Biometric standardization and Presentation Attack Detection

Christoph Busch

Norwegian Biometrics Laboratory - Gjøvik
http://www.christoph-busch.de

The 1st Danish Biometrics Workshop

Copenhagen - November 26th, 2015

European Association for Biometrics
eab
Human Identity in Europe

HØGSKOLEN I GJØVIK

Norwegian Biometrics Laboratory (NBL)

- Faculty-Members:
  - Christoph Busch
  - Patrick Bours
  - Bian Yang
  - Faouzi Alaya Cheikh
  - Sule Yildrim
  - Erik Hjelmås
  - Raghu Ramachandra
  - Katrin Franke (adjunct member)
  - Ivar Farup (adjunct member)
  - Mohammad Derawi

- PhD-Students:
  - Ctirad Sousedik
  - Edlira Martiri
  - Guoqiang Li
  - Kiran Raja
  - Martin Olsen
  - Martin Stokkenes
  - Nabeel Al-Bahbooh
  - Soumik Mondal
  - Marta Gomez (guest from UAM)

- Key-factors:
  - Since 2008, 6 EU FP7 projects,
    2 Norwegian funded project
    1 US-government funded project,
    2 research projects with the German BSI,
    4 industrial projects,
  - cooperated with > 30 research partners
  - approx 110 peer-reviewed publications

Standardization Meetings

Biometric Applications

Biometrics and Access Control

Automated Border Control in Europe

- Automated but supervised border control since 08‘2009
- Self-Service to increase throughput

US VISIT

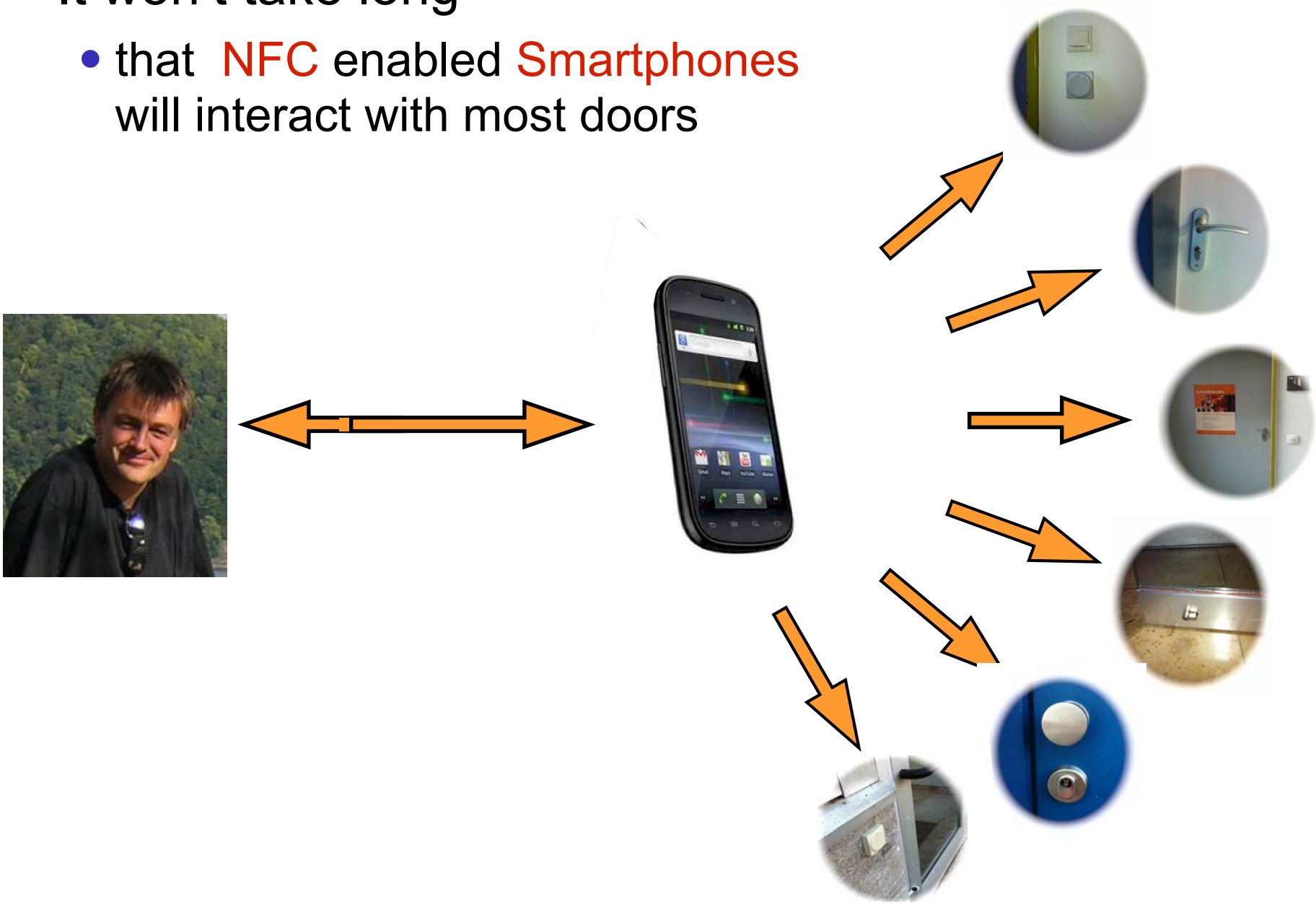
- Visitors with a criminal record are rejected

Source: US Visit

Smartphone Based Access Control

It won‘t take long

- that NFC enabled Smartphones will interact with most doors



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

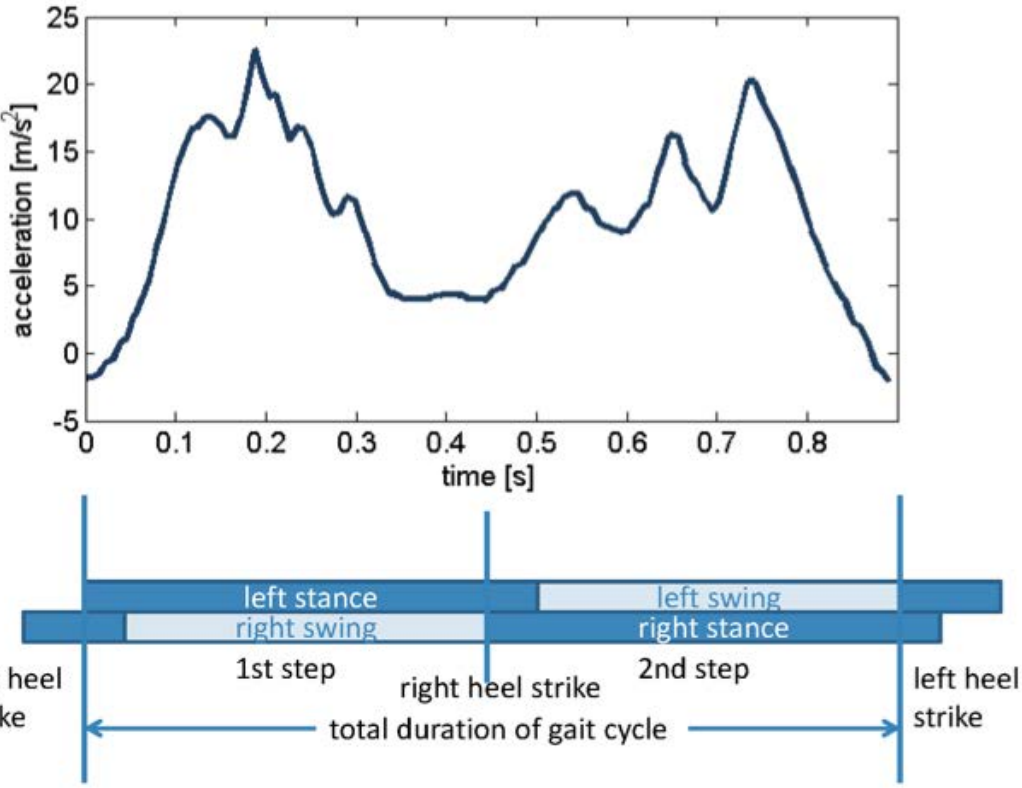
Background authentication (observation of the user)

