Panel 2:
JRC

Mobile Identification in Global Environment
-
Challenges to perform Secure Identification and Verification using New Technologies

Klaus Keus,
JRC IPSC, Ispra, Italy

ANSI Homeland Security Standards Panel:
9th Annual Plenary Meeting: U.S. – European Collaboration on Security Standardisation Systems,
November 9th – 10th , 2010, Arlington, USA

- **Background**
  - **Motivation**
  - **Architecture**
- **Examples**
  - **e-MOBIDIG:** European **E**lectronic **Mob**ile **Id**entification **I**nteroperability **G**roup
  - **e-Refugee**
- **Conclusions**

- New European and international legislation for border crossing related applications and procedures is looking to
  - increase the security of travelers
  - addressing its need for flexibility

- The augmenting implementation of
  - upcoming new identification technologies in the next generation of digital / electronic based identity (and traveling) documents
  - broad use in different scenarios such as law enforcement and border control
  - a substantial contribution for the purposes of identification and verification of individuals and the authentication of documents
- Environment constraints, moving from stationary locations to more flexible ones, and combined with an increasing flexibility and openness require adequate flexible approaches
- mobility of people is becoming a central factor of behavior and life
- usage of new identification technologies as support and improvement in law enforcement should help to ensure the security of the society

Mobile ID devices may be employed for a variety of applications, where stationary booking station type environment is not possible, nor easily attainable.

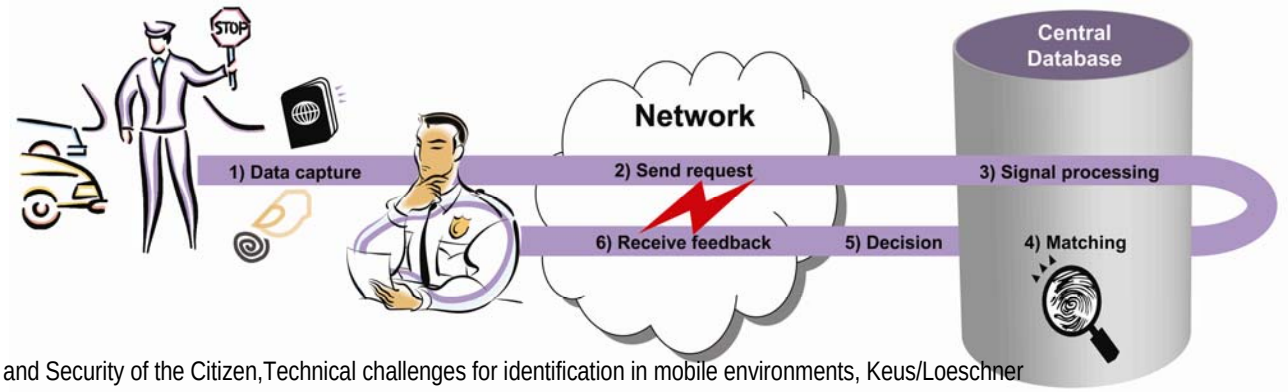
Common applications include:

- Mobile immigration and border control including application for refugees and asylums needs in non stationary environments
- Identification and verification in law enforcement applications
- Access control for buildings, computers and networks in flexible application environments[1]
- Multipurpose applications for defense area (identification and verification of solders in the field, access control to camps, …)[1]
- ....

