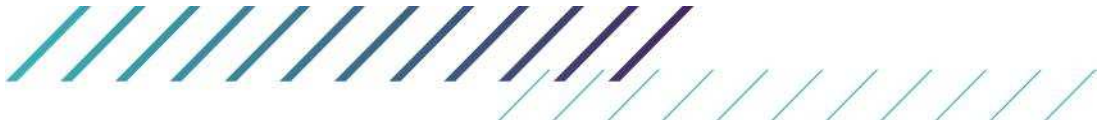
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

IDENTITY MANAGEMENT

An overview about biometric identification

Bernhard Strobl
Sensing and Vision Solutions
Center for Digital Safety & Security
AIT Austrian Institute of Technology



IDENTITY MANAGEMENT

Overview

- Three basic factors
- Combinations
- Enrollment, verifikation and identifikation
- Biometric operation modes
- Different biometric factors
- Performance Measurements – a 3 slides intro
- Presentation Attacks (e.g.: Morphing)
- Example Bordercontrol
- Newest Developments

IDENTITY MANAGEMENT

3 Basic-Factors of Authentifcation

Knowledge (What you know)	**Hardware Token** (What you have)	**Biometrics** (What you are)
		
Password Passphrase PIN Pattern	Key USB Stick Smart Card	Face Fingerprint Iris Voice Signature Gait DNA

IDENTITY MANAGEMENT

Advantages/Disadvantages

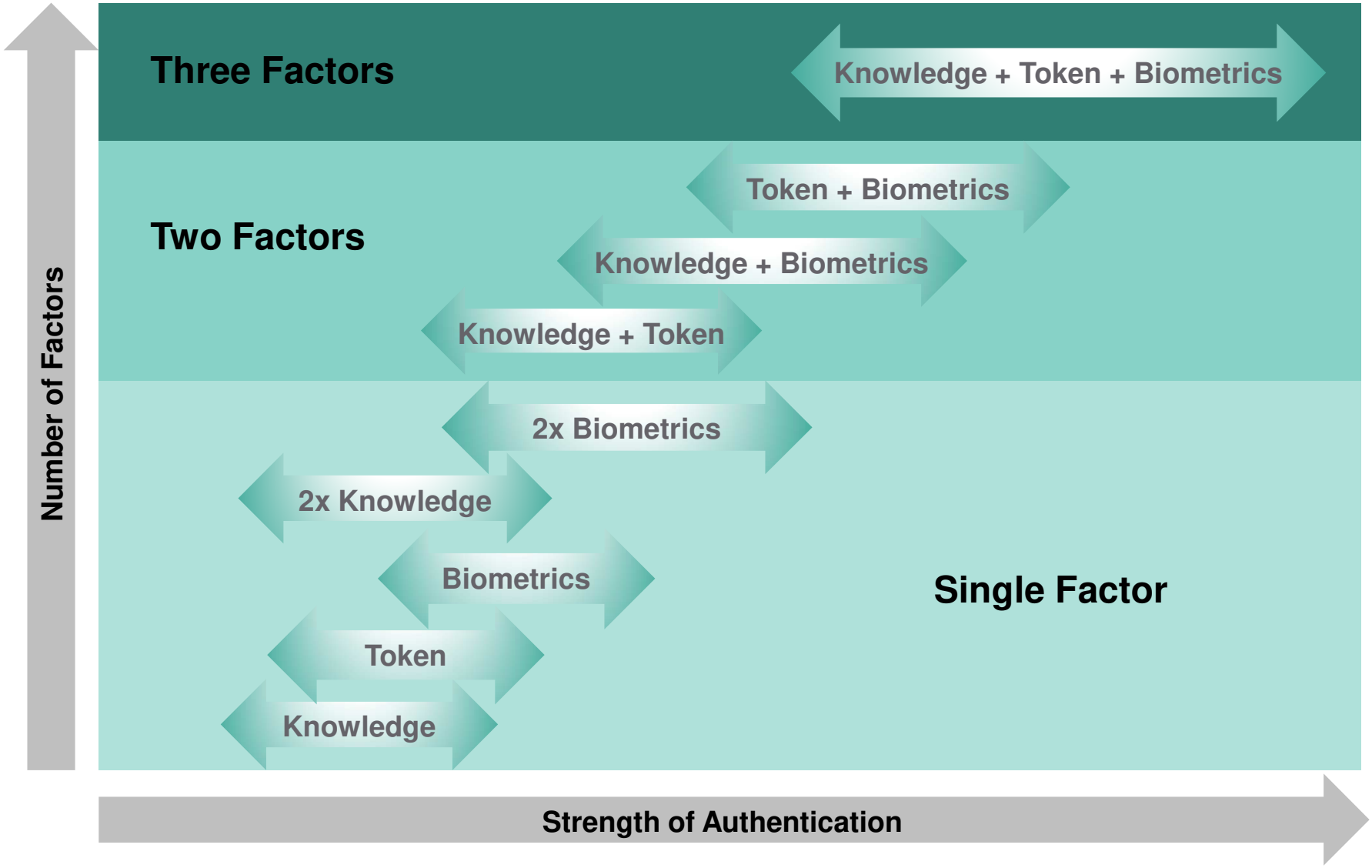
- Knowledge
  - Weak security
  - Can be figured out easily
  - “memos” for so many different accounts
  - Usage of short, simple easy to remember PWDs
  - Transferable, changeable
- Tokens
  - Loss, theft
  - costs
  - In combination with printed info: conclusions to owner !
  - Transferable, changeable
- Biometrics
  - Unique !
  - But good samples necessary-> Capture technique-> Costs
  - Special hardware necessary
  - Impostor Attempts (spoofing)
  - Where are the registered samples stored (privacy issue)?

