Biometrische Systeme und Methoden - Maschinen identifizieren Menschen!

Christoph Busch

Hochschule Darmstadt - CASED
http://www.christoph-busch.de/

Strategiegipfel: IT & Information Security

Berlin - November 17 2015

CASED

European Association for Biometrics
eab
Human Identity in Europe

Biometric Characteristic

Biometric activities

- Convener of the Working Group 3 on Biometric Data Interchange Formats in ISO/IEC JTC1 SC37
- Board-member European Association for Biometrics
- Co-Chair of the GI Special Interest group BIOSIG
- Chair of the TeleTrusT working group on Biometrics
- Co-Chair of the Norsk Biometri Forum

Recent projects related to Biometrics

- Hochschule Darmstadt:
  - LOEWE CASED http://www.cased.de
  - LOEWE BioMobile

CASED

- NISlab:
  - EU-FP7 FIDELITY http://www.fidelity-project.eu
  - EU-FP7 INGRESS http://www.ingress-project.eu
  - EU-FP7 ORIGINS http://cordis.europa.eu/project/rcn/192602_en.html
  - EU-FP7 PIDaaS http://www.pidaas.eu

FIDELITY

Introduction to Biometrics

Biometrics - Fingerprint Recognition

Analog/digital representation of the finger ridges

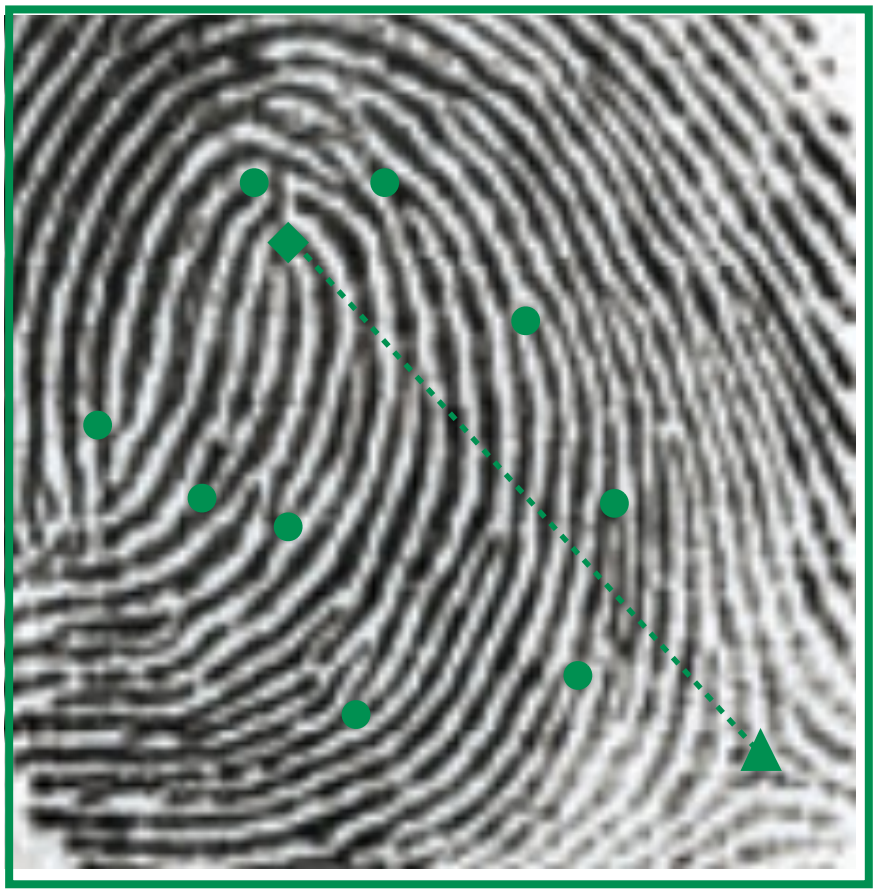
- Distinguished points of the fingerprint: Minutia