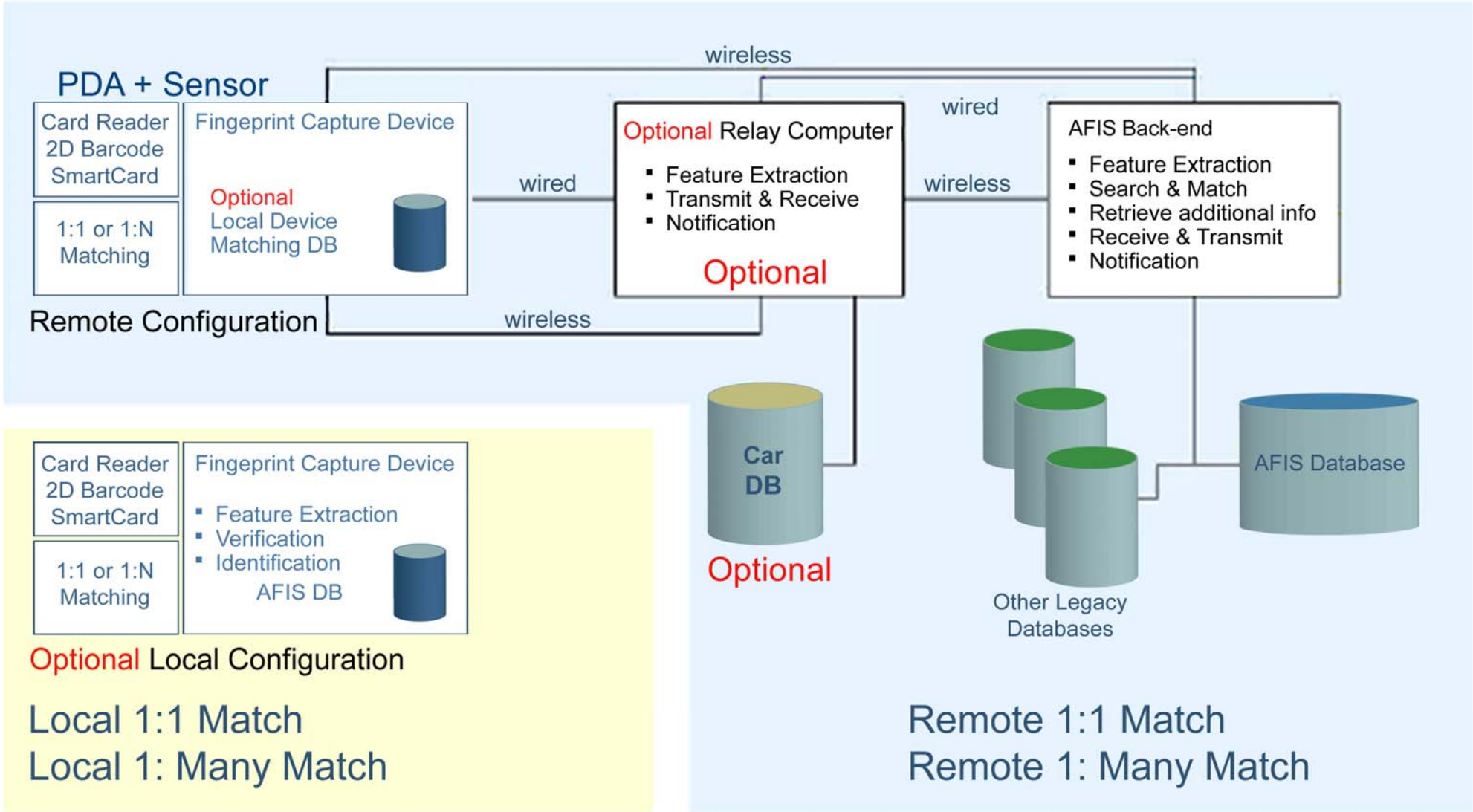
1) This issue will not be addressed here

- two basic objectives
  - secure and reliable identification of persons (*Identification* (1:n) and *verification* (1:1) of people's identity)
  - secure and reliable authentication of the identity token used (e.g. Authenticity of identity enabling documents)

- relevant data
  - held in identity enabling documents, or
  - stored in local and / or remote databases.



