Biometric Recognition – Myths dispelled and Best Practices

Christoph Busch

CRISP / European Association for Biometrics / NTNU
http://www.christoph-busch.de

Biometrics in Finance

Frankfurt - December 07 2018

CRISP
Center for Research in Security and Privacy

European Association for Biometrics
eab
Human Identity in Europe

NTNU

Agenda

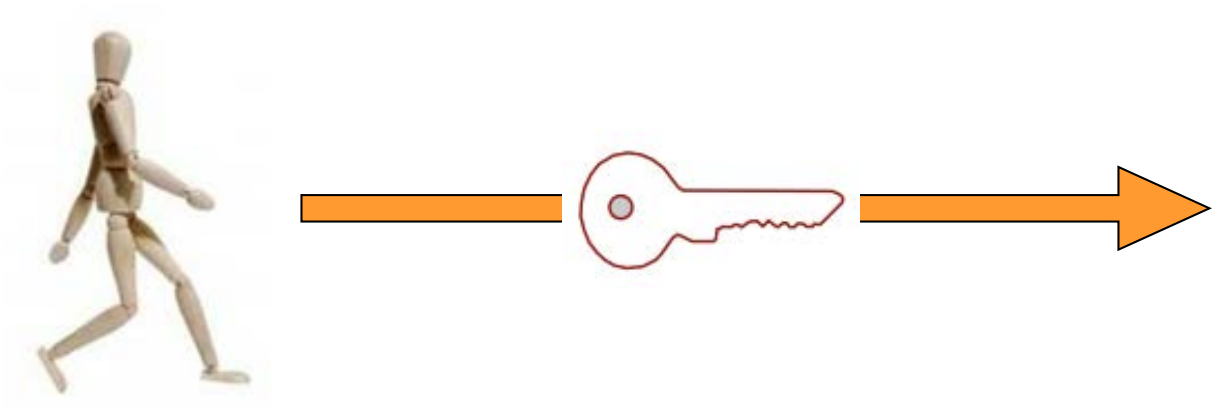
- The foundation of biometrics
- From Biometric Myths to Reality
- Mobile Biometrics
- Standards
- A Privacy Compliant Biometric Payment Protocol
- Some thoughts on Artificial Intelligence

Introduction to Biometrics

Access Control

Traditionally we place between

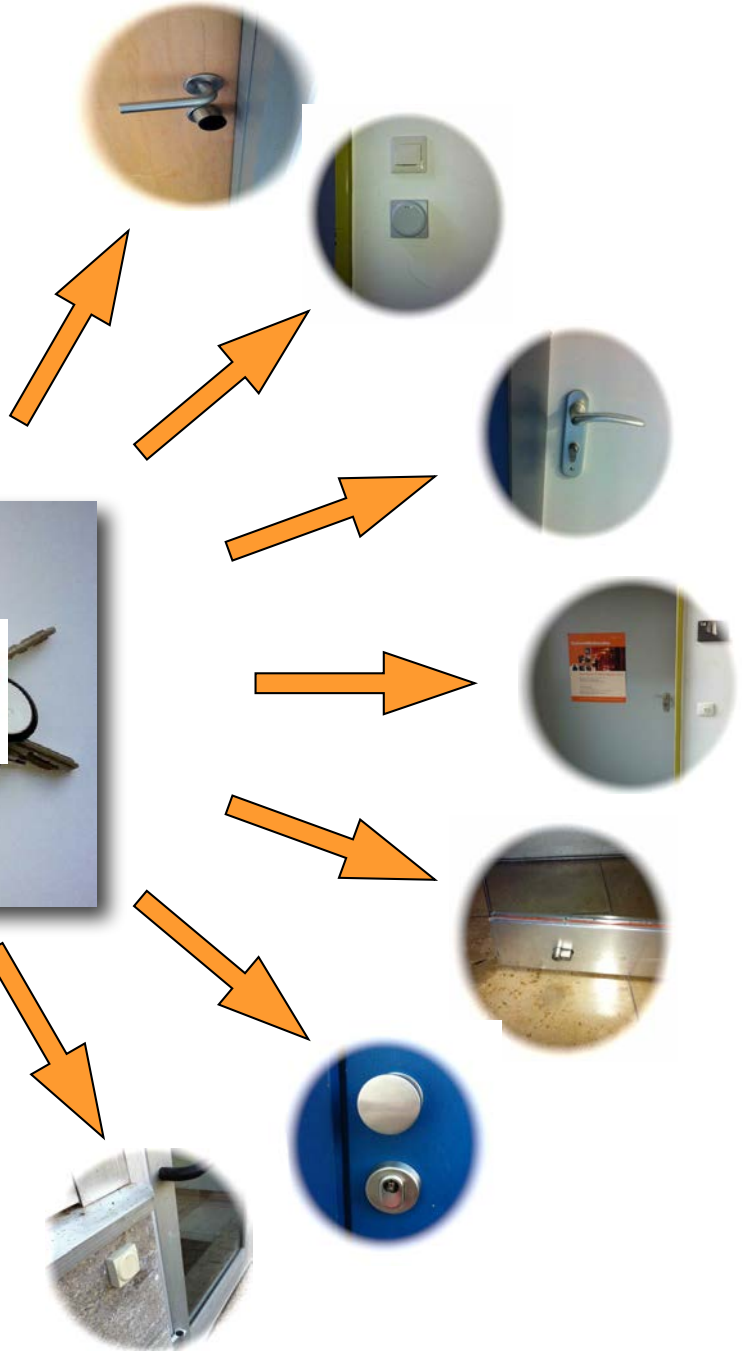
- individuals
- and objects
- a token (i.e. key)



Access Control

But in reality individuals

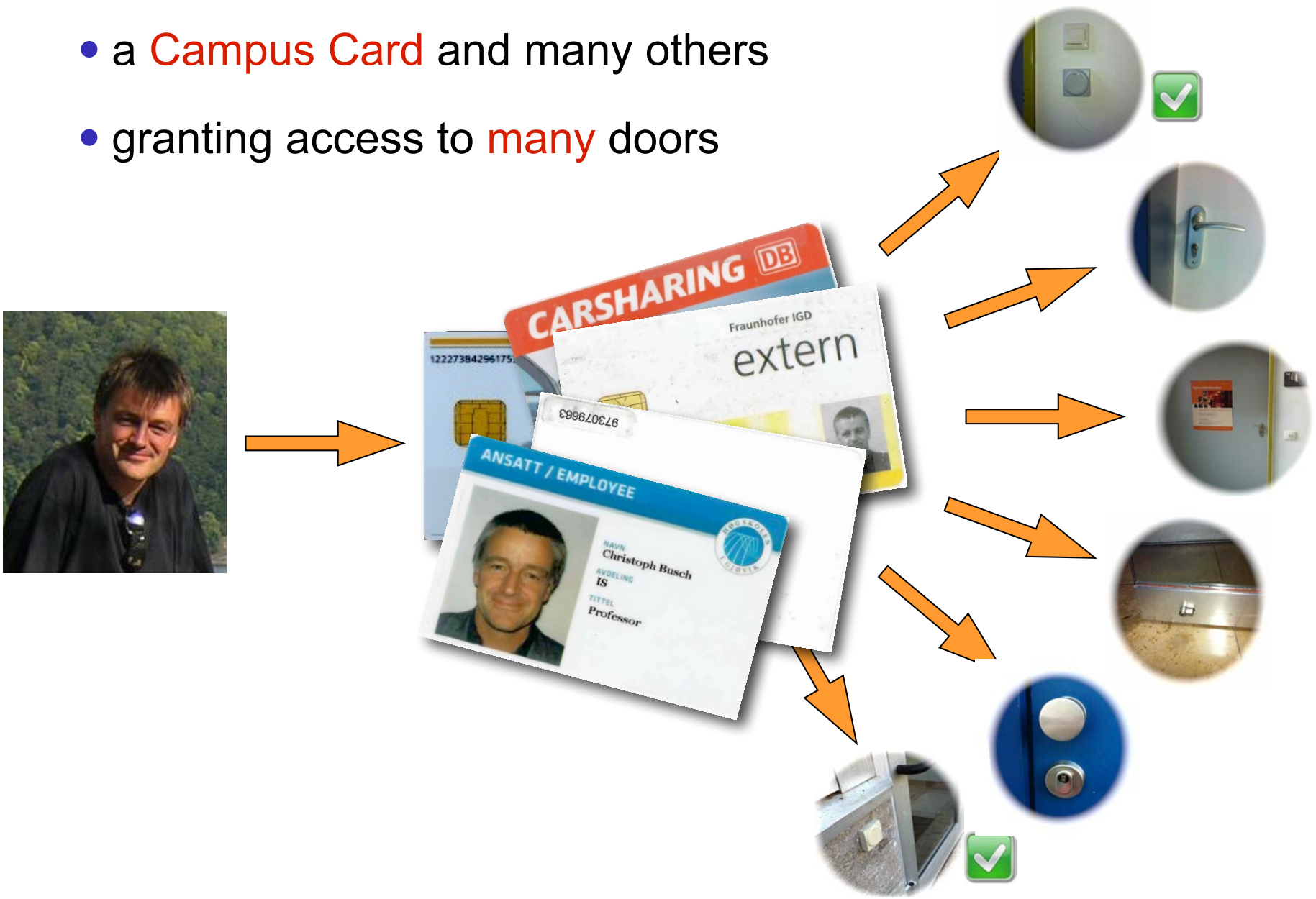
- do not have just one
- but many keys
- granting access to many doors



