
  - ➔ Reprezentace výkonnosti
    - ➔ ROC křivky
    - ➔ FMR / FNMR + FTA, FTE, FTM
    - ➔ Detailní zpráva (pro opakovatelnost)

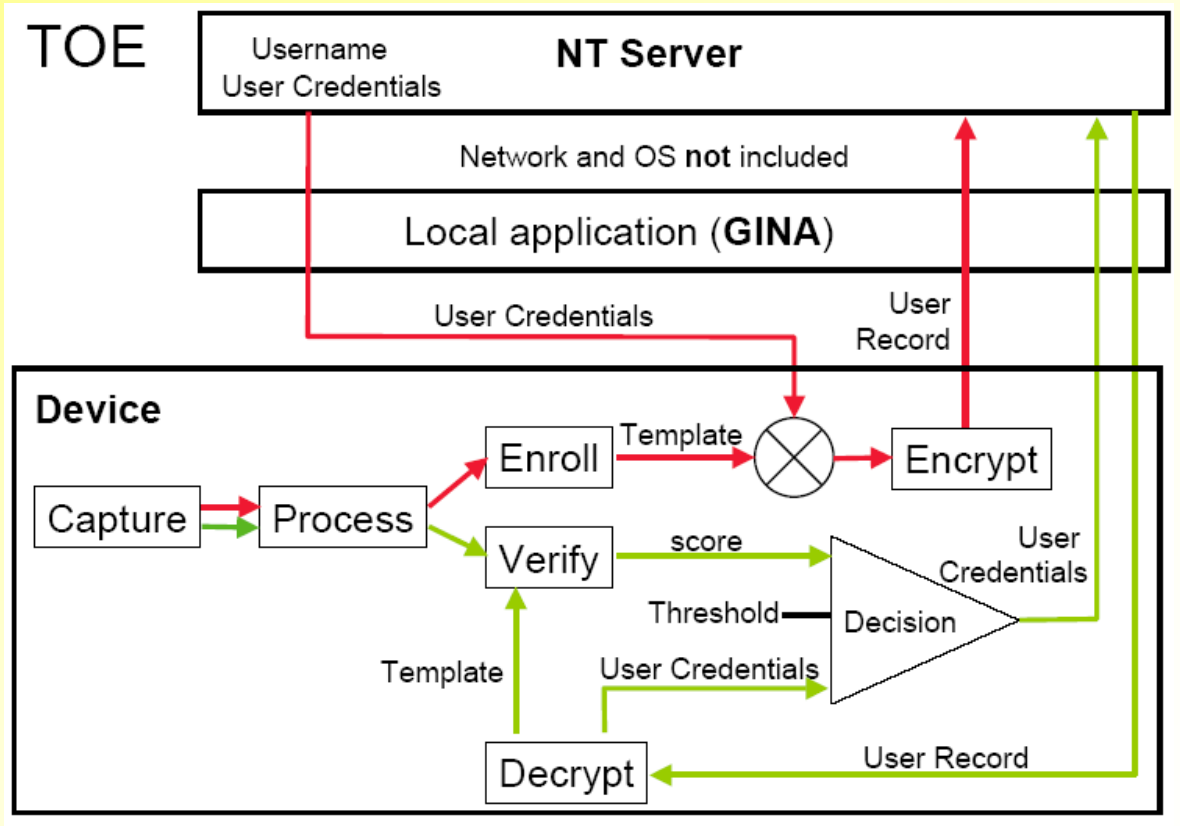
➔Common Criteria (I.)

➔ **Trusted Device**

➔ Šifrované komunikační kanály

➔ Zpracování *on-board* a šifrování

➔ Integrace do bezpečnostní architektury (WinNT)



➔Common Criteria (II.)

- ➔ Definování slabých míst (zranitelnosti):
  - ➔ Důvěrnost uživatelských dat (3DES)
  - ➔ Integrita dat (podpis)
  - ➔ Replikace starých dat (*Replay-Attack*)
  - ➔ Reverzní inženýrství na firmware
  - ➔ Analýza zbytků dat v paměti
  - ➔ Latentní informace, falzifikáty
  - ➔ Nastavení prahu (FMR / FNMR)
  - ➔ Aktivní útok – následky a možnosti

➔Ochrana dat (I.)

- ➔ Může / smí jiná aplikace číst a používat stejnou biometrickou šablonu?
- ➔ Pokud ano, jak je zajištěna důvěra mezi oběma aplikacemi?
- ➔ Jak zajistíme přístup k šabloně od neověřené aplikace?
- ➔ Mohou být data oddělena pro různé aplikace?
- ➔ Může toto všechno být docíleno, budeme-li brát na zřetel také principy ochrany osobních údajů (dat)?

- ➔ Musíme rozlišovat důvěrnost biometrických dat, důvěrnost osobních dat a důvěrnost šablony (souhrn obou dat do jedné množiny).

➔Ochrana dat (II.)

- ➔ Deset principů privátnosti (CSA model):
  - ➔ Zodpovědnost
  - ➔ Účel – identifikace / verifikace
  - ➔ Souhlas – přímý / implikovaný
  - ➔ Limitovaná data (např. data bez os. údajů)
  - ➔ Limitované použití
  - ➔ Přesnost
  - ➔ Důvěrnost
  - ➔ Otevřenost (ochrana)
  - ➔ Individuální přístup
  - ➔ Vyžádané svolení

➔Konec

➔Děkuji za pozornost!

Použitá literatura: [BAP02], [CC02], [DeW05], [DoD04], [Man02], [Mil02], [Pod01], [Sou02], [Sta02], [Til03]