source: EUR 24548 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen,Technical challenges for identification in mobile environments, Keus/Loeschner



source: NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0,

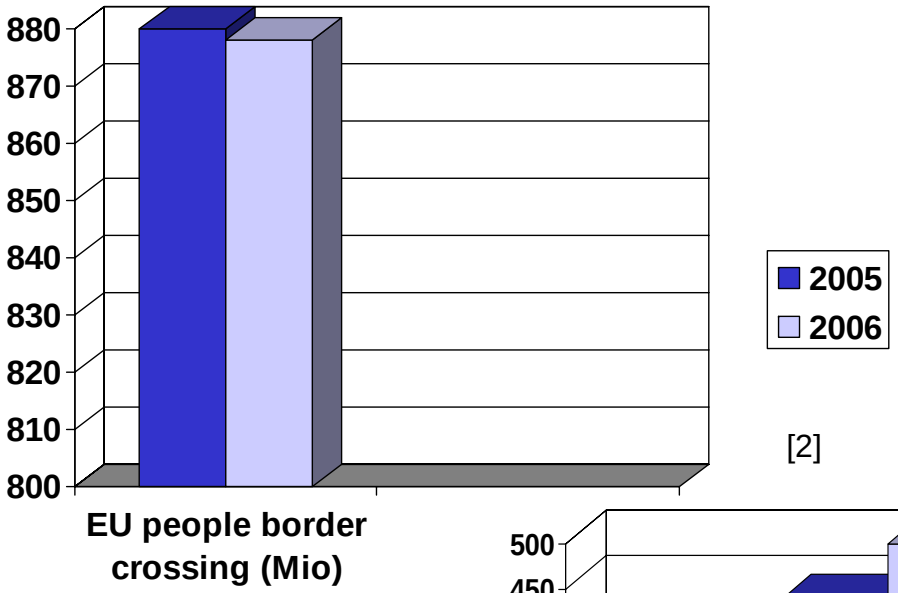
- A complete inventory is needed
  - Reader (e.g. *MRZ,* Chip, barcode, …),
  - Conformity, testing (including compliance and interoperability) and certification of reader and devices,
  - Capturing device requirements (biometrics (e.g. fingerprint, iris, face, ...)), performance, ..
  - Biometrics interchange requirements, matching SW, quality control, compression,
  - Computing platform and human interface,
  - Communication platforms / protocols incl. *MESH*,
  - Additional special requirements for communication (e.g. *GPS, 2G, 3|4G, …*)
  - **Security and Privacy issues** (data resident on the device or central storage),
  - Security of the communication (incl. confidentiality, integrity, availability, robustness, backup / recovery and continuity, user authentication, device authentication, *EAC*, *BAC*, login / audit trail, …),
  - Testing and certification of system,
  - Usability and environmental needs,
  - Ergonomic issues,
  - Charges, battery,
  - …

Example 1: *e-MOBIDIG*

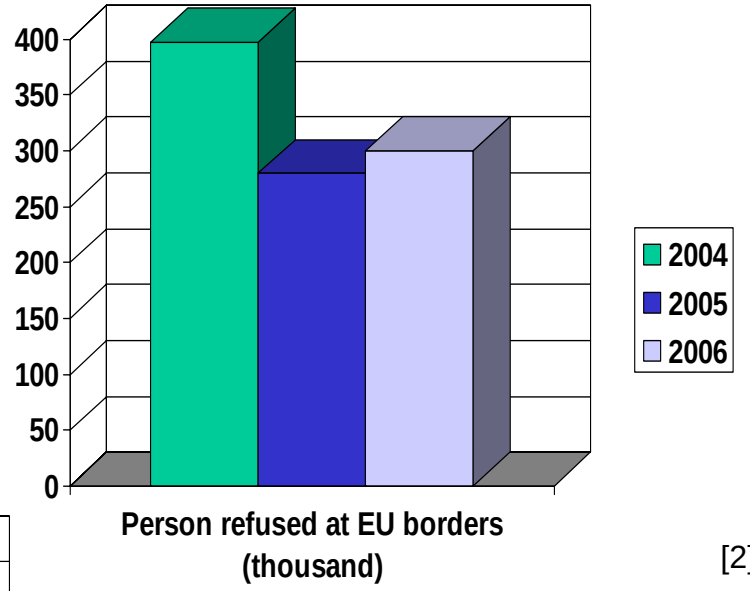
- Background
  - Motivation
  - Architecture
- Examples
  - **e-MOBIDIG**

