Biometrics - From Rumors to Reality

Christoph Busch / Waldemar Grudzien

European Association for Biometrics / Bundesverband Deutscher Banken
http://www.christoph-busch.de/

Nuance Customer Experience Summit

Kronberg - April 22, 2015

Agenda

- European Association for Biometrics
- 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“

European Association for Biometrics

CURRENT STATUS OF THE EAB-ASSOCIATION

- EAB founded on November 17, 2011
- Currently > **170** 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
- European Biometrics Symposium
- Workshops in cooperation with other associations and interest groups
- Network of national contact points (currently 26) and fora

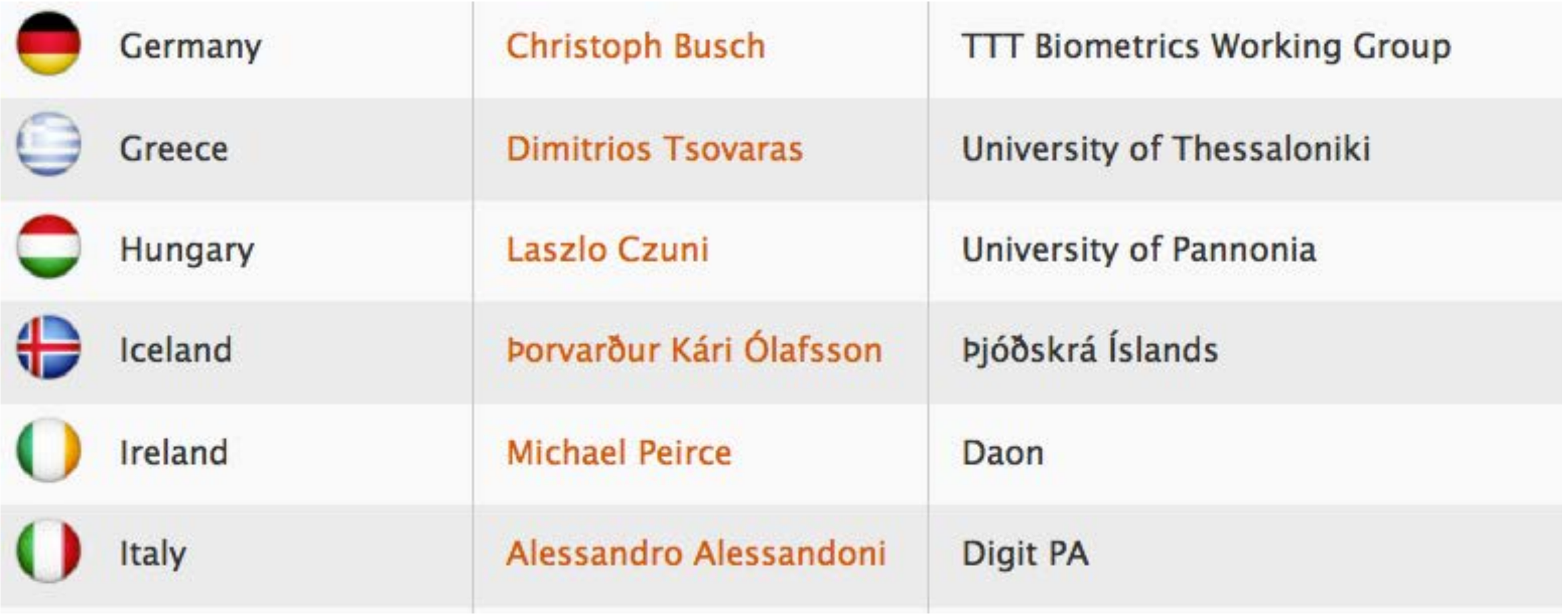
  http://eab.org/information/national_contact_points.html

CURRENT STATUS OF THE EAB-ASSOCIATION

- National Contact Points - see the full list at:

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

  example 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

EAB-COOPERATIVE RESEARCH

- Cooperative Identification Technology Research Consortium (EAB-CITeR)
  - Conditions for Affiliates:
    - Annual membership (SME): 5 kEUR / year (2 years),
    - Premium Annual membership: 30 kEUR / year (2 years).
  - Benefits:
    - Cost effective R&D,
    - Drive research,
    - Access to research results (« non-exclusive royalty free license » or « exclusive fee-bearing license ») from Partners,
    - Access to researchers, students and labs,
    - Initiate new collaborative projects (H2020, ...).

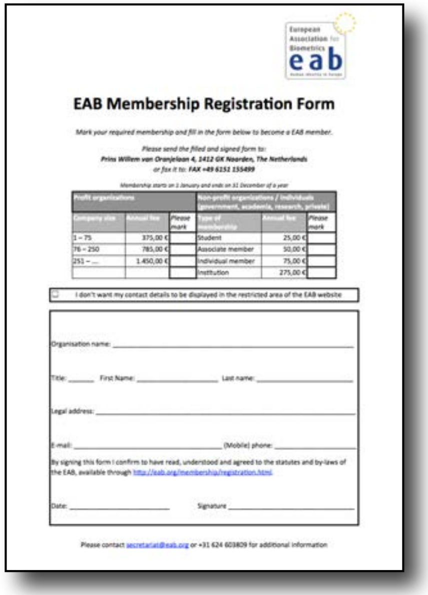
EAB - INTERESTING UPCOMING EVENTS

- Research Projects Conference (EAB-RPC)
  - September 7th and 8th, Darmstadt
  - http://www.eab.org/events/program/79
- Seminar - Biometrics in Banking and Payments
  - Cooperation with BITKOM, September 24th, Frankfurt
  - http://www.eab.org/events/program/92
    - Case studies on biometrics in banking and payments (e.g. business case, integration in business processes and procedures, customer experiences)
    - State of the Art of biometrics for mobile transactions
    - Privacy and legal aspects of biometrics for banking and payments
    - European and international regulatory landscape for payments and financial transactions

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
Human Identity in Europe

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 Noorden, 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

Benchmark 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 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 three striking arguments why biometric authentication is better than the PIN

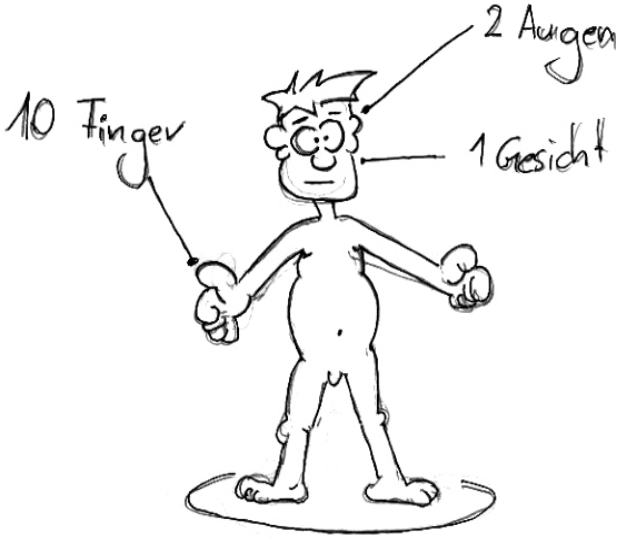
- 3.) PINs can be delegated in violation of the security policy
  - „*This transaction was done by Mr. Popov, who was mis-using my card*“
  - biometric authentication enables non-repudiation of transactions

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“



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 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.
  - Non-invertibility:Original biometric sample can not be reconstructed

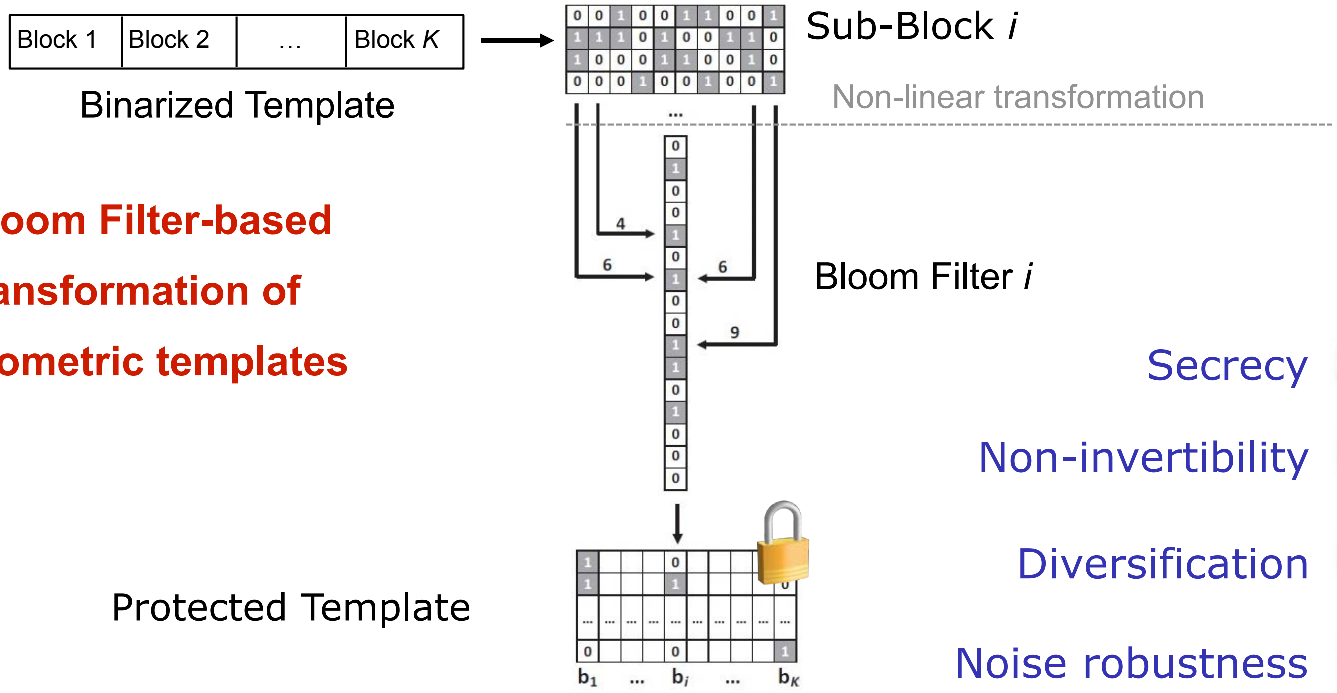
- [Br2008] J. Breebaart, C. Busch, J. Grave, E. Kindt: "A Reference Architecture for Biometric Template Protection based on Pseudo Identities", in BIOSIG-2008, GI-LNI, (2008) http://www.christoph-busch.de/files/Breebaart-BTPReferenceArchitecture-BIOSIG-2008.pdf