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

Biometric Gait Recognition

Data capture process

- periodical pattern in the recorded signal



Best result

- now at 6.1% Equal-Error-Rate (EER)

Biometric Gait Recognition

- All benchmarked publications

Publication	Sensor	Sensor-position	Number Subjects	Best Result [%]
Ailisto [4], 2005	dedicated	back	36	6,4 (EER)
Rong [123], 2007	dedicated	back	21	5,6 (EER)
Pan [61], 2009	Wiimote	hip	30	70,1 (GMR)
Sprager [130], 2009	smartphone	hip	6	92,9 (CCR)
Gafurov [46], 2010	dedicated	ankle	10	59,0 (GMR)
Nickel (CASED)	smartphone	hip	48	6,1 (EER)

[NB11] C. Nickel, C. Busch „Classifying Accelerometer Data via Hidden Markov Models to Authenticate People by the Way they Walk“, 45th IEEE International Carnahan Conference on Security Technology (ICCST 2011)

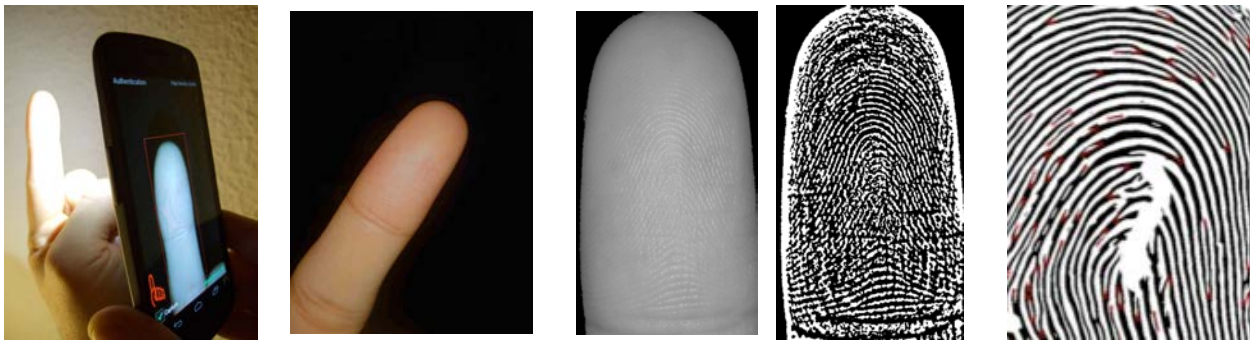
Smartphone Access Control

Capture process

- Camera operating in macro modus

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

- LED permanent on



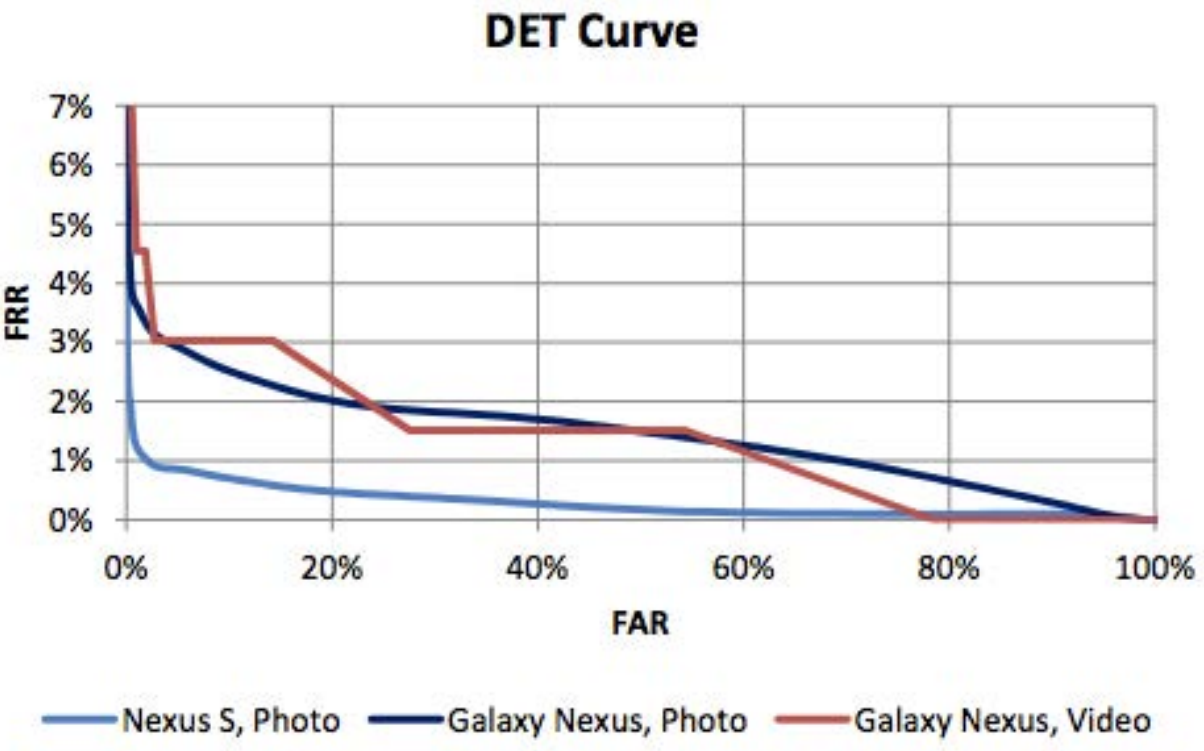
Finger illuminated

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

Smartphone Access Control - with PAD

Finger recognition study - 2012/2013

- Result: biometric performance at 1.2% EER



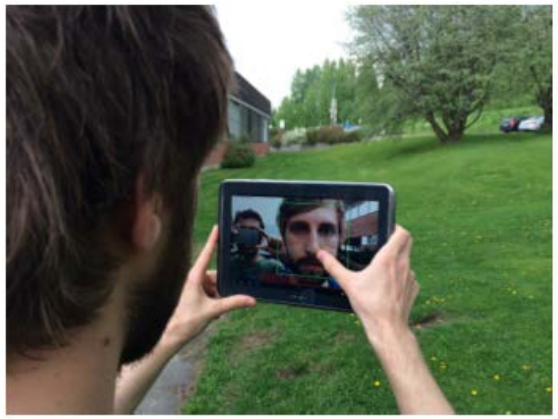
Capture Method and Device	EER from [SC-2012]	EER	FRR (FAR= 0.1%)
Photo, Nexus S	22.3%	1.2%	2.7%
Photo, Galaxy Nexus	19.1%	3.1%	6.7%
Video, Galaxy Nexus	-	3.0%	12.1%

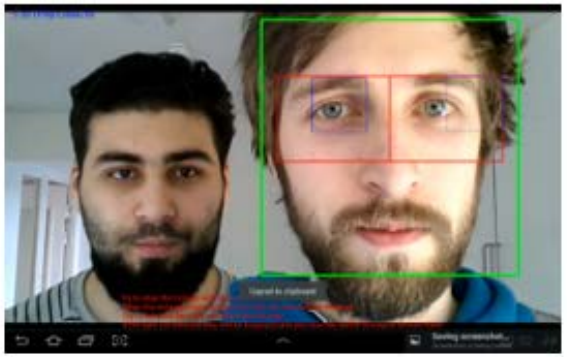
[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Biometric Eye Recognition