20 Of The Most Popular Passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17. dragon
18. passw0rd
19. master
20. hello

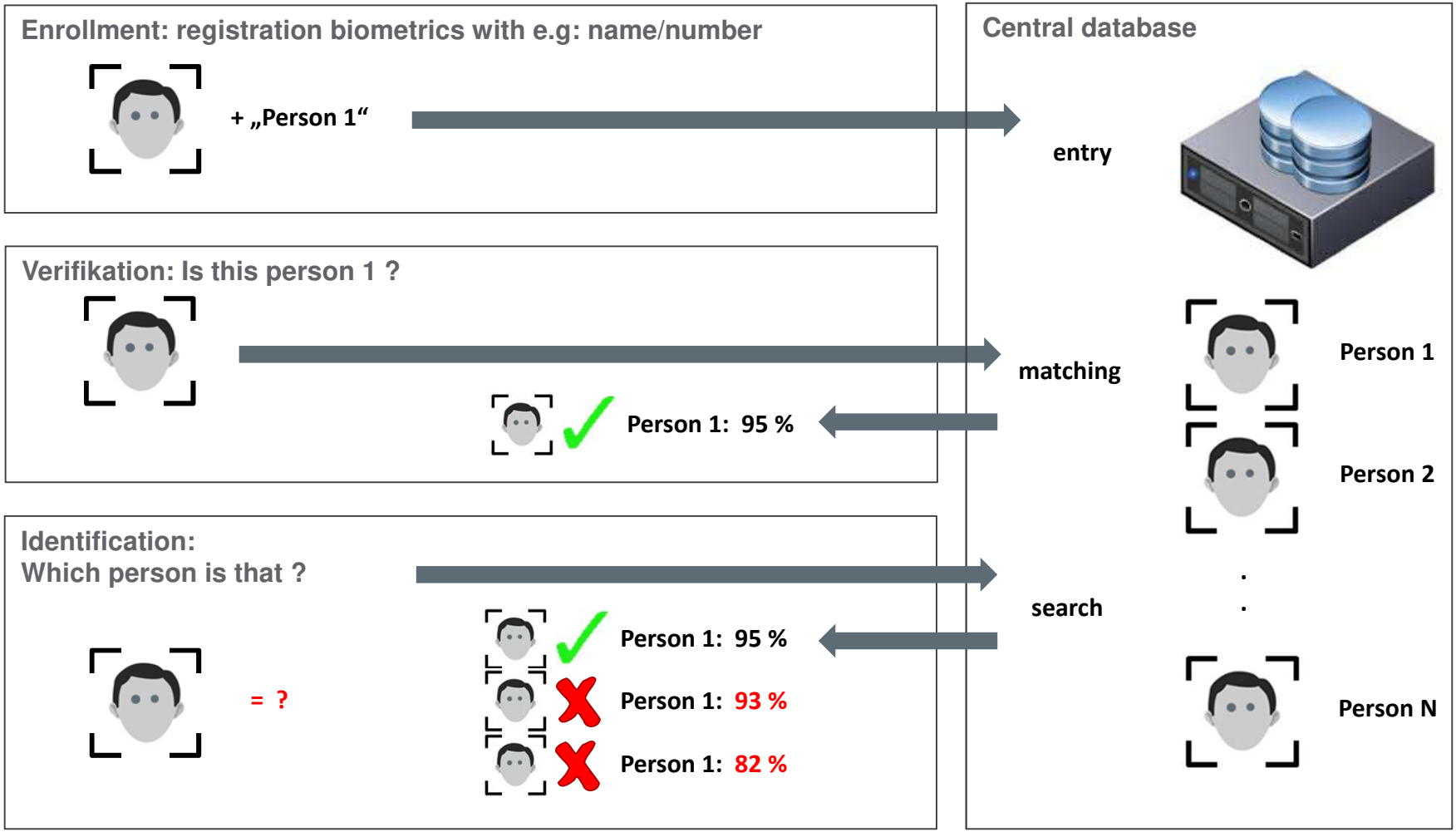
IDENTITY MANAGEMENT

Mixture of factors



IDENTITY MANAGEMENT

Enrollment/Verification/Identification

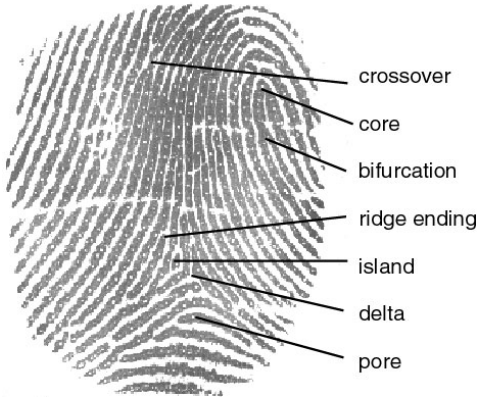