Feature Extraction and Comparison

Comparison of reference image against a probe image

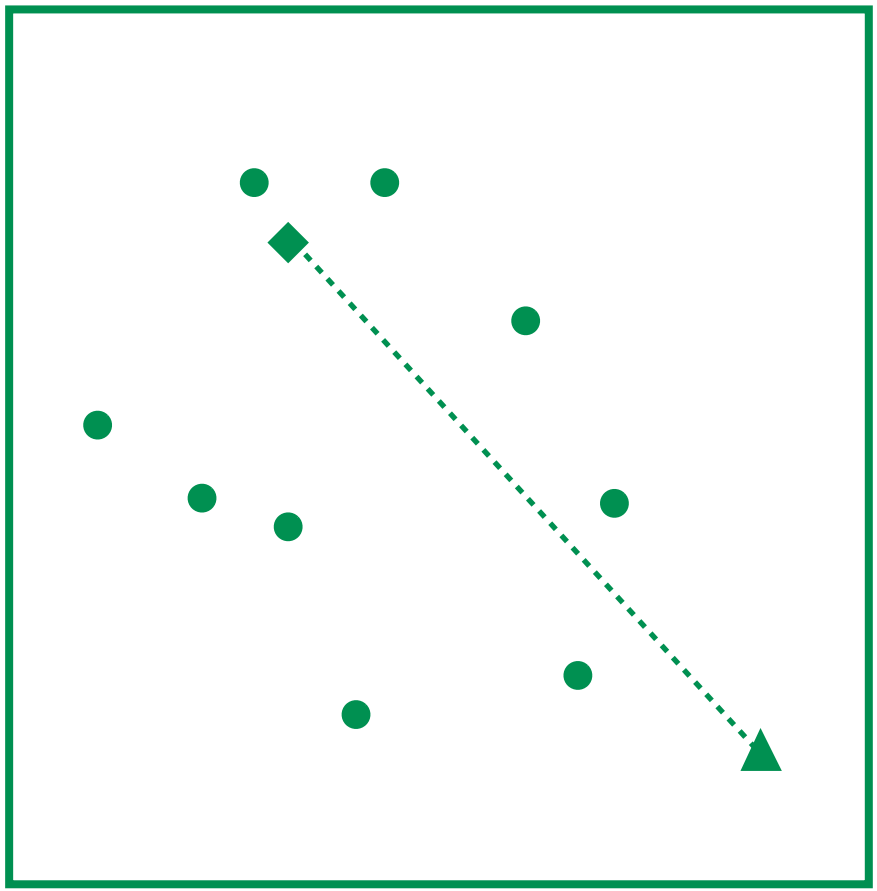
Feature Extraction and Comparison

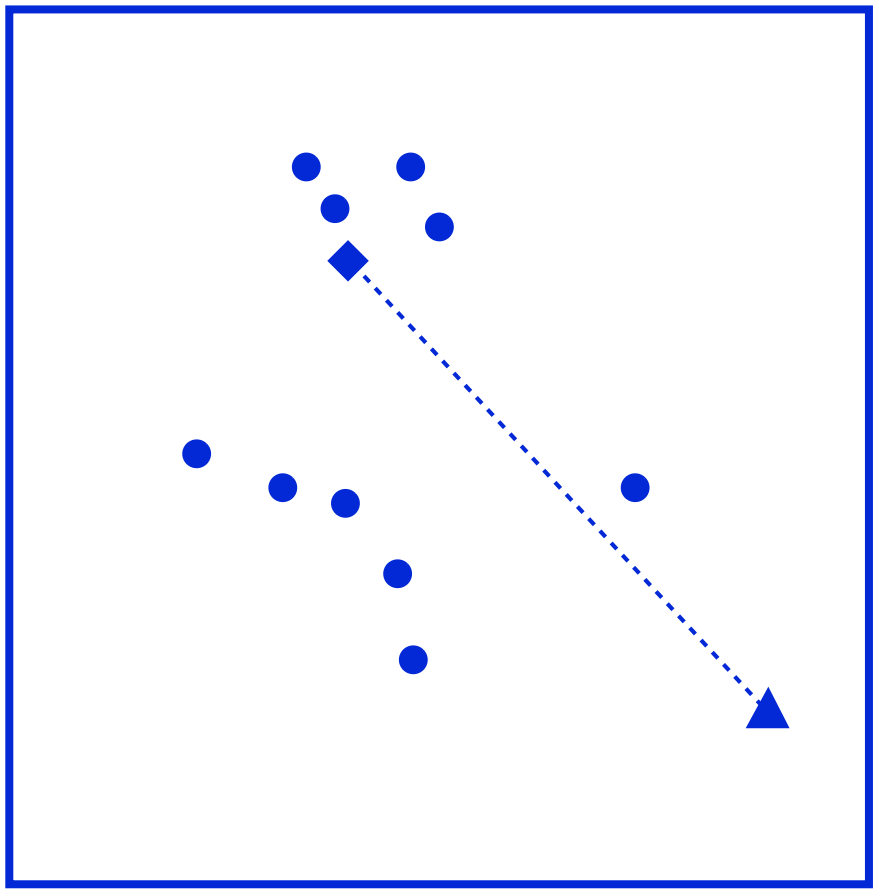
Comparison of reference image
against a probe image



Feature Extraction and Comparison

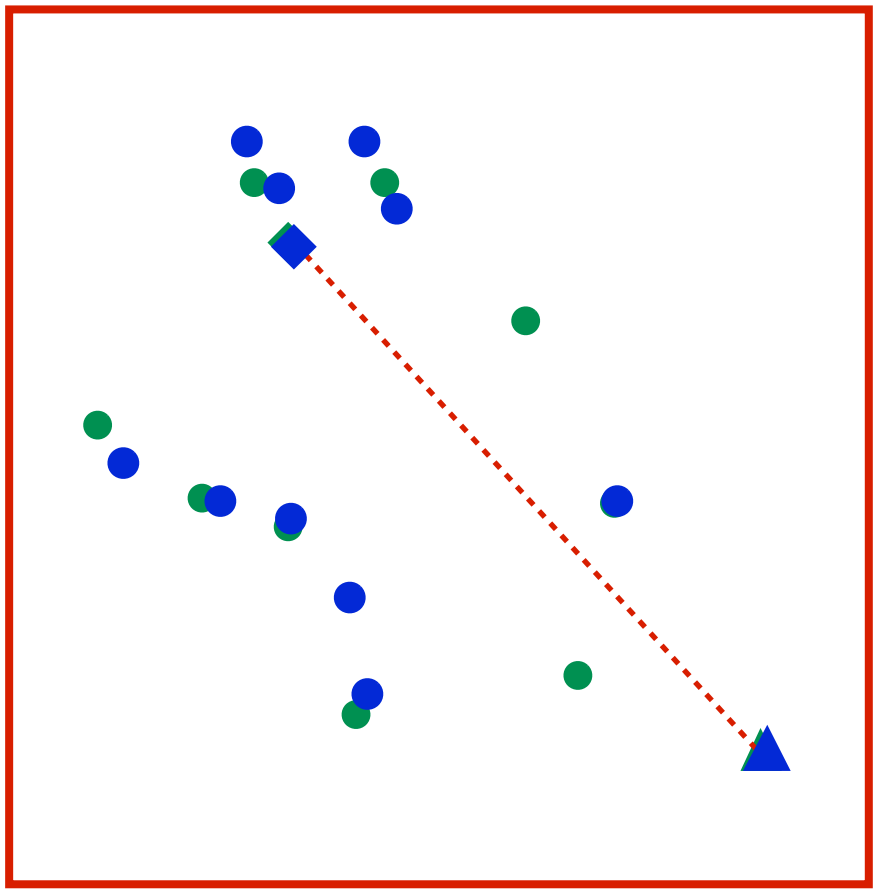
Comparison of reference feature vector against a probe feature vector





Feature Extraction and Comparison

Comparison of reference feature vector against a probe feature vector



Biometric Rumors

Security ?

Operators may think:

„Biometrics are not as secure as PINs“

Benchmark of Biometrics and PIN (cont.)

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.)