Images captured with either front or back camera

- Challenges
  - face and eye localization





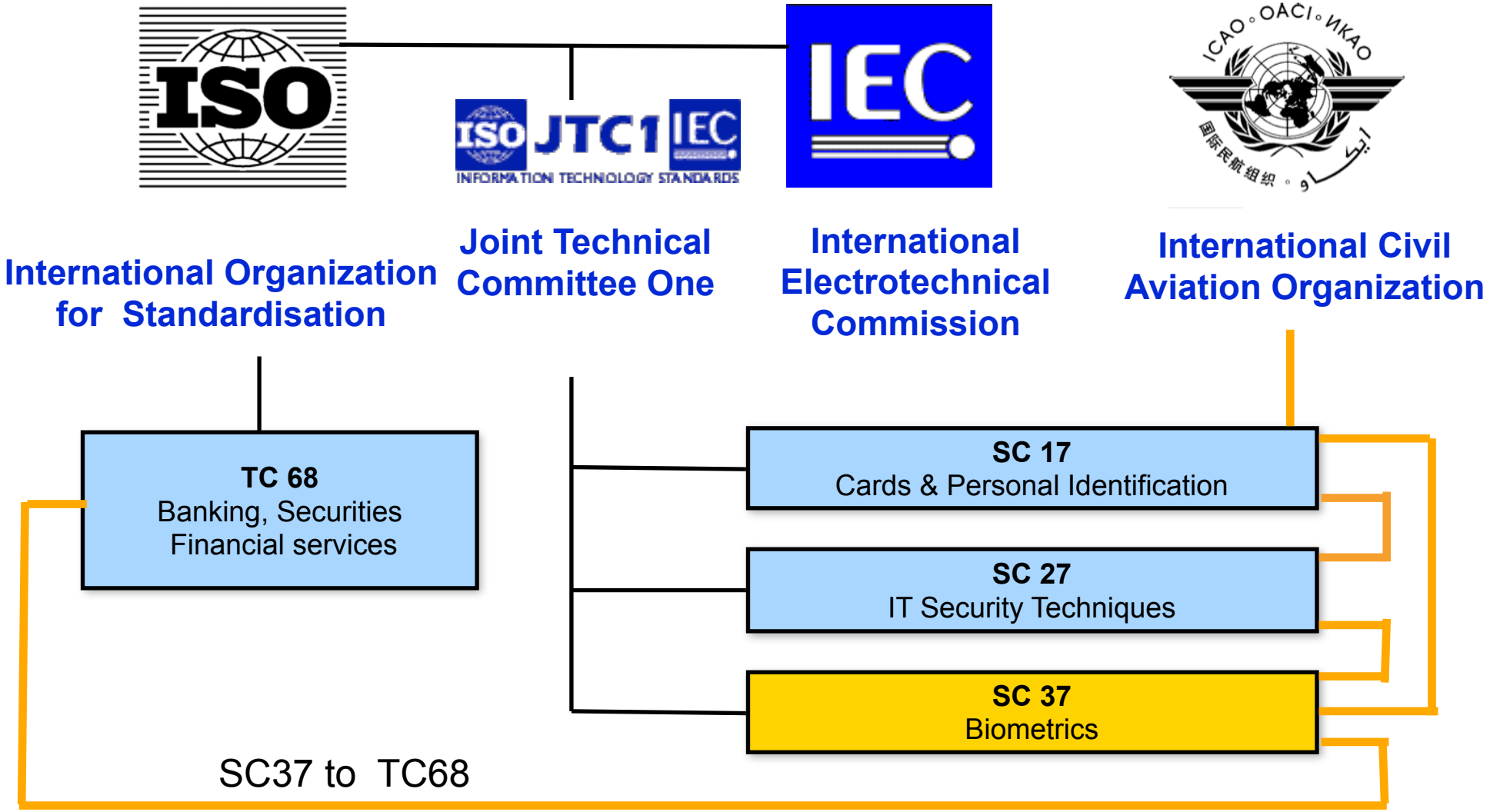
[RRSB14] K. Raja, R. Raghavendra, Martin Stokkenes, Christoph Busch: „Smartphone Authentication System Using Periocular Biometrics“, (BIOSIG 2014)

Standards ?

Operators may think:

„*There are no standards on biometrics*“

Biometric Standardisation



ISO/IEC SC37 Biometrics

Established by JTC 1 in June 2002 to ensure

- a high-priority, focused and comprehensive approach worldwide for the rapid development of formal generic biometric standards

Scope of SC37

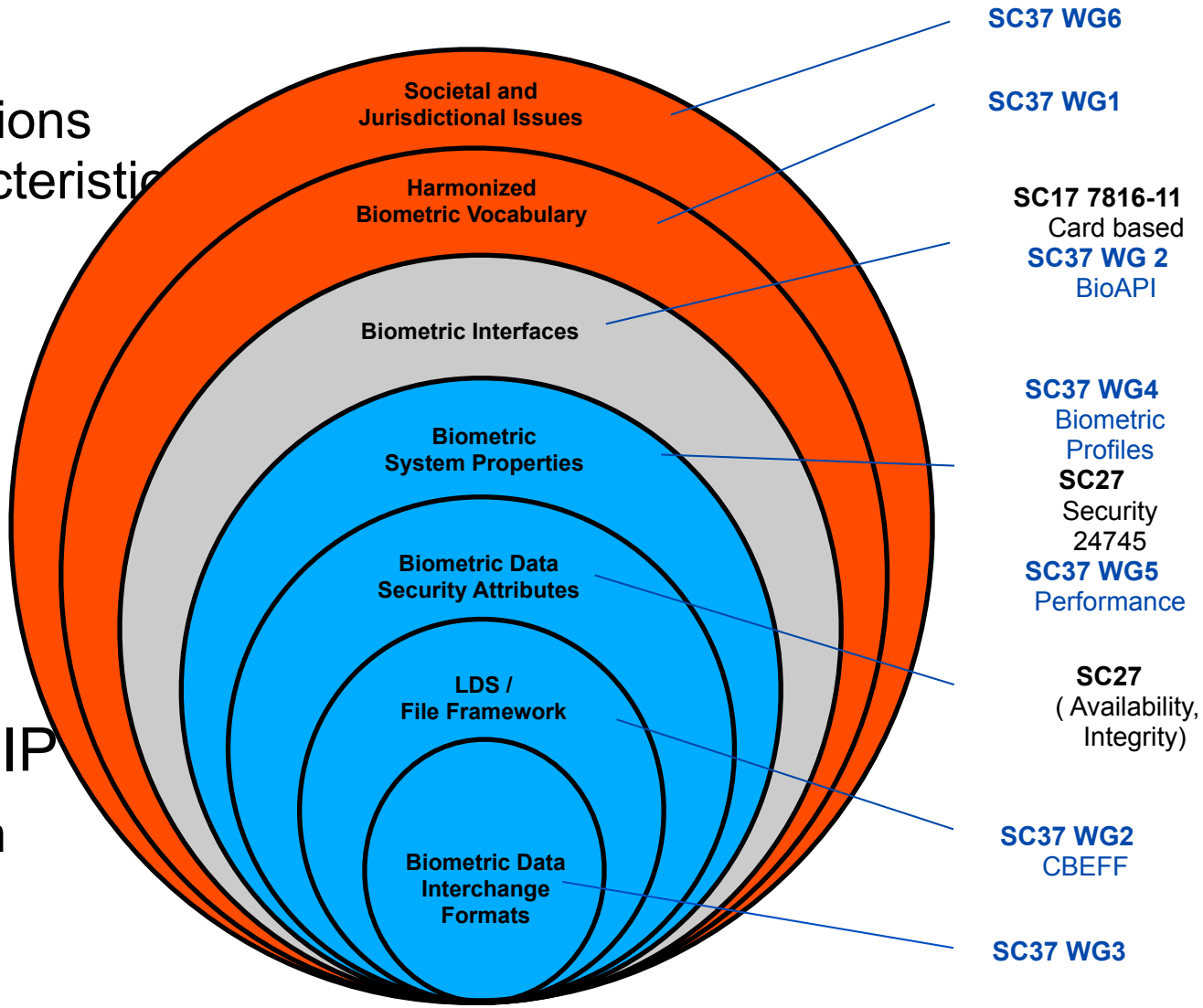
- *"Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects"*
- http://www.jtc1.org