Access Control

In addition i have

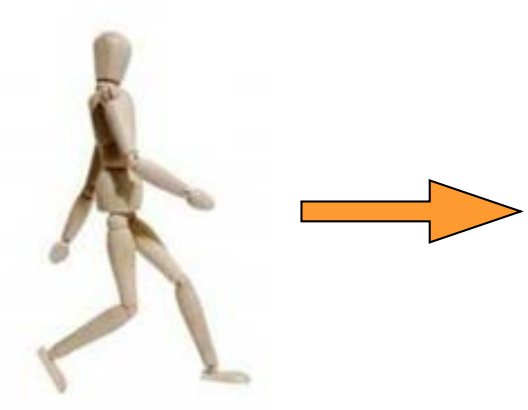
- a Campus Card and many others
- granting access to many doors



Access Control

For some individuals

- the collection of cards is quite impressive and inconvenient



Access Control

Identity authentication can be achieved by:

- Something you know:
  Password, PIN, other secret

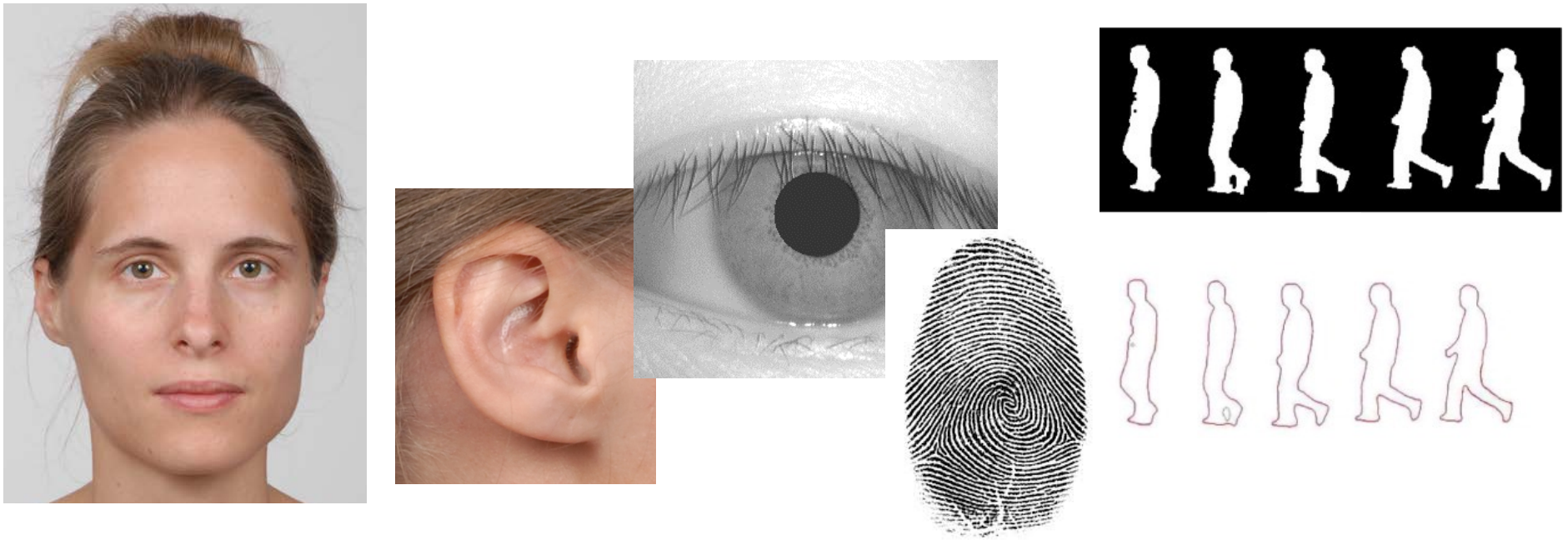
- Something you own:
  SmartCard, USB-token, key

- Something you are:
  Body characteristics

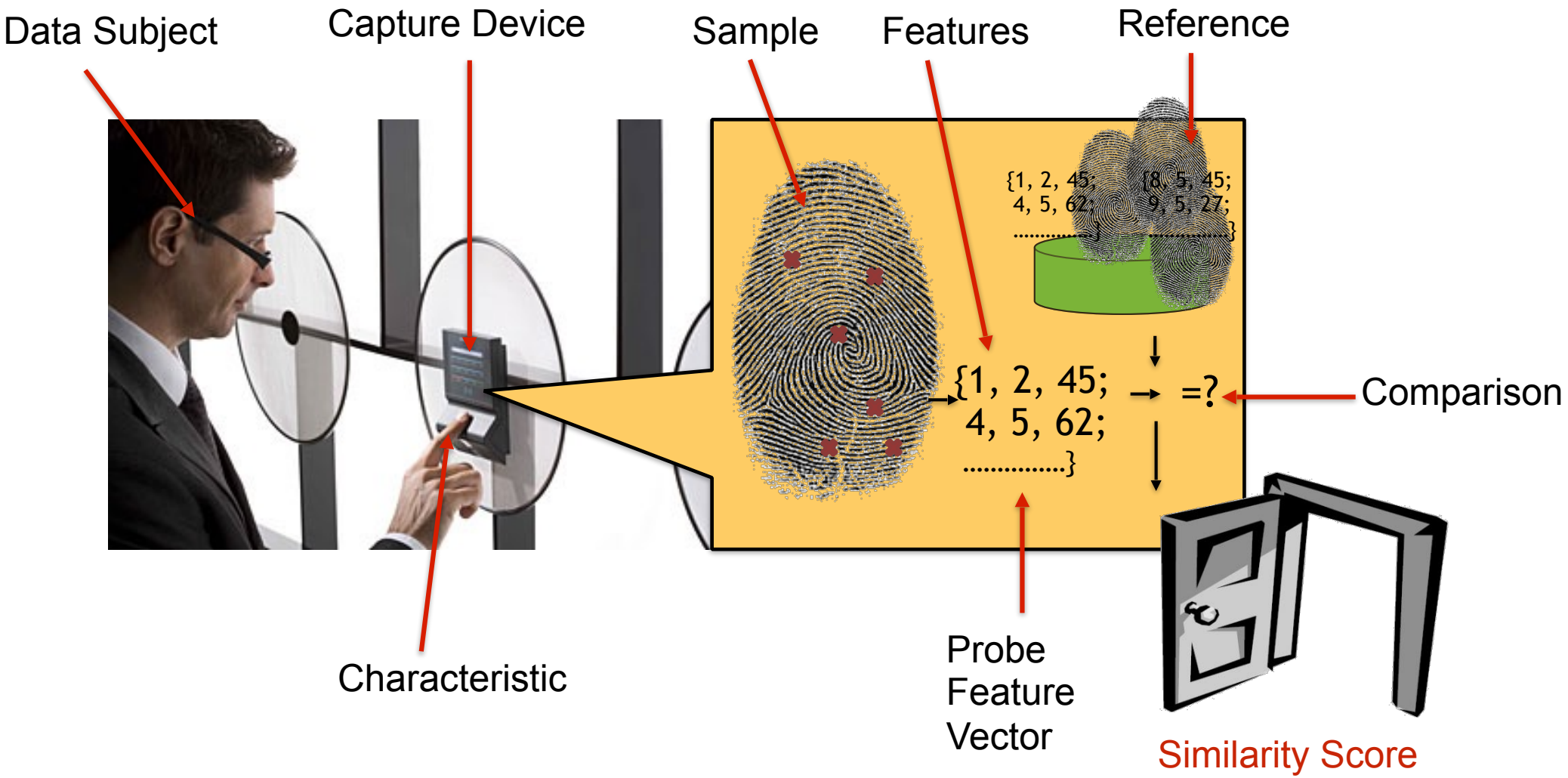
Something you know or own
you may loose, forget or forward to someone else,
with biometrics this is more difficult.

Biometrics - Definition

- International Organization for Standardization defines:
  - **Biometrics**:
    "*automated recognition of individuals based on their behavioural and biological characteristics* "
  - Remark: behavioural has to do with the function of the body
    biological / anatomical has to do with the structure of the body



