Performance, standards and testing: current status in biometrics

Christoph Busch

European Association for Biometrics / Fraunhofer IGD
http://www.christoph-busch.de/

Biometrics in Banking and Payments Frankfurt

Frankfurt - September 24 2015

European Association for Biometrics
eab
Human Identity in Europe

Fraunhofer IGD

Agenda

- From Biometric Rumors to Reality
- Mobile Biometrics
- Mobile Payment Protocol
  - Privacy compliant protocol according to the FIDO Universal Authentication Framework (UAF)
  - a suggestion for a „European derivate of Apple Pay“

Answers on 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*“

Data Protection Requirements

Requirements for data privacy and data protection are formulated in:

- Directive 95/46/EC: On the protection of individuals with regard to the processing of personal data and on the free movement of such data
- EU data protection regulation under development - since 2012
  http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf
- Regulation 45/2001: on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF
- Directive 2002/58/EC: concerning the processing of personal data and the protection of privacy in the electronic communications sector
  http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FIN:EN:PDF

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

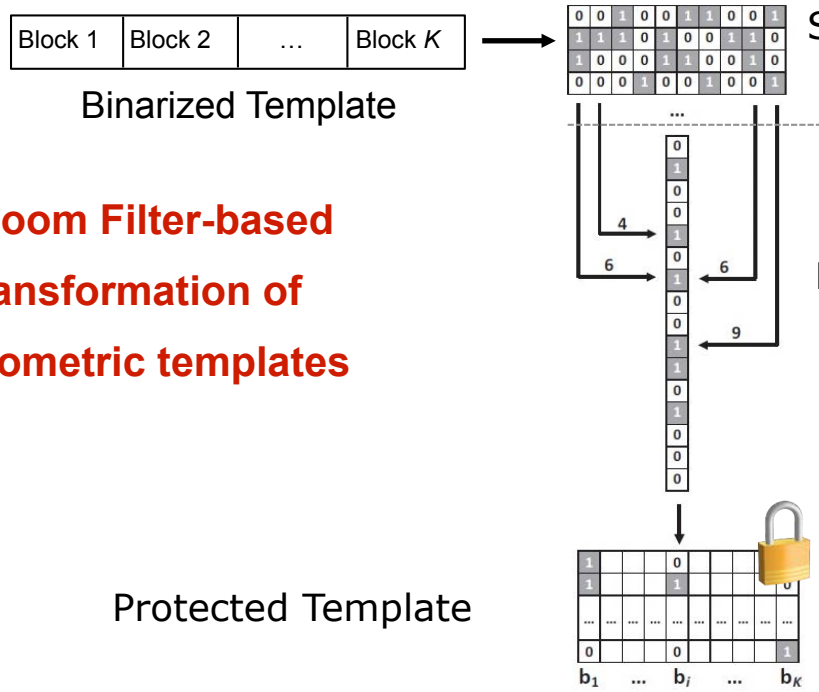
  [RaBBB2013] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014)

  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

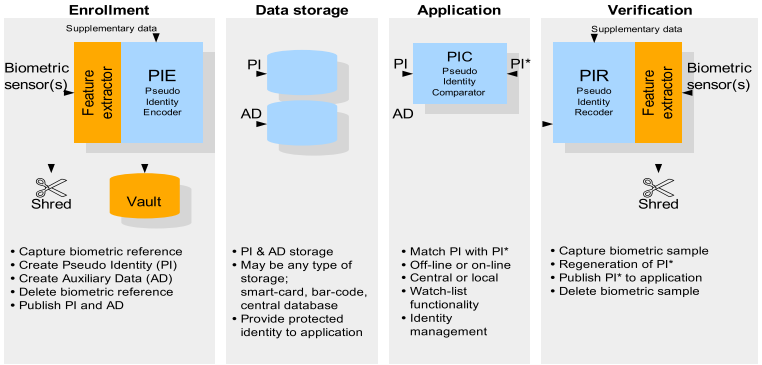
- Secrecy
- Non-invertibility
- Diversification
- Noise robustness

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



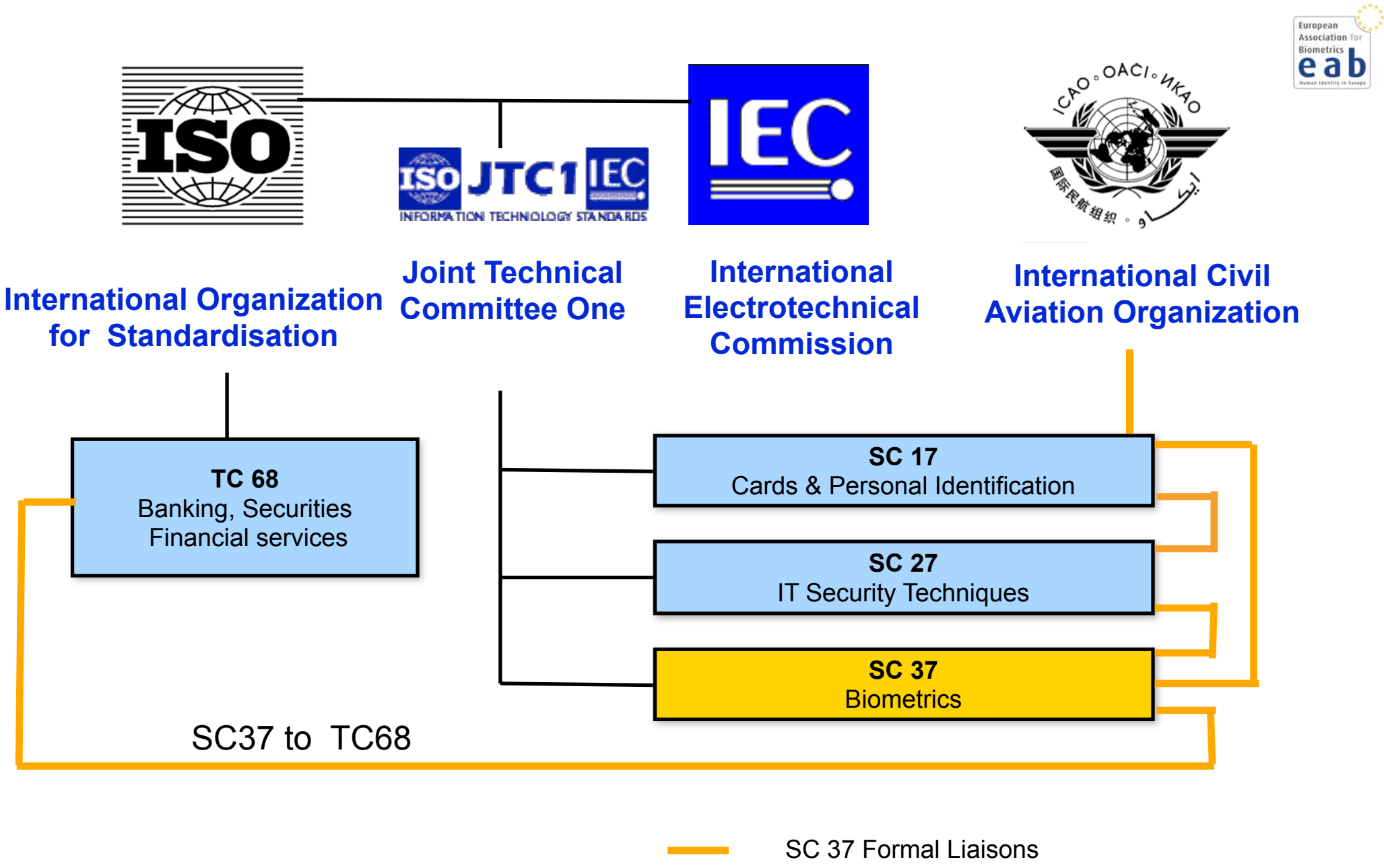
ISO/IEC 24745
Biometric Information Protection !