Next meeting: January, 2016
http://www.biometrics-center.ch/jtc1-sc37-martigny2015

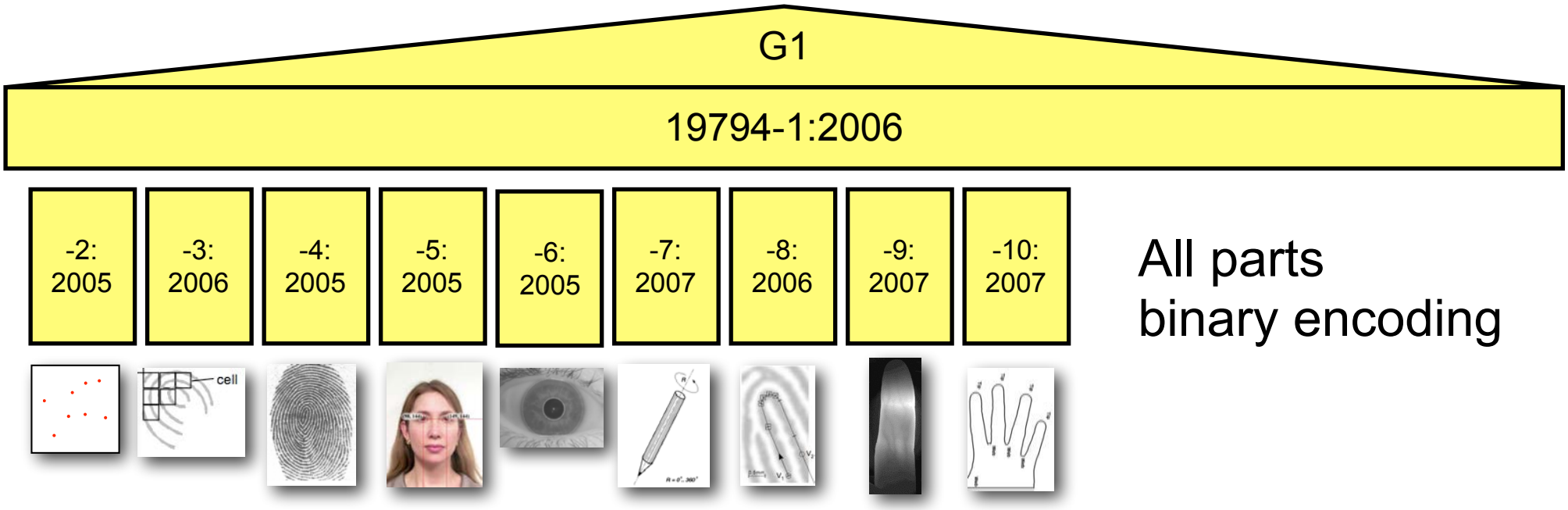
Biometric Standardisation

Onion Layers

- Layer 1: BDIR
  - Digital representations of biometric characteristic
- Layer 2: LDS
  - CBEFF Meta-data
- Layer 3+4: System properties
  - Security
  - Performance
- Layer 5: BioAPI, BIP
  - System Integration



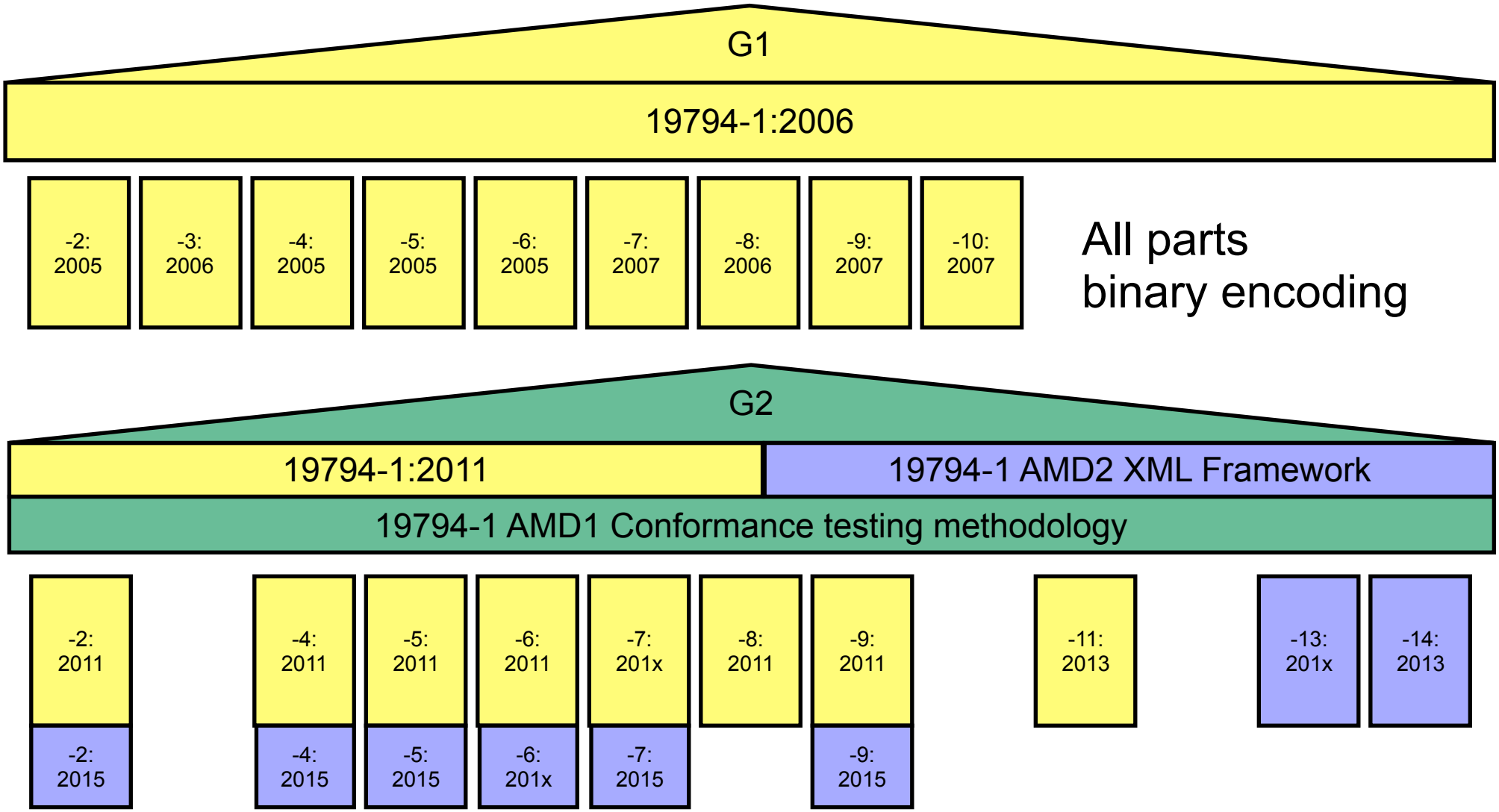
ISO/IEC Interchange Format Standards



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

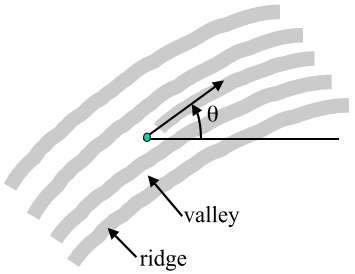
For SmartCards: Finger minutiae data

ISO/IEC 19794-2:2011

- Ridges and valleys, core and delta
- Ridge bifurcation and ridge endings
  - finger minutiae
- Encoded information
  - Minutia point (coordinates x,y)
  - Minutia direction (angle θ)
- How many finger minutiae, and how many ridges between each pair of them?
- A very mature technology