IDENTITY MANAGEMENT

Biometric operation

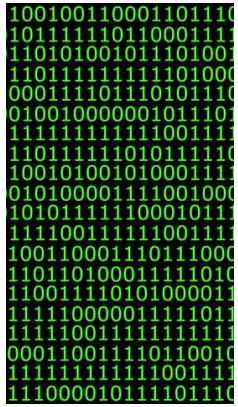
Capture

Feature Calculation



Calculation of digital template

Merkmal 1
Merkmal 2
.
.
Merkmal N



comparision (simplified)

Sample A

Sample B

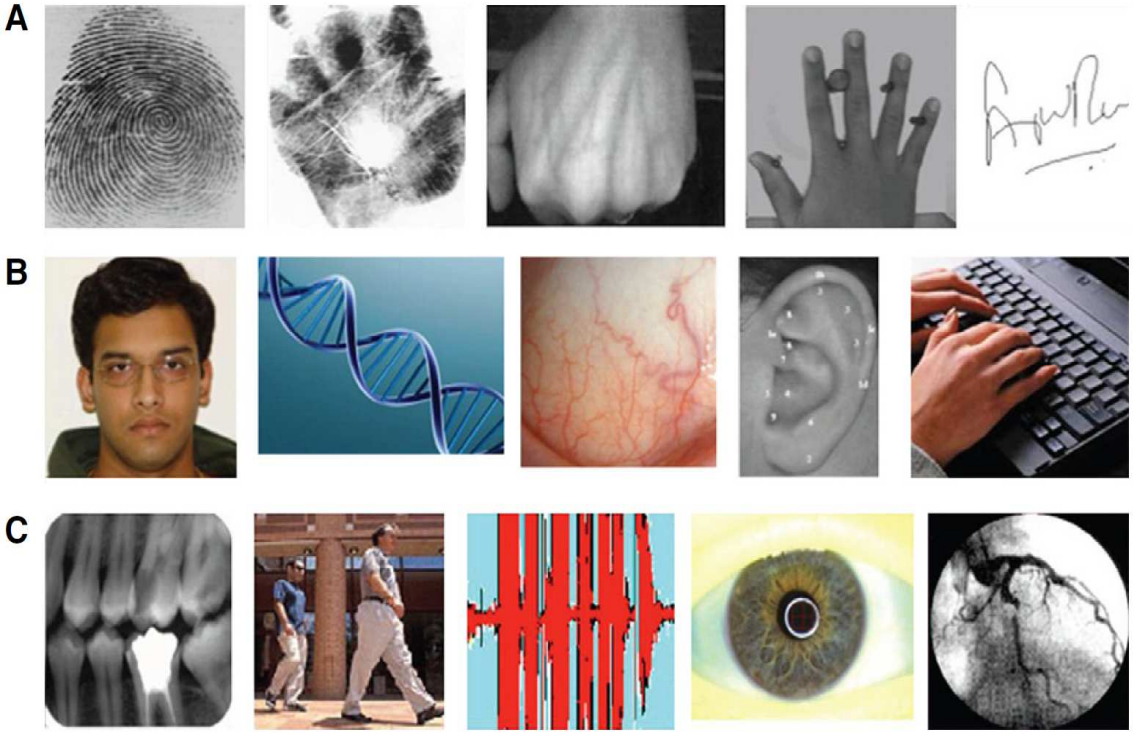
calculate similarity values over all features [1..N]