Standards ?

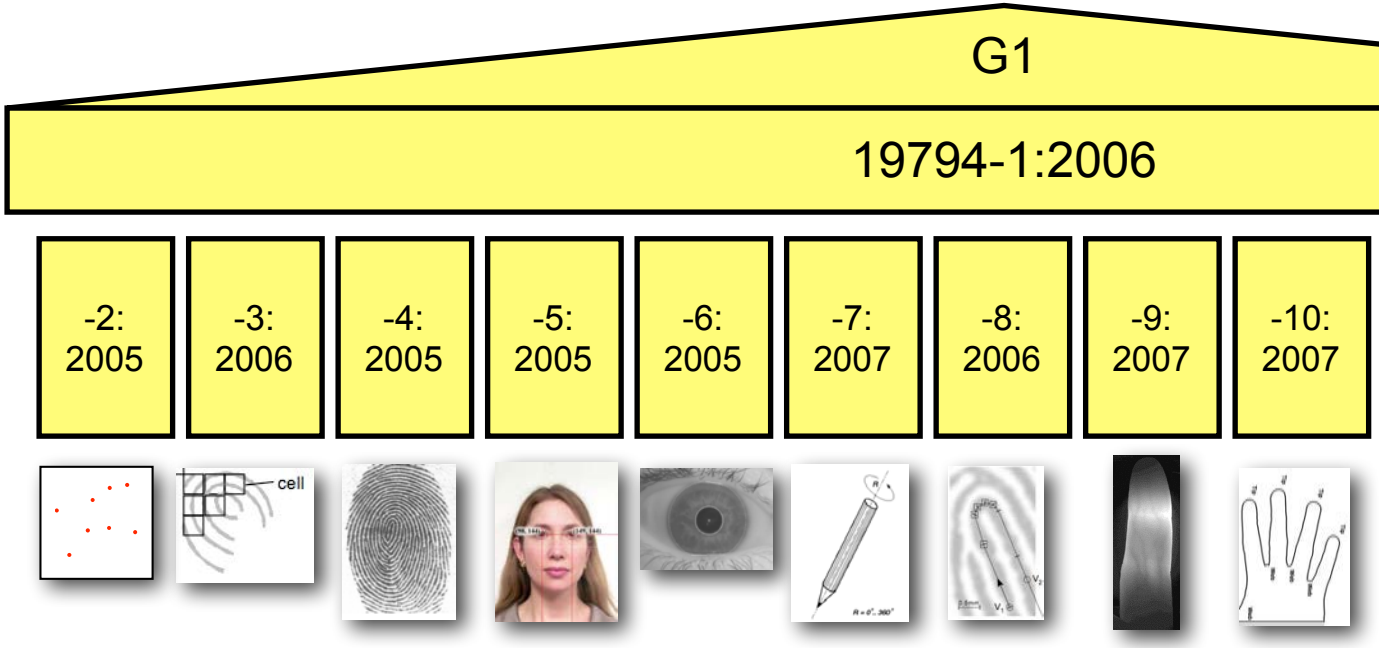
Operators may think:

„*There are no standards on biometrics*“

Biometric Standardisation



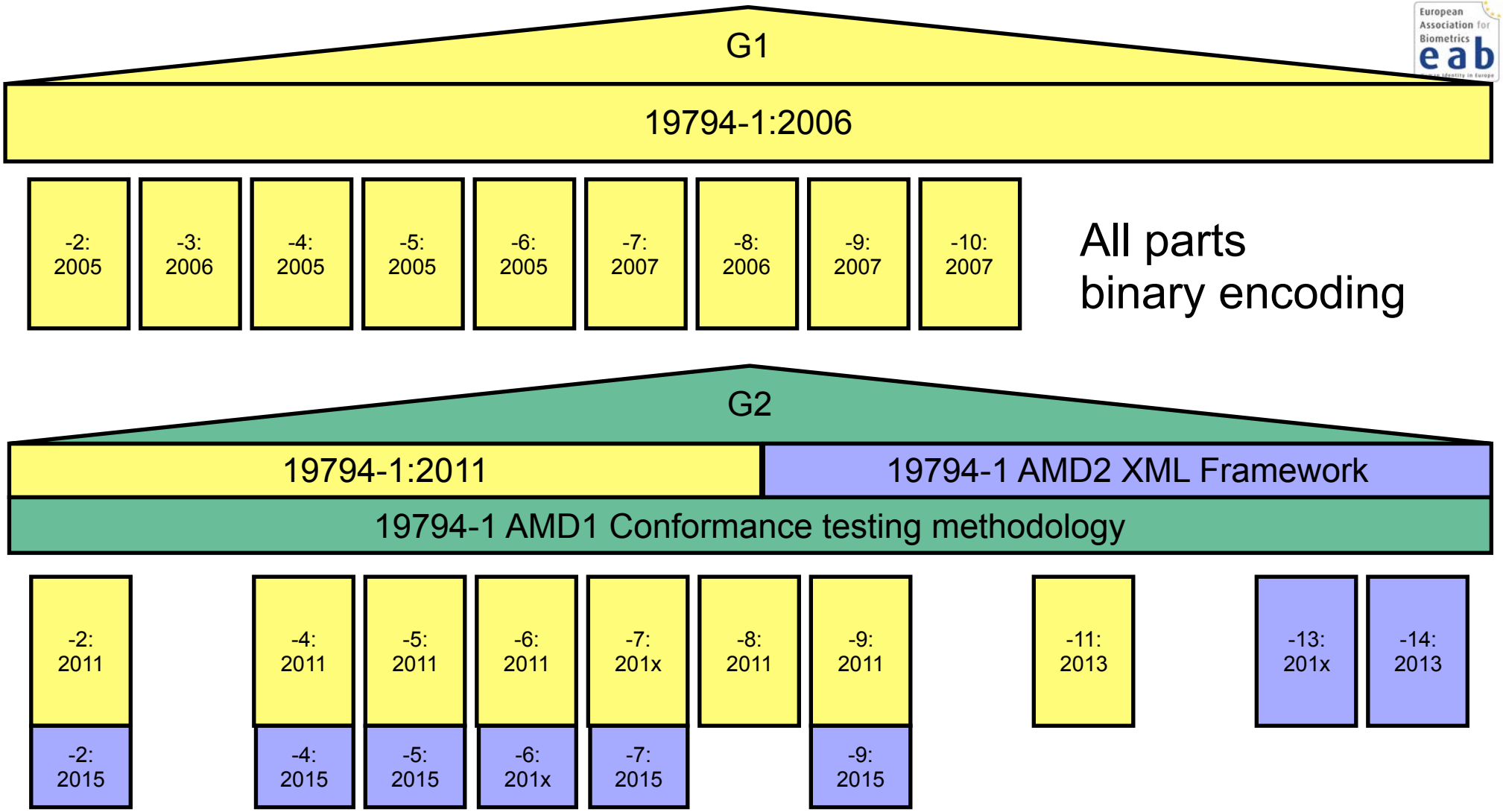
ISO/IEC Interchange Format Standards



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

Biometric Performance Testing Standard

ISO/IEC 19795-x, Information technology - Biometric performance testing and reporting