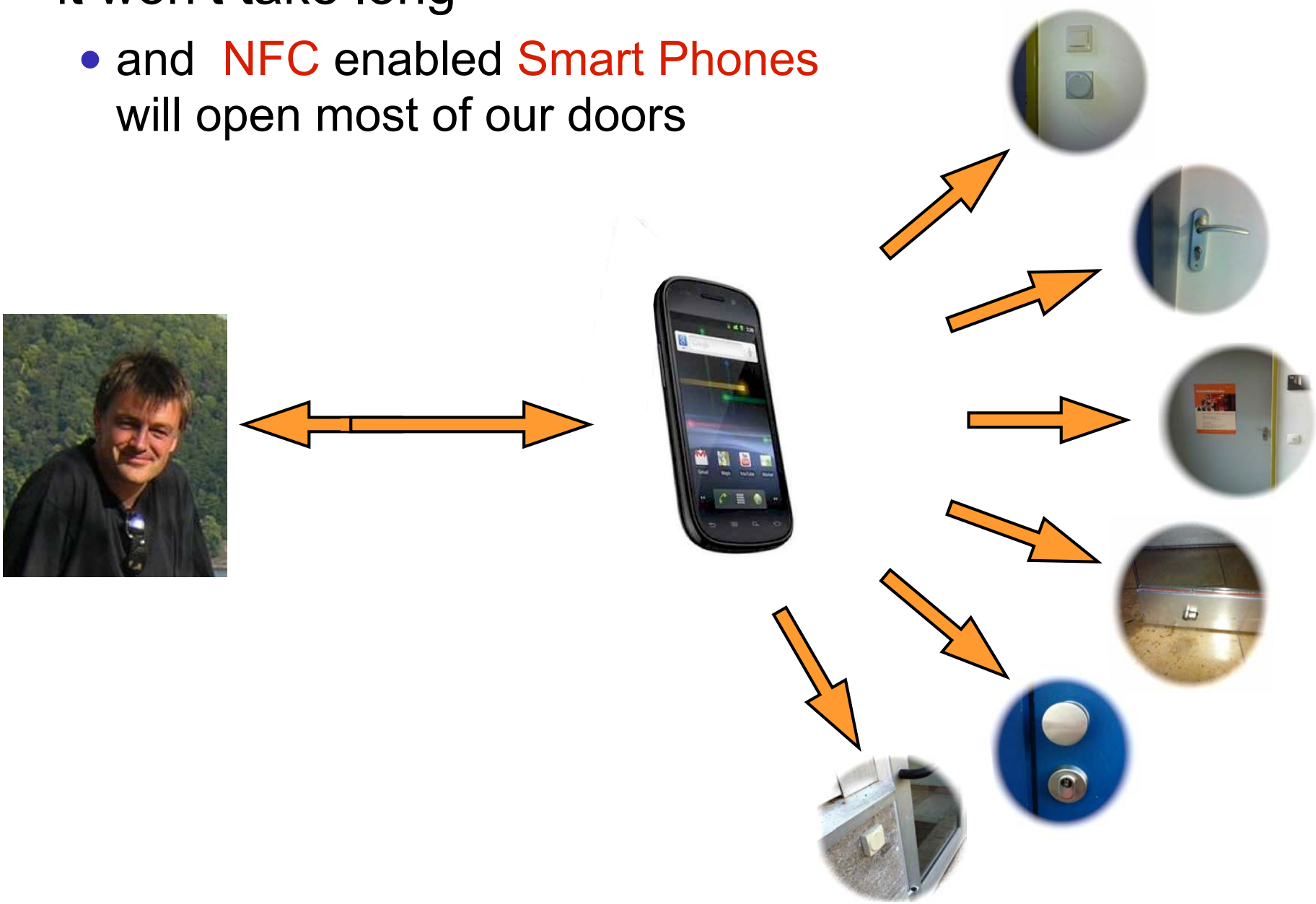
Biometrics - Process



Biometrics - Tomorrow

it won‘t take long

- and NFC enabled Smart Phones will open most of our doors



Biometric Myths Dispelled

Security ?

Operators may think:

„Biometrics are not as secure as PINs“

Benchmark of Biometrics and PIN

There are striking arguments why biometric authentication is better than the PIN

- The entropy of a 4 or 6-digit PIN is very limited
  - Even for a 6 digit numeric PIN (e.g. with the German eID card) the entropy $H = L * log_2 N$ is limited to less than 20bit (with $L=6, N=10$)
  - The reported entropy for different biometric characteristics is
    - Fingerprints 84bit [Ratha2001], Iris 249bit [Daugman2006] Face 56bit [Adler2006], Voice 127bit [Nautsch2015]

[Ratha2001] N. Ratha, J. Connell, R. Bolle: An analysis of minutiae matching strength. In: Audio- and Video-Based Biometric Person Authentication, vol. 2091, pp. 223–228. Springer, (2001)

[Daugman2006] J. Daugman: Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons. Proc. of the IEEE 94(11), 1927–1935 (2006)

[Adler2006] A. Adler, R. Youmaran, S.Loyka: Towards a measure of biometric information. In: Canadian Conference on Electrical and Computer Engineering, (CCECE'06). pp. 210–213 (2006)

[Nautsch2015] A. Nautsch, C. Rathgeb, R. Saeidi, C. Busch: Entropy Analysis of I-Vector Feature Spaces in Duration-Sensitive Speaker Recognition, in 40th IEEE ICASSP Conference, 19-24 April 2015, Brisbane, Australia, (2015)

Benchmark of Biometrics and PIN (cont.)

There are striking arguments why
biometric authentication is better than the PIN

- PINs can be delegated in violation of the security policy
  - „*This transaction was done by Mr. Popov, who was mis-using my card*“
  - biometric authentication enables non-repudiation of transactions

Biometrics are better than PINs !

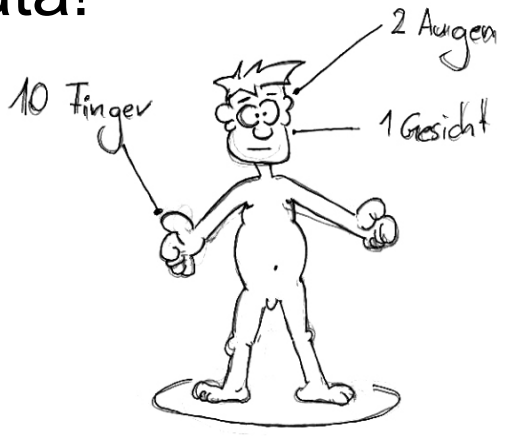
Data Privacy and Data Protection ?

Operators may think:

„Biometric systems are not compliant to data privacy principles“

Biometric Template Protection

We need to protect biometric reference data!
but …



- how to revoke biometric references?

- how to protect sensitive information in biometric data?
  - and align with the General Data Protection Regulation (GDPR)

Wart Fingerprint

Source: TU Brno, 2013

Biometric Template Protection

We do NOT store fingerprint, iris or face images

- we transform templates to pseudonymous identifiers (PI)
- we reach
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: we can revoke and renew template data.
  - Non-invertibility:Original biometric sample can not be reconstructed

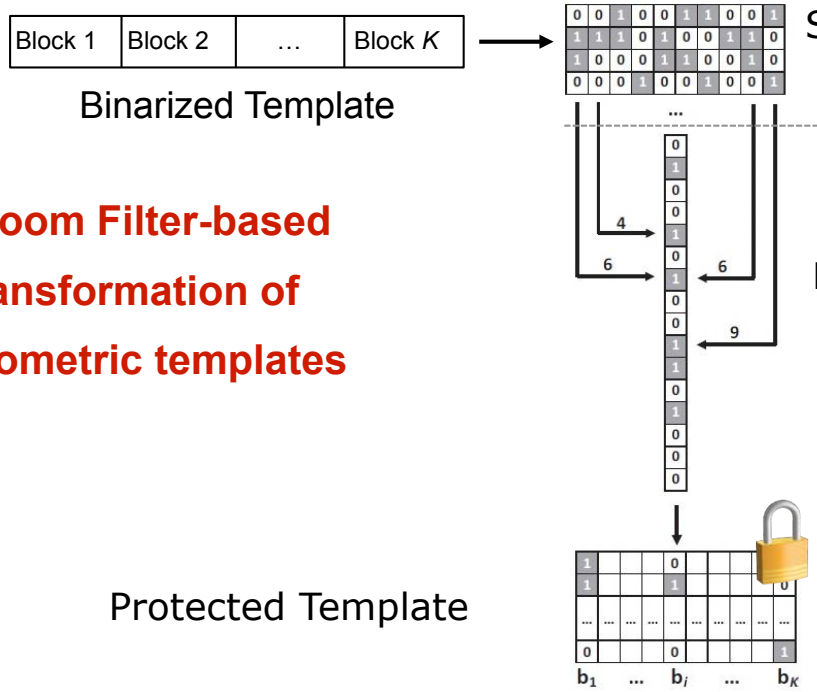
- [Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008) http://www.christoph-busch.de/files/Breebaart-BTPReferenceArchitecture-BIOSIG-2008.pdf

  [RaBBB2013] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014) http://www.christoph-busch.de/files/Rathgeb-BloomFilter-IET-2014.pdf

Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers



Bloom Filter-based transformation of biometric templates

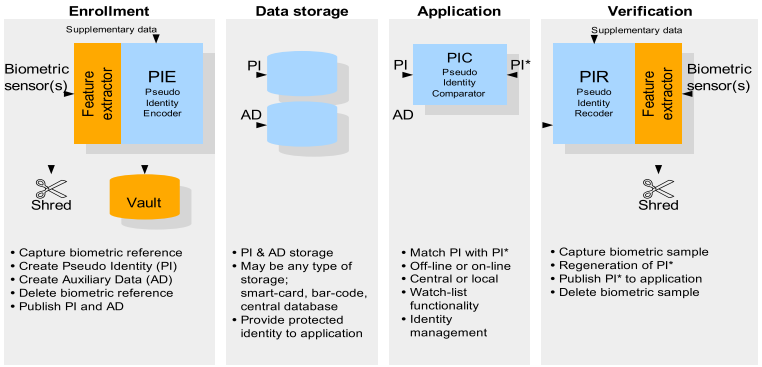
- Secrecy
- Non-invertibility
- Diversification
- Noise robustness

Biometric Template Protection enables revocability in biometric systems!