latent print

Source: ISO/IEC 19794-4



Biometric Quality Standards

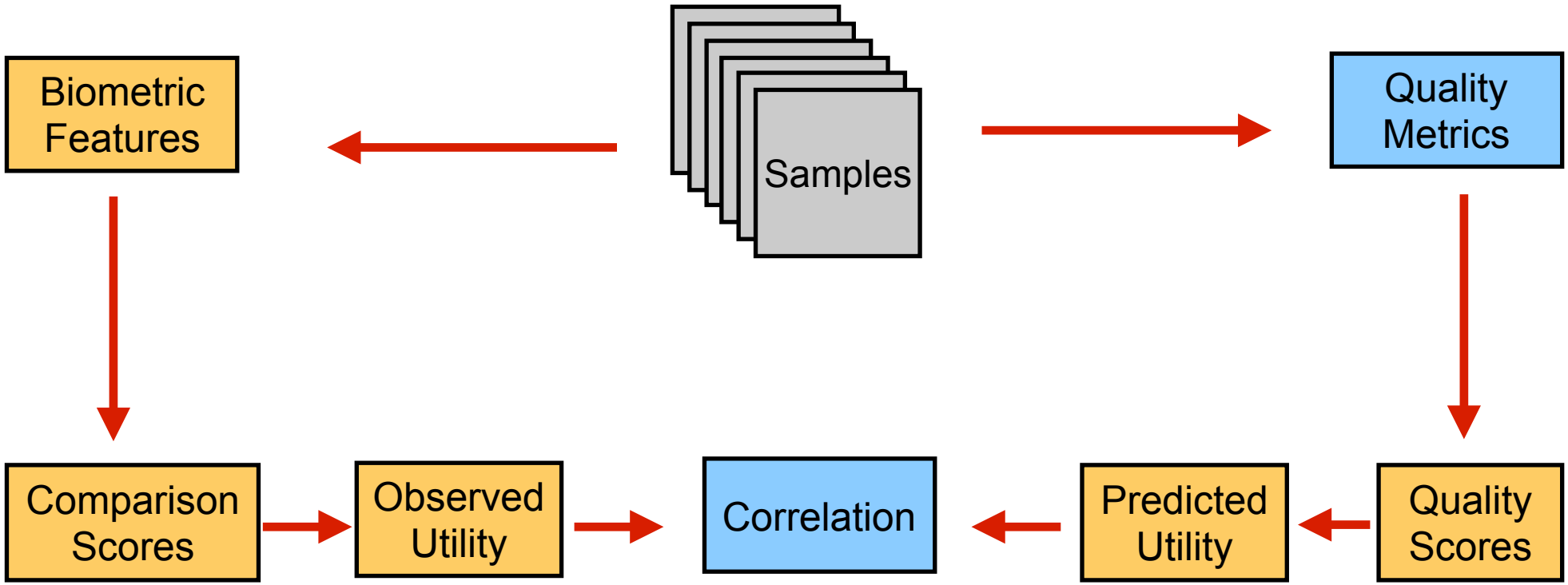
- ISO/IEC 29794-1 Biometric Sample Quality - Part 1: Framework
  - Data Structure of the Quality Block

Quality Block	Quality Score	1 byte	[0,100] 255	0: lowest 100: highest 255: failed attempt to assign a quality score
	Quality Algorithm Vendor ID	2 bytes	[1,65535]	Quality Algorithm Vendor ID shall be registered with IBIA as a CBEFF biometric organization. Refer to CBEFF vendor ID registry procedures in ISO/IEC 19785-2.
	Quality Algorithm ID	2 bytes	[1,65535]	Quality Algorithm ID may be optionally registered with IBIA as a CBEFF Product Code. Refer to CBEFF product registry

  - Quality metrics shall predict recognition accuracy !
    "The correlation between predicted utility and observed utility of each sample is indicative of the effectiveness of the quality algorithm "

Quality Measures vs. Recognition Accuracy

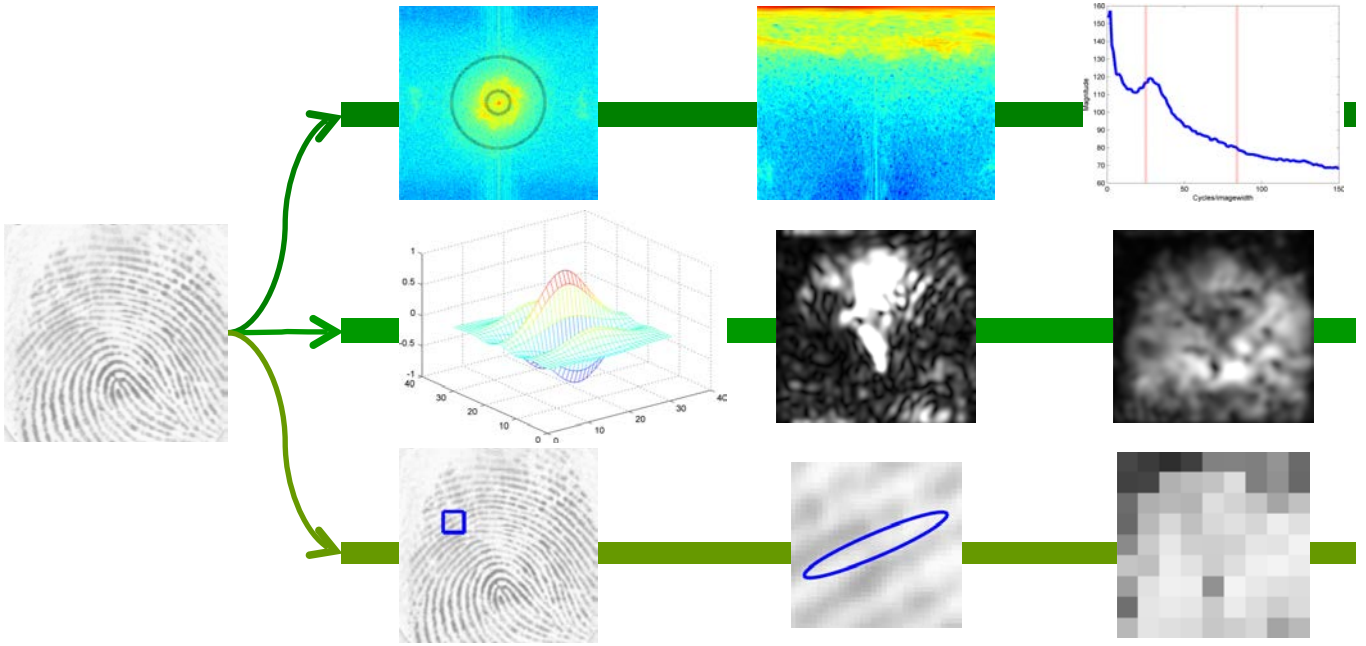
- ISO/IEC 29794-1 Biometric Sample Quality - Part 1: Framework
  - Quality metrics shall predict recognition accuracy (utility)



NFIQ2.0 Features

Investigated Features (Local Metrics and Global Metrics)

- NFIQ 1.0 features (from 2004)
- NFIQ 2.0 will be the bases for revision of ISO/IEC 29794-4:2009
- Open source