Summarize all similarity values

Result is apropability: e.g: 87 %

IDENTITY MANAGEMENT

Overview of biometric modalities



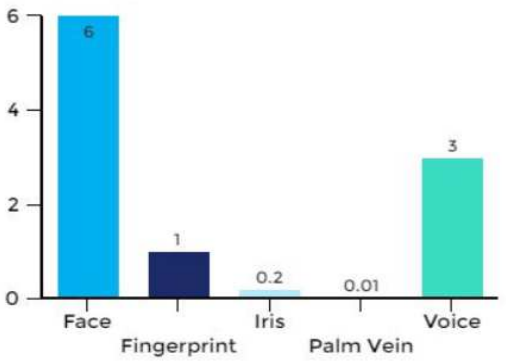
(A)
Fingerprints
Handprint
Hand Veins
Hand Form
Signature

(B)
Face
DNA
Sclera (on the eyeball)
Ear Form
Dynamic keypress pattern

(C)
Teeth
Gate
Speech/Voice
Iris/Retina
Smell

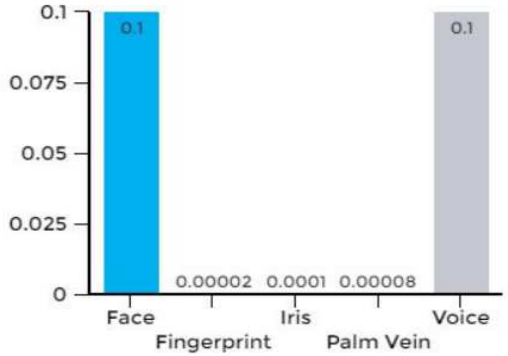
IDENTITY MANAGEMENT

Biometric Overview



False Rejection Rate

False rejection rate (FRR) is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user.



False Acceptance Rate

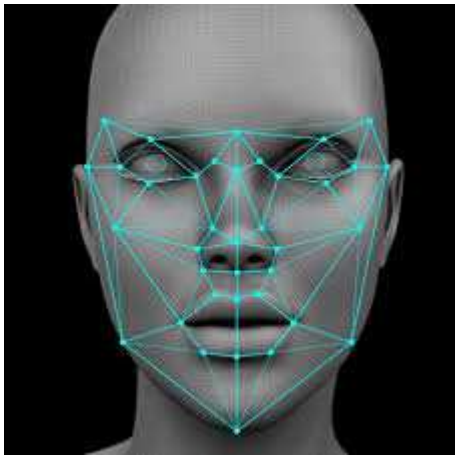
FAR is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