Data Protection Requirements

A technical guideline, how to implement requirements for data privacy and data protection is formulated in:

- ISO/IEC 24745: Biometric Information Protection, (2011)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52946



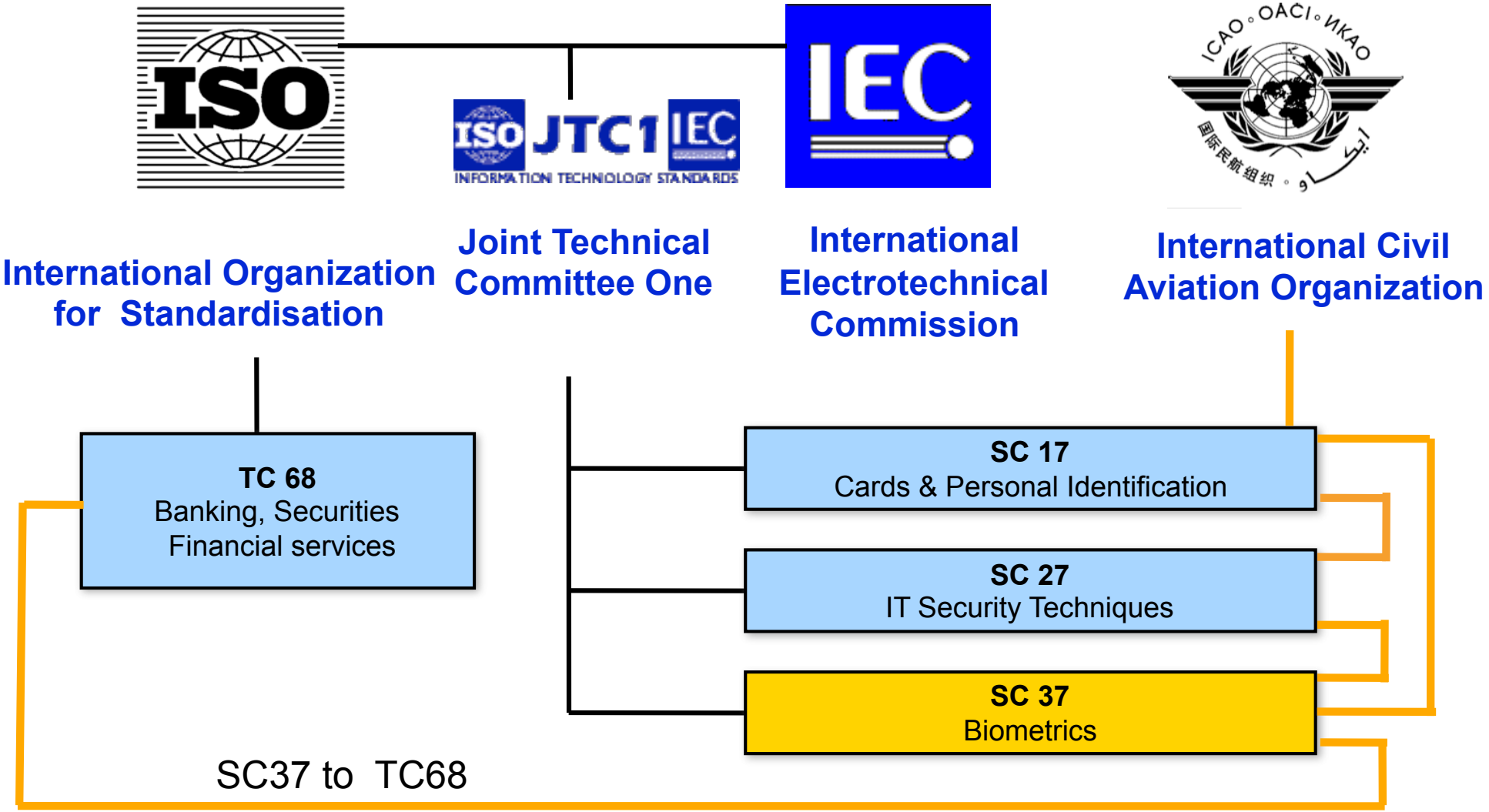
ISO/IEC 24745
Biometric Information Protection !

Standards ?

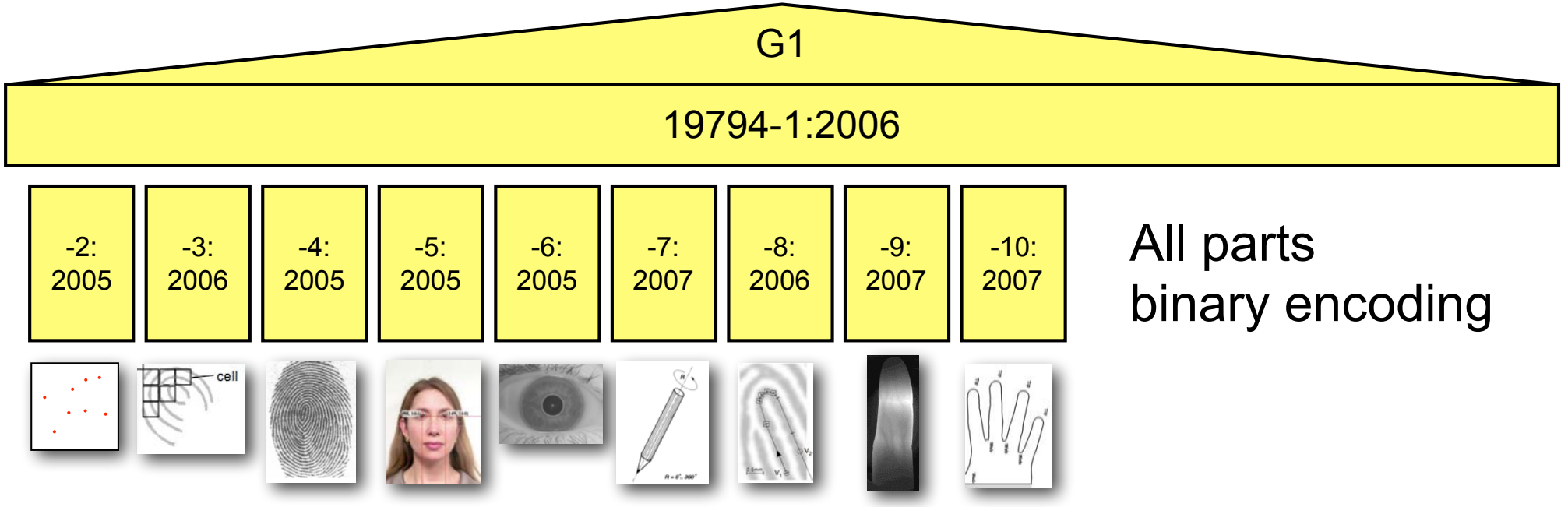
Operators may think:

„*There are no standards on biometrics*“

Biometric Standardisation



ISO/IEC Interchange Format Standards



All parts
binary encoding

The 19794-Family: Biometric data interchange formats

Biometric Performance Testing

ISO/IEC 19795-1: Biometric performance testing and reporting

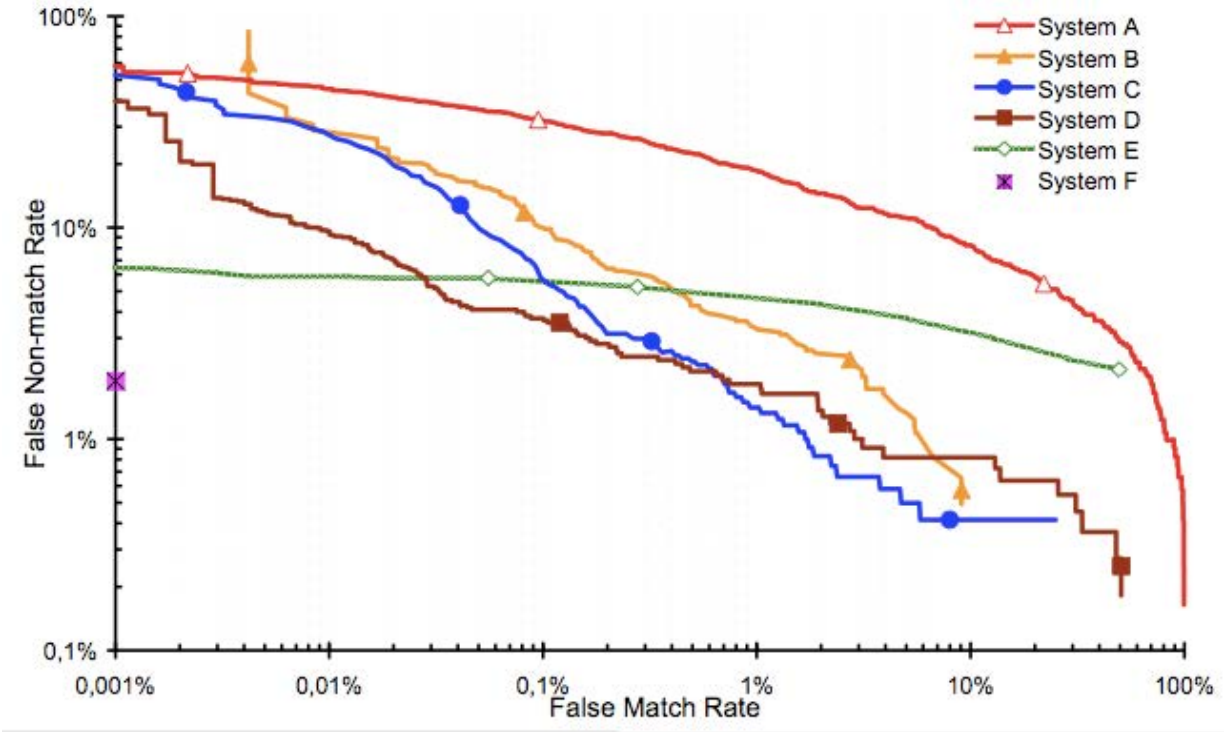
Part 1: Principles & Framework

- Technology testing
  - Algorithmic level verification error
    - False-Match-Rate (FMR) - algorithm accepts „zero-effort“ impostor
    - False-Non-Match-Rate (FNMR) - algorithm rejects true identity
- Scenario testing and operational testing
  - System level verification error
    - False-Accept-Rate (FAR)
    - False-Reject-Rate (FRR)
  - System level error requires observation of:
    - Sample generation: Failure-to-Capture (FTC)
    - Enrolment: Failure-to-Enrol (FTE) - no reference for this subject
    - Verification: Failure-to-Acquire (FTA) - no probe feature vector

Biometric Performance Testing - Report

DET curve (detection error trade-off curve)

- which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)



- Extensive test results: http://www.nist.gov/itl/iad/ig

Your Operator Reality Check

Operators should ask the vendors

- Is the sensor replaceable and robust for presentation attacks?