- Part 1: Principles & Framework
  - Guidance applicable to the broad range of tests
- Part 2: Testing Methodologies for Technology and Scenario Evaluation
  - Multiple visits, habituation, enrolment
- Part 3: Modality-Specific Testing
  - Modality (& application) specific methodologies
- Part 4: Interoperability Performance Testing
  - Performance on other vendors data
- Part 5: Framework for biometric device performance evaluation for access control
- Part 6: Testing Methodologies for Operational Evaluation
- Part 7: Testing of ISO/IEC 7816-based Verification Algorithms

Performance Metrics

Categorization

- 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

Performance Metrics

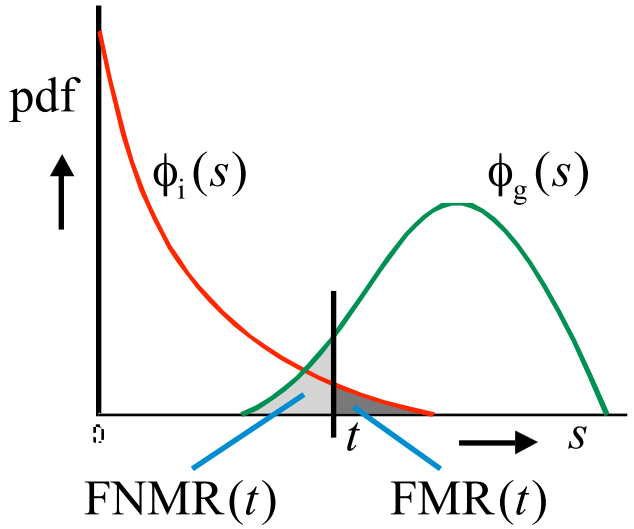
Probability Density Distribution Function (PDF)

$\Phi_g(s)$: PDF of genuine similarity score $s(Q,R)$
$\Phi_i(s)$: PDF of imposter similarity score $s(Q,R)$

False-Match-Rate (FMR)

- **Def in ISO/IEC 2382-37:** *proportion of the completed biometric non-mated comparison trials that result in a false match*
- Note: non-mated comparison trials are also referred to as impostor trials

$$FMR(t) = \int_t^1 \Phi_i(s)ds$$



Performance Metrics

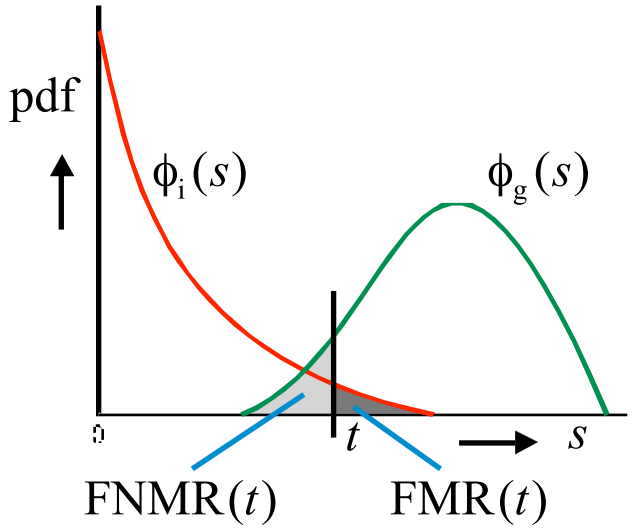
Probability Density Distribution Function (PDF)

$\Phi_g(s)$: PDF of genuine similarity score $s(Q,R)$
$\Phi_i(s)$: PDF of imposter similarity score $s(Q,R)$

False-Non-Match-Rate (FNMR)

- **Def in ISO/IEC 2382-37:** *proportion of the completed biometric mated comparison trials that result in a false non-match*
- Note: mated comparison trials are also referred to as genuine trials

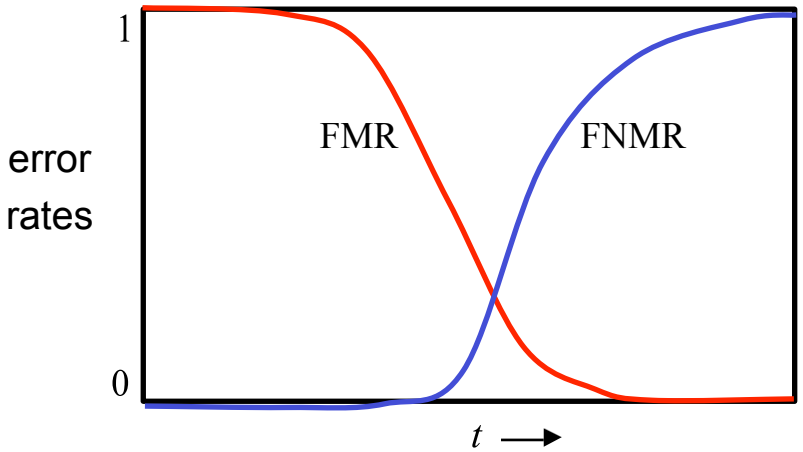
$$FNMR(t) = \int_0^t \Phi_g(s)ds$$



Performance Metrics

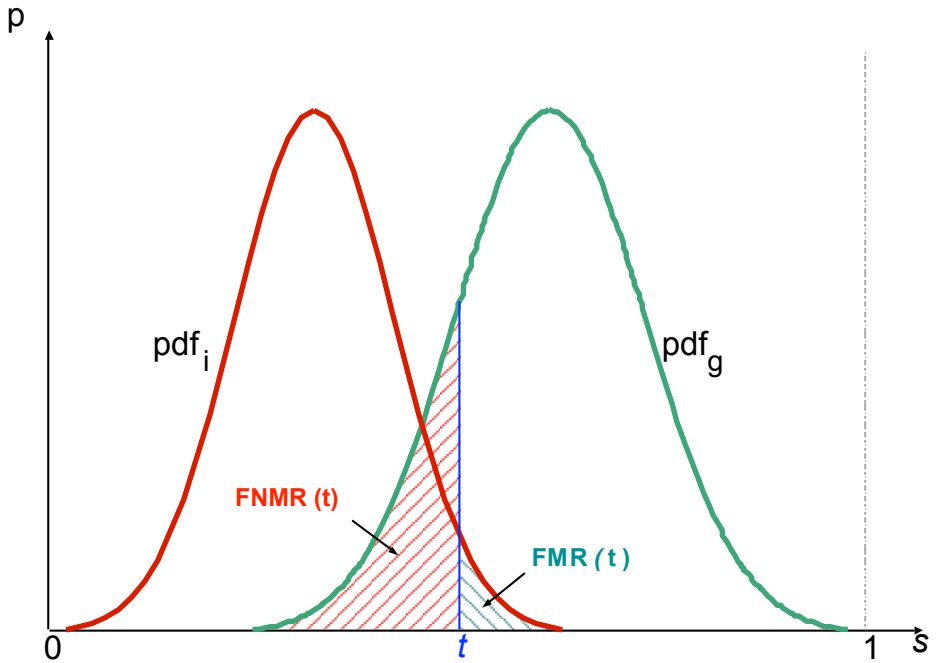
Algorithm error rates

- Equal-Error-Rate (EER)
  - both errors (FMR and FNMR) are equal
  - single number
- FNMR @ FMR=0,001
  - more reasonable single number
- Constraints:



$$FMR(0) = 1, FMR(1) = 0$$

$$FNMR(0) = 0, FNMR(1) = 1$$

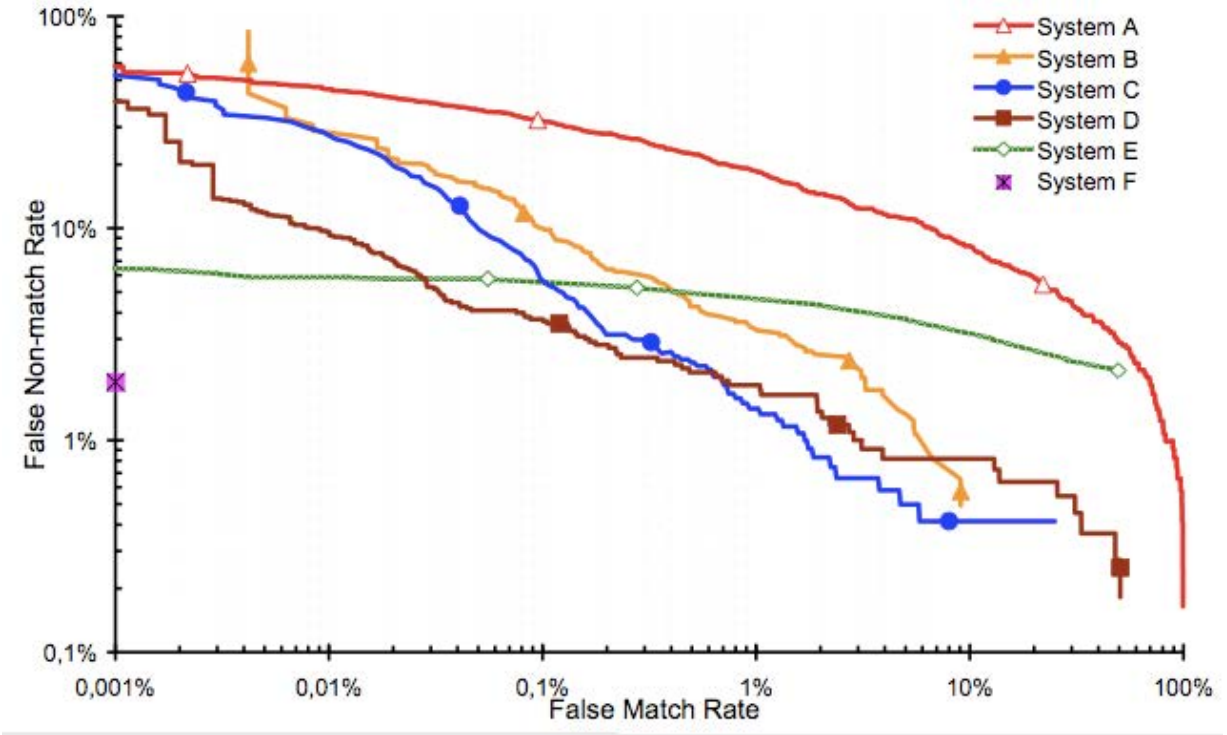


Threshold

Graphical Presentation

DET curve (detection error trade-off curve)

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

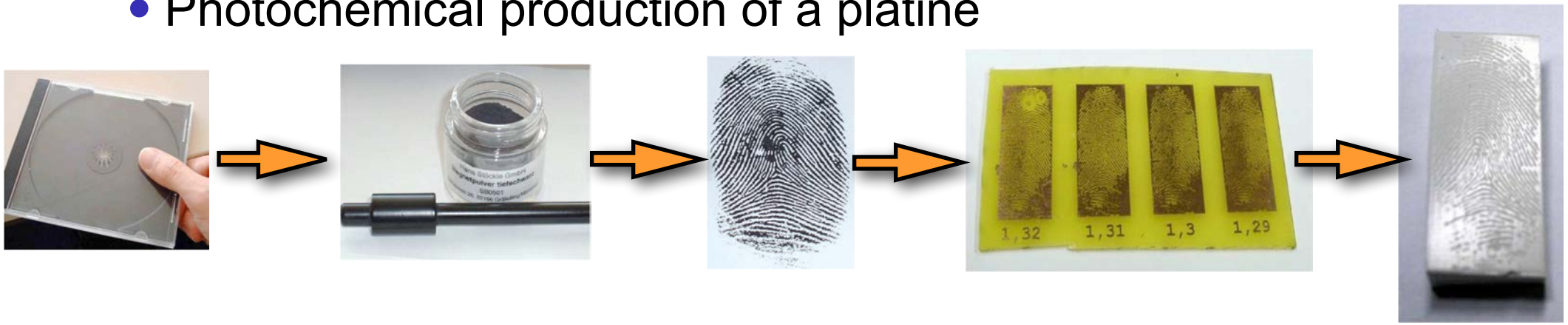


- Extensive test results: http://www.nist.gov/itl/iad/ig

Gummy Finger Production in 2000 !

Attack without support of an enroled individual

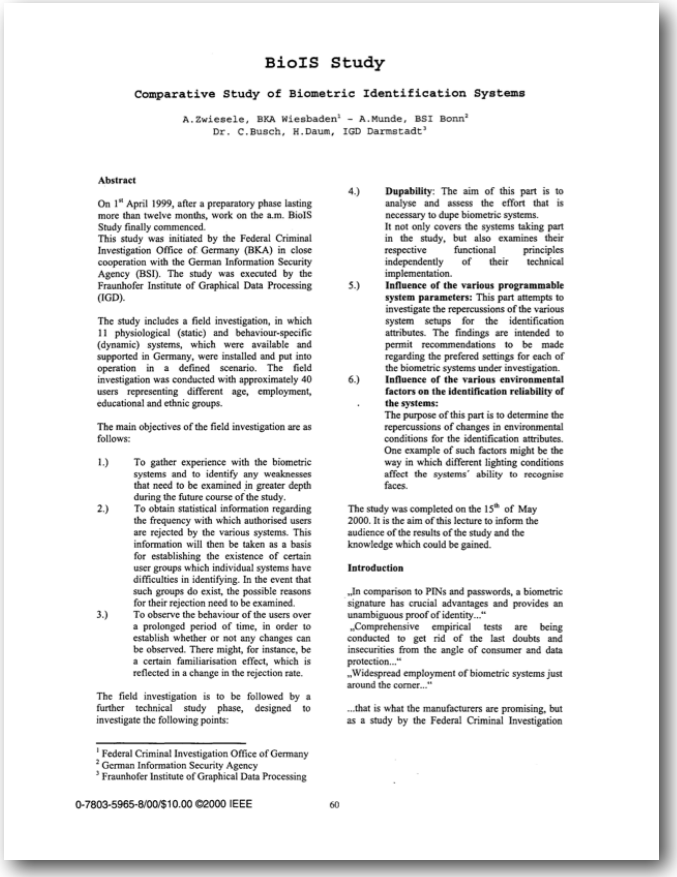
- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production 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 60

Attacks on the Biometric Sensor

ISO/IEC 30107 - Biometric Presentation Attack Detection

Scope

- terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods;
- a common data format for conveying the type of approach used and the assessment of presentation attack in data formats;
- principles and methods for performance assessment of presentation attack detection algorithms or mechanisms; and

Outside the scope are

- standardization of specific PAD detection methods;
- detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;
- overall system-level security or vulnerability assessment.