Modality	Accuracy	Ease to Use	User Acceptance
Face	Low	High	High
Fingerprint	High	Medium	Low
Iris	High	Medium	Medium
Palm Vein	High	High	Medium
Voice	Medium	High	High

https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/

IDENTITY MANAGEMENT

Face

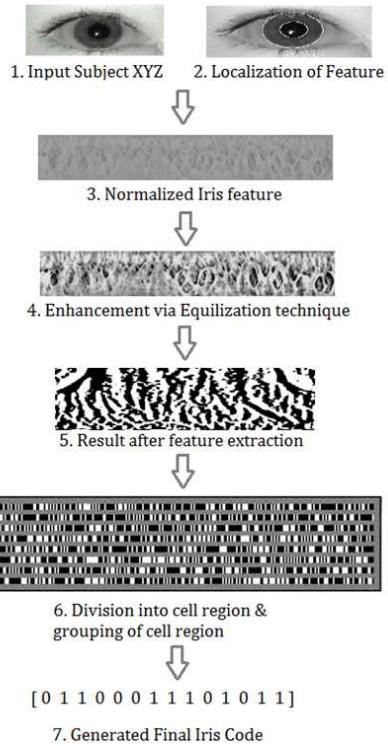


- Pros
  - Capture process relatively simple
  - Integration relatively simple
  - Broad supplier field
  - Also works on video streams
  - Application at border control (live with pass face/fingerprints)
- Cons
  - Good image quality is necessary
  - High FAR und FRR
  - Problems with capture angle
  - Face changes over time (glasses, beard, make-up, weight)

IDENTITY MANAGEMENT

Iris

- Pros
  - Extrem good entropy
  - Matching calculates very fast
  - Best sample India: 3 years enrollment, 1 Mio/day
- Cons
  - Capture process technically complex
  - Infrared



IDENTITY MANAGEMENT

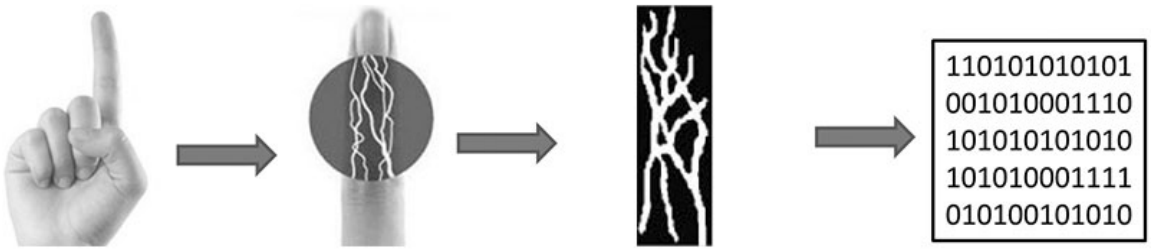
Fingerprints

- Most used biometric trait
- Problems with dry/wet fingers
- Some people don’t have a lot of features on the fingertips
- Latent finger prints on the scanner

IDENTITY MANAGEMENT

Veins

- Hemoglobin in Veins absorbs light in infrared wave length, therefore visible as dark markings
- Rarely used
- Only on supplier
- Claimed to have excellent recognition rates (supplier)
  But rare independent studies known
- Liveness detection included



AIT Sensor

Available Sensor

IDENTITY MANAGEMENT

ROC: Receiver Operating Characteristic (a 3 slides intro)

- Evalution of recognition capabilities
  - Genuine Attempts (good ones)
  - Impostor Attempts (spoofing)
  - Generation of ROCs on biometric match server