  - e-Refugee
- Conclusions

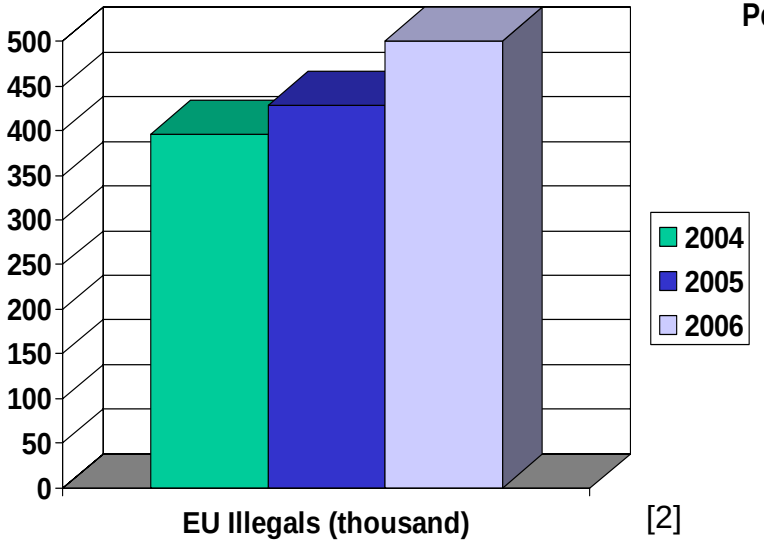
Example 1: *e-MOBIDIG - Background Facts*



[2]



[2]



[2]

up to 8 million illegal immigrants stayed within the EU in 2006, an estimated 80% of them within the Schengen area

⇒:

As of October 2008:

~ 733.000 persons were registered in the SIS for refusal of entry.

<u>Example</u> for Regional Commission:

~ 167.000 workers commute daily in the Greater Luxembourg Region,

crossing an internal Schengen border to get to their workplace

[2]: Source of data: http://en.wikipedia.org/wiki/Schengen_Area

- Existing experiences of Conformity and Interoperability Testing for stationary devices
  - Certify e-Passports for ICAO or ISO conformity
  - Conformity tests of reading devices under development (joint ETSI-JRC project)
- National mobile identity pilot projects have started or will be started soon in European MSs!
- The EU MSs initiated and launched a WG called e-MOBIDIG (electronic (European) Mobile Identification Interoperability Group) to:
  - Solve possible upcoming related challenges
  - Build a bridge between different national solutions, i.e. close the gaps between current offerings and upcoming requirements in Europe
- Respecting the outcome of the NIST WG: Mobile ID Device: Best Practice Recommendation, Version 1.0, Summer 2009[1]

[1]: NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0, S. Orandi / R. M. McCabe, NIST, Information Access Division, Information Technology Laboratory, 08/ 2009

Example 1: *e-MOBIDIG - The Application Area*

for border control and law enforcement applications:

- Identification and verification of people's identity
- Authentication of identity enabling documents

through the use of

- data held in identity enabling documents,
- identity data held on local and/ or remote databases (e.g. in those cases where an individual cannot or will not provide identity documentation).

- MOBIDIG will
  - Promote Information exchange and pave the way for further knowledge-based developments
  - Provide guidance towards harmonization and standardization
  - Give guidance on interoperability, technical challenges and related evaluation, certification and testing
  - Promote alignment, synergies, co-operation and co-ordination