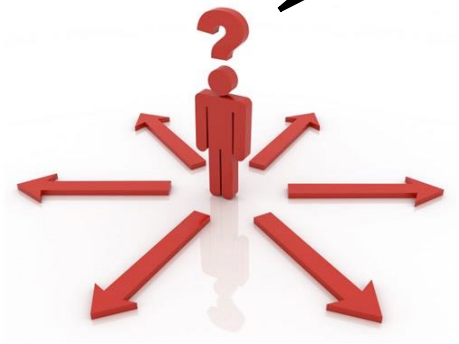
There are striking arguments why
biometric authentication is better than the PIN

- 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 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.
  - Diversifiability / 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

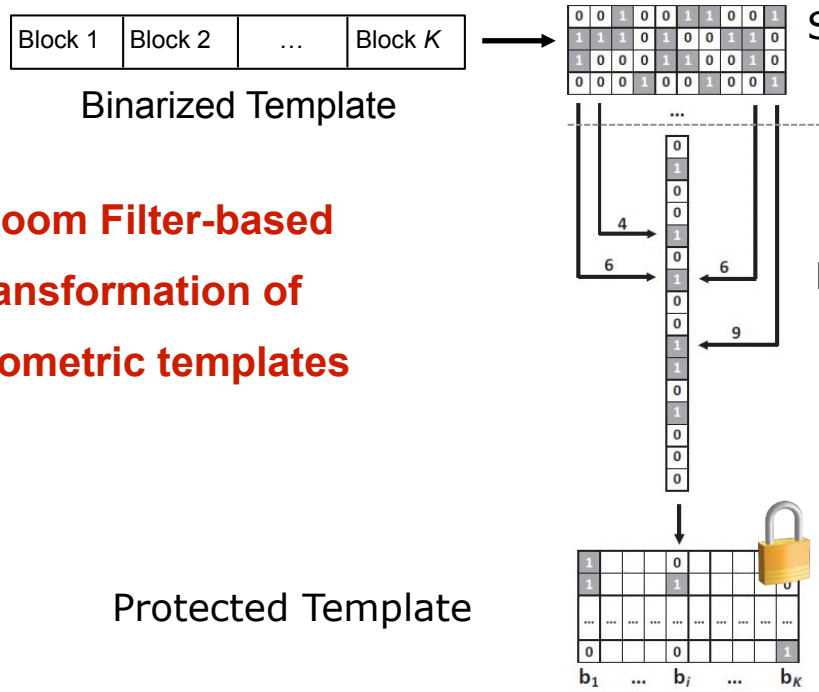
[RaBBB2013] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014)

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

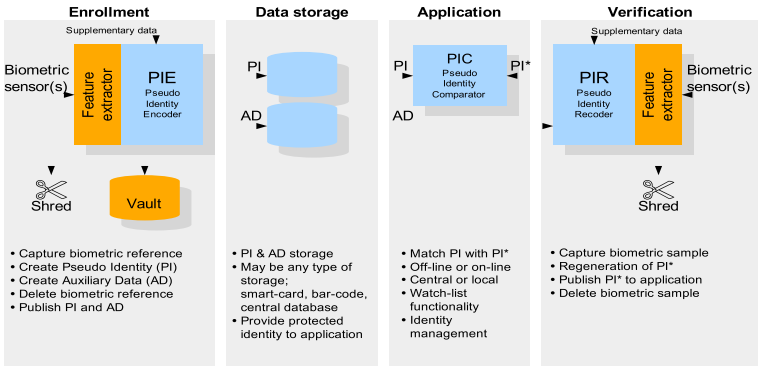
- Secrecy
- Non-invertibility
- Diversification
- Noise robustness

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



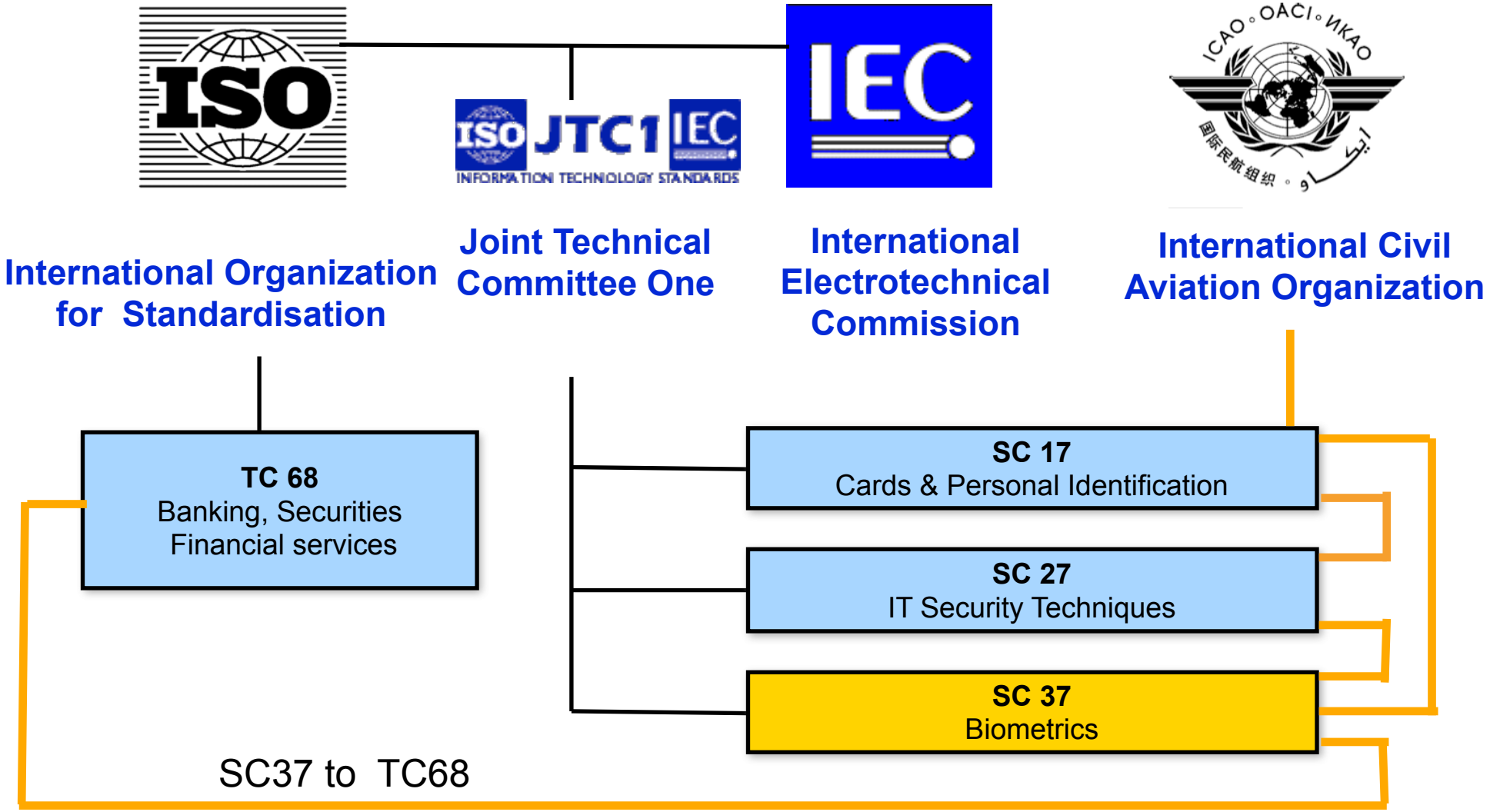
ISO/IEC 24745
Biometric Information Protection !