I want the biometric capture device to be operated via BioAPI interface according ISO/IEC 19784 and tested for PAD according ISO/IEC 30107-3

- Can comparison algorithms be replaced?

I want the biometric reference data to be stored in standardised interchange format according ISO/IEC 19794!

- Is the accuracy of the algorithm good?

I want to see the technology performance test report with a DET curve according ISO/IEC 19795!

- Is there data protection of stored biometric reference data?

I want the design of the systems to be compliant to ISO/IEC 24745

Mobile Biometrics

Smartphone Access Control

Foreground authentication (user interaction)

- Deliberate decision to capture (willful act)
- Camera-Sensor
  - Fingerprint recognition
    - Apples iPhone 5S / Samsung Galaxy 5
    - Fingerphoto analysis
  - Face recognition
  - Iris recognition
- Touchpad: allows signature recognition

Image Source: Apple 2013

Background authentication (observation of the user)

- Microphone
  - Speaker recognition
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive

Mobile Biometric Payment - Biometric Transaction and Authentication Protocol (BTAP)

Transaction-Authentication-Protocol

Biometric Transaction Authentication Protocol (BTAP)

1.) Shared secret

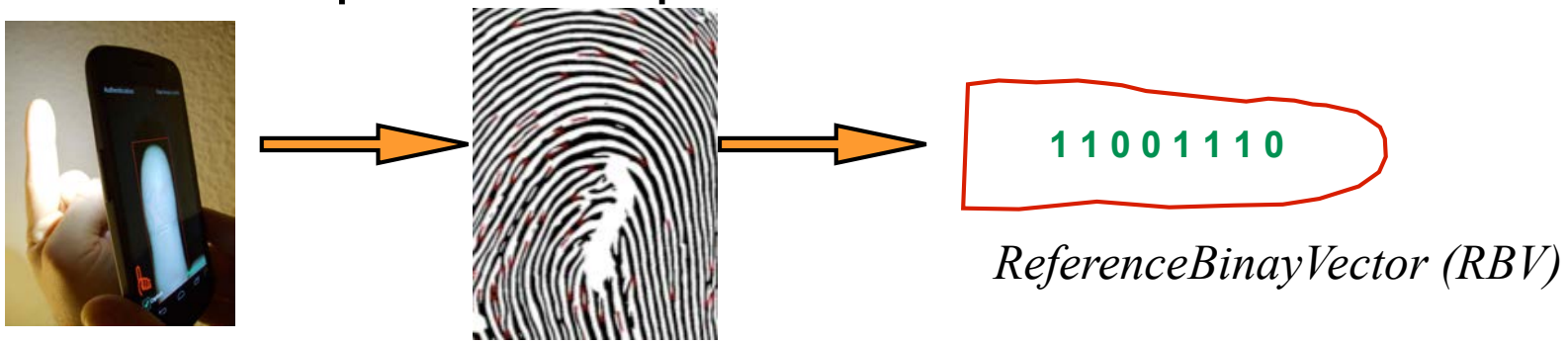
- received via subscribed letter from the bank
- entered once to the smartphone
  - hash over the secret constitutes a Pseudonymous Identifier (PI)

PIN = 4768 0569

CodeBookVector (CBV)

2.) Biometric enrolment

- Biometric samples are captured



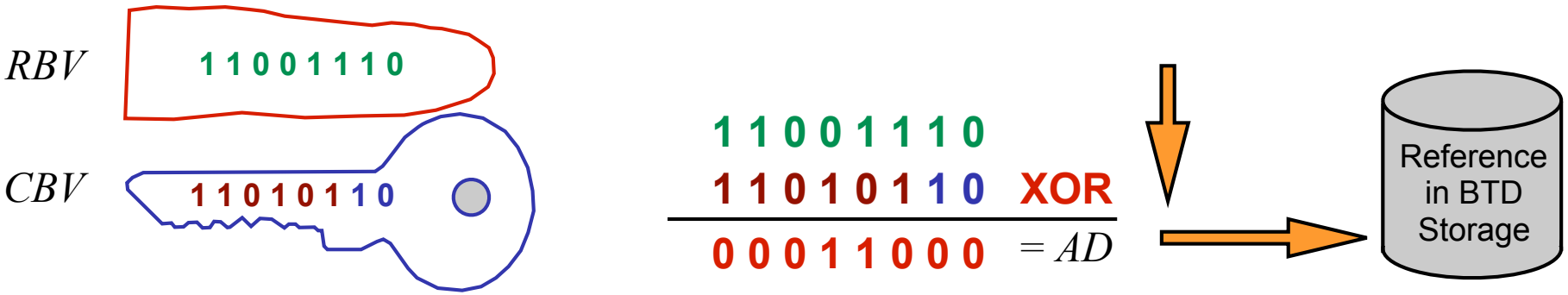
ReferenceBinayVector (RBV)

Transaction-Authentication-Protocol

Biometric Transaction Authentication Protocol (BTAP)

3.) Secure storage of auxilliary data

- we neither store the confidential secret nor the sensitive biometric data (i.e. feature vector)
- the secret and biometric data are merged



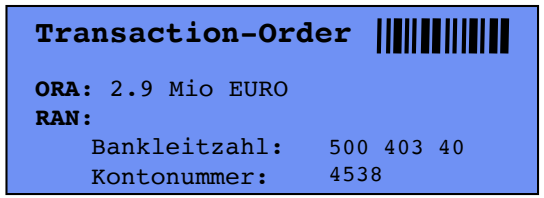
- Auxilliary data (AD) stored in the Smartphone
  - Biometric Transaction Device = FIDO Authenticator

Transaction-Verification

BTAP - Transaction

1.) Operations of the Online-Banking-Software (BSW)

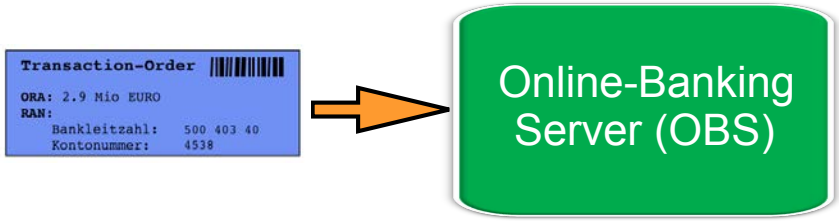
- Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)



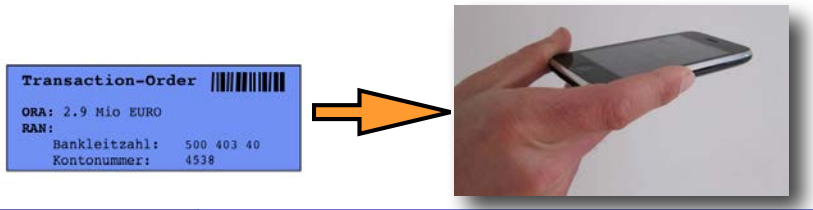
  This TOR consist of:

  - Transaction-Identifier (TID), Sender-Account-Number (SAN) Receiver-Account-Number (IBAN), Ordered Amount (ORA)

- BSW transfers TOR to the Online-Banking-Server (OBS)



- BSW transfers TOR to Smartphone (BTD / FIDO Authenticator)

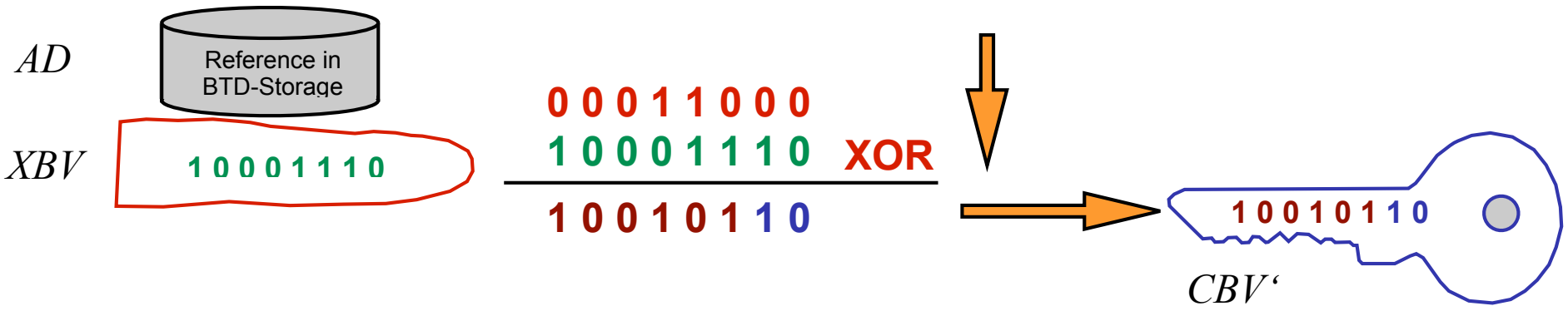


Transaction-Verification

BTAP - Transaction

2.) Operations on the Smartphone (BTD)