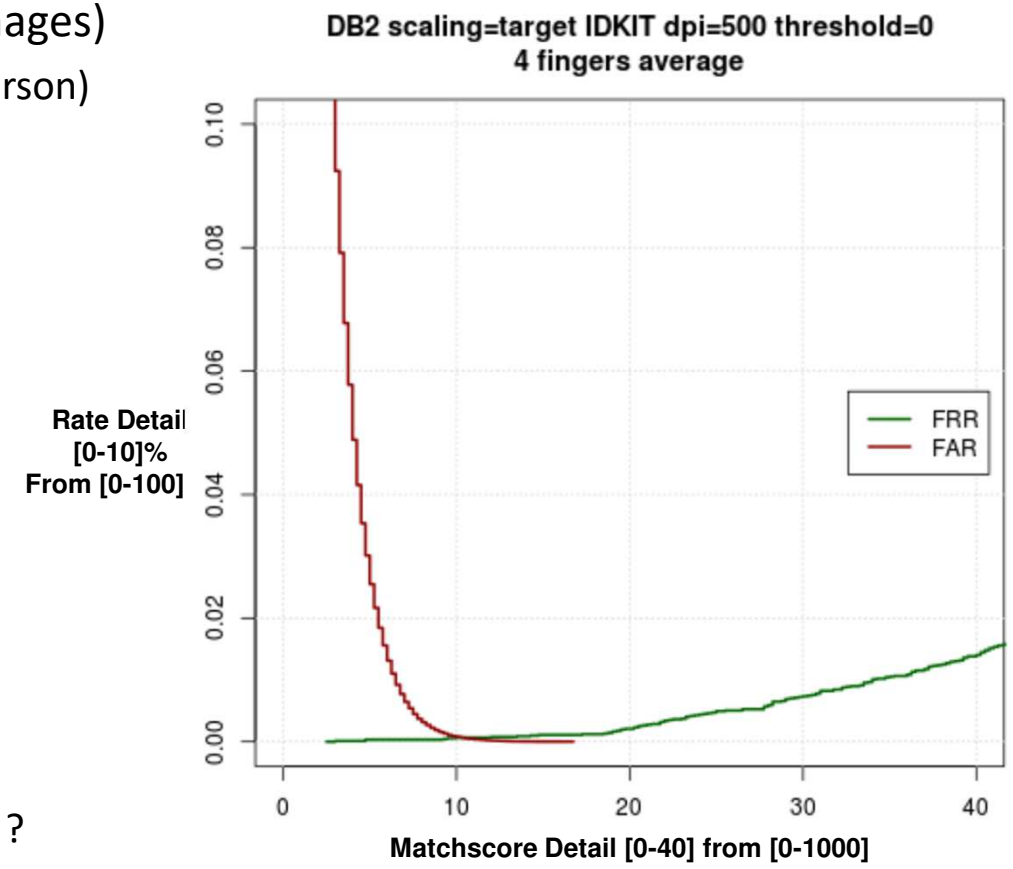
- FAR - False Acceptance Rate:
  - How man are (wrongly) accepted, which should be rejected (Impostors)
- FRR - False Rejection Rate:
  - How many are (wrongly) rejected, which should be accepted (Genuines)

- EER – Equal Error Rate
  - FAR und FRR are equal, to allow comparisons among different systems
- DET – Detection Error Trade-off:
  - E.g.: 0.1% FRR @ 1/10000 FAR

IDENTITY MANAGEMENT

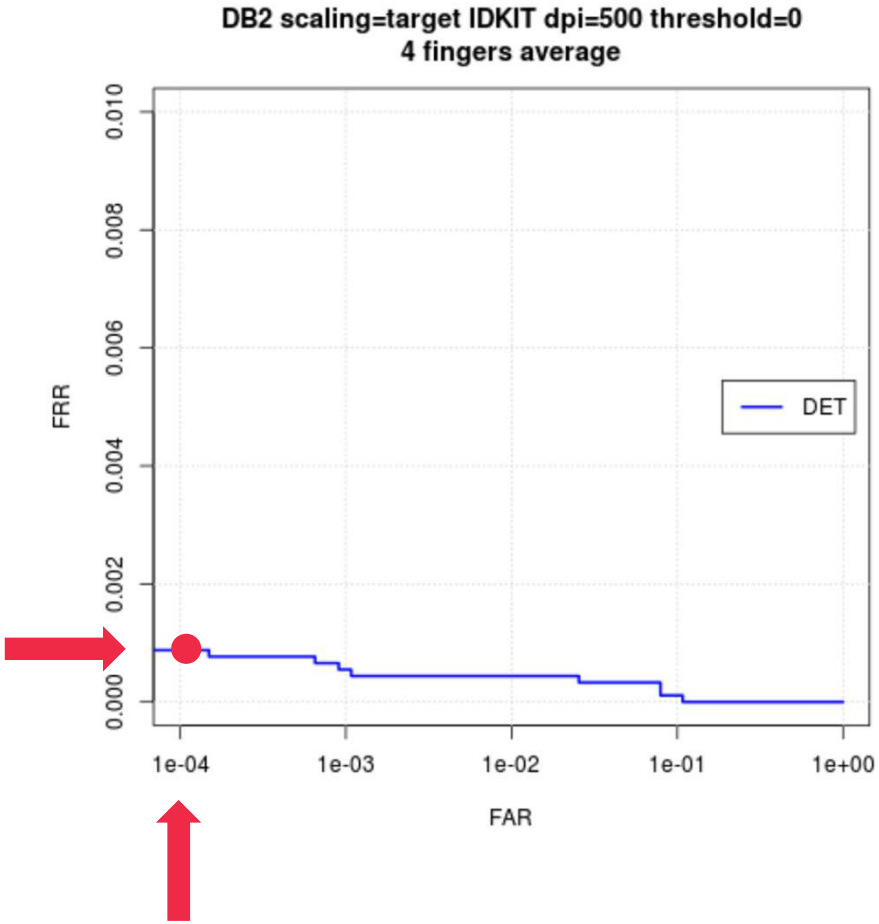
Example ROC for AIT contactless Fingerprints:

- Data Set (1920 fingerprints images)
  - 10 genuine attempts (same person)
  - 12 different persons
  - 8 fingers (2 hands)
  - 2 smartphones
  - -> ~ 2 Mio matches
  - FRR/FAR graph
  - Rate [0-100%]
  - Matchscores [0-1000]
  - -> EER @ ~0,1%
  - -> operational bias score: 12
    - What do you want ?
    - Better FRR or better FAR ?



IDENTITY MANAGEMENT

Example ROC:



- DET Graph Interpretation:

AIT 4 FP Contactless:
0.1% FRR @ 1/10.000 FAR

Every 1000th person is wrongly rejected when
every 10.000th person is wrongly accepted

MS Surface pro 4 (Infrared Face):
5% FRR @ 1/100.000 FAR

Every 20th person is wrongly rejected when
every 100.000th person is wrongly accepted

IDENTITY MANAGEMENT

Face Spoofing:

- Applied during livecheck
- -> liveness detection (micromovements, eyelids)
- -> multispectral capturing, infrared images

IDENTITY MANAGEMENT

Morphing Attack:

- Applied during Enrollment
- -> Enrollment not with Foto but Live(!)

IDENTITY MANAGEMENT

Fingerprint Spoofing:

- Needs a lot of time
- Complicated to use latent fingerprints from (e.g. a glass)
- 4 fingers to spoof at the same time is tricky
- Does not work for attended systems
- -> Liveness check of samples: color, light response, heartbeat

IDENTITY MANAGEMENT

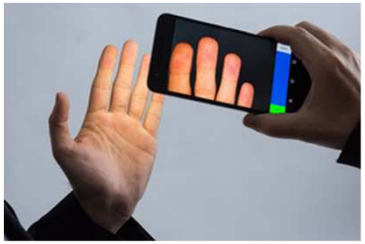
Grenzkontrolle:

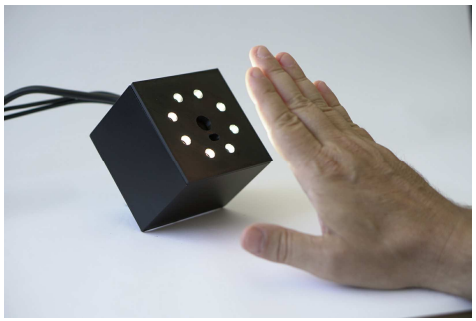
- Biometric, electronic traveldocuments (eMRTD)
  - Face, 2x finger
  - Active & Passive Authentication of eMRTD
  - Until now, now passport was copied/cloned/changed
  - Readout of fingerprints only by police/LEA
- Check process (for Schengen Citizens)
  - Read of MRZ
  - Enables access to level 1 via BAC protocol (digital face image)
  - If certificates available, access to level 2 via EAC protocol (fingerprints)
  - Compare passport nr. and name in SIS-II database
    (lost and stolen travel documents, persons search)
  - eGate: automatic passport read with face recognition
- Check process (for NON Schengen Citizens)
  - Validity of eMRTD (passport)
  - MRZ and face recognition
  - If Visa available/necessary; check if fingerprints are the same (VIS database)

IDENTITY MANAGEMENT

Newest developments

- There is no “Silver Bullit” to solve all challenges
- But a combination of 2 Traits or 2 factors increases security
  Iris and face; chipcard and Iris
- MOC: Matcher on Card
- Mobile Systems: MobilePass or Smartphone based
- Contactless biometrics for fingerprints





AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Bernhard Strobl

Thematic Coordinator
Intelligent Cameras and Video Analytics
Center for Digital Safety & Security
bernhard.strobl@ait.ac.at