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

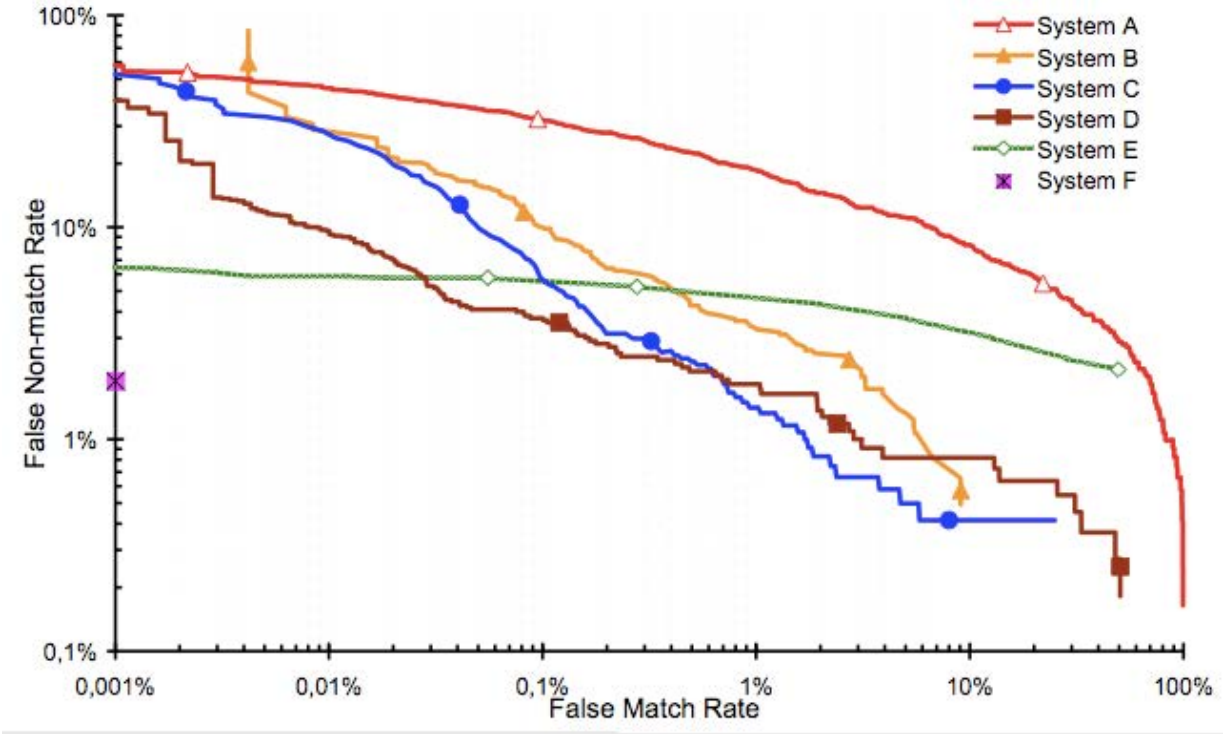
Categorization in ISO/IEC 19795-1

- 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

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)



Security ?

Operators will think:

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

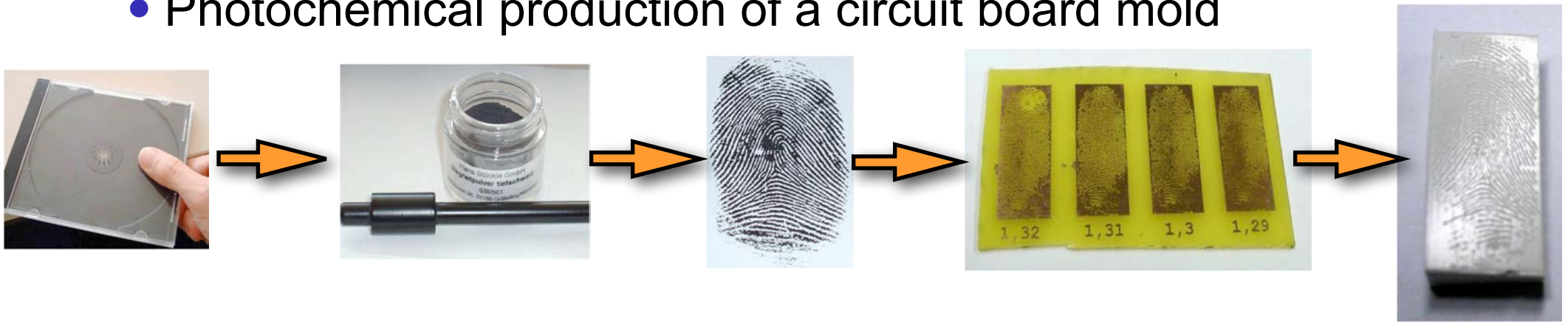
Security ?

- Presentation Attacks

Gummy Finger Production in 2000 !

Attack without support of an enroled individual

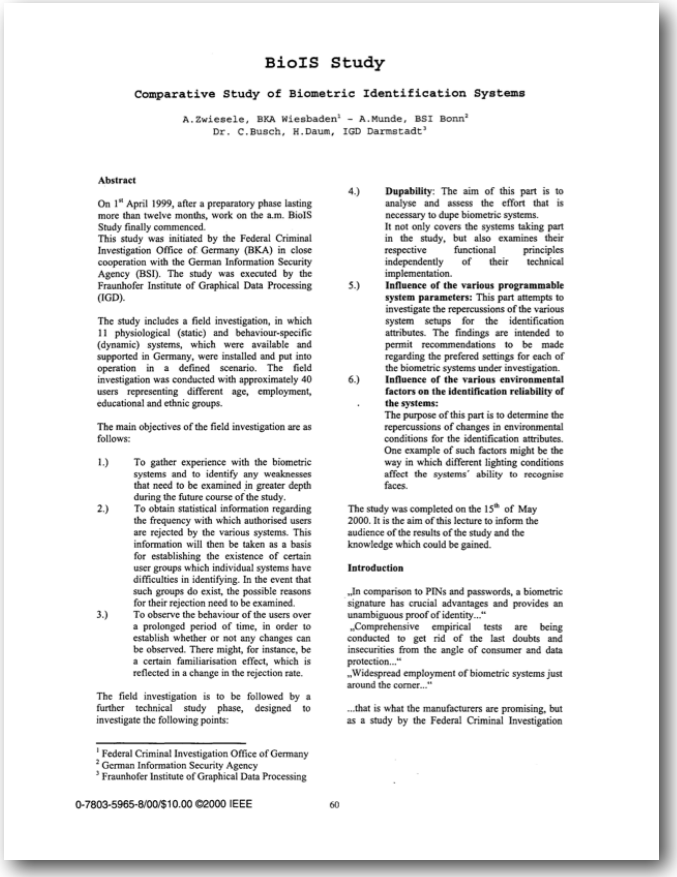
- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production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



Gummy Finger Production in 2000 !

Reported in a publication by the German Federal Police

- 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

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 30107-1
Examples of Artificial and Human Attack Presentation

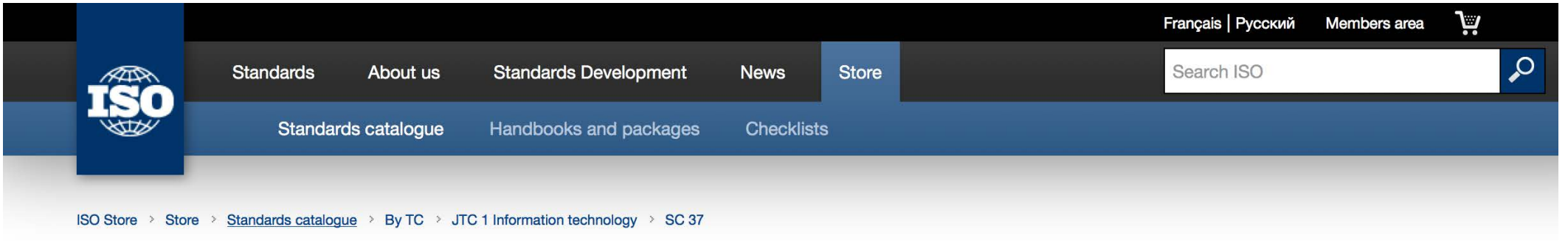
Artificial	*Complete*	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up
Human	*Lifeless*	cadaver part, severed finger/hand
	Altered	mutilation, surgical switching of fingerprints between hands and/or toes
	Non-Conformant	facial expression/extreme, tip or side of finger
	Coerced[1]	unconscious, under duress
	Conformant	zero effort impostor attempt