Example 1: *e-MOBIDIG – History and Current Status*

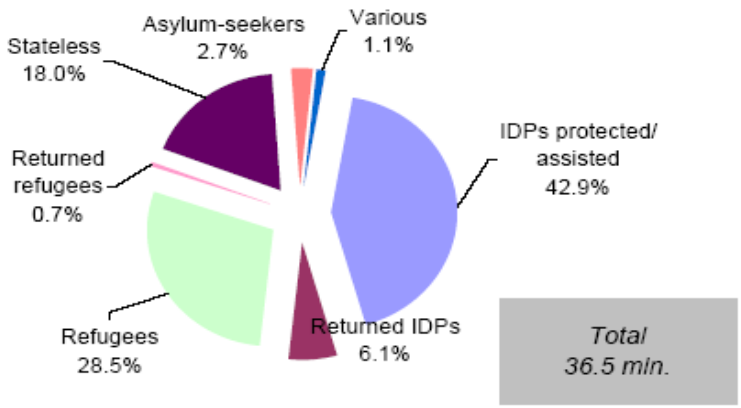
- Initiative started with 2 preparation WSs in November 2008 and June 2009 to look for a common European approach and understanding about Mobile ID
- 3 further WSs have been performed in the meantime (Oct. 2009, March 2010, June 2010)
- The 6th WS is running this week, Eindhoven, NL (in combination with a vendor day)

- Background
  - Motivation
  - Architecture
- Examples
  - e-MOBIDIG: European Electronic Mobile Identification Interoperability Group
  - **e-Refugee**
- Conclusions

Mobile Identification of Refugees using biometrics based mobile solutions

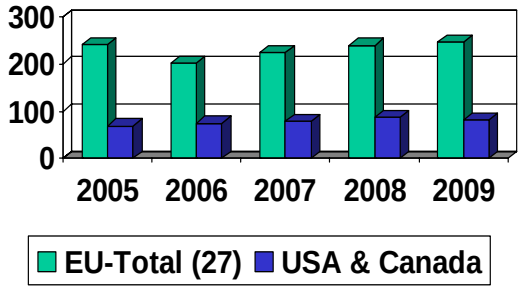
- Mobile based Identification of refugees in camps will contribute to **improve the security situation worldwide** (e.g. as part of peace keeping missions support)

Total population of concern to UNHCR by category, end-2009 [1]



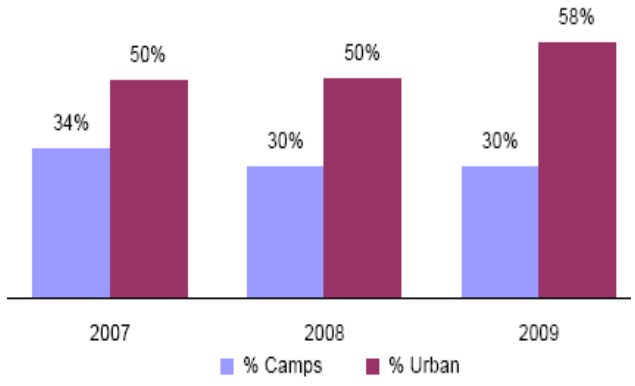
[3]

Number of Asylum applications submitted in Europe and USA/Canada in 2005-2009 (thousand)



[3]

Distribution of refugees by type of location *, end-2009



* Excludes unknown locations

[3]

[3] source: UNHCR : UNHCR 2009 Global Trends report: selected graphs, www.unhrc.org

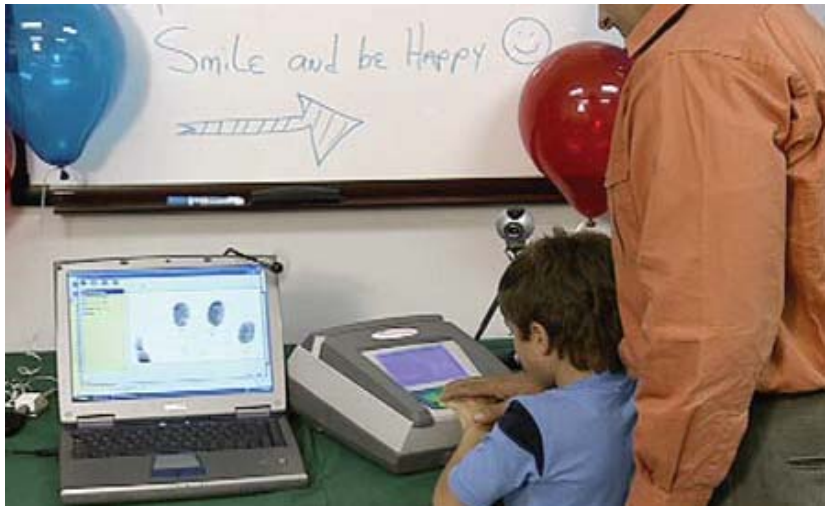
Example 2: e-Refugee – *a special technical Challenge: Fingerprint Identification for kids and Juveniles*