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

ISO/IEC 30107 - Definitions

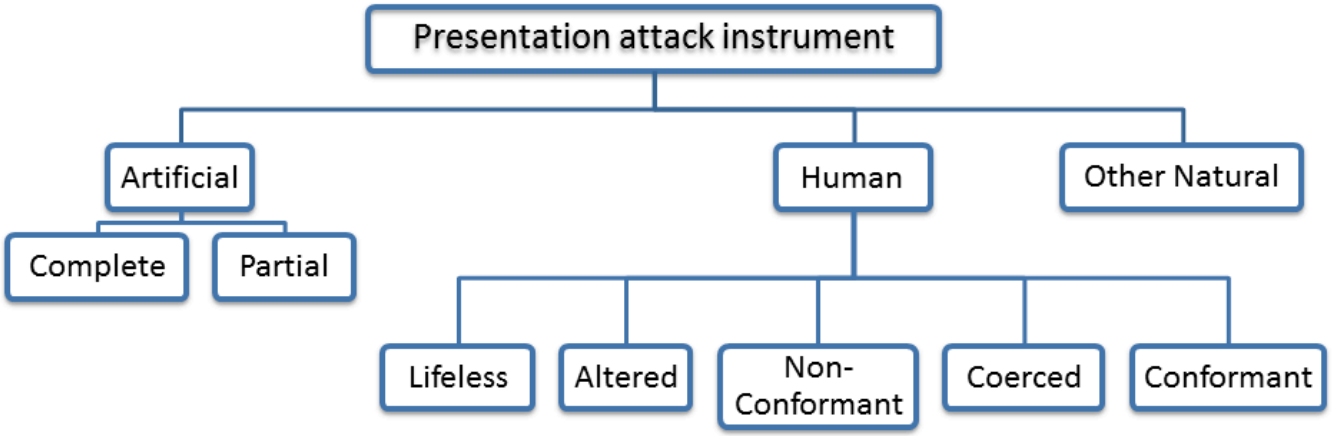
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

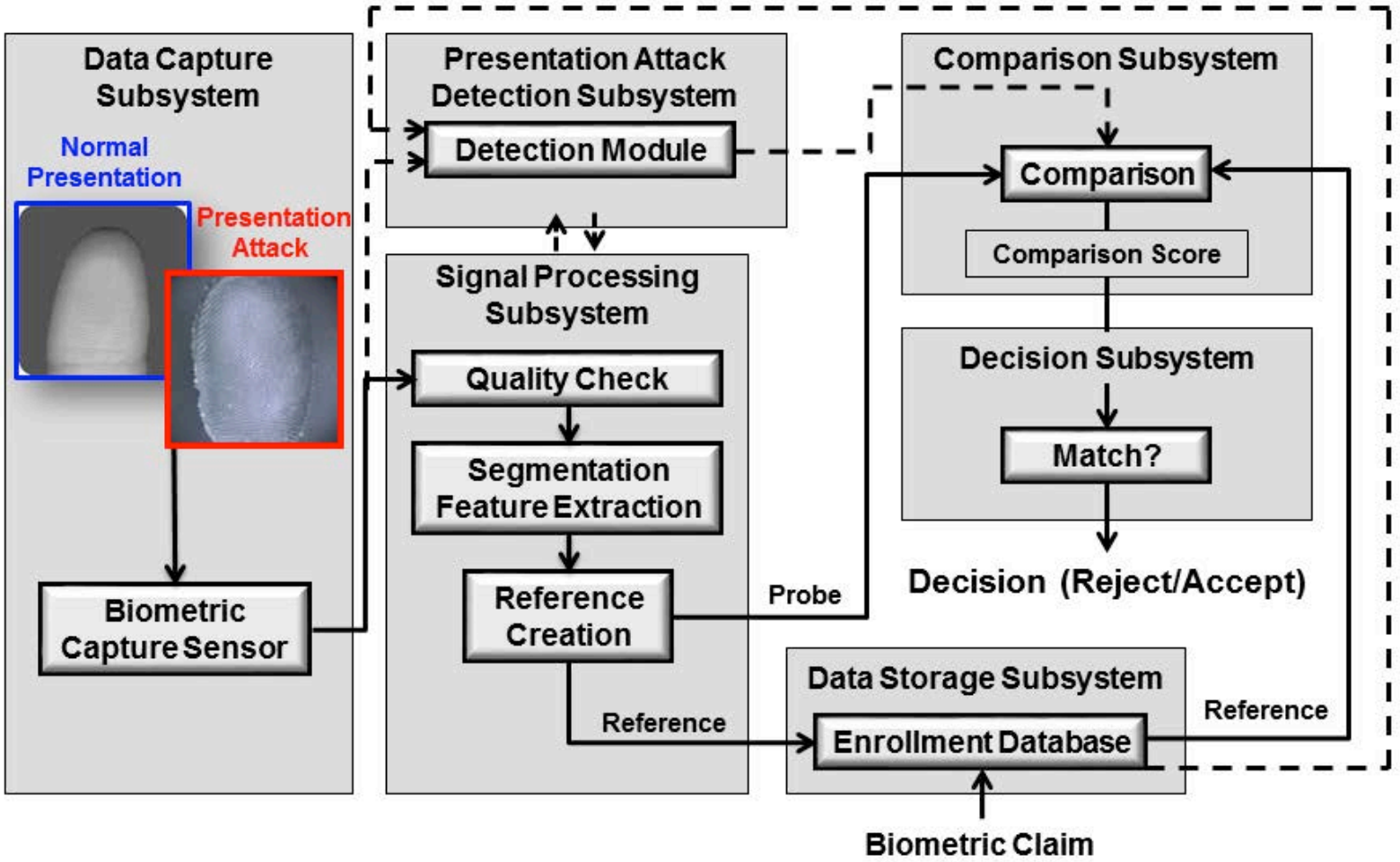
(Qualifying adjectives)



Source: ISO/IEC 30107-1

Presentation Attack Detection

Biometric framework with PAD

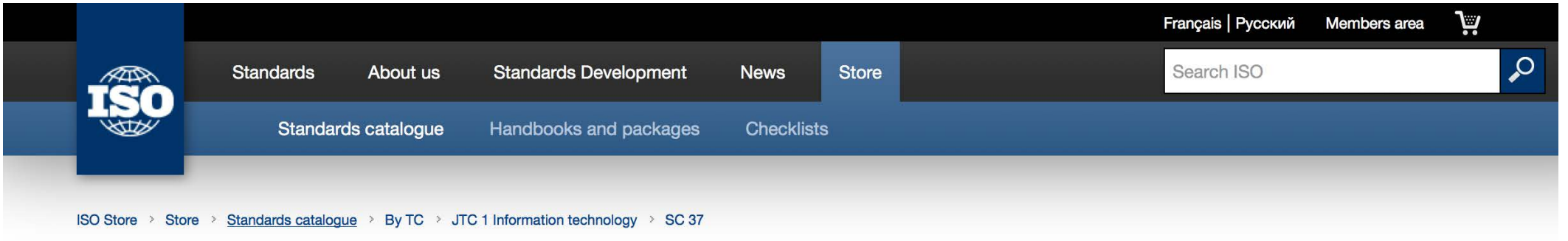


Source: ISO/IEC 30107-1

Presentation Attack Detection

ISO/IEC IS 30107-1 Standard

- **soon available in the ISO-Portal**
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53227