Standards ?

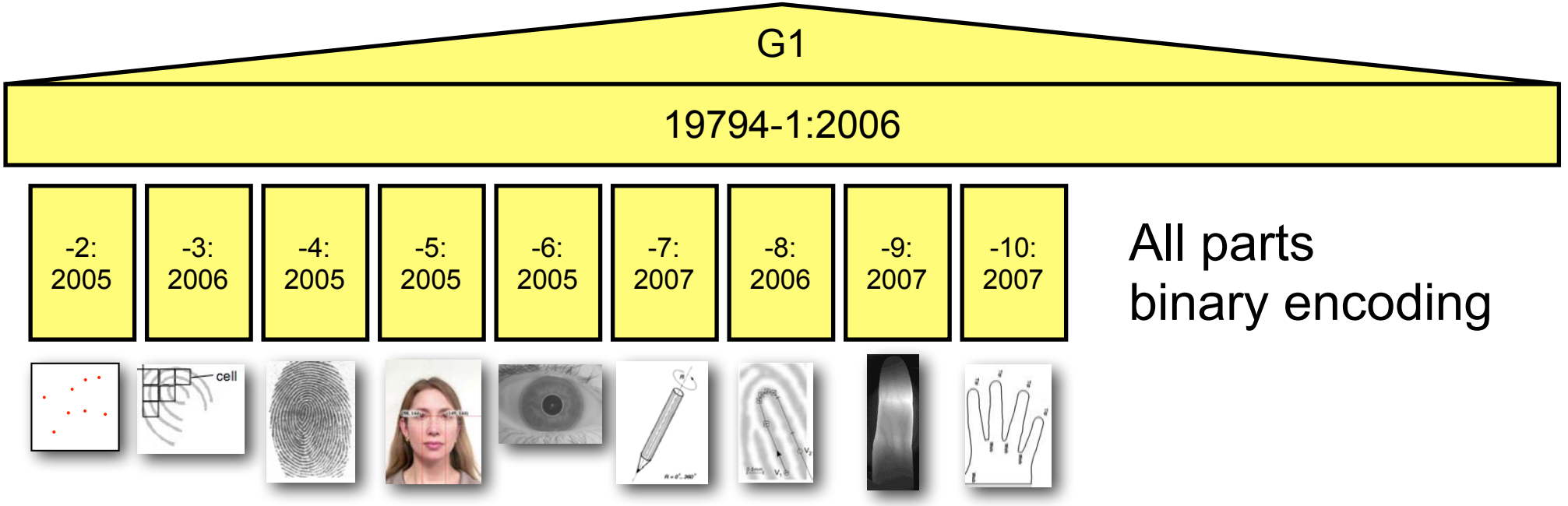
Operators may think:

„*There are no standards on biometrics*“

Biometric Standardisation



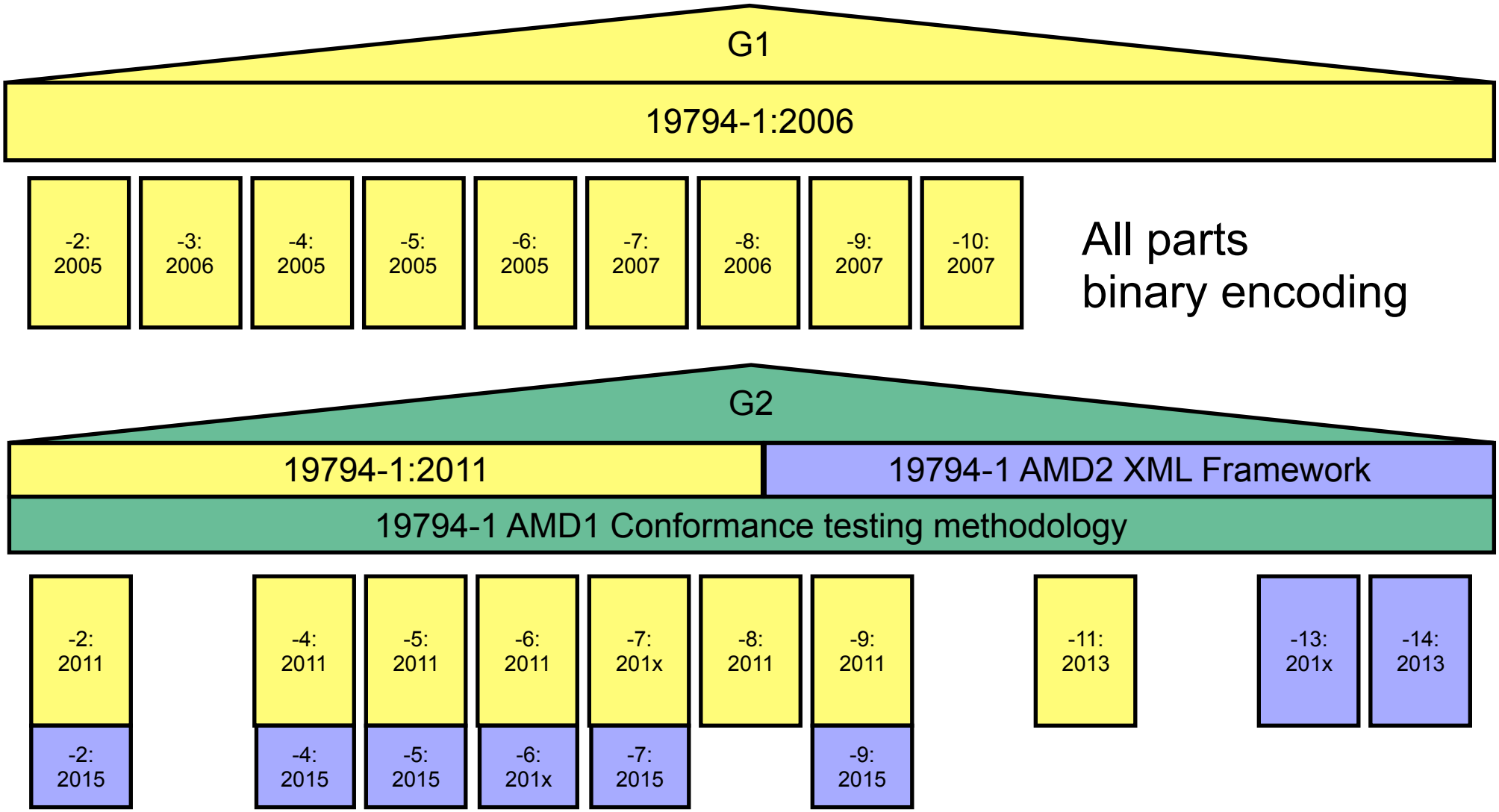
ISO/IEC Interchange Format Standards



All parts
binary encoding

The 19794-Family: Biometric data interchange formats

Generation 2 of ISO/IEC 19794



the semantic is equivalent for binary encoded and XML encoded records

Security ?

Operators will think:

„*The biometric sensors must be robust against fake attacks*“

Gummy Finger Production in 2000 !

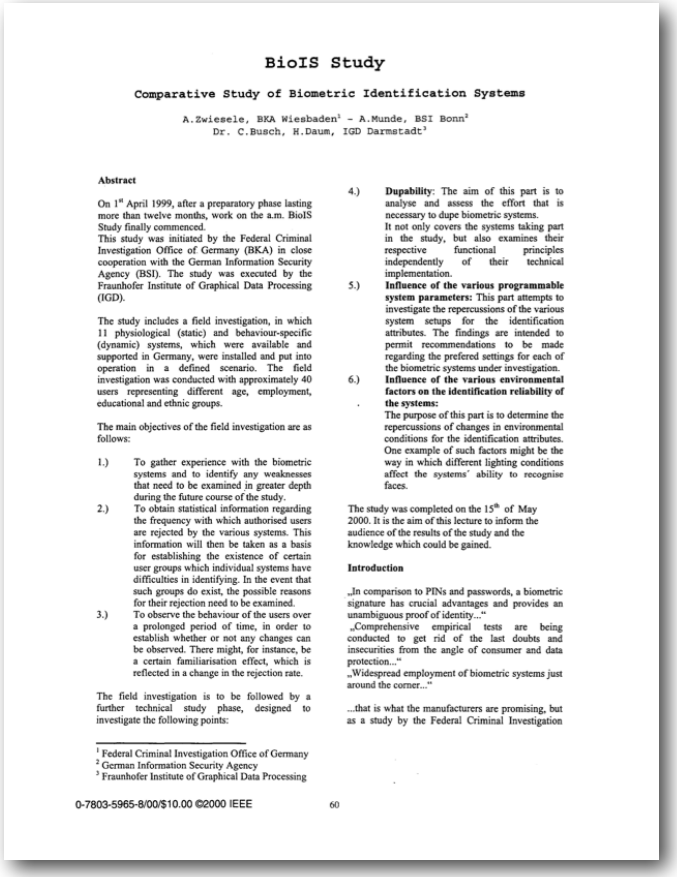
Attack without support of an enroled individual

- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production of a platine

Gummy Finger Production in 2000 !

Reported in a publication by BKA

- A. Zwiesele et al. „BioIS Study - Comparative Study of Biometric Identification Systems“, In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)



BioIS Study

Comparative Study of Biometric Identification Systems

A.Zwiesele, BKA Wiesbaden[1] - A.Munde, BSI Bonn[2]
Dr. C.Busch, H.Daum, IGD Darmstadt[3]

Abstract

On 1st April 1999, after a preparatory phase lasting more than twelve months, work on the a.m. BioIS Study finally commenced.
This study was initiated by the Federal Criminal Investigation Office of Germany (BKA) in close cooperation with the German Information Security Agency (BSI). The study was executed by the Fraunhofer Institute of Graphical Data Processing (IGD).

The study includes a field investigation, in which 11 physiological (static) and behaviour-specific (dynamic) systems, which were available and supported in Germany, were installed and put into operation in a defined scenario. The field investigation was conducted with appoximately 40 users representing different age, employment, educational and ethnic groups.

The main objectives of the field investigation are as follows:

1.) To gather experience with the biometric systems and to identify any weaknesses that need to be examined in greater depth during the future course of the study.
2.) To obtain statistical information regarding the frequency with which authorised users are rejected by the various systems. This information will then be taken as a basis for establishing the existence of certain user groups which individual systems have difficulties in identifying. In the event that such groups do exist, the possible reasons for their rejection need to be examined.
3.) To observe the behaviour of the users over a prolonged period of time, in order to establish whether or not any changes can be observed. There might, for instance, be a certain familiarisation effect, which is reflected in a change in the rejection rate.

The field investigation is to be followed by a further technical study phase, designed to investigate the following points:

4.) **Dupability**: The aim of this part is to analyse and assess the effort that is necessary to dupe biometric systems.
It not only covers the systems taking part in the study, but also examines their respective functional principles independently of their technical implementation.
5.) **Influence of the various programmable system parameters:** This part attempts to investigate the repercussions of the various system setups for the identification attributes. The findings are intended to permit recommendations to be made regarding the prefered settings for each of the biometric systems under investigation.
6.) **Influence of the various environmental factors on the identification reliability of the systems:**
The purpose of this part is to determine the repercussions of changes in environmental conditions for the identification attributes. One example of such factors might be the way in which different lighting conditions affect the systems' ability to recognise faces.

The study was completed on the 15th of May 2000. It is the aim of this lecture to inform the audience of the results of the study and the knowledge which could be gained.

Introduction

„In comparison to PINs and passwords, a biometric signature has crucial advantages and provides an unambiguous proof of identity..."
„Comprehensive empirical tests are being conducted to get rid of the last doubts and insecurities from the angle of consumer and data protection..."
„Widespread employment of biometric systems just around the corner..."

...that is what the manufacturers are promising, but as a study by the Federal Criminal Investigation

[1] Federal Criminal Investigation Office of Germany
[2] German Information Security Agency
[3] Fraunhofer Institute of Graphical Data Processing

0-7803-5965-8/00/$10.00 ©2000 IEEE

Presentation Attack Detection

ISO/IEC 30107 - Definitions

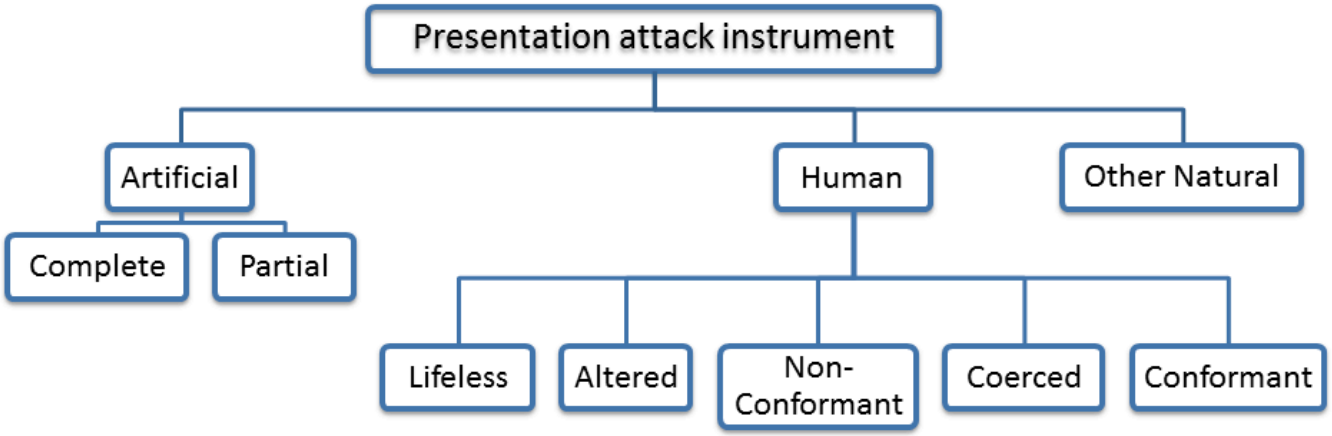
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

Acceptability ?

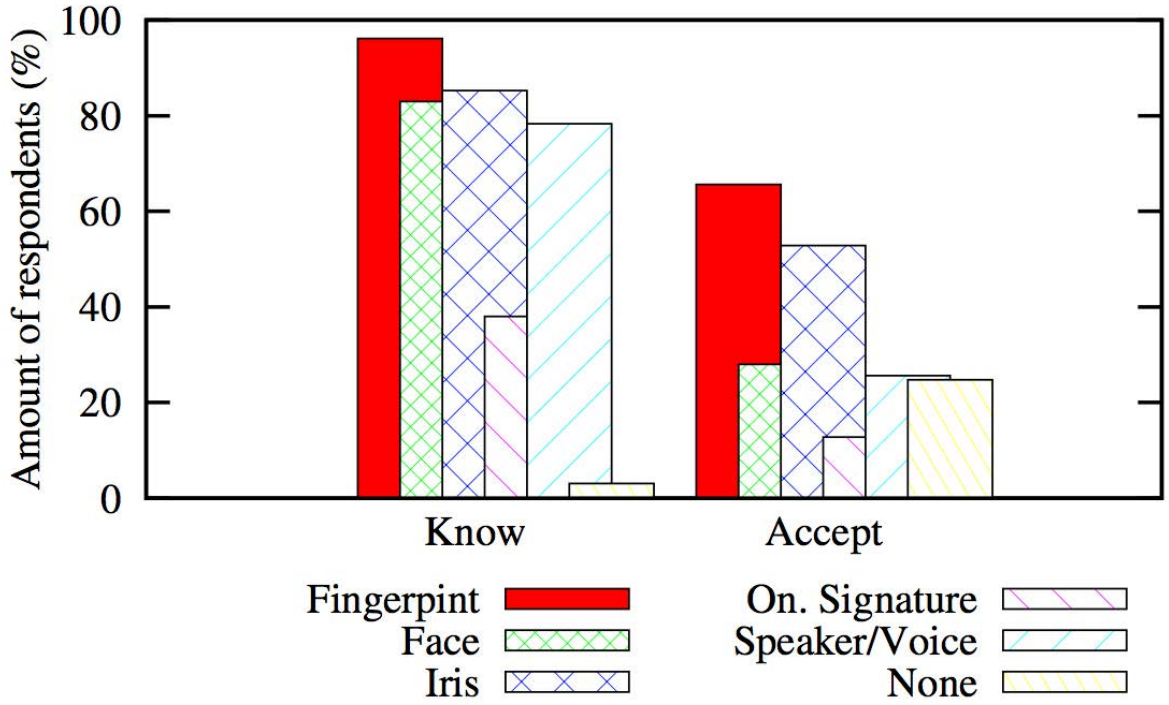
Operators will think:

„*Biometric application must be acceptable for the users*“

Acceptability

Survey in Germany - among 140 individuals

- Biometrics is widely acceptable
  "Biometric recognition based on which characteristics do you know/ accept?"

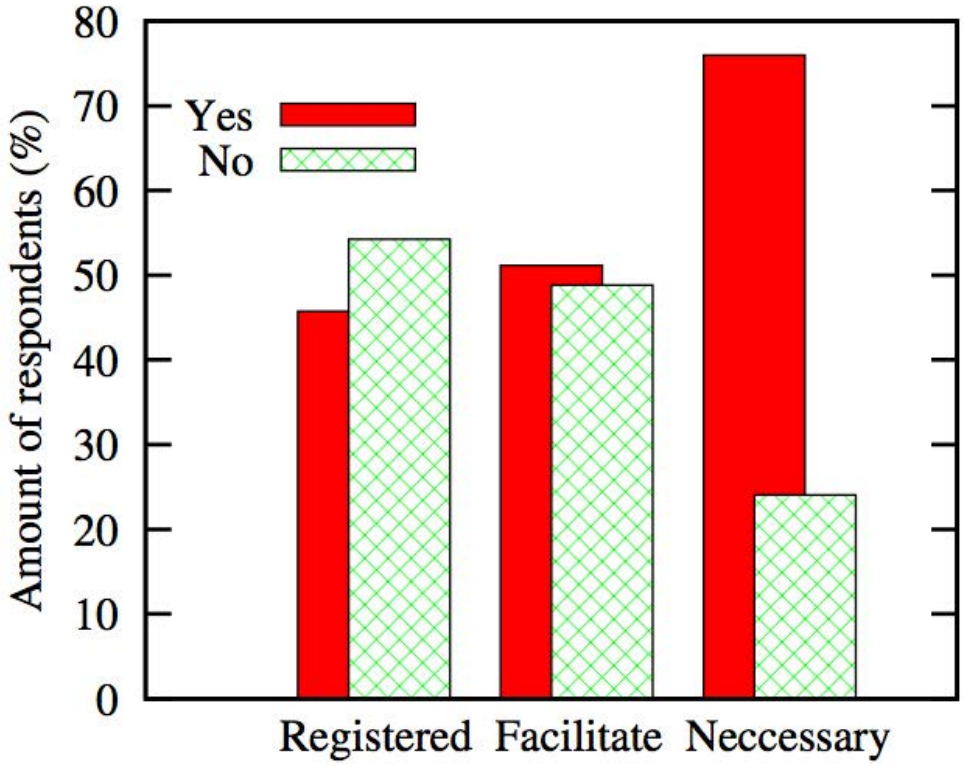


[KRB2013] A. Krupp, C. Rathgeb, C. Busch: "Social Acceptance of Biometric Technologies in Germany: A Survey", in Proceedings of the BIOSIG conference, (2013)

Acceptability

Survey in Germany - among 140 individuals

- Biometrics is widely acceptable
  “Have you used biometrics?”
  “Do biometrics facilitate daily life/ are they necessary?