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

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

Smartphone Access Control

Finger recognition study - 2012/2013

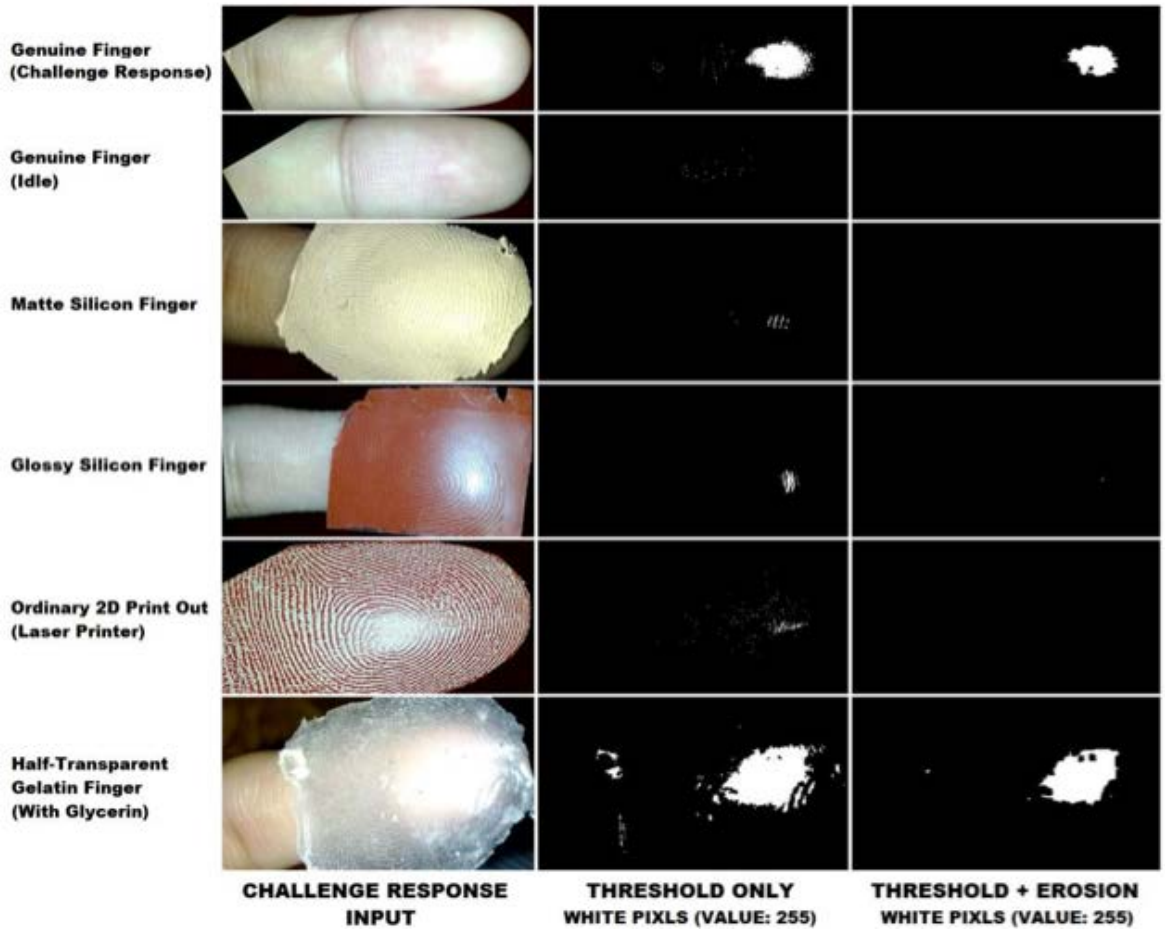
- Observation
  - significant strong light reflection near the fingertip
  - from the cameras LED
- Reflection depends on
  - Shape of the finger
  - Consistency of the finger
  - Angle of the finger to the camera
- Attack detection, as light reflection differs from artefacts to genuine fingers

[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Smartphone Access Control - with PAD

Finger recognition study - 2012/2013

- Results: Presentation Attack Detection (PAD)



- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Smartphone 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

Smartphone Access Control - with PAD

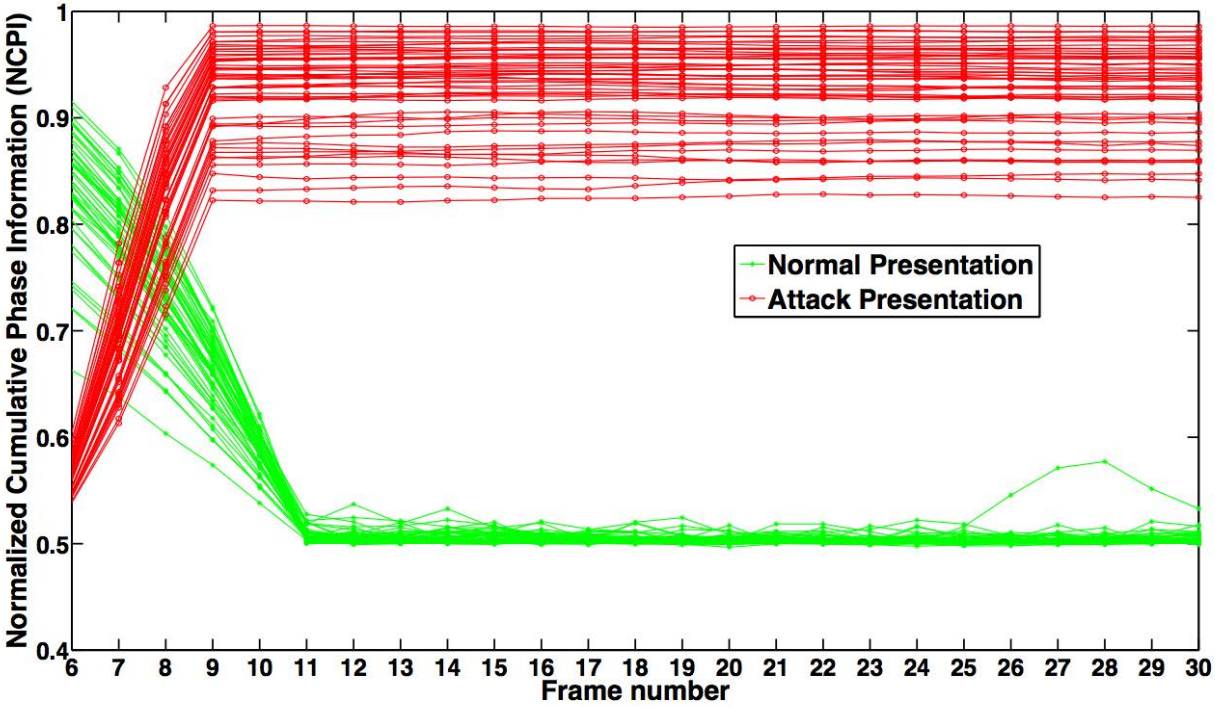
Method based on Eulerian Video Magnification (EVM)

[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)

Smartphone Access Control - with PAD

Eye recognition study - 2015

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

Privacy Protection ?