- **Children yet to be excluded when it comes to verification against templates older than 1 or 2 years:**
  - **Children <12 currently not fingerprinted for neither EU passport nor Visa Information System**
  - **EU Parliament and EDPS not convinced about feasibility and accuracy performance**
  - **Identification and verification to be guaranteed over time, given the validity of an enrolment for about 5 years**

Example 2: e-Refugee – *Fingerprint Identification for kids and Juveniles: Current Situation*

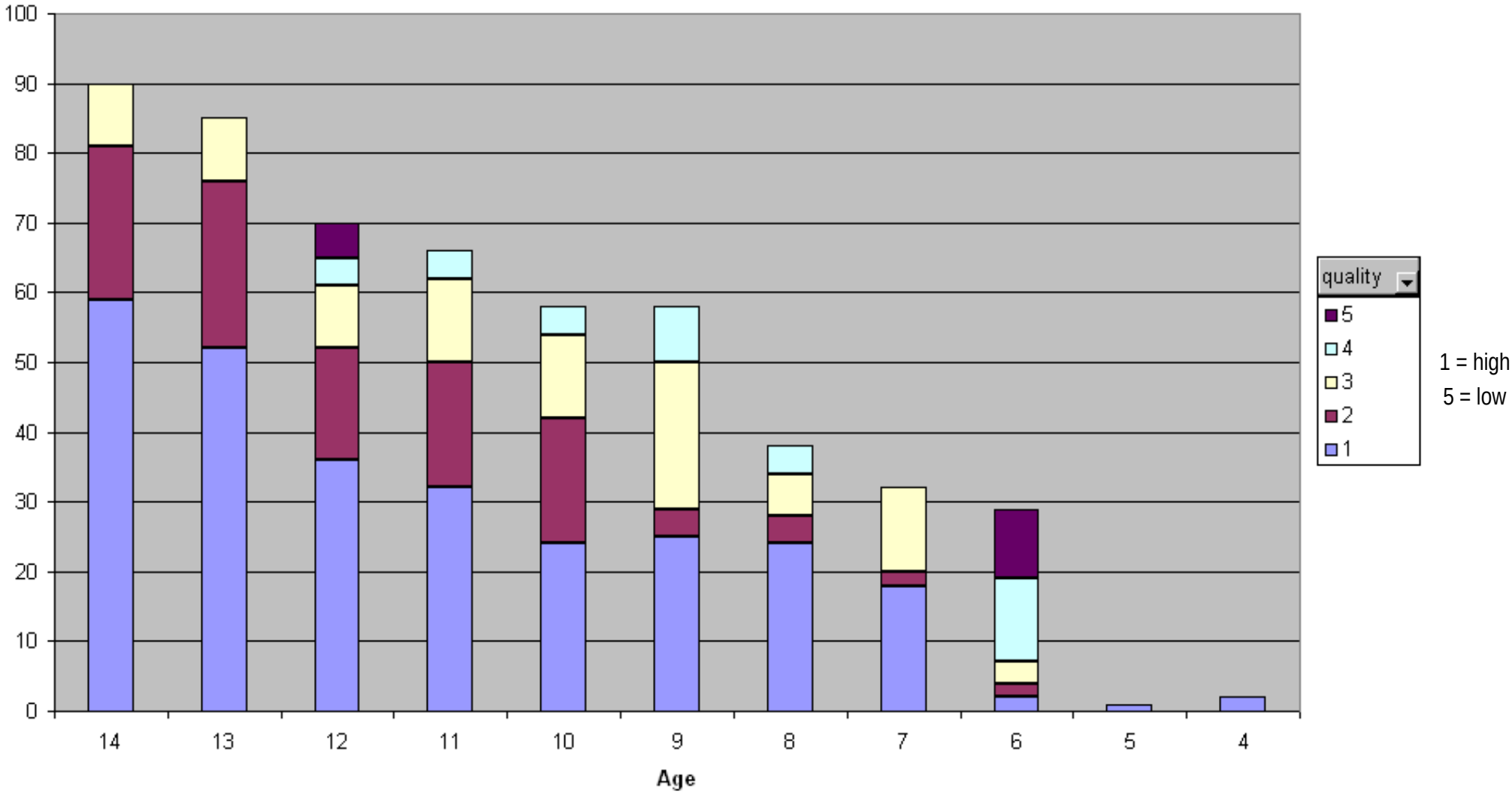
- **Matchers do not directly take into account the growing of the ridge pattern**
- **Resolution of scanners and assumptions about dimension of ridge structure is another obstacle**
- **Children fingerprinting exists only for documentation purposes but is hardly applicable to AFIS**

→ **Dedicated feasibility study is required !**



Source: Anthony's Mobile Fingerprinting

Example 2: e-Refugee – *Fingerprint Identification for kids and Juveniles: NFIQ: Examples from BIODEV*[4]



[4]: BIODEV = European study on operational aspects of visa application including biometric enrolment

Example 2: e-Refugee – *Fingerprint Identification for kids and Juveniles: Conclusions*

- **500 dpi images of very young children can be excellent**
  → ***Elaboration on relevant conditions necessary***

- **Some vendors have already introduced ridge distance adoption and experimented with assumed ageing**
  → ***Feedback to vendors on measured growing effect***

- **Yet no statistics available on recognition performance against aged templates in case of juveniles**
  → ***Need for a test database with significant time period between enrolments of individual juvenile test subjects***

Example 2: e-Refugee – *Current Situation*

- US Solutions (US-VISIT (United States Visitor and Immigrant Status Indicator Technology Program)):
  - Arrival and Departure Information System (ADIS):
    - US-CIS (Citizenship and Immigration Service)
    - Fingerprint (4 -> 10 finger)
    - 65 portable biom. collection devices (world wide)
    - Photo capture
    - Refugee directory
    - VPN, WINZIP encryption, …
    - Juveniles: OPEN
    - NOT compliant with NIST WS results[1] (because installed before summer 2009)
  - Automated Biometric Identification System (IDENT)
- **Australian DIAC** (juveniles fingerprint: > 15 years, facial image)
- **UK IAFS System** (Immigration Fingerprint System, replacement of the former IABS (Immigration and Asylum Biometrics System)
- ….

[1]: NIST: Mobile ID Device: Best Practice Recommendation, Version 1.0,

- Background
  - Motivation
  - Architecture
- Examples
  - e-MOBIDIG: European Electronic Mobile Identification Interoperability Group
  - e-Refugee
- **Conclusions**

- **Increasing importance for Mobile Identification and verification**
  - Police and Immigration need ID assurance and alerts on identity in all areas of operations
  - Complex range in technology and operations to manage - Fast changing capabilities, technology and system/enterprise integration
  - Enforcement, defense and Immigration - different from mass retail market
  - Mobile access to confidential systems: = RISK
  - Business justification - Economical pressure for value of money and cash savings

- **Multipurpose Application areas**
  - **Local**
  - **Regional**
  - **National**
  - **Transnational**
  - **global**

- **Mobile ID for refugees in camps is a global challenge requiring an international harmonised approach**
- **Excellent technical input is available (e.g. from US, EU, other?)**
- **Excellent topic for cooperation and joint international standardisation initiative / work, supporting UN HCR**
- **….**

Thank you for your attention !

Questions?