Presentation Attack Detection - Testing

Methodology in ISO/IEC 30107 Presentation Attack Detection - Part 3: Testing and reporting

- Security Evaluation
  - for evaluations using the Common Criteria Framework
  - Protection Profile (PP) (e.g. from German BSI)
  - Security Target (ST)
  - Evaluation Assurance Level (EAL)
  - Assessment of the attack potential
  - *„if there is at least one aretefact that can reproducibly successful attack the PAD-component - then the PAD failed the test“*
- Other approaches
  - for evaluations in academic and technology development
  - tolerating the limited statistical significance of small test set
    - the statistical distribution is unknown and for sure not normal
  - *„ a score based metric can tell us, if the method improved“*

Presentation Attack Detection - Testing

Definition of harmonized metrics in ISO/IEC 30107-3

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations incorrectly classified as normal presentations at the component level in a specific scenario

- **Normal presentation classification error rate (NPCER)**
  proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario

PAD-Standard and FIDO

FIDO - on 9th September 2015

What about rubber fingers?

- Protection methods in FIDO
  1. Attacker needs access to the Authenticator and have swipe rubber finger on it. This makes it a non-scalable attack.
  2. Authenticators might implement presentation attack detection methods.

Remember:

Creating hundreds of millions of rubber fingers + stealing the related authenticators is expensive. Stealing hundreds of millions of passwords from a server is not.