Operators will think:

„Biometric systems must be compliant to data privacy and data protection 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

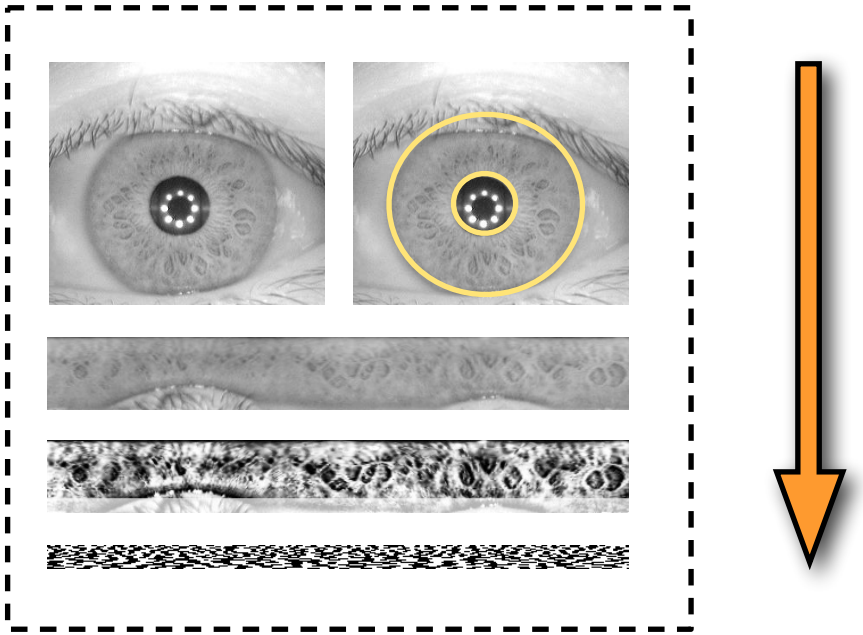
  [RaBBB2013] C. Rathgeb, F. Breitinger, C. Busch, H. Baier: "On the Application of Bloom Filters to Iris Biometrics", in IET Journal on Biometrics 3(1), (2014) http://www.christoph-busch.de/files/Rathgeb-BloomFilter-IET-2014.pdf

Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers
- Successfully applied to iris, face, fingerprint and fingervein

- Example: Iris Segmentation



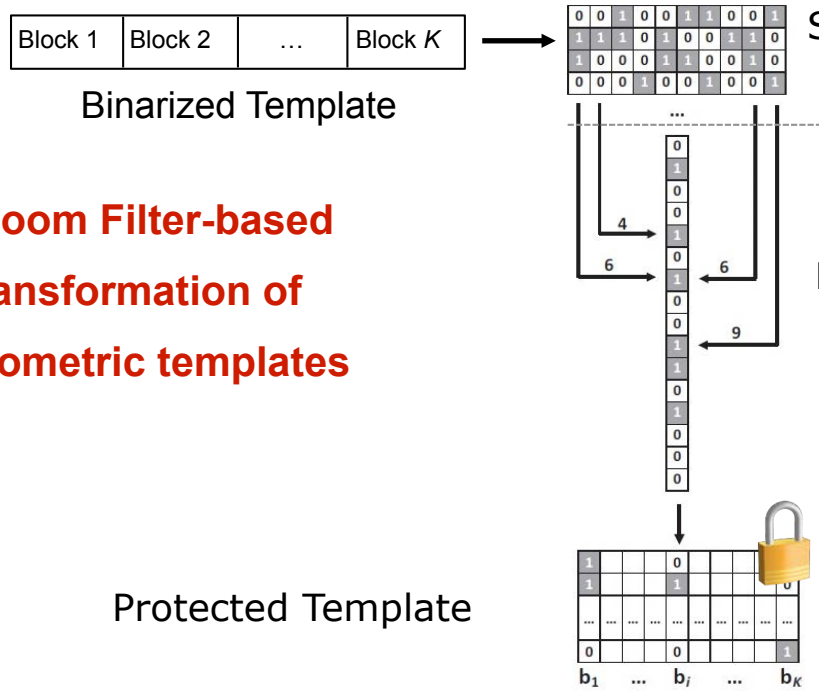
- Normalized Iris Texture
- Iris Feature Vector
- Binarised Iris Feature Vector

[Ra2014] 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

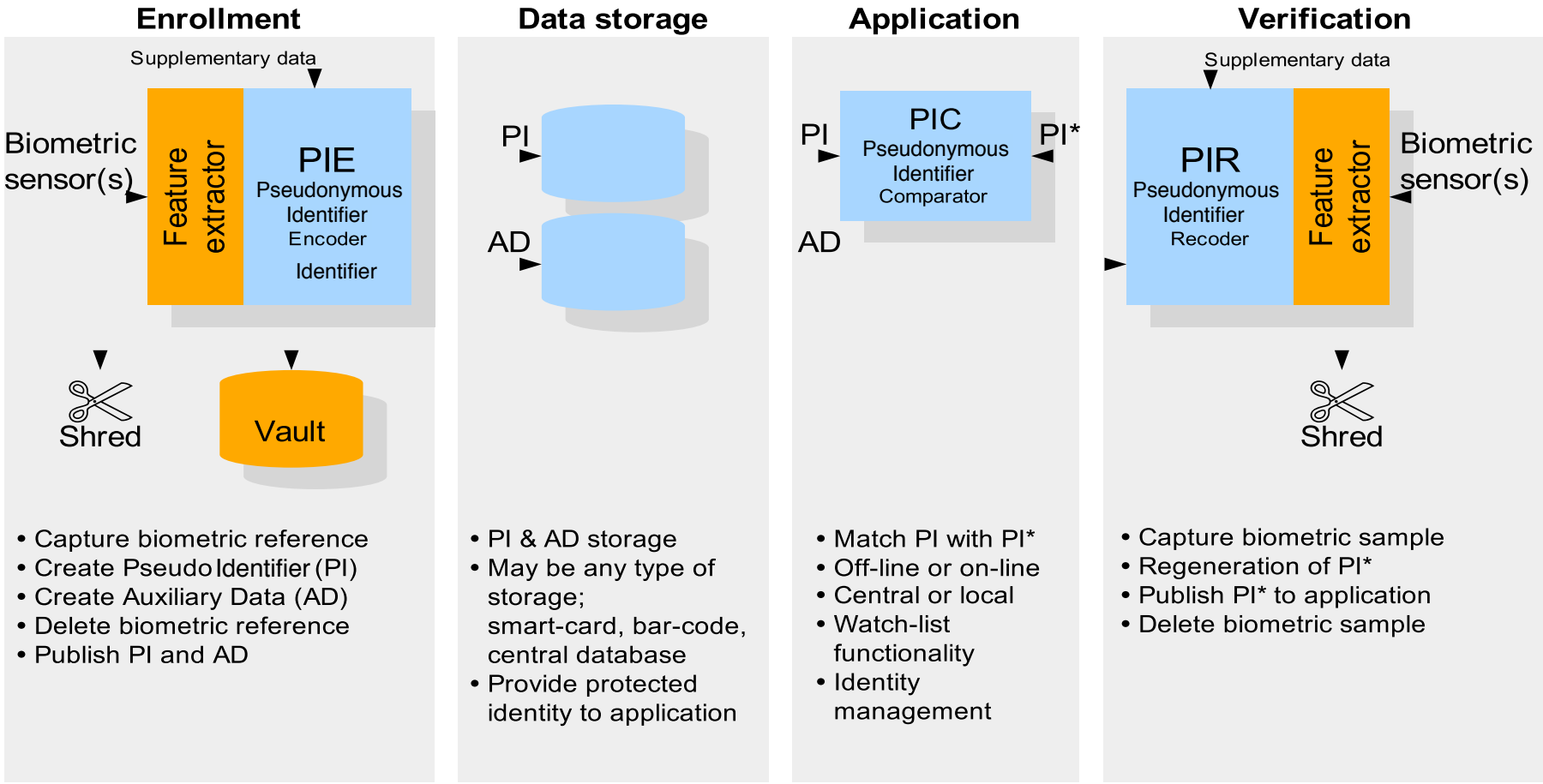
- Secrecy
- Non-invertibility
- Diversification
- Noise robustness

Biometric Template Protection enables revocability in biometric systems!

Data Protection Requirements

Technical framework on how to implement requirements for data privacy and data protection

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



Your Operator Reality Check

Operators should ask the vendors

- Is there a vendor lock-in due to proprietary sensors?

I want the biometric capture device to be operated via BioAPI interface according ISO/IEC 19784!

- 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 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

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

Biometric system should be

- based on international ISO/IEC standards
- privacy friendly and not store plain biometric data on central servers

References

Further information on Biometric Standardization

- on ISO/IEC SC37
  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on
- on SC37 working group 3
  http://www.christoph-busch.de/standards-sc37wg3.html
- Next meeting: January, 2016
  http://www.biometrics-center.ch/jtc1-sc37-martigny2015

Contact

Contact: