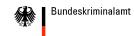# Motivation and Use Cases for NFIQ 2.0

Oliver Bausinger
Federal Office for Information Security

Section
Inspection Infrastructures and Architectures

Bundeskriminalamt
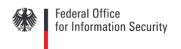
Fraunhofer IGD

CASED

secunet

Status

- **Official documents with fingerprints**
  - European ePassports
  - European Residence Permits
  - Identity Cards (partially)

- **European Visa Information System (VIS)**
  - Tenprints from all Schengen (short-time) Visa applicants
    - Data stored for 5 years
  - Target size up to 100 Mio. records
  - Biometric verification will soon be mandatory at all Schengen border checks

- **Criminal AFIS**

- **Future RTP programs might use fingerprints**

Federal Office
for Information Security

Challenges in fingerprint biometrics deployment

Federal Office for Information Security

- Problems
    - Technical
        - Heterogenous environments
        - Different software vendors and versions
        - Interoperability issues
    - Organizational
        - Multiple enrolment processes have to be conducted by the same operator
    - System design
        - At enrolment stage, typically the biometric verification or identification system vendor is unknown
        - Large scale identification scenarios (AFIS) have immensly high quality requirements
            - Garbage in, garbage out!

Challenges in fingerprint biometrics deployment (2)

Federal Office
for Information Security

- Timing considerations
  - Timing constraints are the biggest driver in the design of an enrolment and verification process
  - For many instances, quality correlates directly with time
    - No only technical, but als organizational, e.g. user guidance
  - Time is expensive
    - Officers are expensive
    - Room is expensive
  - Which quality is required by the system?
    - How much time (on average) do I need to reach the desired level?

Stages of possible quality control

- Scanner level

  - Hardware built-in auto capture

  - Hard to tweak to a specific application scenario

- Capture software level

  - Beyond the vendor SDK

  - Run things like NFIQ, vendor software kits, other QA algorithms

  - Implement target system specific thresholds

- Process level

  - A background system rejects the fingerprints

  - Trigger recapture only when necessary

    - Avoid this as often as possible because of timing considerations, especially when round trips to central systems are involved

Federal Office
for Information Security

Problem statement

- There's no common understanding of a term like **fingerprint of sufficient quality**

  - Sufficient for which application?

  - Quality requirements differ a lot for different applications (e.g obviously between 1:1 and 1:n)

  - But, you say, there's quality in the standards.

    - An algorithm should produce a value in [0, 100].

    - Most don't.

    - And even if, those scores are not calibrated to an accepted base line.

    - And even if, there's no consense on any kind of thresholds for specific applications

- OK, let's try again …

Problem statement (2nd try)

- There's no common language to establish an interoperable definition of **fingerprint of sufficient quality** for a specific application scenario

    - When developing an application scenario, define a common understanding of the required image quality

    - We need the language for doing this

    - And we need a baseline tool for doing this

Expectations for the future

- NFIQ 2 will be good enough to be used as baseline tool for defining **fingerprint of sufficient quality**

- NFIQ 2 will be the calibration base for vendor QA tools

    - Vendor QA tools will not go away, but – at least – for large scale applications will be comparable (statistically, not on a by-image-basis) to NFIQ 2

    - Vendor QA tools should not have a need to augment NFIQ 2 itself, but it should be sufficient for a vendor to define a specific threshold for a specific application

- NFIQ 2 will be used in all major fingerprint-based biometrics systems.

- Of course, the term of fingerprint quality will not be stable, but the biometric community will have a way to adapt, refine, reformulate it according to the evolution of fingerprint technology

Questions

Contact

Federal Office for Information Security
Inspection Infrastructures and Architectures

Oliver Bausinger
oliver.bausinger@bsi.bund.de