Biometrics and Banking

Christoph Busch

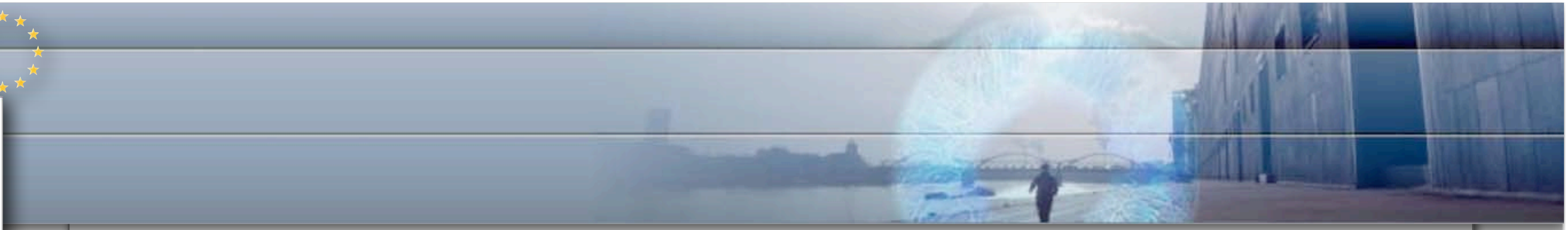
Hochschule Darmstadt / European Association for Biometrics
http://www.christoph-busch.de

BITKOM Banking & Financial Services
Frankfurt June 24, 2014

Agenda

- European Association for Biometrics
- From Biometric Rumors to Reality
- Mobile Biometrics
- Mobile Payment Protocol

European Association for Biometrics

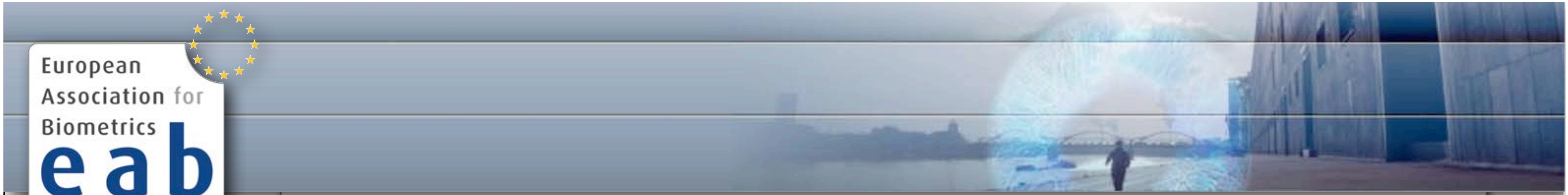


CURRENT STATUS OF THE EAB-ASSOCIATION

- EAB founded on November 17, 2011

- Currently > **140** members
  - Including major biometric vendors and integrators, several government agencies, most acknowledged testing labs and academia
  - Most members are European institution but also U.S. or JP based
  - Key players from 10 years of European projects: BioVision, BioSecure, BITE, Crescendo, Staccato, 3DFace, HIDE, RISE, BioTesting, MTIT, Mobio, 3D Face, TURBINE, FIDELITY, BEAT, TABULA RASA etc.

- Informative and dynamic website
- European Research and Industry Award (10 September 2014)
- European Biometrics Symposium
- Workshops in cooperation with other associations and interest groups
- Network of national contact points (currently 26) and fora

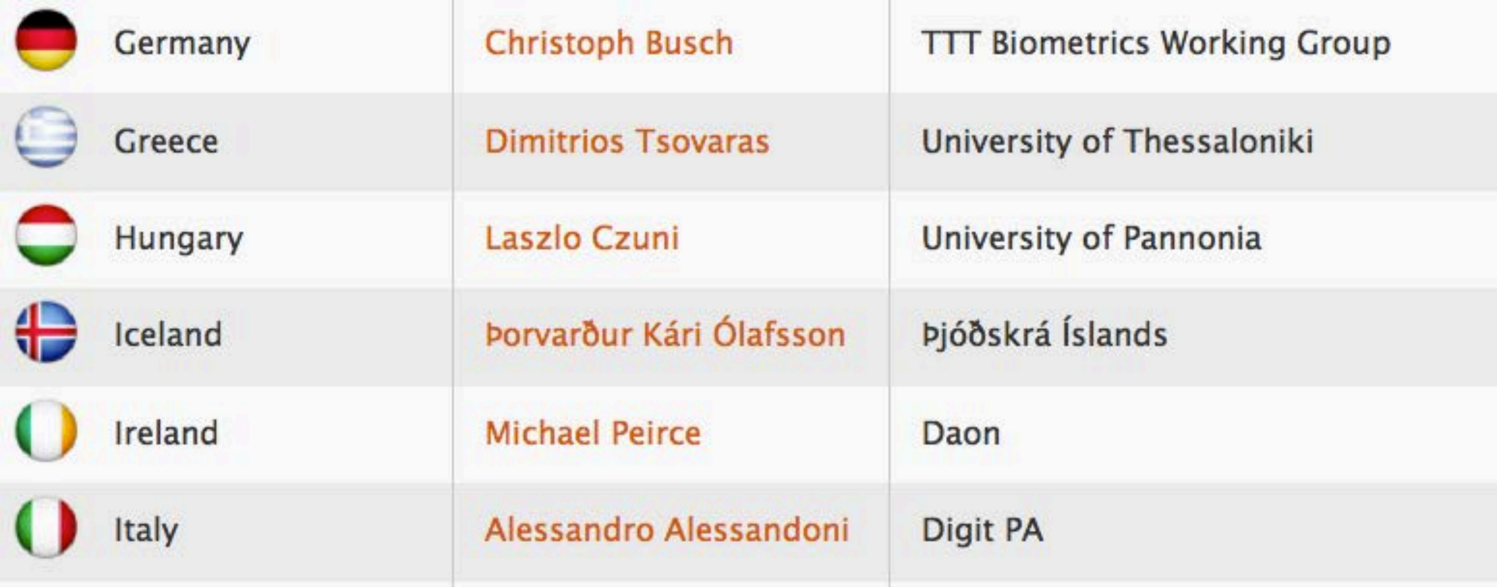


CURRENT STATUS OF THE EAB-ASSOCIATION

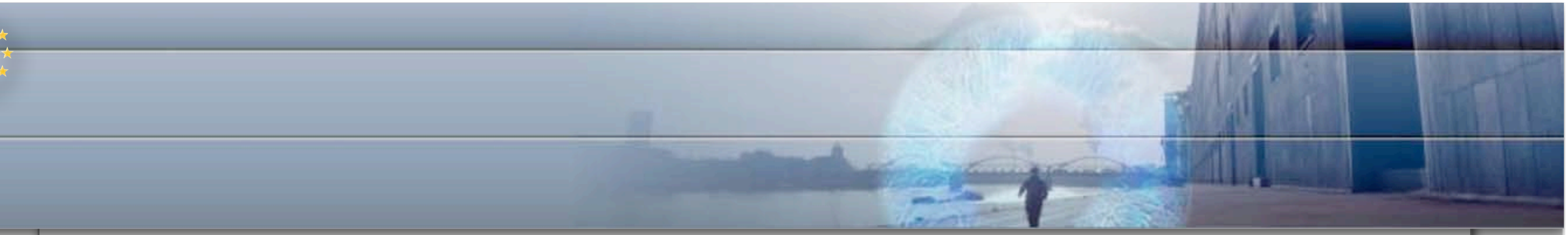
- National Contact Points - see the full list at:

  http://eab.org/information/national_contact_points.html

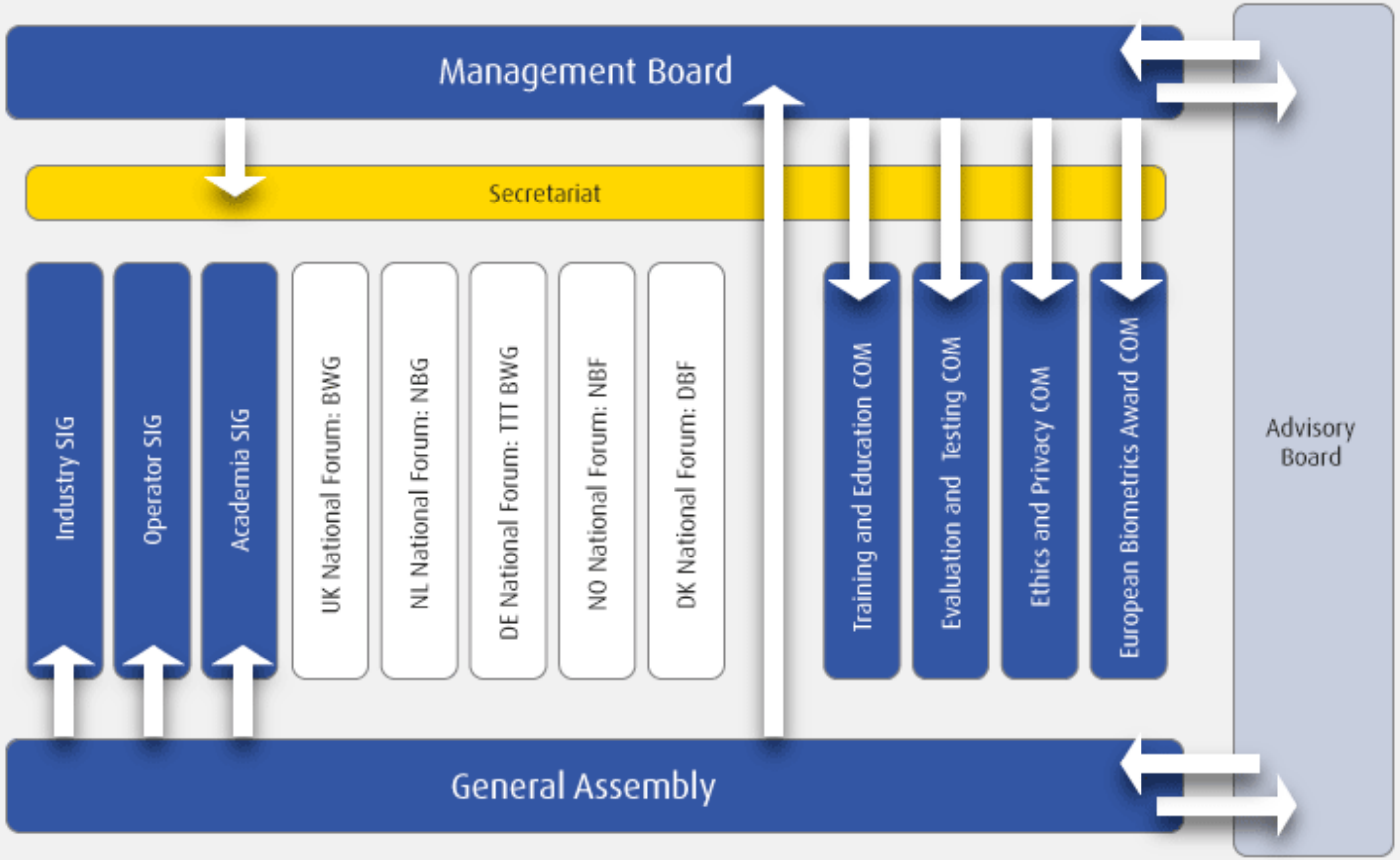
  exsample sub-set of the contacts:



Germany	Christoph Busch	TTT Biometrics Working Group
Greece	Dimitrios Tsovaras	University of Thessaloniki
Hungary	Laszlo Czuni	University of Pannonia
Iceland	Þorvarður Kári Ólafsson	Þjóðskrá Íslands
Ireland	Michael Peirce	Daon
Italy	Alessandro Alessandoni	Digit PA



Organisational Structure



Management Board

Secretariat

Industry SIG

Operator SIG

Academia SIG

UK National Forum: BWG

NL National Forum: NBG

DE National Forum: TTT BWG

NO National Forum: NBF

DK National Forum: DBF

Training and Education COM

Evaluation and Testing COM

Ethics and Privacy COM

European Biometrics Award COM

Advisory Board

General Assembly

COOPERATION AND PARTNERSHIP

- Asian Biometric Consortium (ABC)
- TeleTrusT Association (TTT)
- BioSecure Association
- EUROSMART
- WORLD e-ID
- Biometrics London
- SDW 2014
- ID World
- Biometrics Institute
- BEAT
- IEEE Biometrics Council

ABC
ASIAN BIOMETRIC CONSORTIUM

TeleTrusT
Pioneers in IT security.

BIOSECURE

EUROSMART
The Voice of the Smart Security Industry

WORLD e-ID
CONGRESS

biometrics
EXHIBITION AND CONFERENCE 2013

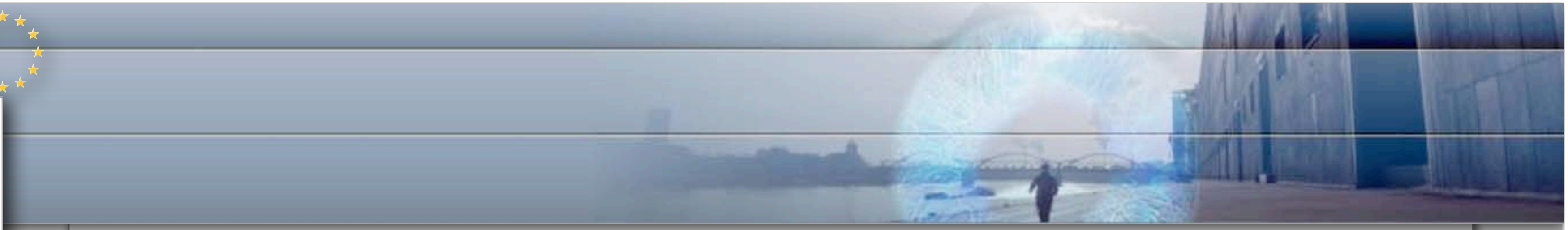
SDW2014

ID WORLD
INTERNATIONAL CONGRESS

BIOMETRICS
INSTITUTE

BEAT

IEEE
Biometrics Council



EAB ADVISORY COUNCIL (EABAC)

- Members
  - 10 members
    - Edgar Beugels (Head of Capacity Building, Frontex)
    - Christer Bergman (Board Member IBIA, USA)
    - Ann Cavoukian (IPC Ontario, Canada)
    - Vincent Boautou (Safran Morpho, France)
    - Krum Garkov (Director, EU-LISA)
    - Waldemar Grudzien (Director German Banking Association)
    - Marek Rejman Greene (UK Home Office)
    - Jason Kim (Director of Korea-National Biometric Test Center)
    - Vijay Madan (UIDAI)
    - Ruth Wandhöfer (Citigroup, European Payment Council - EPC)
    - Jim Wayman (San José University, USA)
- See details at: http://eab.org/about/eabac.html

7TH EUROPEAN BIOMETRICS RESEARCH AND INDUSTRY AWARD 2013

Front (left to right): Tom Kevenaar, Jean-Christophe Fondeur, Peter Wild, Finnian Kelly, Huiibin Li, Patrizio Campisi - Back (left to right): Anil Jain, Christoph Busch, Raymond Veldhuis, Geunther Schumacher, Ajay Kumar, Alexander Nouak

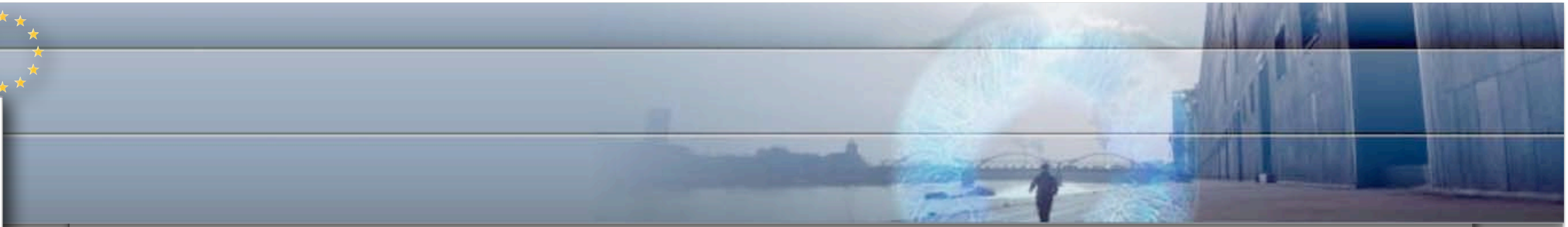
EUROPEAN BIOMETRICS RESEARCH AND INDUSTRY AWARD 2014

SAFRAN
Morpho

- European Biometric Research Award 2014
  - 2.000,00 € honorarium
  - Ph.D. or candidate at European University

SAFRAN
Morpho

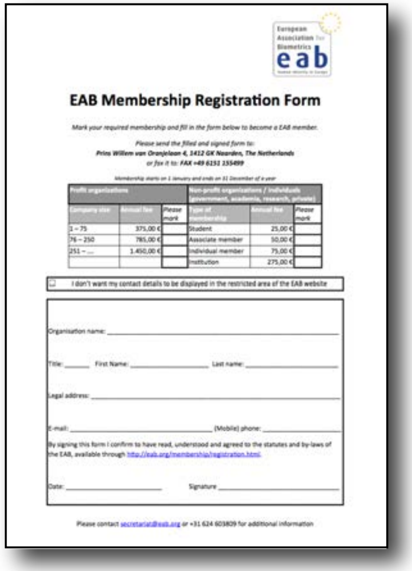
- European Biometric Industry Award 2014
  - 2.000,00 € honorarium
  - Employee of a European company with core business biometrics
- Deadline
  - May 31, 2014
- see more details at: www.eab.org/award/cfp.html



JOIN EAB NOW! - WHY?

- Membership fee is **low**
  - Profit organisation (375 €, 785 €, 1.450 €)
  - Non-profit organisation (government, academia, research, private)

    Student (25 €) , Associate member (50 €), Individual member (75 €) Institution (275 €)
- Membership benefits are **high**
  - For details visit: http://eab.org/membership/benefits.html
- Stay connected to developments in Europe
- Return your application form today



European Association for Biometrics
eab

EAB Membership Registration Form

Mark your required membership and fill in the form below to become a EAB member.

Please send the filled and signed form to:
Prins Willem van Oranjelaan 4, 1412 GK Naarden, The Netherlands
or fax it to: ***FAX +49 6151 155499***

Membership starts on 1 January and ends on 31 December of a year

Profit organizations			Non-profit organizations / individuals (government, academia, research, private)		
Company size	Annual fee	Please mark	Type of membership	Annual fee	Please mark
1 – 75	375,00 €		Student	25,00 €	
76 – 250	785,00 €		Associate member	50,00 €	
251 – ...	1.450,00 €		Individual member	75,00 €	
			Institution	275,00 €	

□ I don't want my contact details to be displayed in the restricted area of the EAB website

Organisation name: ______________________________

Title: ______ First Name: ________________ Last name: ________________

Legal address: ______________________________

E-mail: ________________________ (Mobile) phone: ________________

By signing this form I confirm to have read, understood and agreed to the statutes and by-laws of the EAB, available through http://eab.org/membership/registration.html

Date: ________________ Signature ________________

Please contact secretariat@eab.org or +31 624 603809 for additional information

Answers on Biometric Rumors

Security ?

Operators may think:

„Biometrics are not as secure as PINs“

Benchmark of Biometrics and PIN

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

- Tragedy of the commons

http://en.wikipedia.org/wiki/Tragedy_of_the_commons

- 1.) PINs are exploiting (brains) commons
  - the concept works well, when we have to manage only a few passwords but in reality we are expected to remember more than 100 passwords and we fail to do so

Comparison of Biometrics and PIN (cont.)

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

- 2.) 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 dfferent biometric characteristics is
    - Fingerprints 84bit [Ratha2001]
    - Iris 249bits [Daugman2006]
    - Face 56bit [Adler2006]

[Bu2014] N. Buchmann, C. Rathgeb, H. Baier, C. Busch: Towards electronic identification and trusted services for biometric authenticated transactions in the Single Euro Payments Area, in Proceedings of the 2nd Annual Privacy Forum (APF'14), 2014

Comparison of Biometrics and PIN (cont.)

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

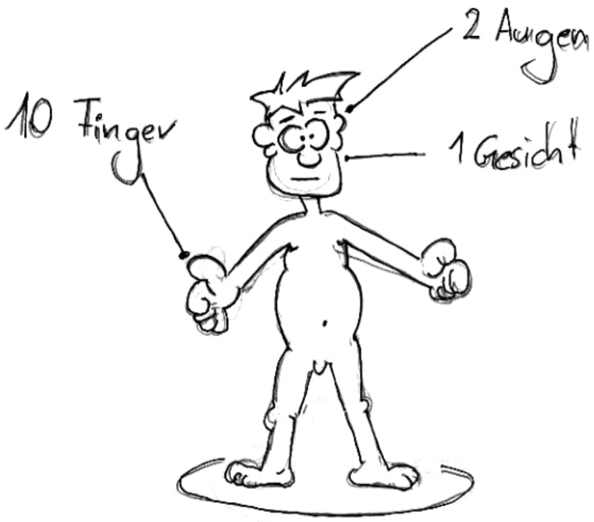
- 3.) PINs can be delegated in violation of the security policy
  - *„This transaction was done by Mr. Popov, who was mis-using my card*“
  - biometric authentication enables non-repudiation of transactions

Biometrics are better than PINs !

Revocability ?

Data subjects may think:

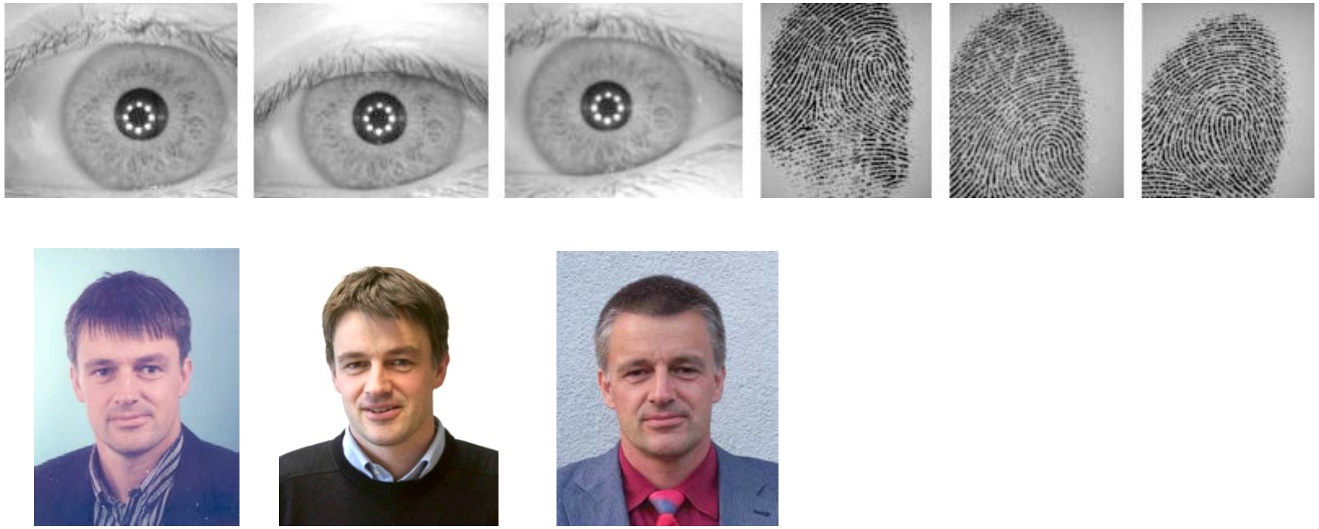
„The number of biometric characteristics is limited (e.g. we have only 10 fingers) - we can not revoke the biometric reference“



Variation of Biometric Measurement ?

Operators may think:

„There is a strong variance in biometric measurements“



Biometric Template Protection

We do NOT store fingerpint, iris or face images

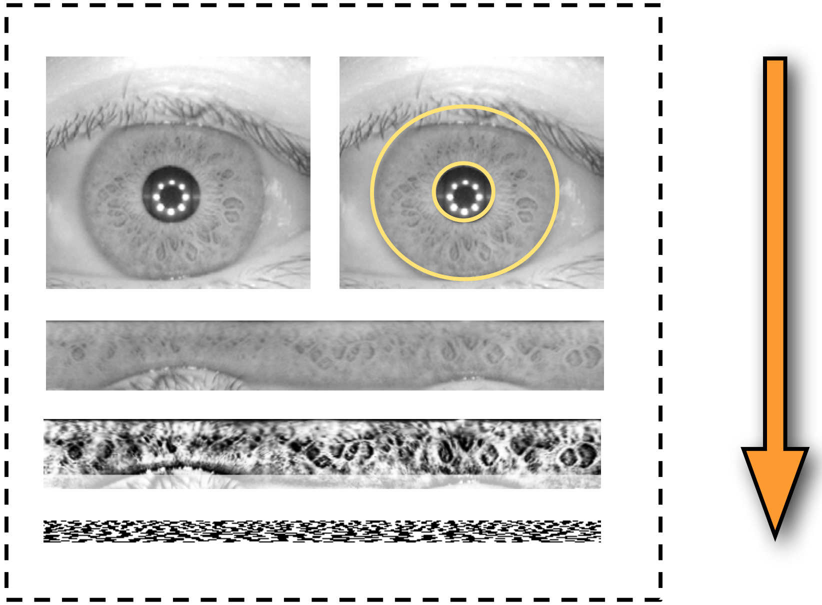
- we transform templates to pseudonymous identifiers (PI)
- we reach
  - Secrecy: biometric references (PI) can be compared without decryption.
  - Diversifiability / Unlinkability: Unique pseudonymous identifier can be created for each application to prevent database cross-comparison
  - Renewability: we can revoke and renew template data.
  - Noise-robustness: Stored information can be used for authentication with noisy biometric samples
  - 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

Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers
- Example: Iris Recognition



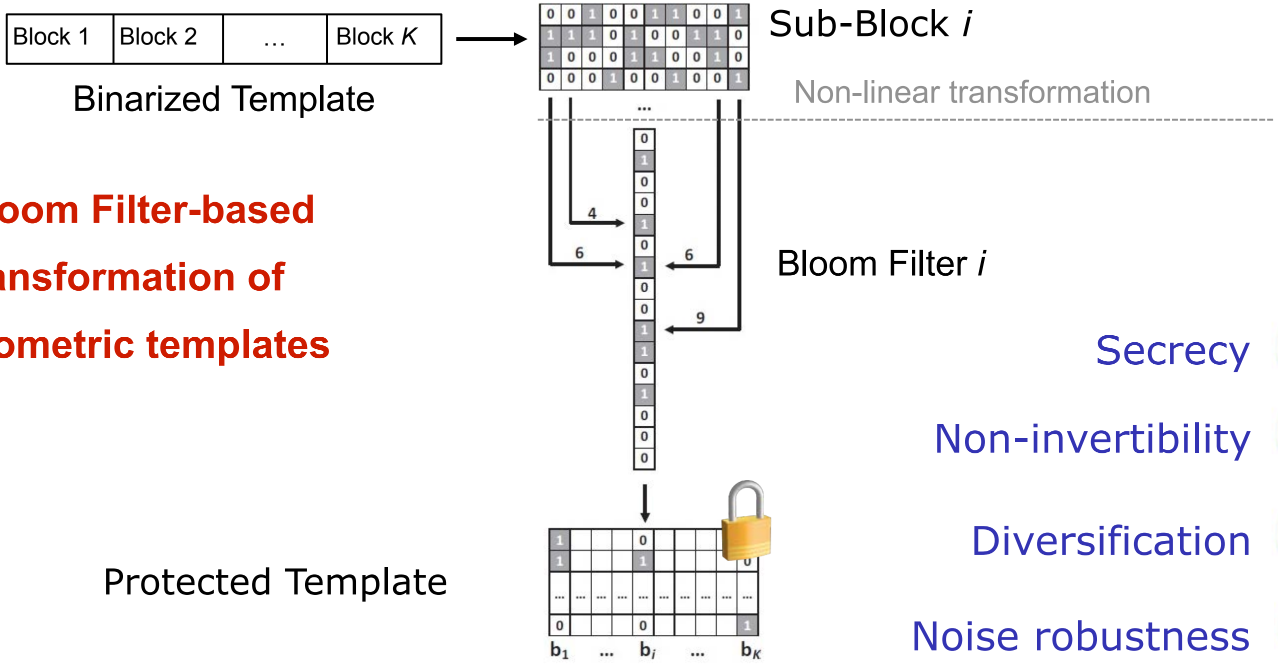
- Iris Segmentation
- Normalized Iris Texture
- Iris Feature Vector
- Binarized Iris Feature Vector

[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 Privacy and Data Protection ?

Operators may think:

„*Biometric systems are not compliant to data privacy principles*“

Data Protection Requirements

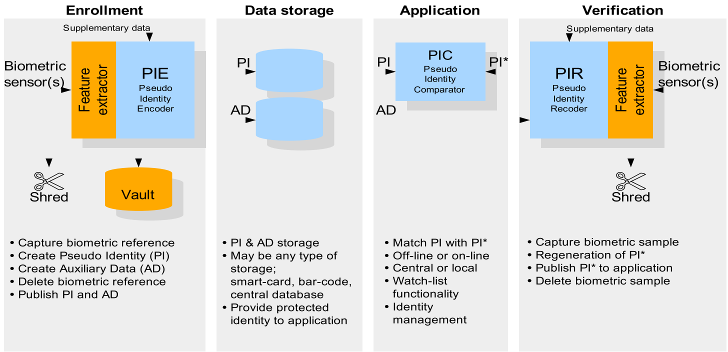
Requirements for data privacy and data protection are formulated in:

- 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

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



Enrollment
- Capture biometric reference
- Create Pseudo Identity (PI)
- Create Auxiliary Data (AD)
- Delete biometric reference
- Publish PI and AD

Data storage
- PI & AD storage
- May be any type of storage; smart-card, bar-code, central database
- Provide protected identity to application

Application
- Match PI with PI*
- Off-line or on-line
- Central or local
- Watch-list functionality
- Identity management

Verification
- Capture biometric sample
- Regeneration of PI*
- Publish PI* to application
- Delete biometric sample

ISO/IEC 24745
Biometric Information Protection !

Bio-Hacking ?

Operators may think:

„Biometric sensors can not detect gummy and cut-off fingers“

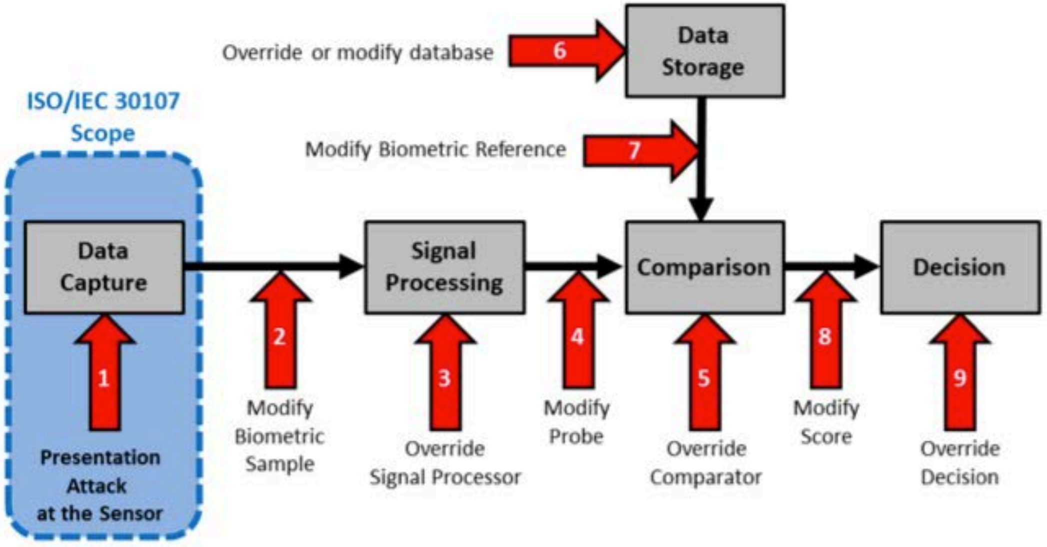
Presentation Attack Detection

Attacks on capture devices

- ISO/IEC 30107 Presentation Attack Detection
  - aka spoof detection

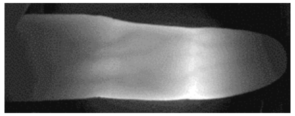
silicon finger

Half-transparent gelatin with glycerin

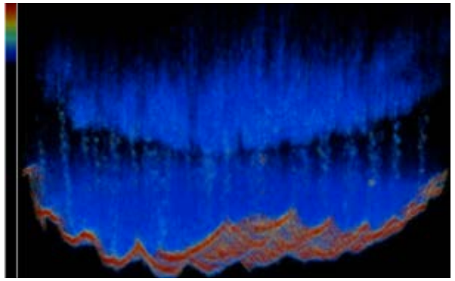


Countermeasure

- Vein recognition



- Fingerprint Recognition with Optical Coherence Tomography (OCT)

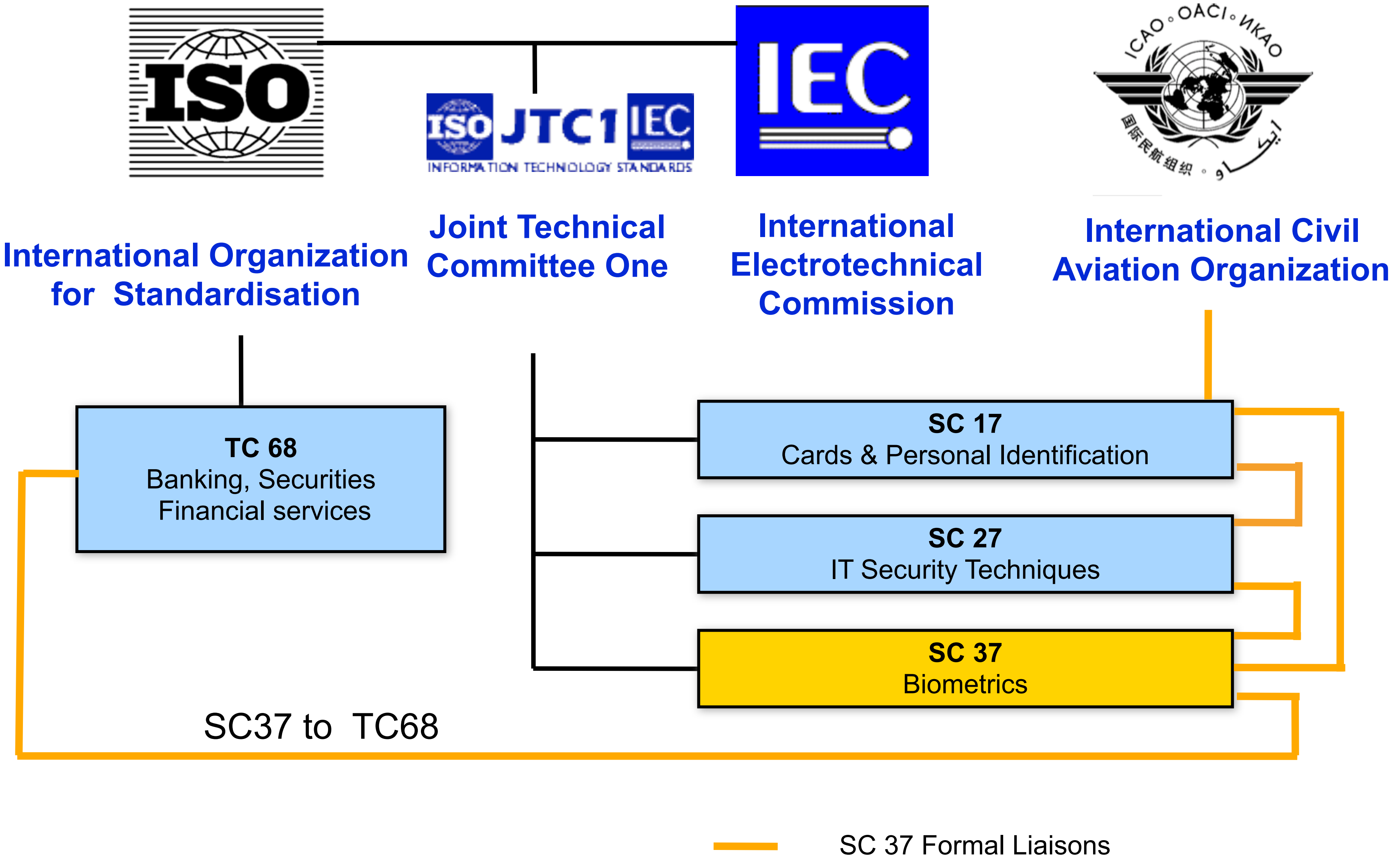


Standards ?

Operators may think:

„There are no standards on biometrics“

Biometric Standardisation



International Organization for Standardisation

Joint Technical Committee One

International Electrotechnical Commission

International Civil Aviation Organization

TC 68
Banking, Securities
Financial services

SC 17
Cards & Personal Identification

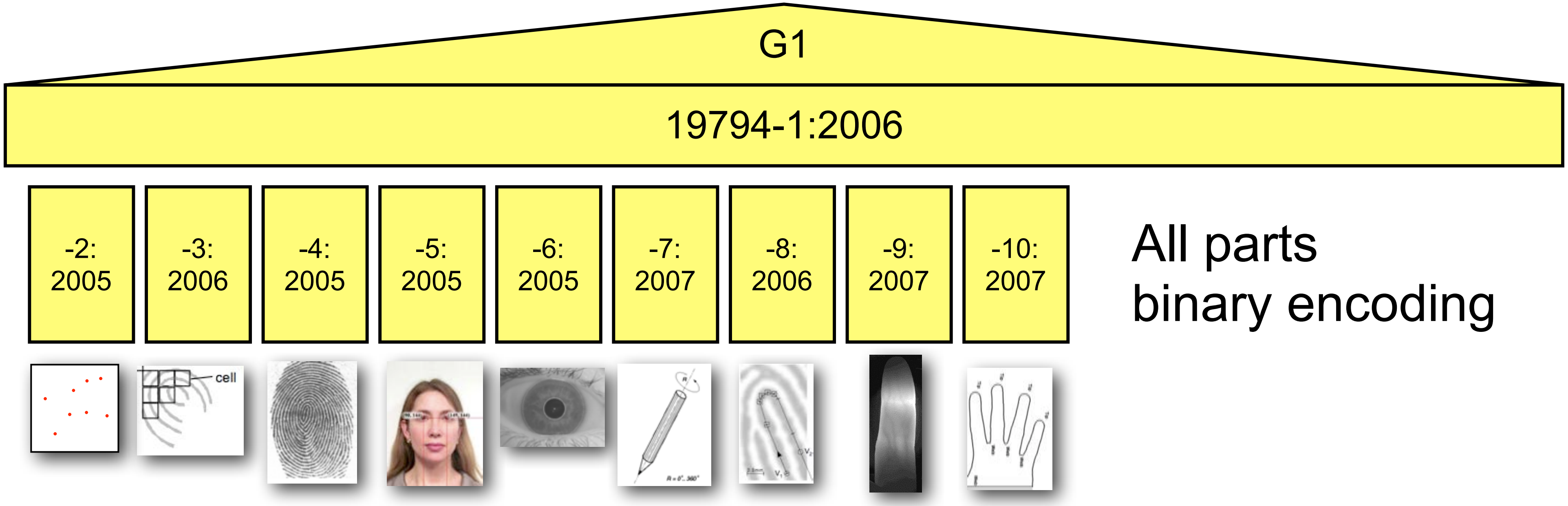
SC 27
IT Security Techniques

SC 37
Biometrics

SC37 to TC68

SC 37 Formal Liaisons

ISO/IEC Interchange Format Standards



G1

19794-1:2006

-2: 2005

-3: 2006

-4: 2005

-5: 2005

-6: 2005

-7: 2007

-8: 2006

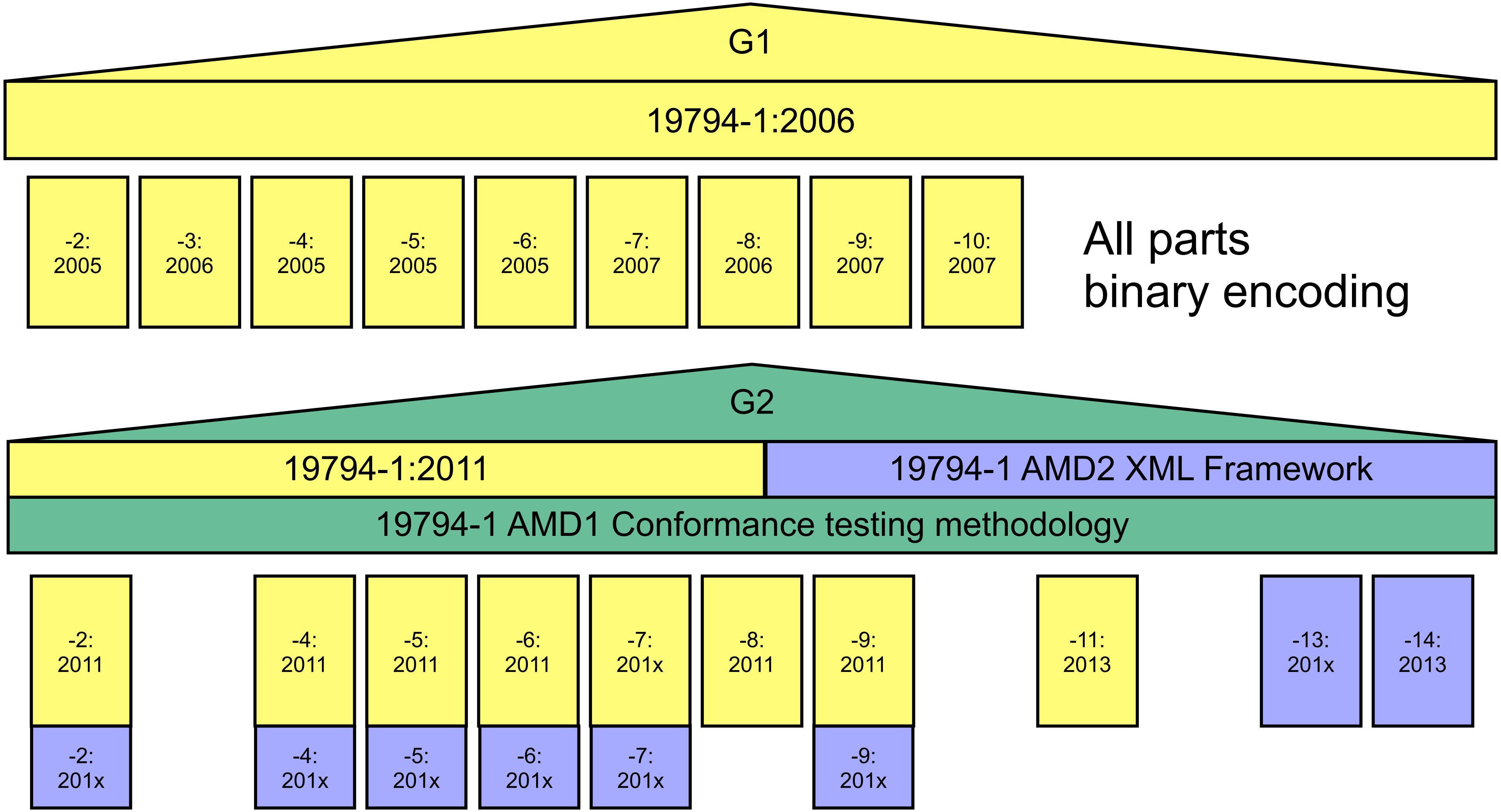
-9: 2007

-10: 2007

All parts
binary encoding

The 19794-Family: Biometric data interchange formats

Generation 2 of ISO/IEC 19794

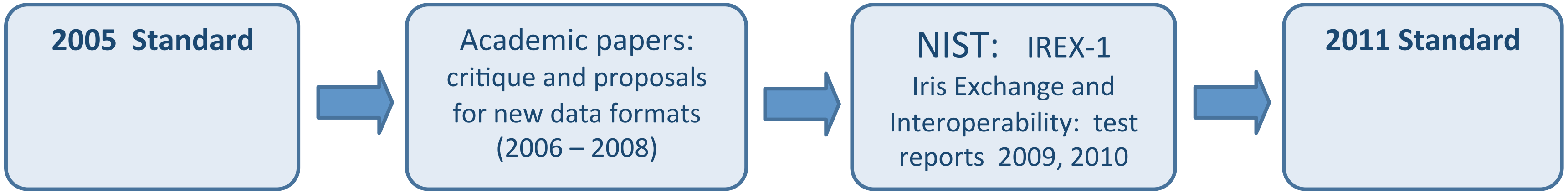


All parts
binary encoding

the semantic (i.e. general header / structure of representation header) equivalent for binary encoded and XML encoded parts in G2

Part 6: Iris image data

ISO/IEC 19794-6:2011



2005 Standard

Academic papers: critique and proposals for new data formats (2006 – 2008)

NIST: IREX-1
Iris Exchange and Interoperability: test reports 2009, 2010

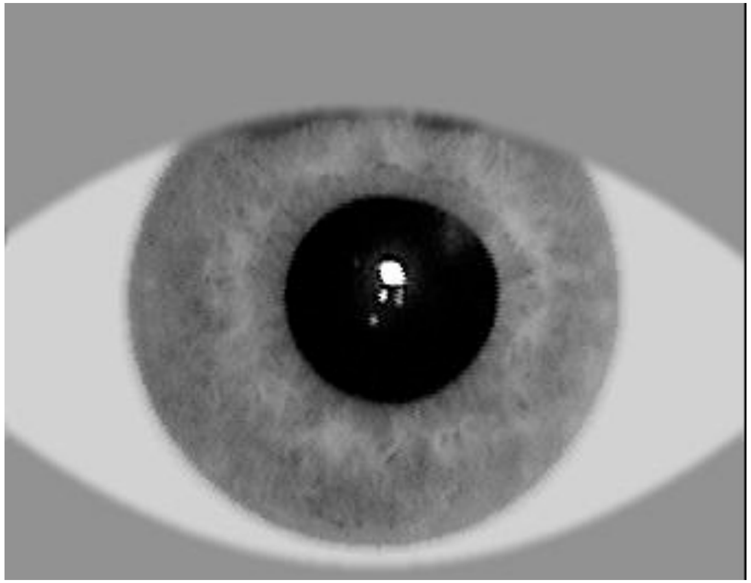
2011 Standard

- 4 new iris image formats, compressible to as little as 2,000 bytes
- Iris formats are now highly empirically based, thanks to NIST IREX testing results
- Recommended target record sizes for different applications
- Recommended compression for different applications
- Formats differ in their required amount of image pre-processing
- Original 19794-6:2005 raw image format retained as one case
- Iris sample quality (29794-6) will become normative Annex

Part 6: Iris image data

One new data format in 19794-6:2011

- highly compact iris image, compressed to 2,000 bytes



Source: ISO/IEC 19794-6

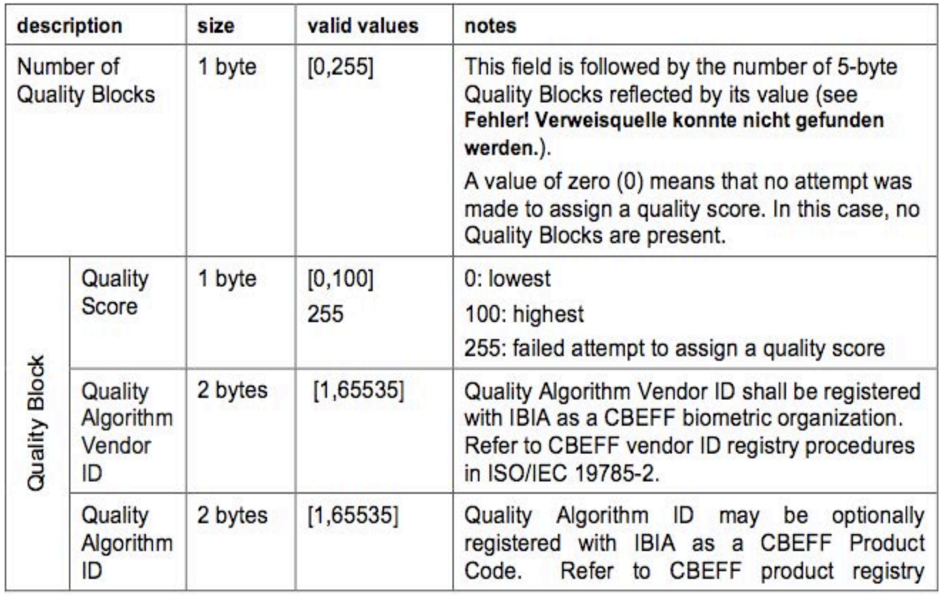
  - Cropping, and masking non-iris regions, preserves the coding budget
  - Pixels outside the ROI fixed to constant values, for normal segmentation
  - Softening the mask boundaries also preserves the coding budget
  - Interoperability of this vendor-neutral format confirmed by IREX results
  - At only 2,000 bytes, iris images are now much more compact than fingerprints

Biometric Sample Quality

Previous edition ISO/IEC IS 29794-1:2009
"Information technology -
Biometrics sample quality Part 1: Framework"

Definitions

- quality: "the degree to which a biometric sample fulfils specified requirements for a targeted application"
- quality score: "a quantitative expression of quality"
- utility: "the observed performance of a biometric sample or set of samples in one or more biometric systems"
- Quality score from 0 to 100



description		size	valid values	notes
Number of Quality Blocks		1 byte	[0,255]	This field is followed by the number of 5-byte Quality Blocks reflected by its value (see **Fehler! Verweisquelle konnte nicht gefunden werden.**). A value of zero (0) means that no attempt was made to assign a quality score. In this case, no Quality Blocks are present.
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

Source: ISO/IEC 29794-1

Biometric Sample Quality

Revision running for

- ISO/IEC 29794 Part 1: framework
- ISO/IEC 29794 Part 4: finger image data
  - upgrade from TR to IS to incorporate NFIQ2.0 findings
    see: http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm

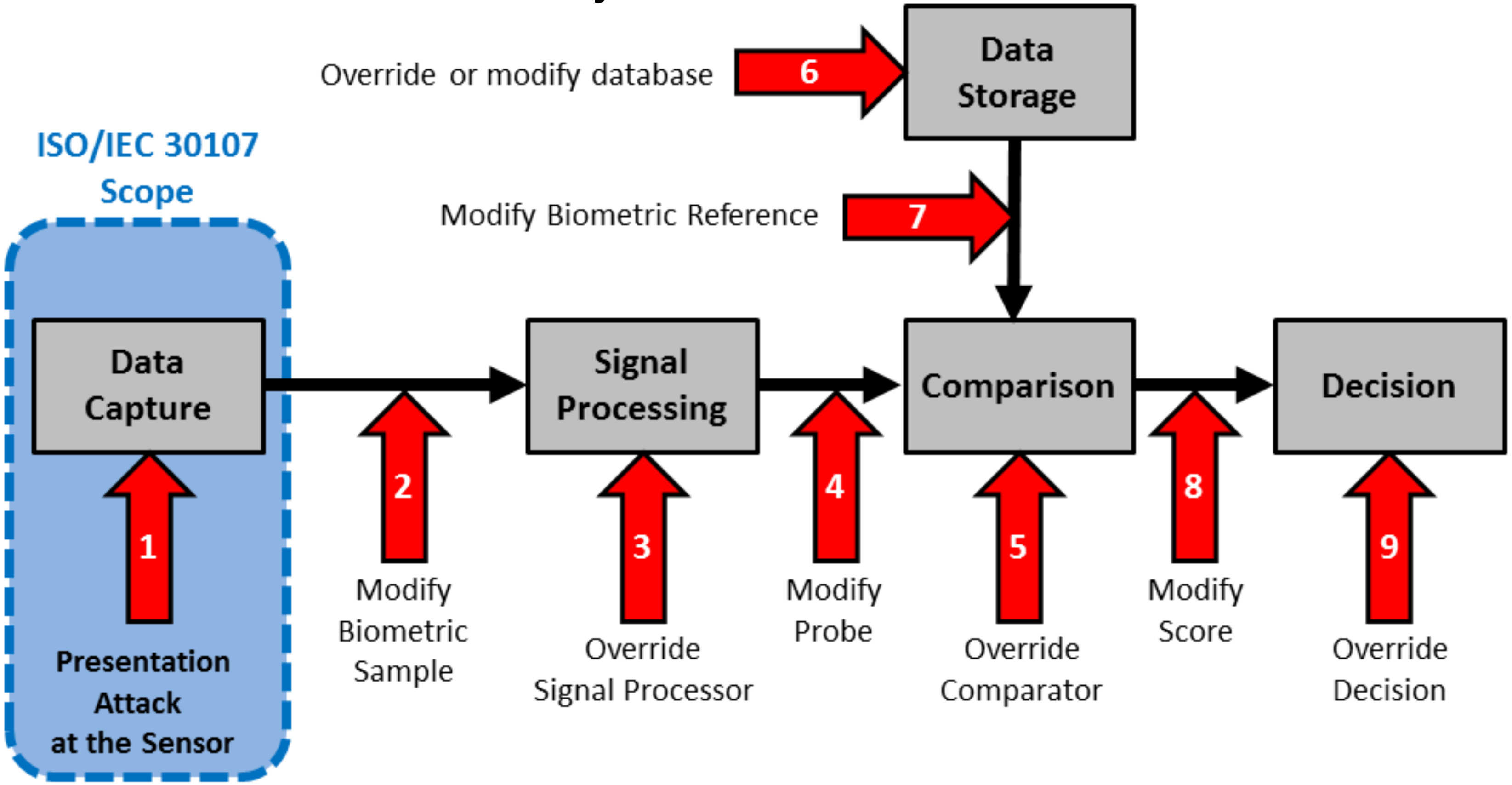
NEW

- DIS ISO/IEC 29794-6 iris image data

Liveness Detection

ISO/IEC 30107 - Presentation Attack Detection

- Attacks on Biometric Systems



Source: ISO/IEC 30107-1 inspired by N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, Vol 40. NO 3, 2001.

Presentation Attack Detection

ISO/IEC 30107 - 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
- a classification of known attacks types (in an informative annex).

Outside the scope are

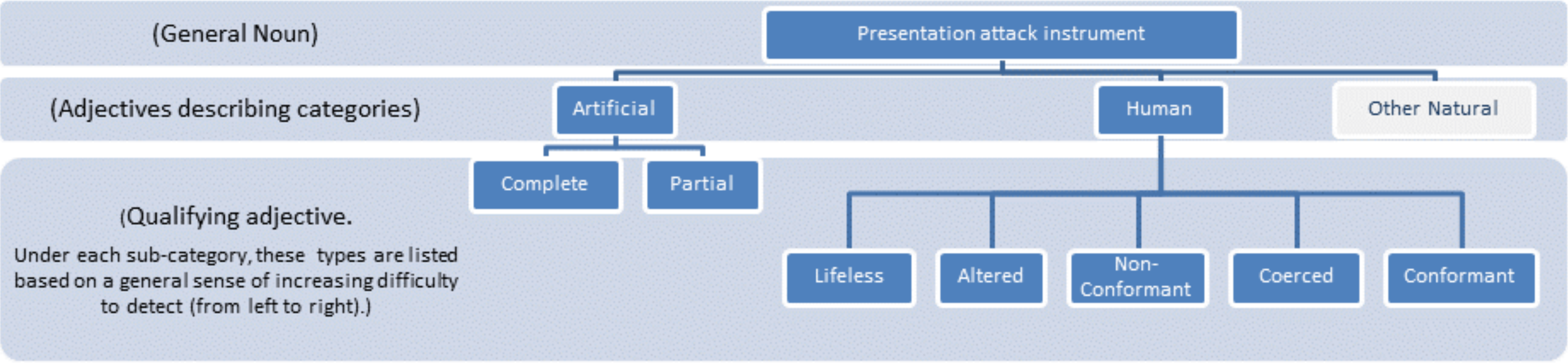
- standardization of specific PAD detection methods;
- detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;
- overall system-level security or vulnerability assessment.

Presentation Attack Detection

ISO/IEC 30107 - Definitions

- artefact: *„artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns“*
- spoof: *„to subvert a system by presentation of an artefact.“*
- change of term: Suspicios presentation detection became biometric Presentation Attack Detection (bPAD)

Types of presentation attacks


(General Noun)
Presentation attack instrument
(Adjectives describing categories)
Artificial
Human
Other Natural
(Qualifying adjective.
Under each sub-category, these types are listed based on a general sense of increasing difficulty to detect (from left to right).)
Complete
Partial
Lifeless
Altered
Non-Conformant
Coerced
Conformant

Source: ISO/IEC 30107-1

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?

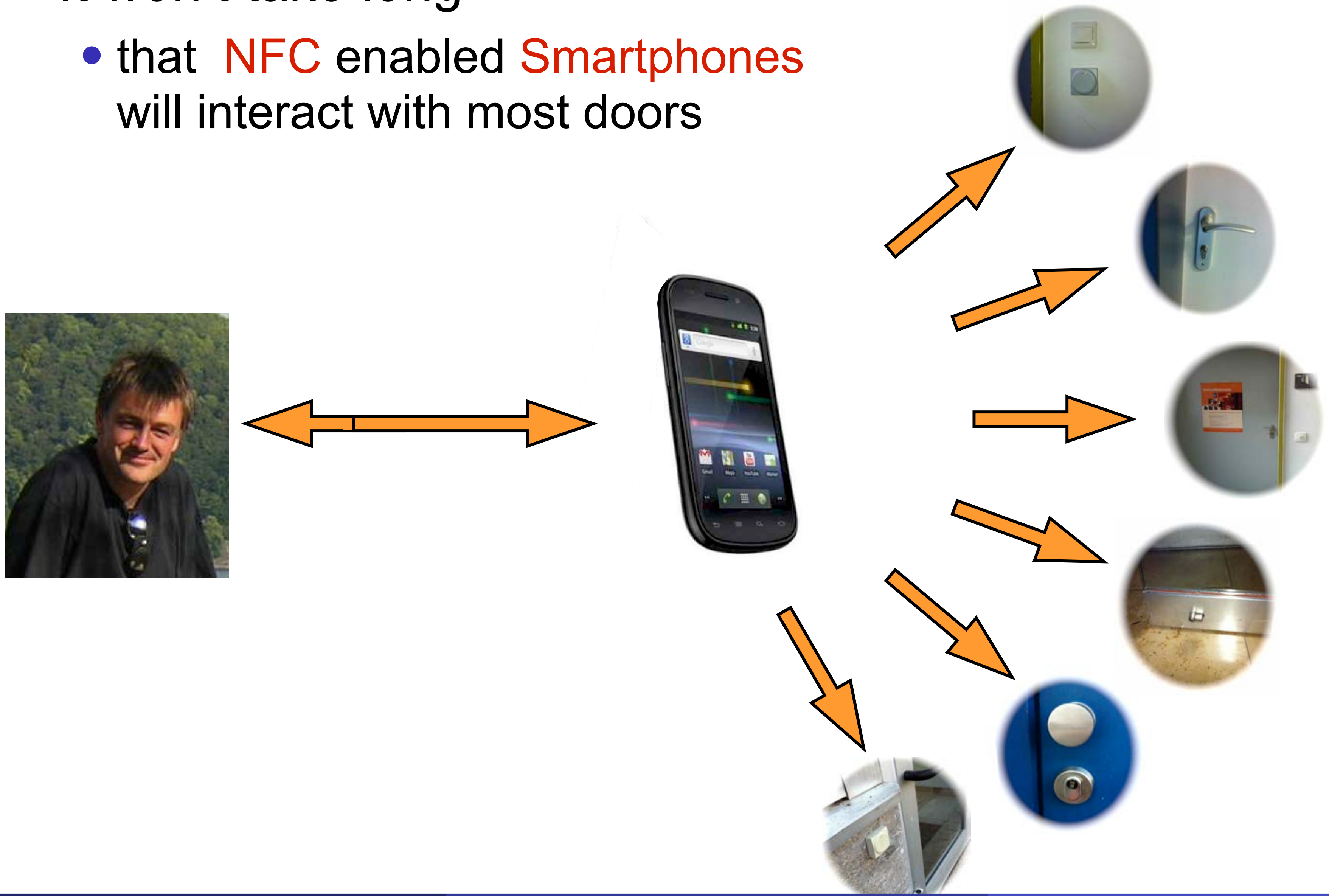
  I want the design of the systems to be compliant to ISO/IEC 24745

Mobile Biometrics

Smartphone Based Access Control

It won‘t take long

- that NFC enabled Smartphones will interact with most doors

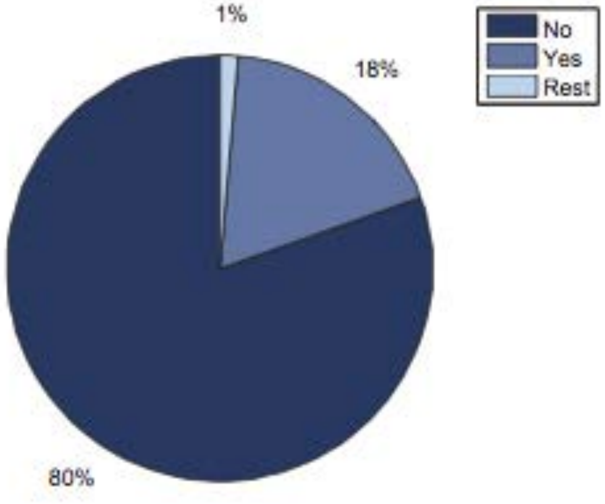


Do we use Access Control
before we unlock our Smartphone?

End-User Survey

Data in mobile devices is often insufficiently protected

- No PIN-authentication required after stand-by phase
  - Survey-result with 962 users : only 18% use PIN code or visual pattern to unlock
- All data on the phone is freely available
  - Emails, addresses, appointments, photos
  - PINs etc.



Reason for this:

- PIN-authentication is too much effort (30%)
- People are self-responsible for their phones

[Ni12] C. Nickel: „Accelerometer-based Biometric Gait Recognition for Authentication on Smartphones“, PhD-thesis, TUD, 2012

Smartphone Access Contol

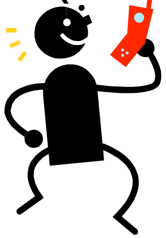
Foreground authentication (user interaction)

- Deliberate decision to capture (wilful 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)

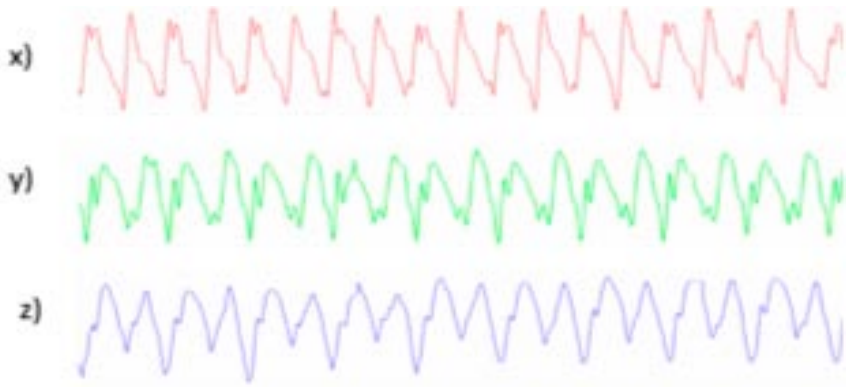
- Microphone
  - Speaker recogntion
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive



Biometric Gait Recognition

Offer an unobtrusive authentication method

- Use accelerometers - already embedded in mobile devices to record the gait
  - Many phones contain accelerometers
  - No extra hardware is necessary
  - Acceleration measured in 3-directions

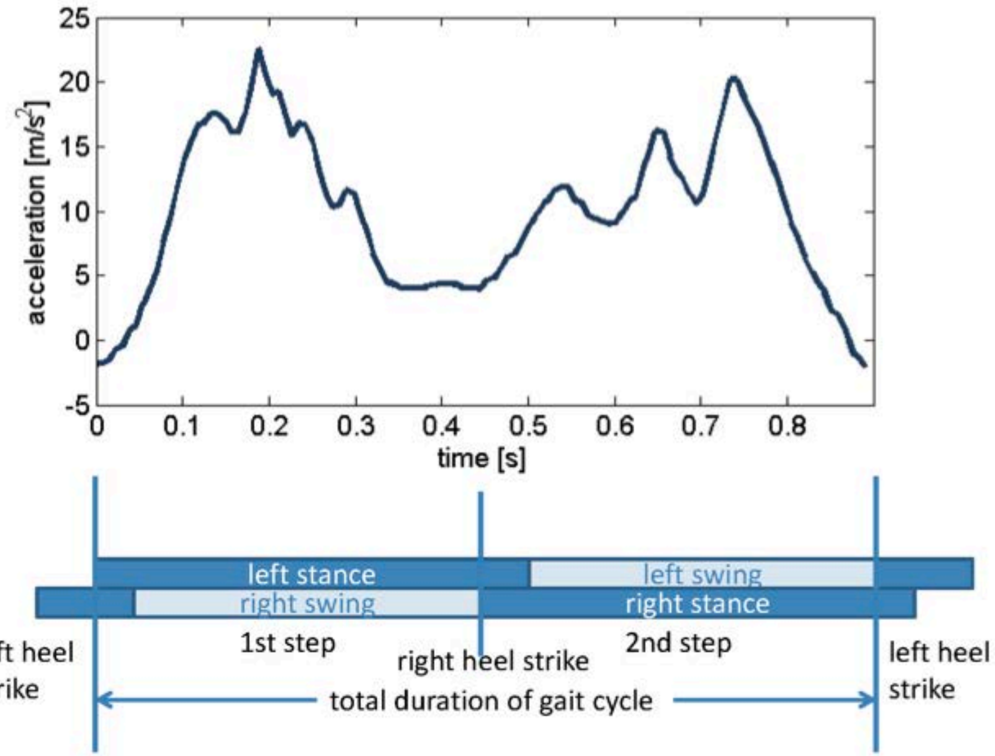


- First paper on this topic:
  [DNBB12] M. Derawi, C. Nickel, P. Bours, C. Busch: „Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition“, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2010)
- EER 20% at that time

Biometric Gait Recognition

Data capture process

- periodical pattern in the recorded signal



Best result

- now at 6.1% EER

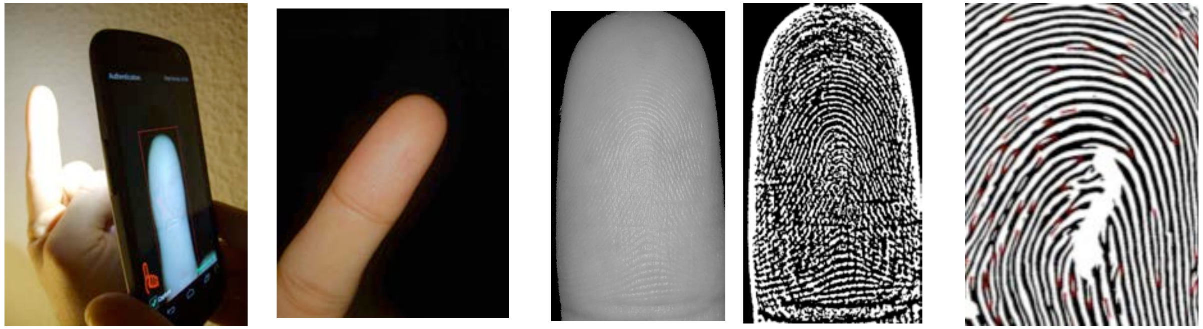
Smartphone Access Contol

Capture process

- Camera operating in macro modus

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

- LED permanent on



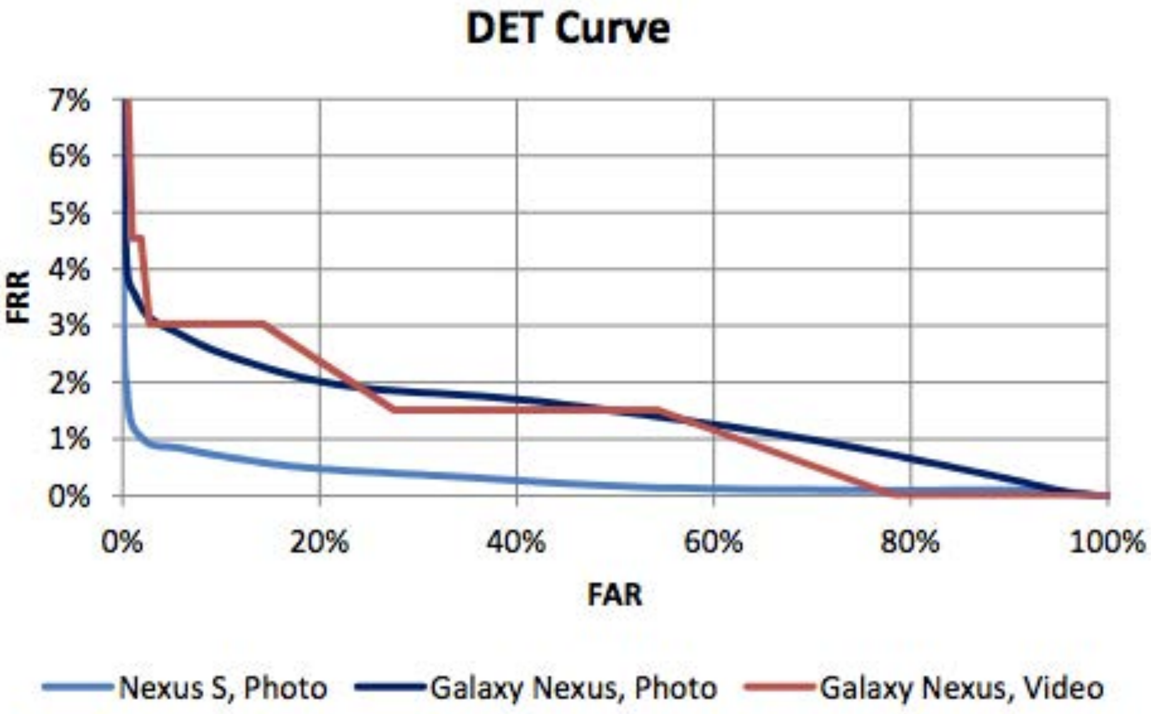
Finger illuminated

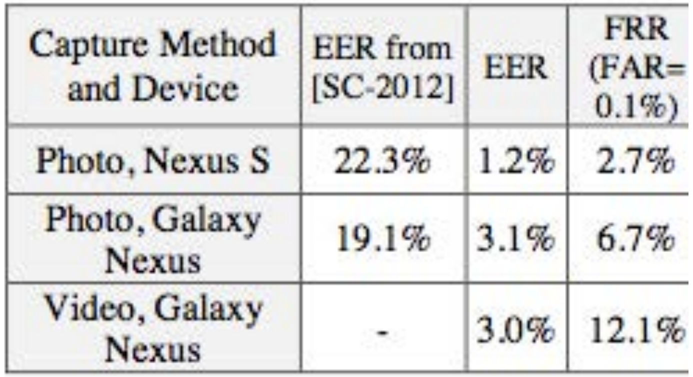
[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

Smart Phone Access Contol

Finger recognition study - 2012/2013

- Results: biometric performance at 1.2% EER





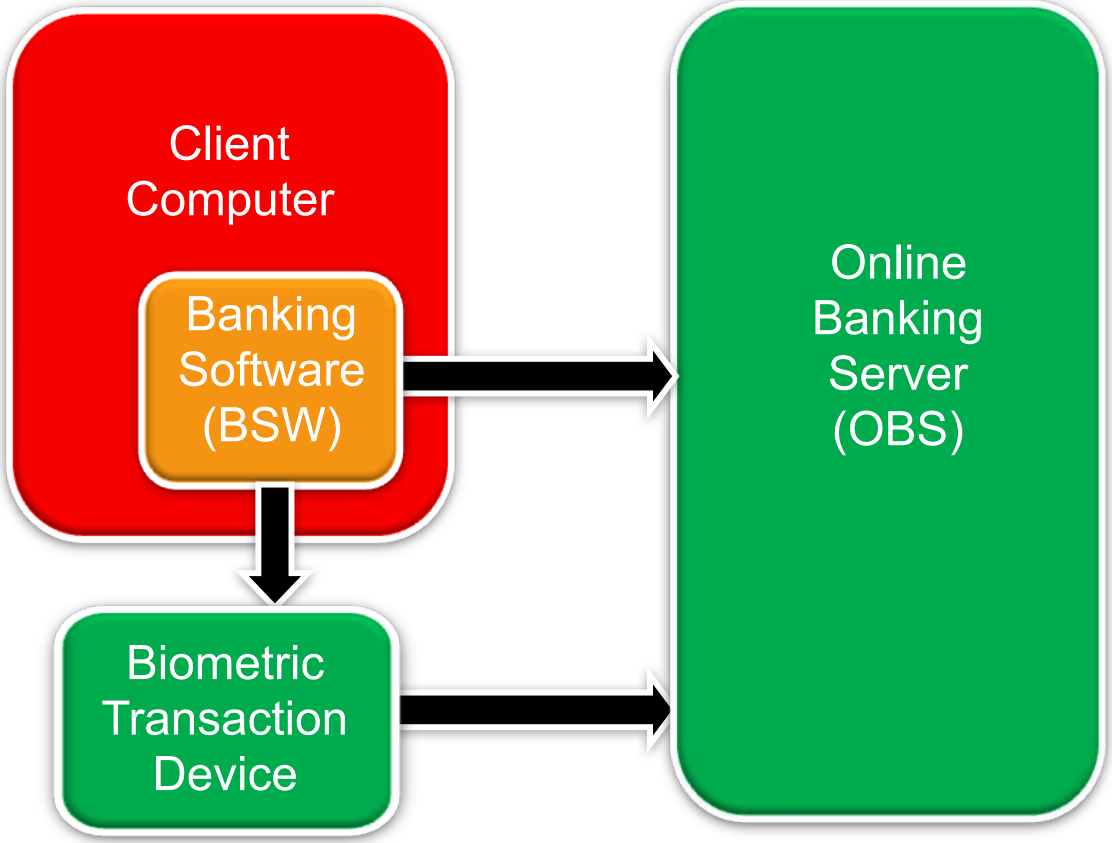
Capture Method and Device	EER from [SC-2012]	EER	FRR (FAR= 0.1%)
Photo, Nexus S	22.3%	1.2%	2.7%
Photo, Galaxy Nexus	19.1%	3.1%	6.7%
Video, Galaxy Nexus	-	3.0%	12.1%

[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)

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

Online-Banking-Scenario

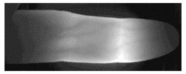
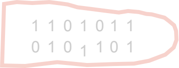
Elements in the Online-Banking-Scenario:



Transaction-Authentication-Protocol

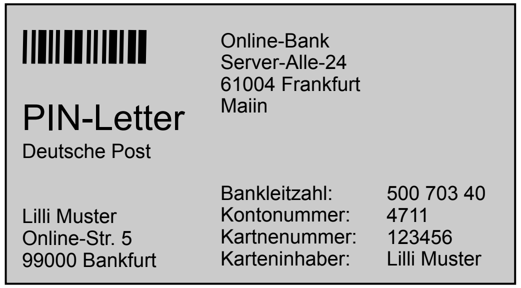
BTAP - Enrolment

1.) Enrolment with Biometric Transaction Device (BTD)

- Biometric samples  are captured with BTD
- Quantized binary vector 

generated from features
- Binary vector reduced down to reliable features (RBV)

and relevant positions (AD1) are stored { 0,1,2,4,5,8,11,12 }
- Customer receives analog letter with PIN and enter this once



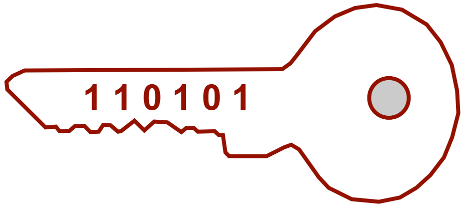
PIN-Letter
Deutsche Post

Online-Bank
Server-Alle-24
61004 Frankfurt
Maiin

Lilli Muster
Online-Str. 5
99000 Bankfurt

Bankleitzahl:	500 703 40
Kontonummer:	4711
Kartnenummer:	123456
Karteninhaber:	Lilli Muster

PIN = 4768 0569

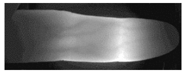


SBV = 110101

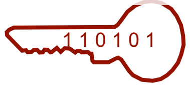
Transaction-Authentication-Protocol

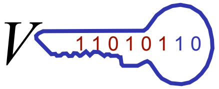
BTAP - Enrolment

1.) Enrolment with Biometric Transaction Device (BTD)

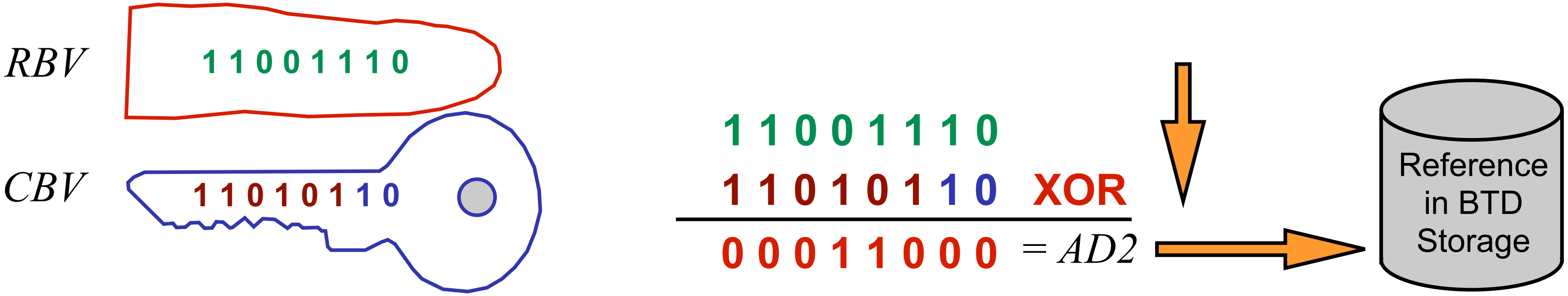
- Biometric samples  are captured with BTD
- Quantized binary vector

generated from features
- Binary vector reduced down to reliable features (*RBV*)

and relevant positions (AD1) are stored { 0,1,2,4,5,8,11,12 }
- Postal PIN letter provides unique key 

- Secret vectore *CBV* 

is generated
- Reduced binary vector *RBV* will be combined with the secret vector *CBV* with a XOR operation



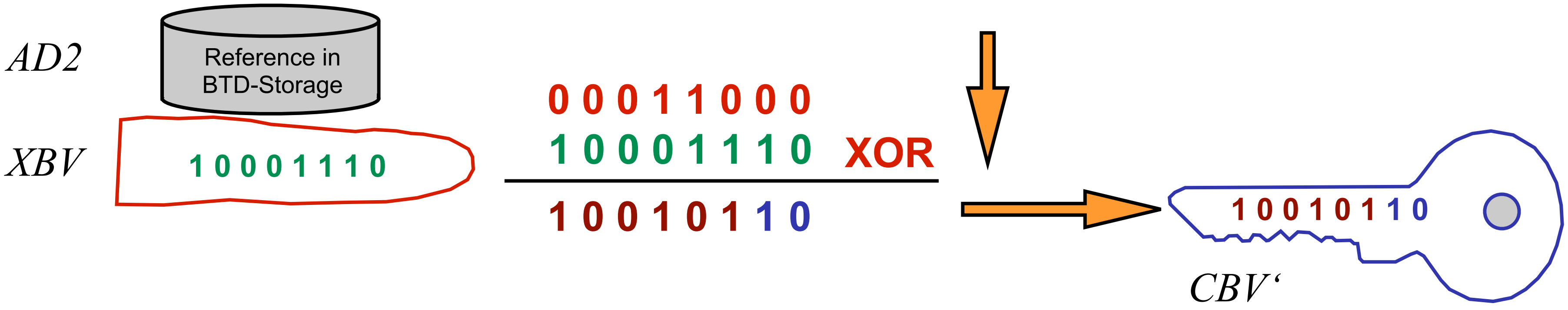
- Auxilliary data stored in personal secure memory (BTD)

Transaction-Verification

BTAP - Transaction

2.) Operations of the Biometric-Transaction-Device (BTD)

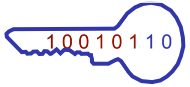
- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $AD1_{\{0,1,2,4,5,8,11,12\}}$ is extracted from BTD-storage
- A binarized feature vector XBV 10001110 is reconstructed
- A secret vector CBV' is reconstructed with XOR operation from the Auxilliary Data $AD2$ Reference that was stored in the BTD and from the binarized feature vector XBV 10001110



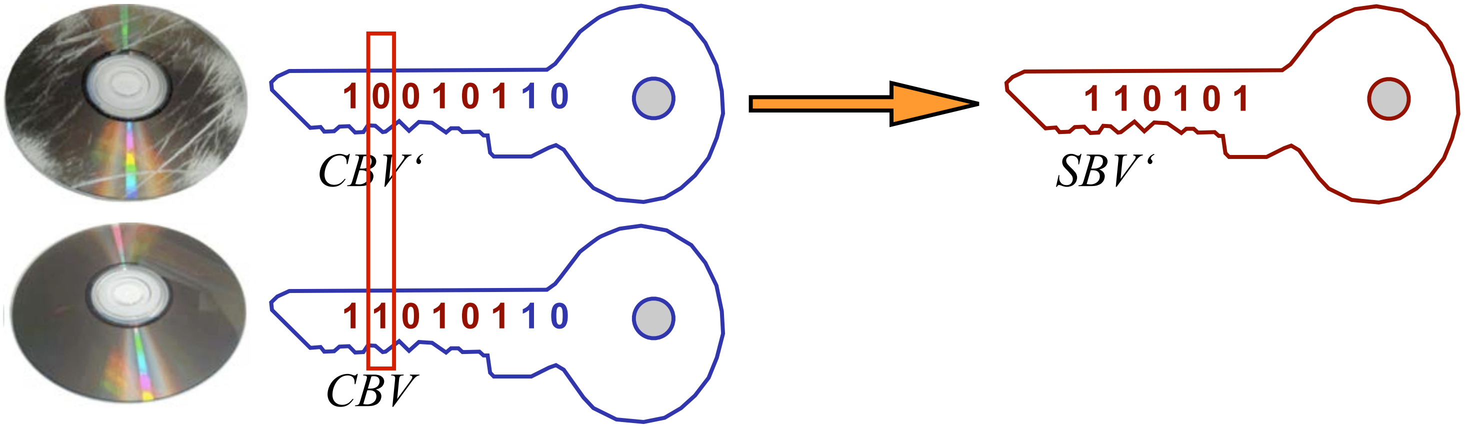
Transaction-Verification

BTAP - Transaction

2.) Operations of the Biometric-Transaction-Device (BTD)

- The relevant Information of the Transaction-Order-Record (TOR) is visualized in the display of the BTD:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Approval of the intended transaction by probe sample
- Auxilliary Data $AD1_{\{0,1,2,4,5,8,11,12\}}$ is extracted from BTD-storage
- A binarized feature vector XBV is reconstructed
- A secret vector CBV'  is reconstructed
- The secret key SBV' is freshly re-computed from CBV'

$SBV' = dec\ (CBV')$

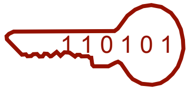


Transaction-Verification

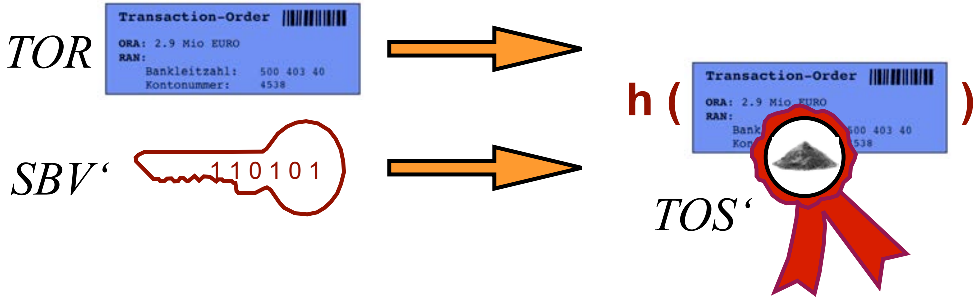
BTAP - Transaction

2.b) Mirror-Operations of the BTD and the OBS

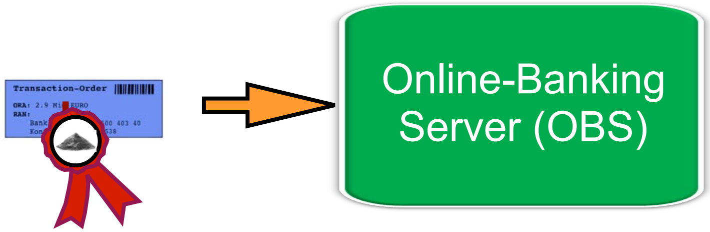
- A Transaction-Order-Seal (TOS‘) is computed
  - of the Transaction-Order-Record *TOR*
  - and the reconstructed secret key *SBV‘*



$TOS' = MAC\,(h(TOR),\, h(SBV'))$



- The seal (TOS‘) is transfered to the Online-Banking-Server

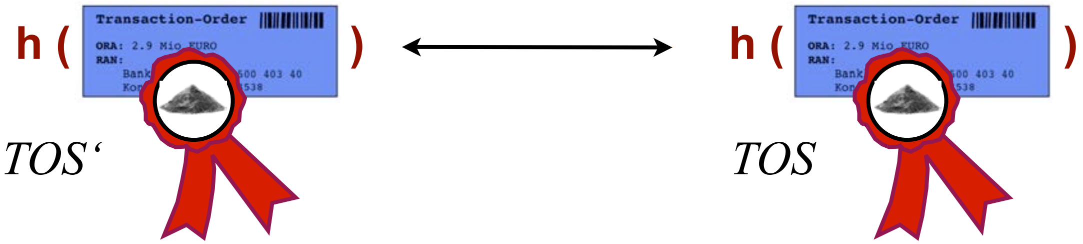


Transaction-Verification

BTAP - Transaction

3.) Operation of the Online-Banking-Server (OBS)

- Compares his own reconstruction of the seal (TOS) with the delivered seal (TOS ‘) from the device (BTD‘): $TOS == TOS‘$



- The transaction is person- and data-authentic, if both seals are identical.
- Then and only then the transaction is implemented

Conclusion

Biometric Transaction Authentication Protocoll (BTAP)

- A biometric authentication factor can effectively prevent automated attacks

Biometric transaction authentication can spot

- Manipulation of transaction amount or receiver information
- Unauthorized delegation /loss of a transaction device

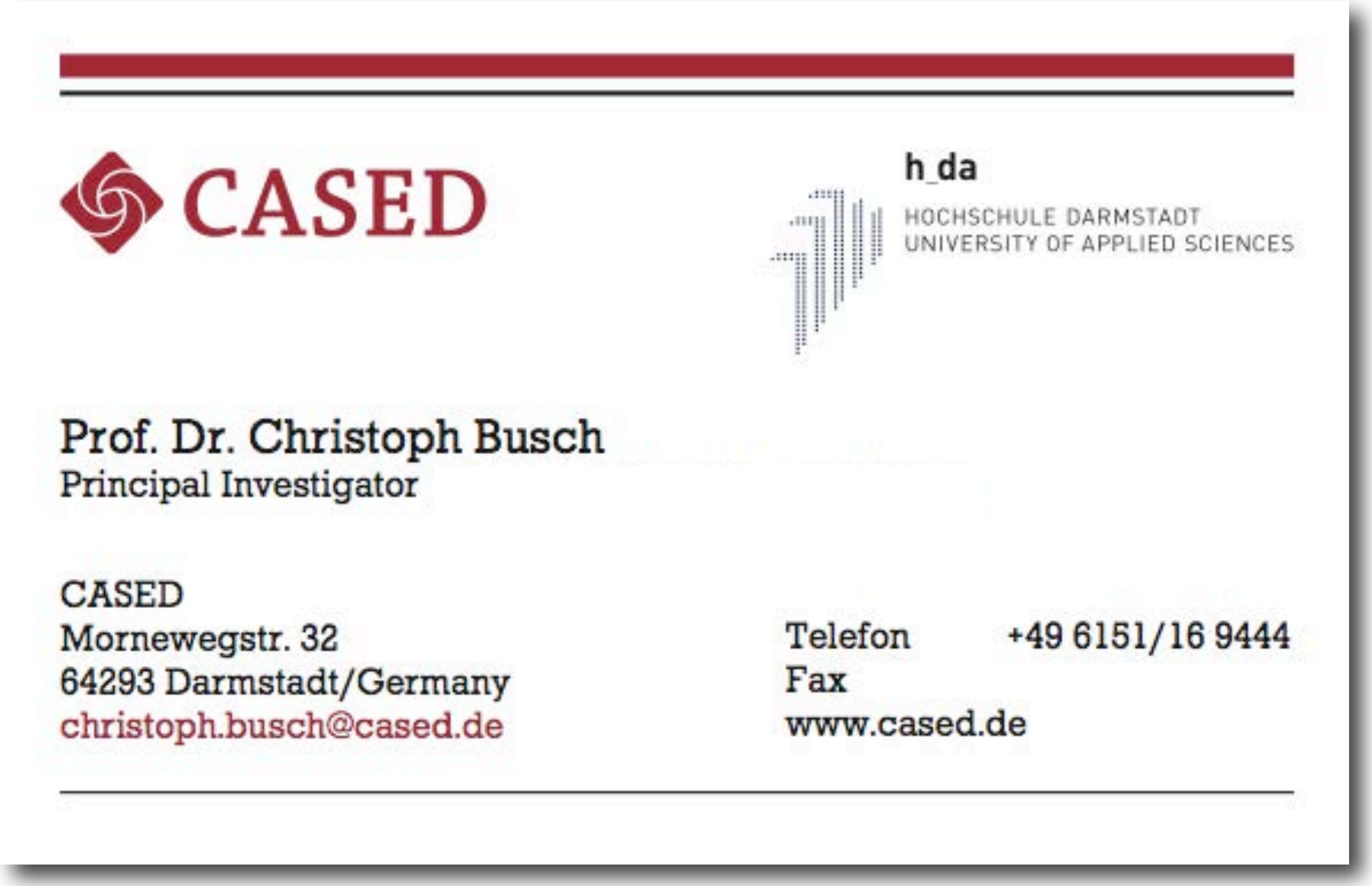
BTAP follows the two channel concept

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

More 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	