[KRB2013] A. Krupp, C. Rathgeb, C. Busch: "Social Acceptance of Biometric Technologies in Germany: A Survey", in Proceedings of the BIOSIG conference, (2013)

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

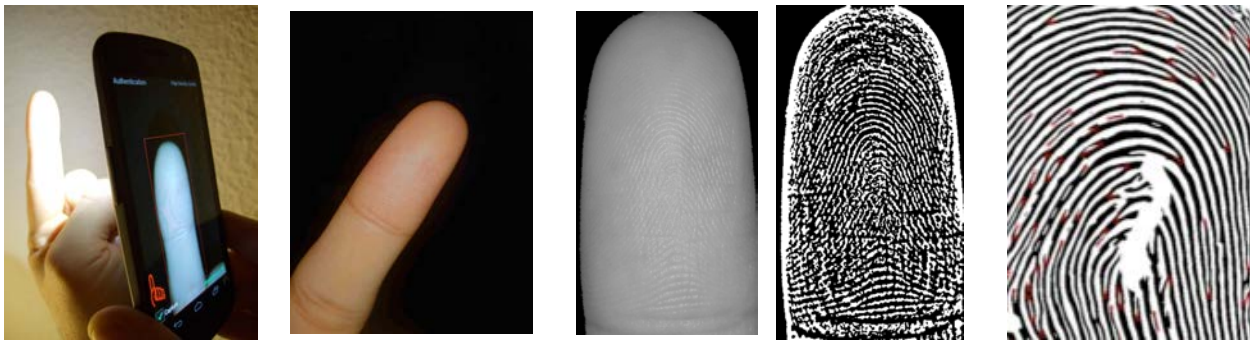
Smartphone Access Control - with PAD

Capture process

- Camera operating in macro modus

Preview image of the camera with LED on (left) and LED off (right)

- LED permanent on



Finger illuminated

[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

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

Transaction-Authentication-Protocol

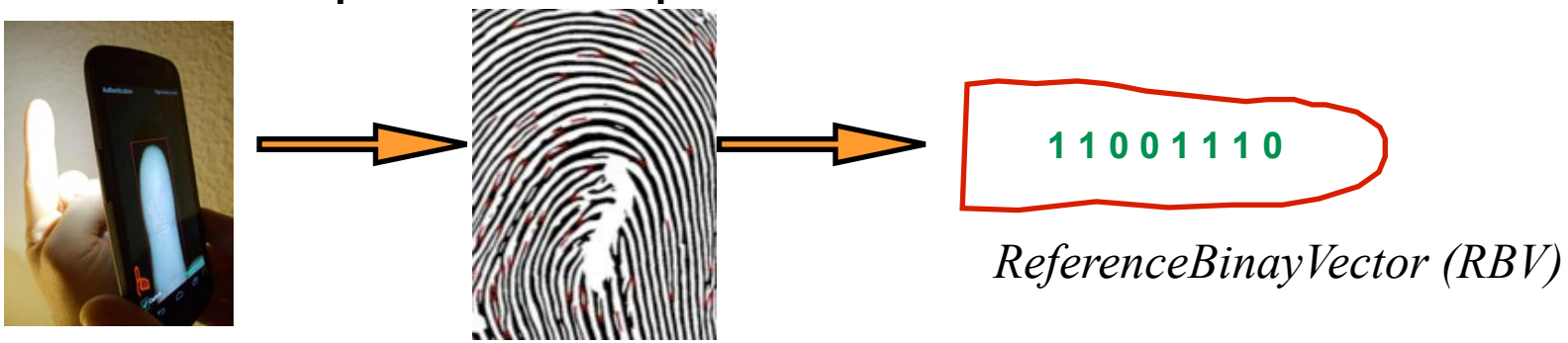
Biometric Transaction Authentication Protocol (BTAP)

1.) Shared secret

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

2.) Biometric enrolment

- Biometric samples are captured

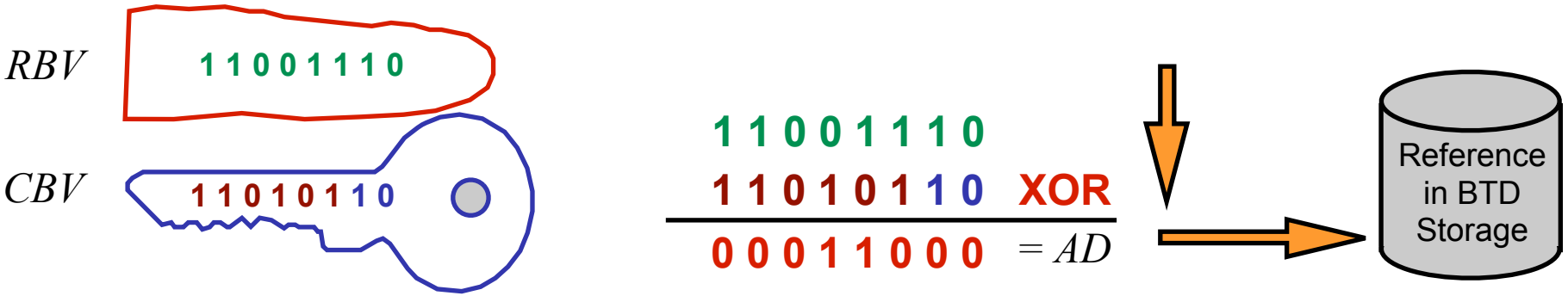


Transaction-Authentication-Protocol

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

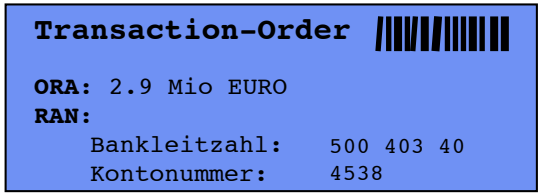
  - Biometric Transaction Device = FIDO Authenticator

Transaction-Verification

BTAP - Transaction

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

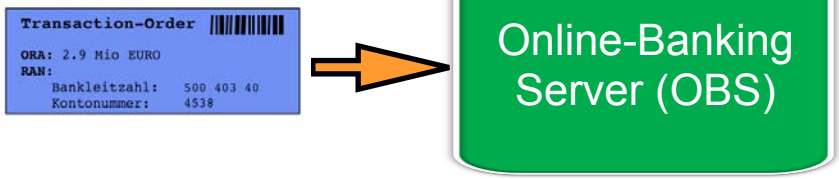
- Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)



  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)



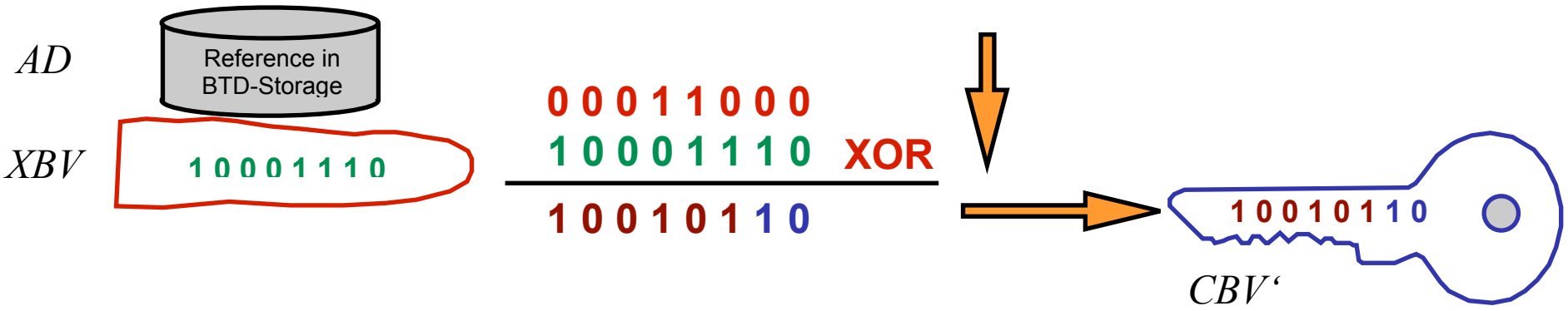
- BSW transfers TOR to Smartphone (BTD / FIDO Authenticator)

Transaction-Verification

BTAP - Transaction

2.) Operations on the Smartphone (BTD)

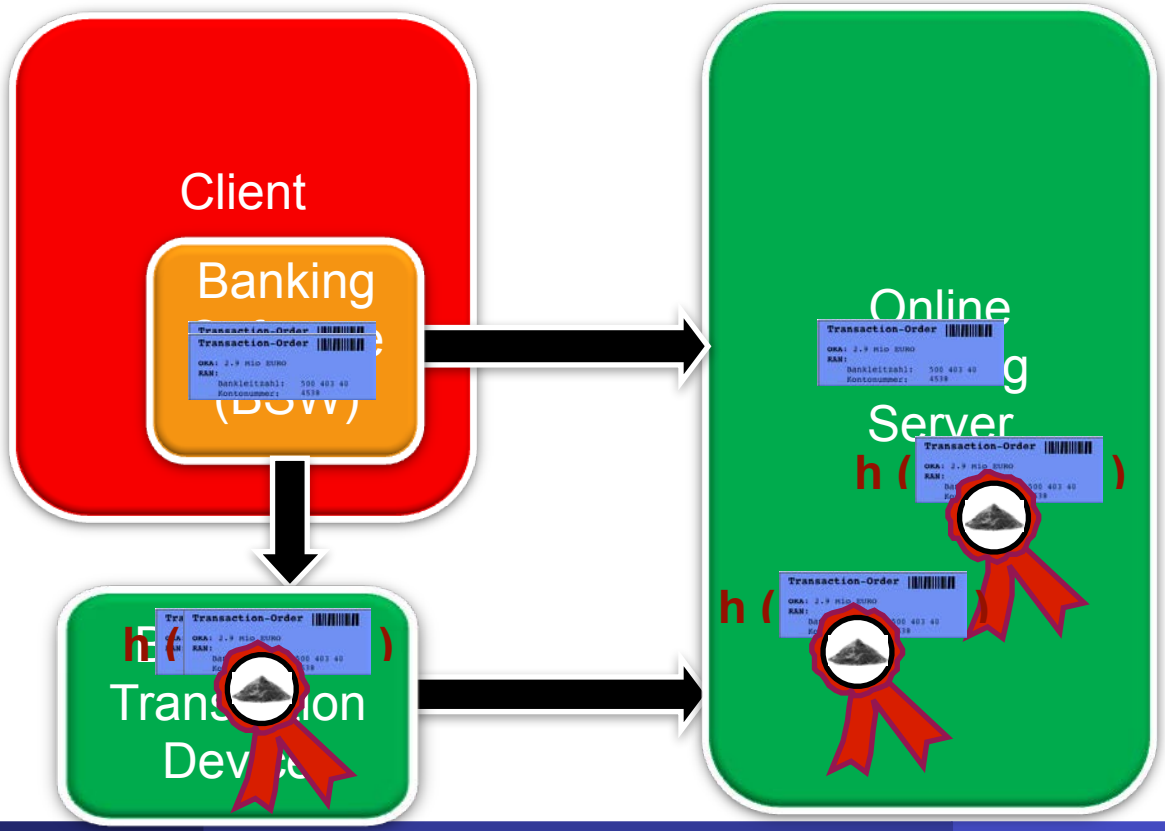
- Approval of the intended transaction by capturing a probe sample
- A secret vector CBV' is reconstructed with XOR operation from the Auxilliary Data AD that was stored in the BTD and from the binarized feature vector XBV



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



Conclusion

Biometrics is possible with todays smartphones

- a multi-biometric authentication scheme with scaling factors is a good choice with respect to security threats

Biometric standards are available

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

BTAP 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


CASED
h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
Prof. Dr. Christoph Busch
Principal Investigator
CASED
Mornewegstr. 32
64293 Darmstadt/Germany
christoph.busch@cased.de
Telefon +49 6151/16 9444
Fax
www.cased.de