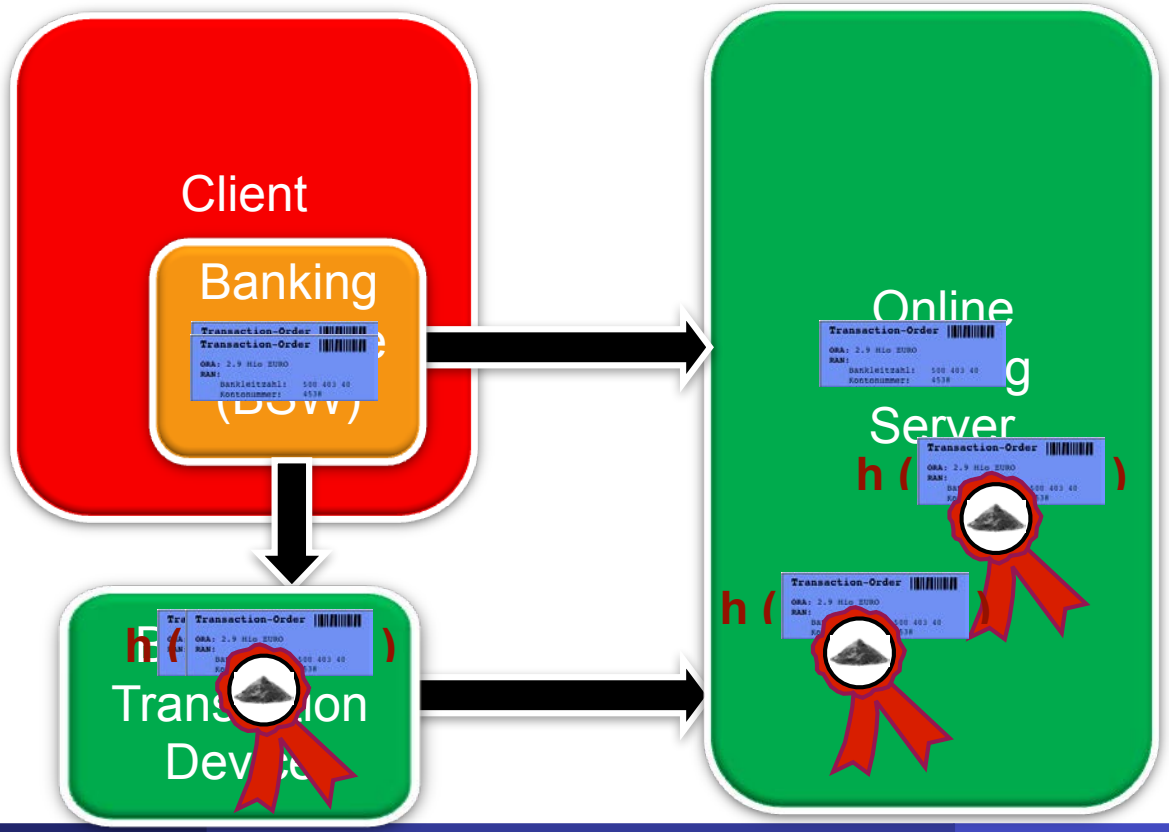
- Approval of the intended transaction by capturing a probe sample
- A secret vector CBV' is reconstructed with XOR operation from the Auxilliary Data AD that was stored in the BTD and from the binarized feature vector XBV



Transaction-Verification

Key features of BTAP

- independent two channel verification
- reconstruction of shared secret
- the Pseudonymous Identifier (PI) constitutes a seal
- seal operation over the TOR to authenticate the transaction



Transaction-Verification

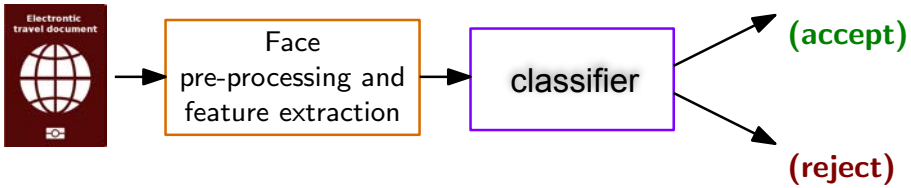
BTAP-Video

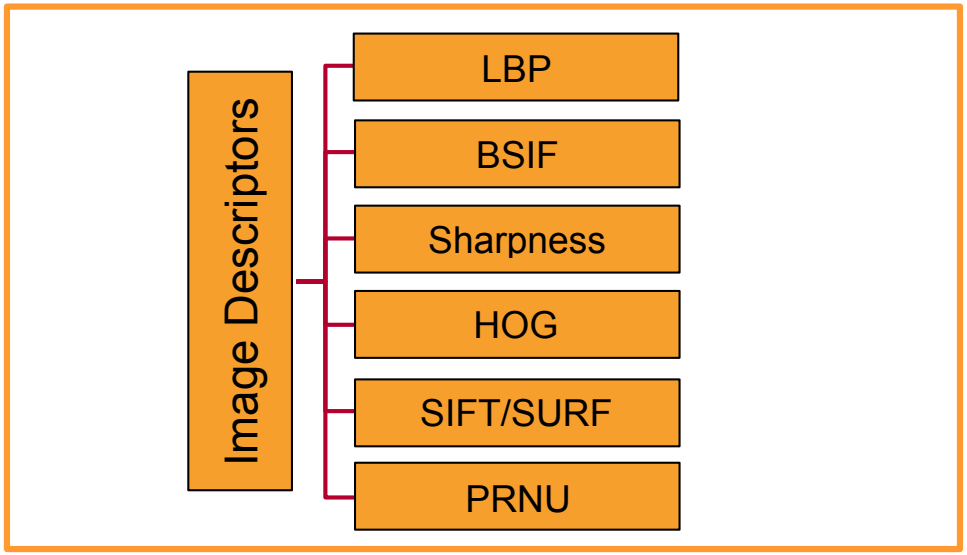
- http://christoph-busch.de/files/BTAP.mp4

Biometrics and Artificial Intelligence

The classical approach with texture analysis

- Image descriptors as hand-crafted features



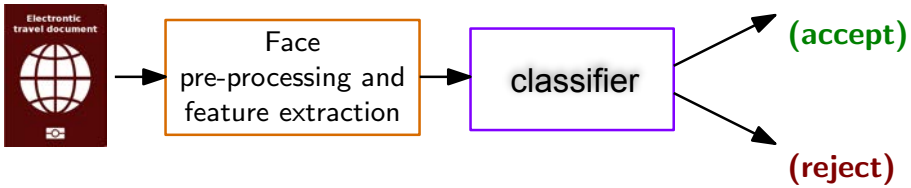


Classifier

Biometrics and Artificial Intelligence

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as Deep features



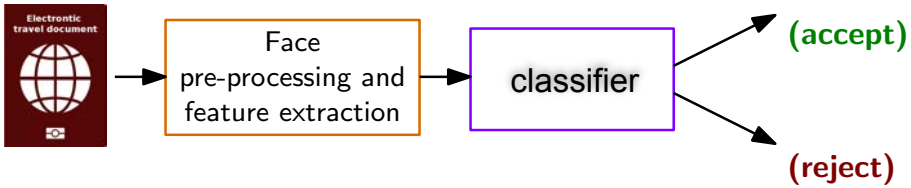
CNN BlackBox

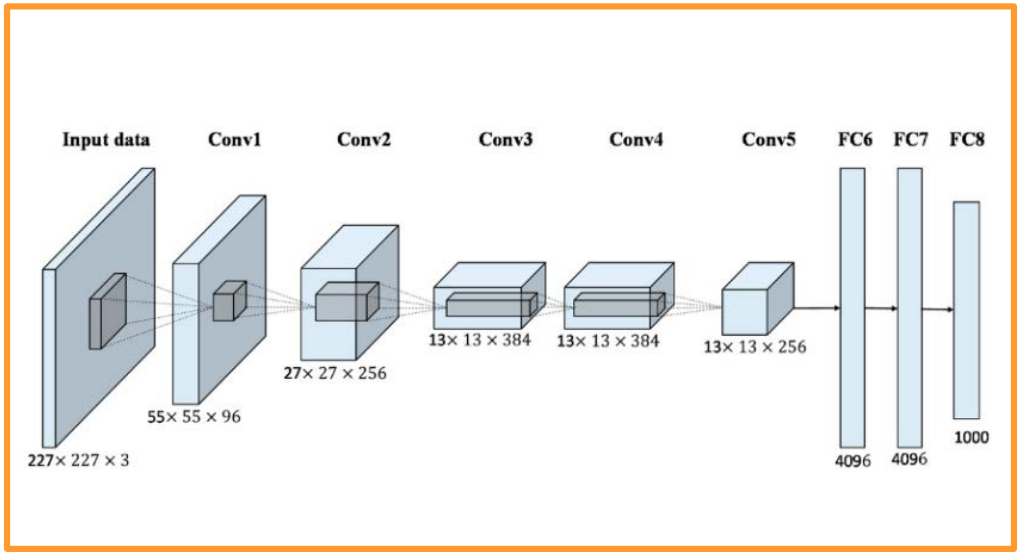
Classifier

Biometrics and Artificial Intelligence

Morphing Attack Detection (MAD) with texture analysis

- Image descriptors as Deep features





Classifier

Conclusion

Biometrics is possible with todays smartphones

Biometric standards are available

- financial transaction schemes should follow technical standards
- financial transaction schemes should follow privacy standards

BTAP satisfies PSD2 and follows the two channel concept

- is based on international ISO/IEC standards
- is privacy friendly as no biometric reference is stored on a banking server

More and detailed information on BTAP at:

http://www.christoph-busch.de/projects-btap.html

Contact

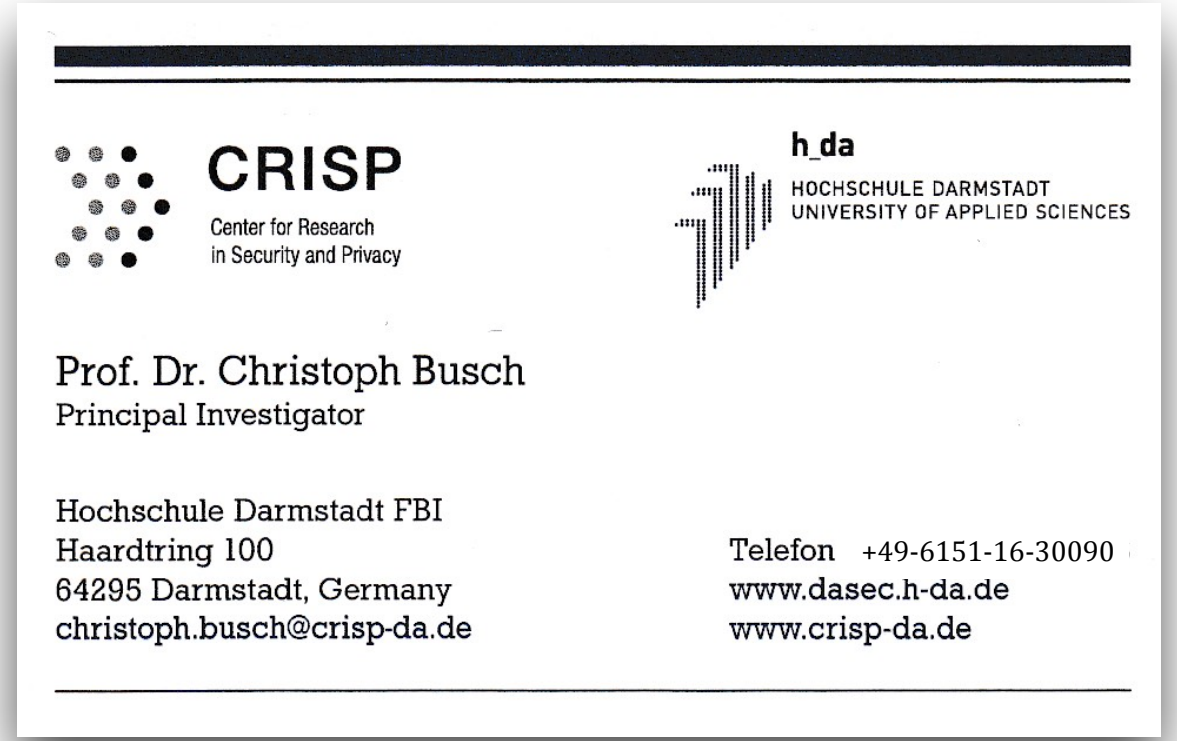
Contact:

NTNU

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194

Contact


CRISP
Center for Research
in Security and Privacy
h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
Prof. Dr. Christoph Busch
Principal Investigator
Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@crisp-da.de
Telefon +49-6151-16-30090
www.dasec.h-da.de
www.crisp-da.de

References - General

Web

- U.S. NIST https://www.nist.gov/topics/biometrics
- European Association for Biometrics http://www.eab.org
- da/sec biometric research group https://www.dasec.h-da.de/
- TeleTrusT working group on Biometrics
  http://www.christoph-busch.de/about-ag-biometrie.html
- Norwegian Biometrics Laboratory (NBL)
  http://www.ntnu.edu/nbl
- ISO/IEC JTC1 SC37 Working Group 3
  http://isotc.iso.org/livelink/livelink/open/jtc1sc37wg3
  http://www.christoph-busch.de/standards-sc37wg3.html

References

Complementary reading

- ISO/IEC TR 24741, “Biometrics tutorial”, 2007
  https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-1:v1:en
- ISO/IEC SC37 SD11, “General biometric system architecture”, 2010
  http://isotc.iso.org/livelink/livelink?func=ll&objId=8755976&objAction=Open
- ISO/IEC 2382-37, “Harmonized biometric vocabulary, 2012
  http://www.christoph-busch.de/standards.html
- ISO/IEC 24722, “Multimodal biometrics”, 2015
  https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24722:ed-2:v1:en
- ISO/IEC 19795-1, “Biometric performance testing and reporting”, 2006
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19795:-1:ed-1:v1:en

References

Complementary reading - interchange formats

- ISO/IEC 19794-1, “Biometric data interchange formats - Part 1: Framework”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-1:ed-2:v1:en
- ISO/IEC 19794-2, “Biometric data interchange formats - Part 2: Finger minutiae data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-2:ed-2:v1:en
- ISO/IEC 19794-4, “Biometric data interchange formats - Part 4: Finger image data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-4:ed-2:v1:en
- ISO/IEC 19794-5, “Biometric data interchange formats - Part 5: Face image data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-5:ed-2:v1:en
- ISO/IEC 19794-6, “Biometric data interchange formats - Part 6: Iris image data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-6:ed-2:v1:en

References

Complementary reading - quality

- ISO/IEC 29794-1, “Biometric sample quality - Part 1: Framework”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:29794:-1:ed-2:v2:en
- ISO/IEC 29794-4, “Biometric sample quality - Part 4: Finger image data”
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62791
- ISO/IEC TR 29794-5, “Biometric sample quality - Part 5: Face image data”, 2010
  https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:29794:-5:ed-1:v1:en
- ISO/IEC 29794-6, “Biometric sample quality - Part 6: Iris image data”, 2011
  https://www.iso.org/obp/ui/#iso:std:iso-iec:29794:-6:ed-1:v1:en

References

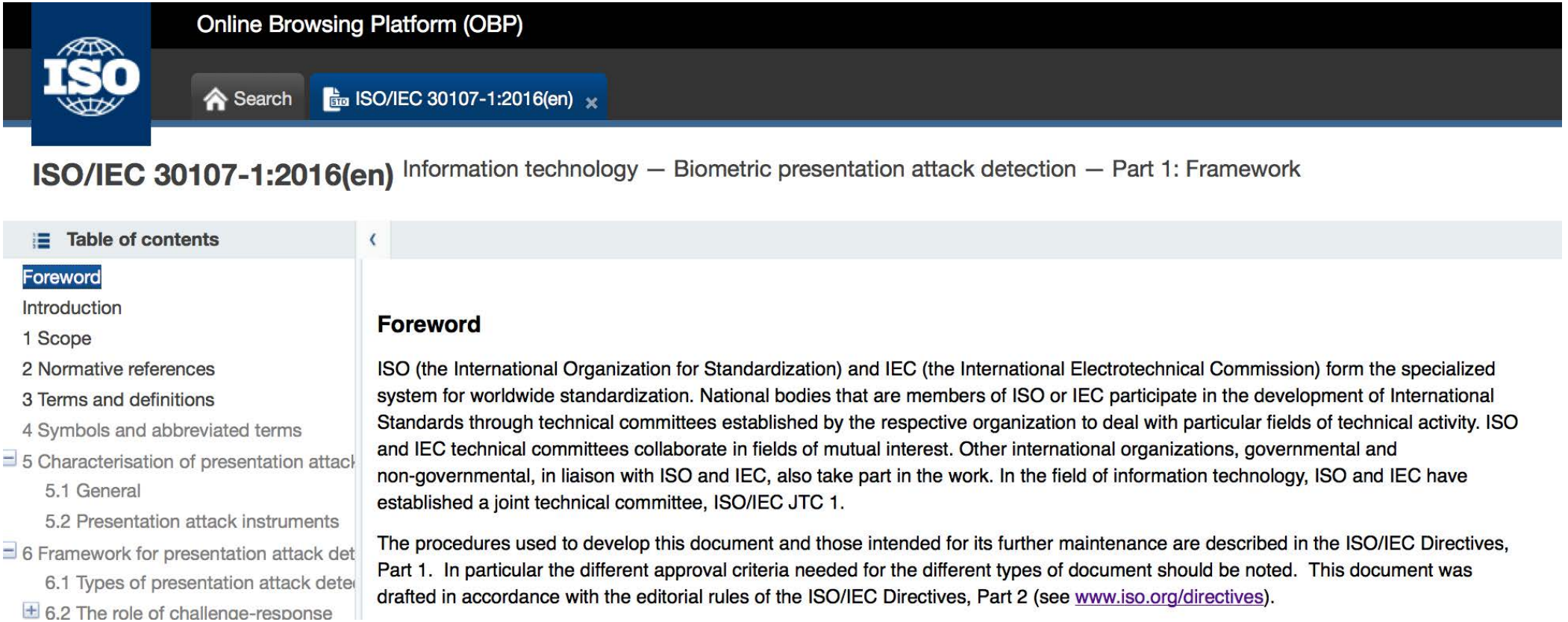
Complementary reading - protection, PAD and mobile

- ISO/IEC 24745, “Biometric Information Protection”, 2011
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52946
- ISO/IEC 30107-1, “Biometric presentation attack detection - Part 1: Framework”, 2016
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip
- ISO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Testing and reporting”, 2016
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67381
- ISO/IEC TR 30125, “Biometrics used with mobile devices”, 2016
  https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:30125:ed-1:v1:en
- ISO/IEC 15408: “Security Techniques - Evaluation Criteria for IT Security / Common Criteria“

Presentation Attack Detection - Framework

ISO/IEC 30107-1

- now freely available in the ISO-Portal
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip



Presentation Attack Detection

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

- **presentation attack**
  presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system
- **presentation attack detection (PAD)**
  automated determination of a presentation attack

Definitions in ISO/IEC 2382-37: Vocabulary
http://www.christoph-busch.de/standards.html

- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference
- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

Presentation Attack Detection

Impostor

- impersonation attack
  - positive access 1:1 (two factor application)
  - positive access 1:N (single factor application)
- finding a look-a-like
- making appearance similar to the reference
- artefact presentation

Image Source: http://upshout.net/game-of-thrones-make-up

Concealer

- evasion from recognition
  - negative 1:N identification (watchlist application)
- depart from standard pose

- evade face detection

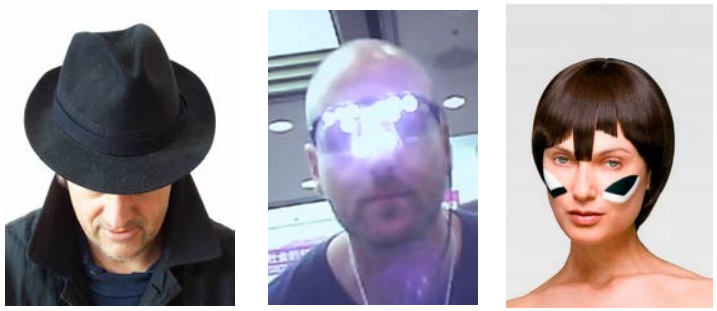


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Image Source: https://cvdazzle.com

Presentation Attack Detection

ISO/IEC 30107-1 - Definitions

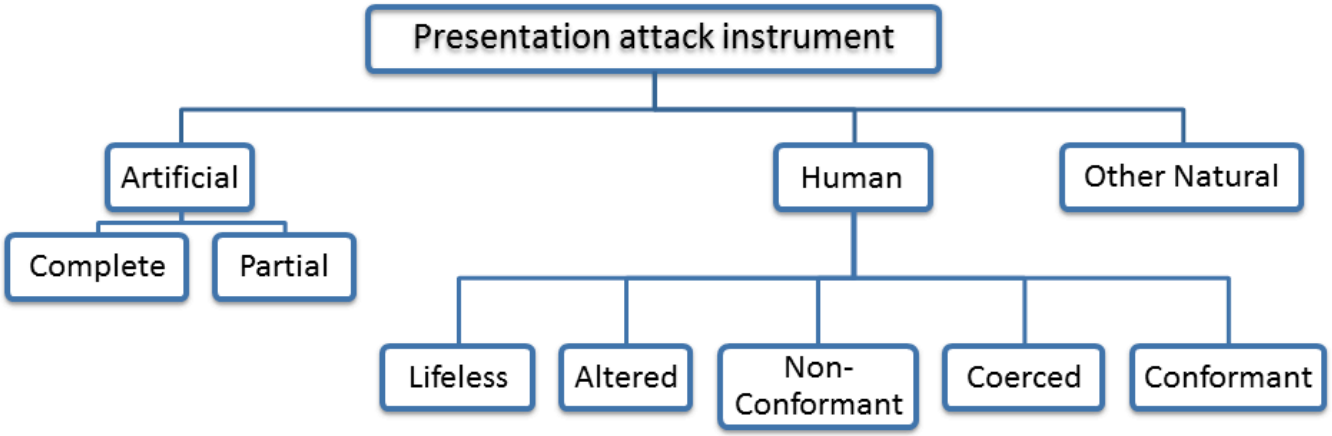
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



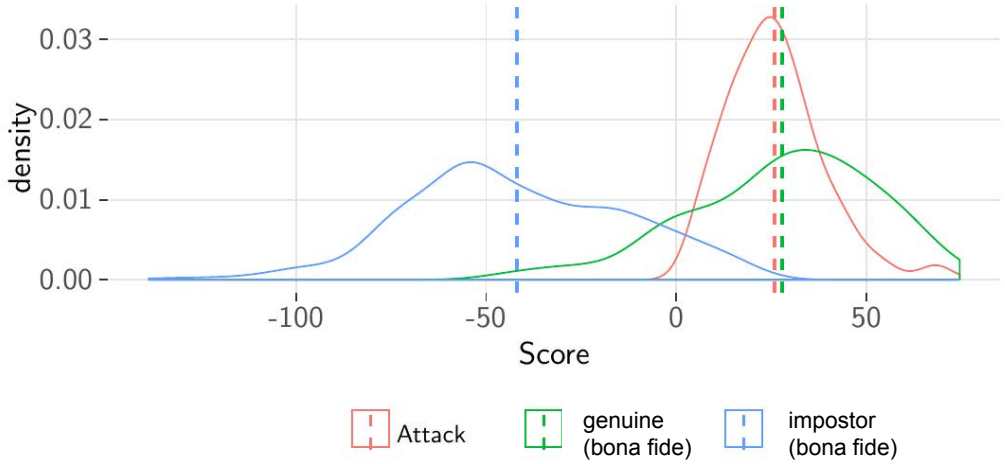
Source: ISO/IEC 30107-1

Presentation Attack Detection - Testing

Definition of full system vulnerability metric w.r.t attacks

- **Impostor attack presentation match rate (IAPMR)**
  <in a full-system evaluation of a verification system> the proportion of impostor attack presentation using the same PAI species in which the target reference is matched

Source: ISO/IEC 30107-3



- **Concealer attack presentation non-match rate (CAPNMR)**
  in a full-system evaluation of a verification system, the proportion of concealer attack presentations using the same PAI species in which the target reference is not matched.

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with false-negative and false-positive errors:

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario

- **Bona fide presentation classification error rate (BPCER)**
  proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics elements

- **PAI species**
  class of presentation attack instruments created using a common production method and based on different biometric characteristic
- **Attack potential**
  measure of the capability to attack a TOE given the attacker's knowledge, proficiency, resources and motivation
- **target of evaluation (TOE)**
  within Common Criteria, the IT product that is the subject of the evaluation

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with false-negative errors:

- **Attack presentation classification error rate (APCER)** *proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario*

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right) \sum_{i=1}^{N_{PAIS}} Res_i$$

Source: ISO/IEC 30107-3

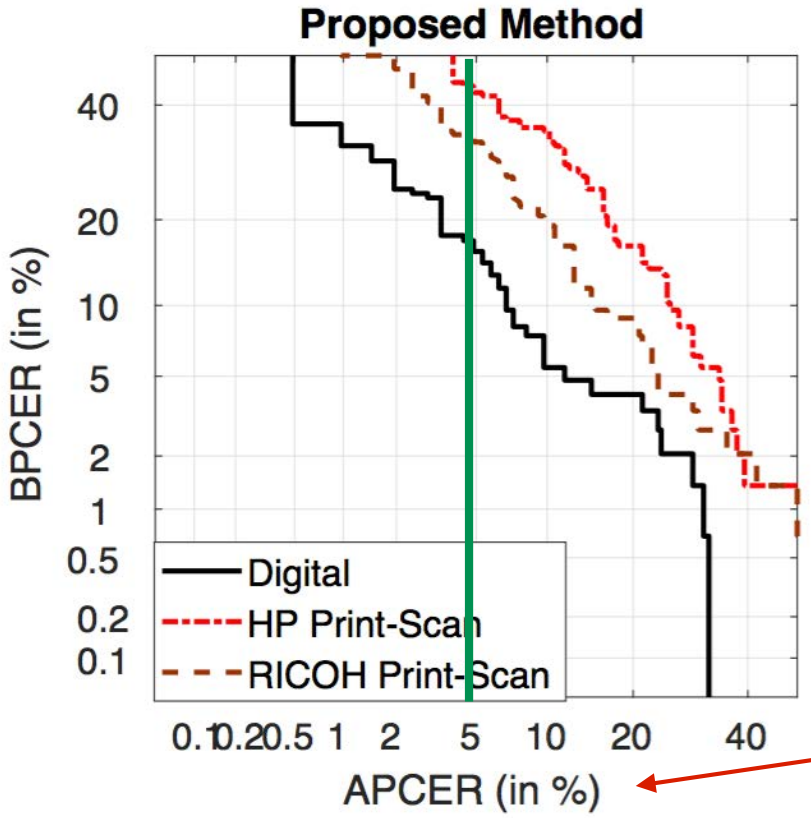
- N_{PAIS} *is the number of attack presentations for the given PAI species*
- Res_i *takes value 1 if the* i^{th} *presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- DET curve analyzing operating points for various security measures and convenience measures
- Example:

convenience measure



security measure (strength of function)

Source: IR. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)