Source: R. Lindemann (NokNok) - 2015

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

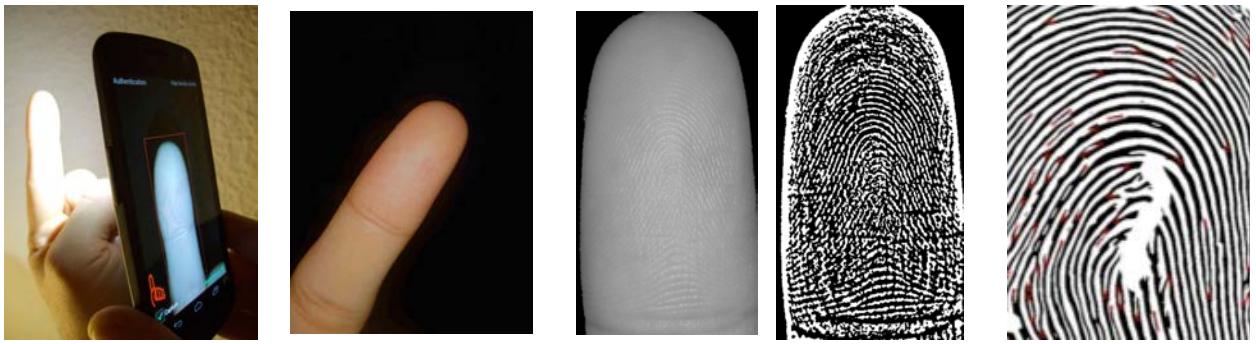
Smartphone Access Control - with PAD

Capture process

- Camera operating in macro modus

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

- LED permanent on



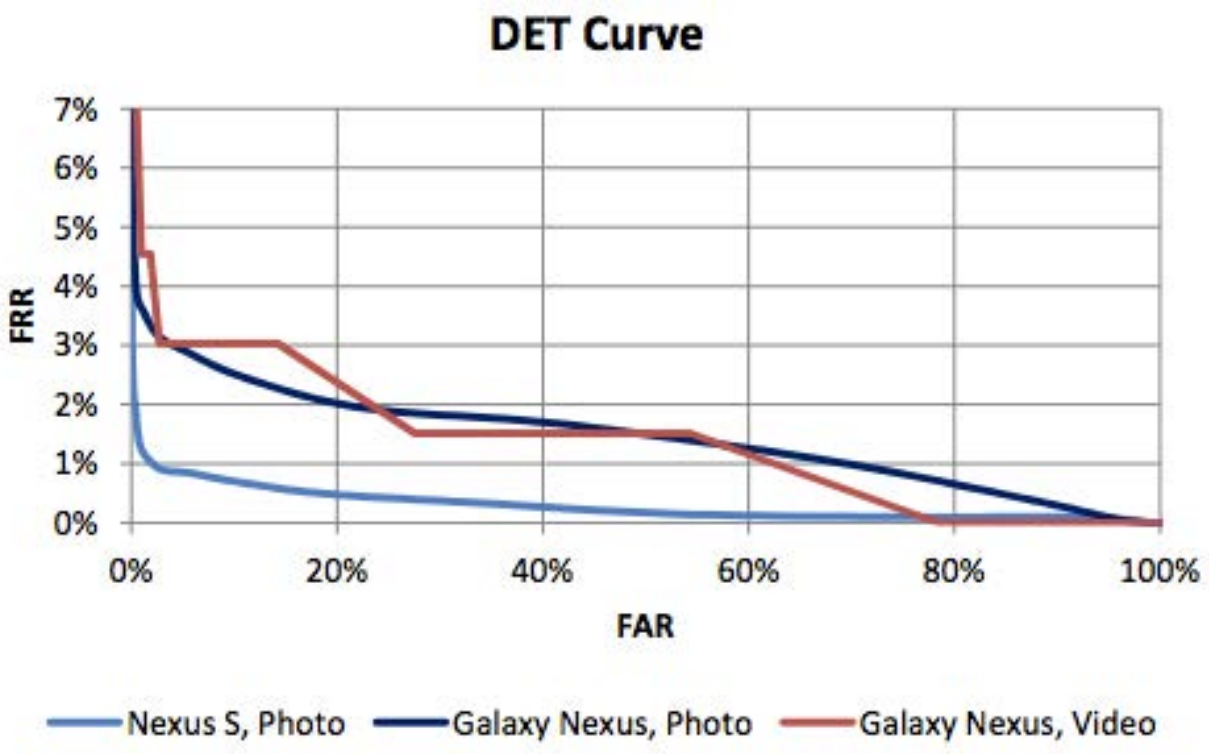
Finger illuminated

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

Smart Phone Access Control - with PAD

Finger recognition study - 2012/2013

- Result: biometric performance at 1.2% EER



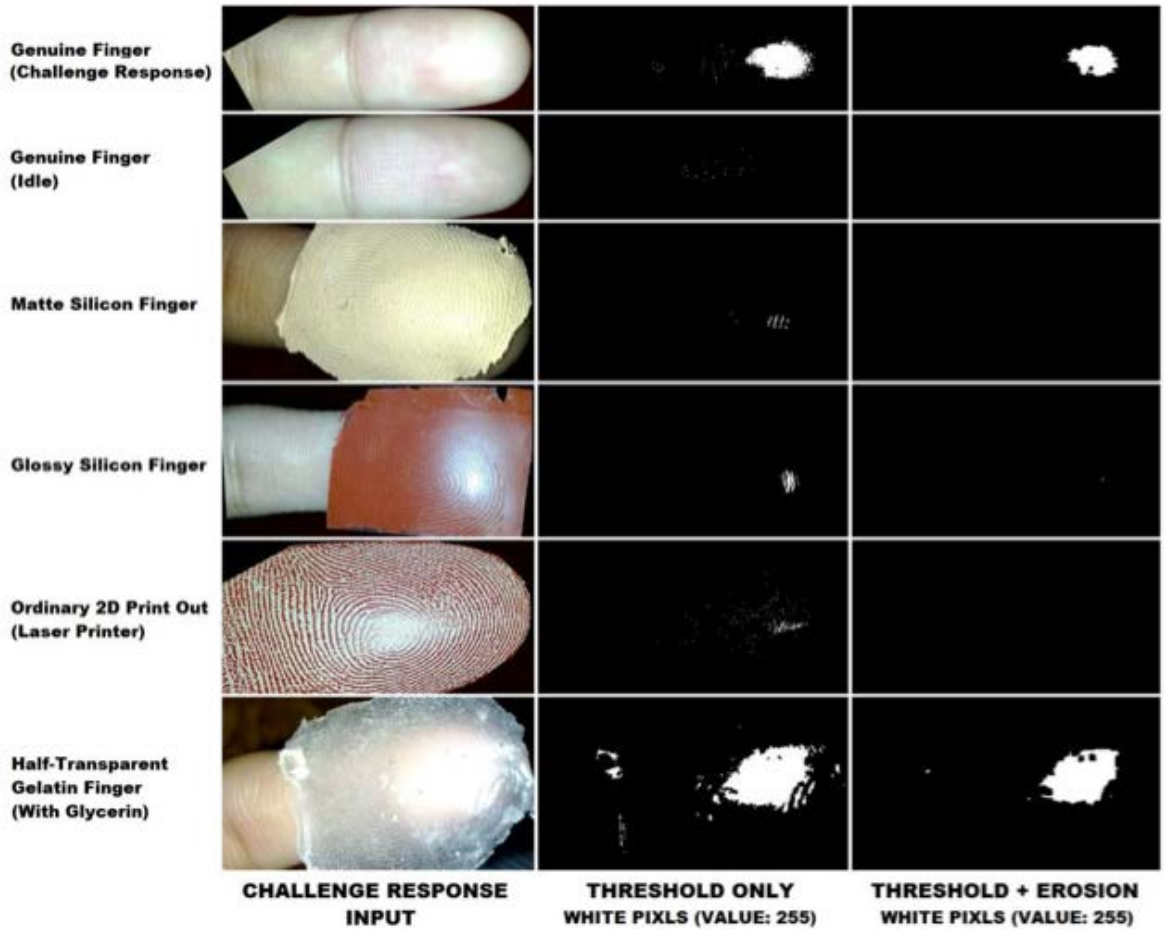
Capture Method and Device	EER from [SC-2012]	EER	FRR (FAR=0.1%)
Photo, Nexus S	22.3%	1.2%	2.7%
Photo, Galaxy Nexus	19.1%	3.1%	6.7%
Video, Galaxy Nexus	-	3.0%	12.1%

[SBB2013] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Smart Phone Access Control - with PAD

Finger recognition study - 2012/2013

- Results: Presentation Attack Detection (PAD)



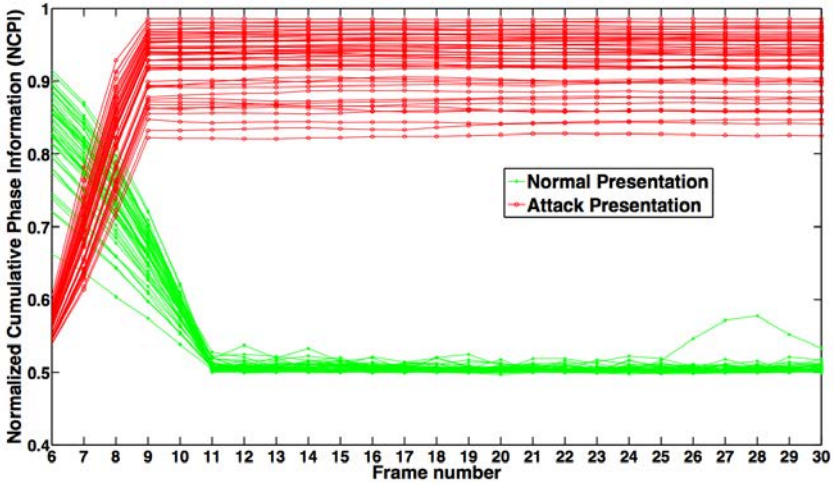
- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Smart Phone Access Control - with PAD

Eye recognition study - 2015

- Presentation Attack Detection (PAD) videos on iPhone 5 S and Nokia 1020

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information



- Error Rates:
  - APCER = 0 %
  - NPCER = 0 %

[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

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

Transaction-Authentication-Protocol

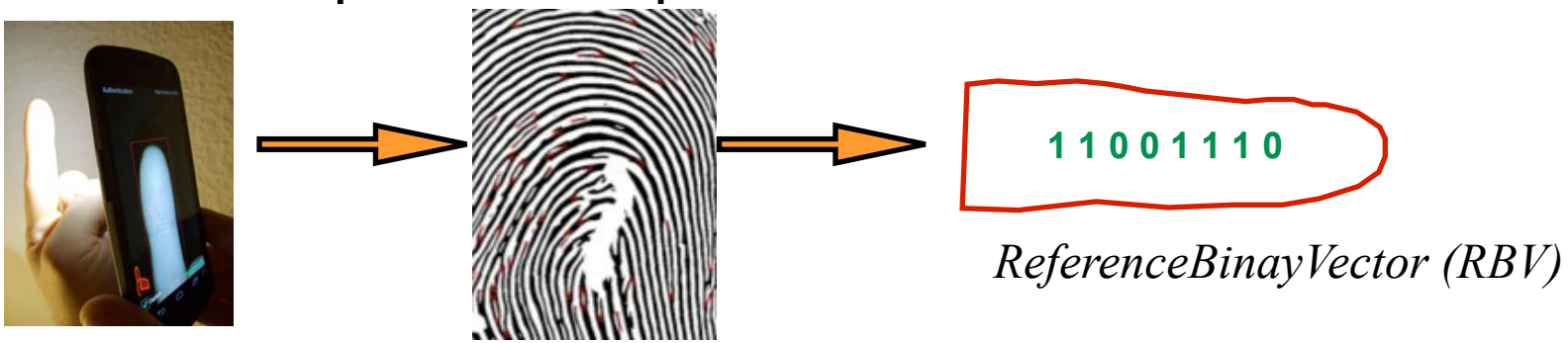
Biometric Transaction Authentication Protocol (BTAP)

1.) Shared secret

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

2.) Biometric enrolment

- Biometric samples are captured

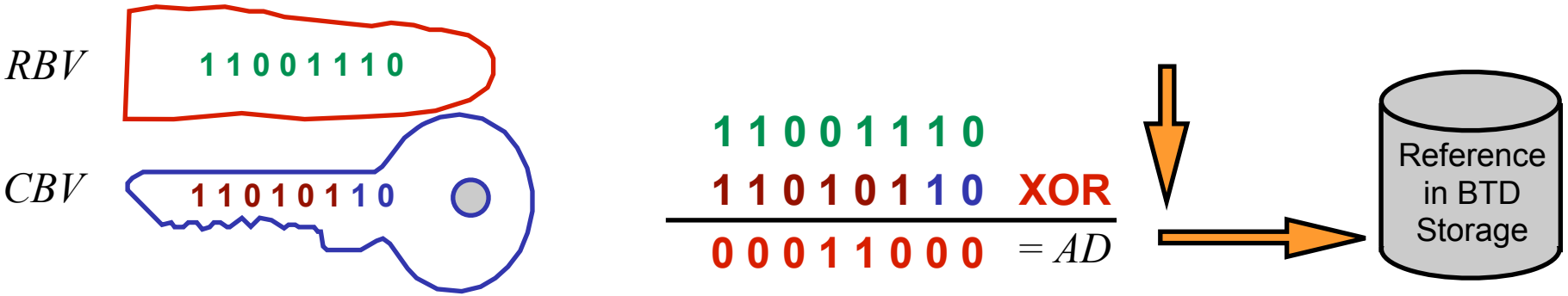


Transaction-Authentication-Protocol

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



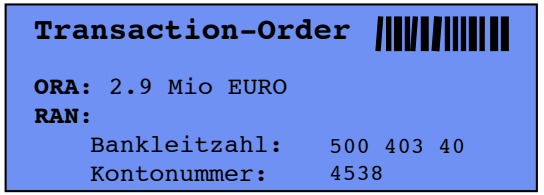
- Auxilliary data (AD) stored in the Smartphone
  - Biometric Transaction Device = FIDO Authenticator

Transaction-Verification

BTAP - Transaction

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

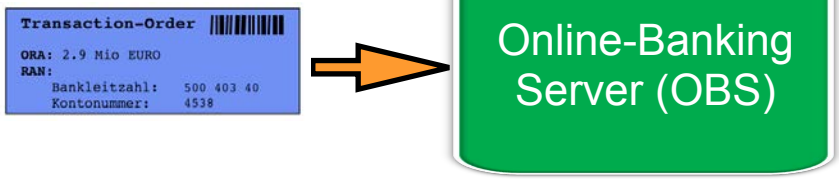
- Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)



  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)



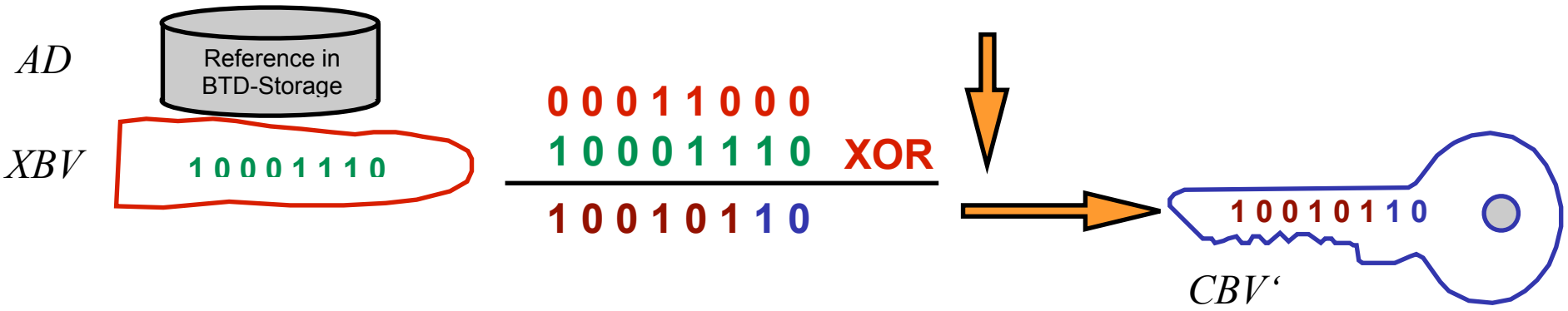
- BSW transfers TOR to Smartphone (BTD / FIDO Authenticator)

Transaction-Verification

BTAP - Transaction

2.) Operations on the Smartphone (BTD)

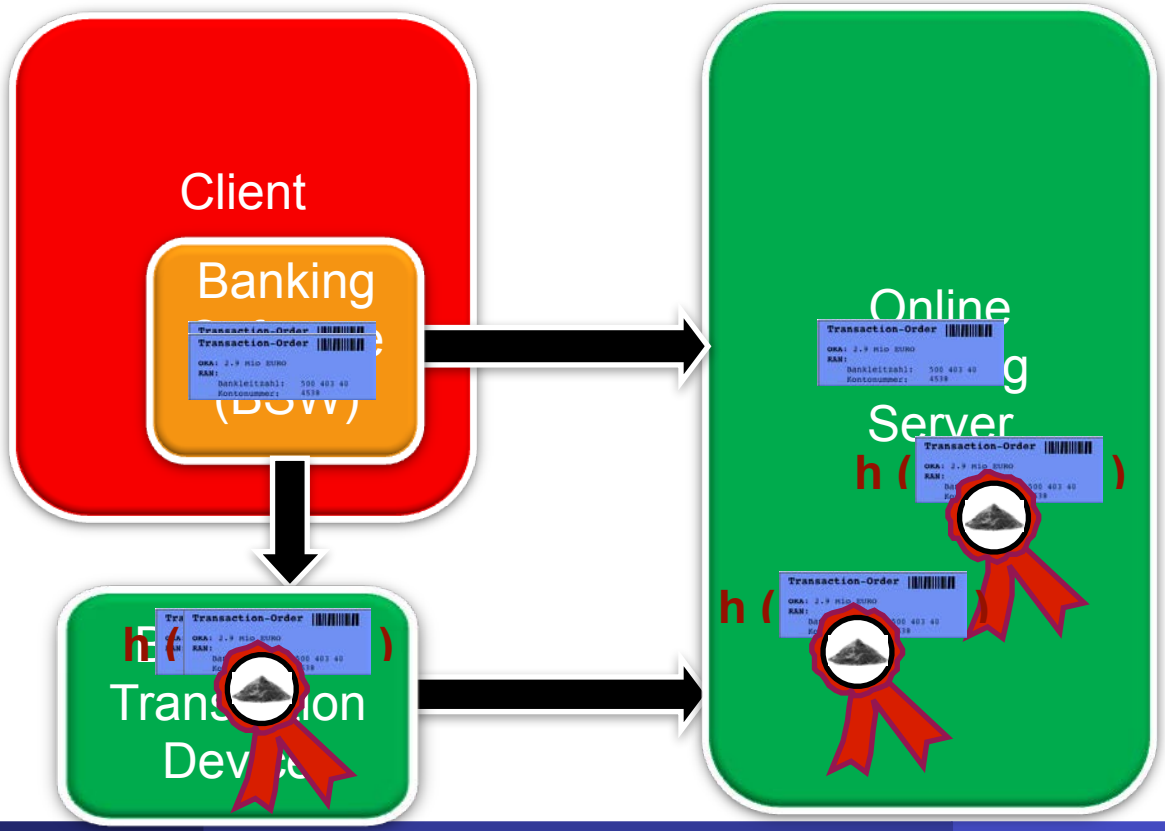
- Approval of the intended transaction by capturing a probe sample
- A secret vector CBV' is reconstructed with XOR operation from the Auxilliary Data AD that was stored in the BTD and from the binarized feature vector XBV



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



Transaction-Verification

BTAP-Video

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

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

Kontakt

Prof. Dr. Christoph Busch

Fraunhoferstrasse 5
64283 Darmstadt, Germany
Phone: +49-6151-155-536
christoph.busch@igd.fraunhofer.de
www.igd.fraunhofer.de/~busch