Biometric Template Protection

Protection at the same accuracy level is possible

- Bloom filter-based pseudonymous identifiers

Bloom Filter-based transformation of biometric templates



Secrecy ✓

Non-invertibility ✓

Diversification ✓

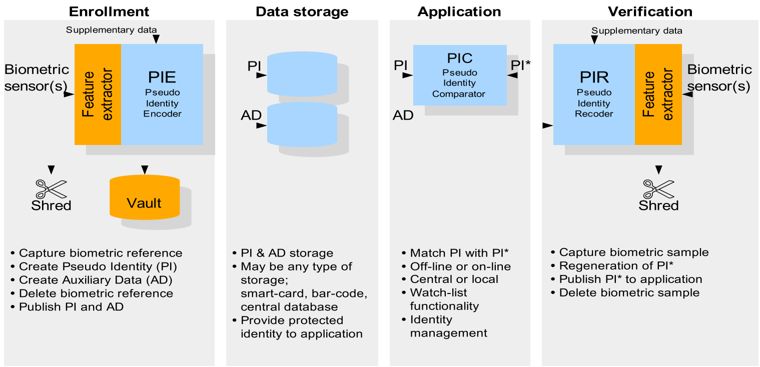
Noise robustness ✓

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



Enrollment

Supplementary data

Biometric sensor(s)

Feature extractor

PIE Pseudo Identity Encoder

Shred

Vault

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

Data storage

PI

AD

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

Application

PI

PIC Pseudo Identity Comparator

PI*

AD

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

Verification

Supplementary data

PIR Pseudo Identity Recoder

Feature extractor

Biometric sensor(s)

Shred

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

ISO/IEC 24745
Biometric Information Protection !

Bio-Hacking ?

Operators may think:

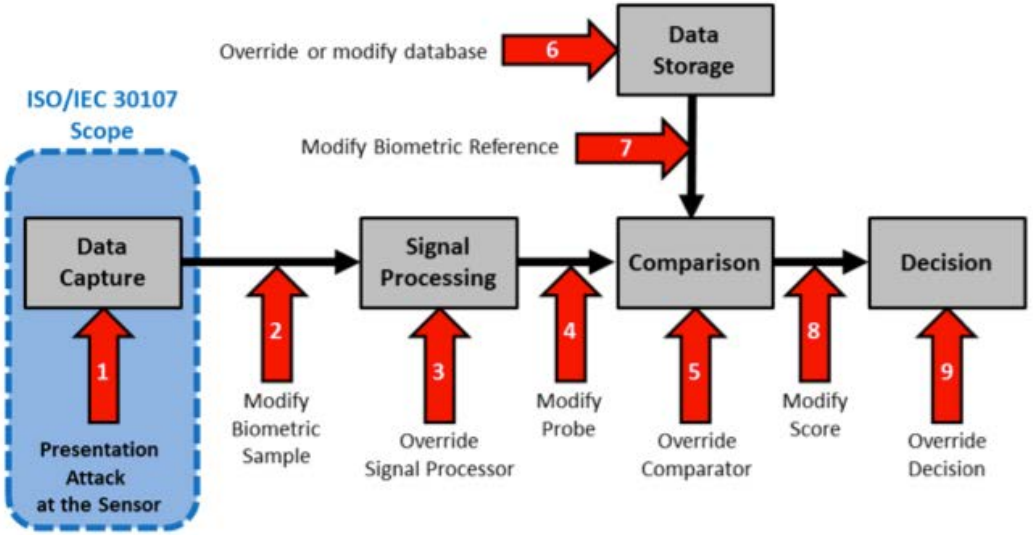
„Biometric sensors can not detect gummy and cut-off fingers“

Presentation Attack Detection

Attacks on capture devices

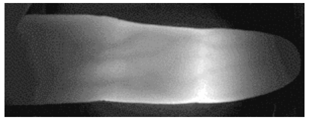
- ISO/IEC 30107 Presentation Attack Detection (PAD)
  - aka spoof detection

silicon finger



Countermeasures

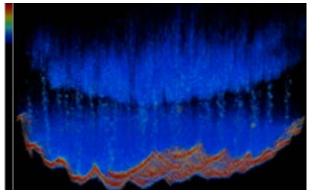
- Vein recognition



Fingervein image

- Fingerphoto recognition
  - Fingerprint Recognition with Optical Coherence Tomography (OCT)

Half-transparent gelatinwith glycerin



3D Finger OCT scan

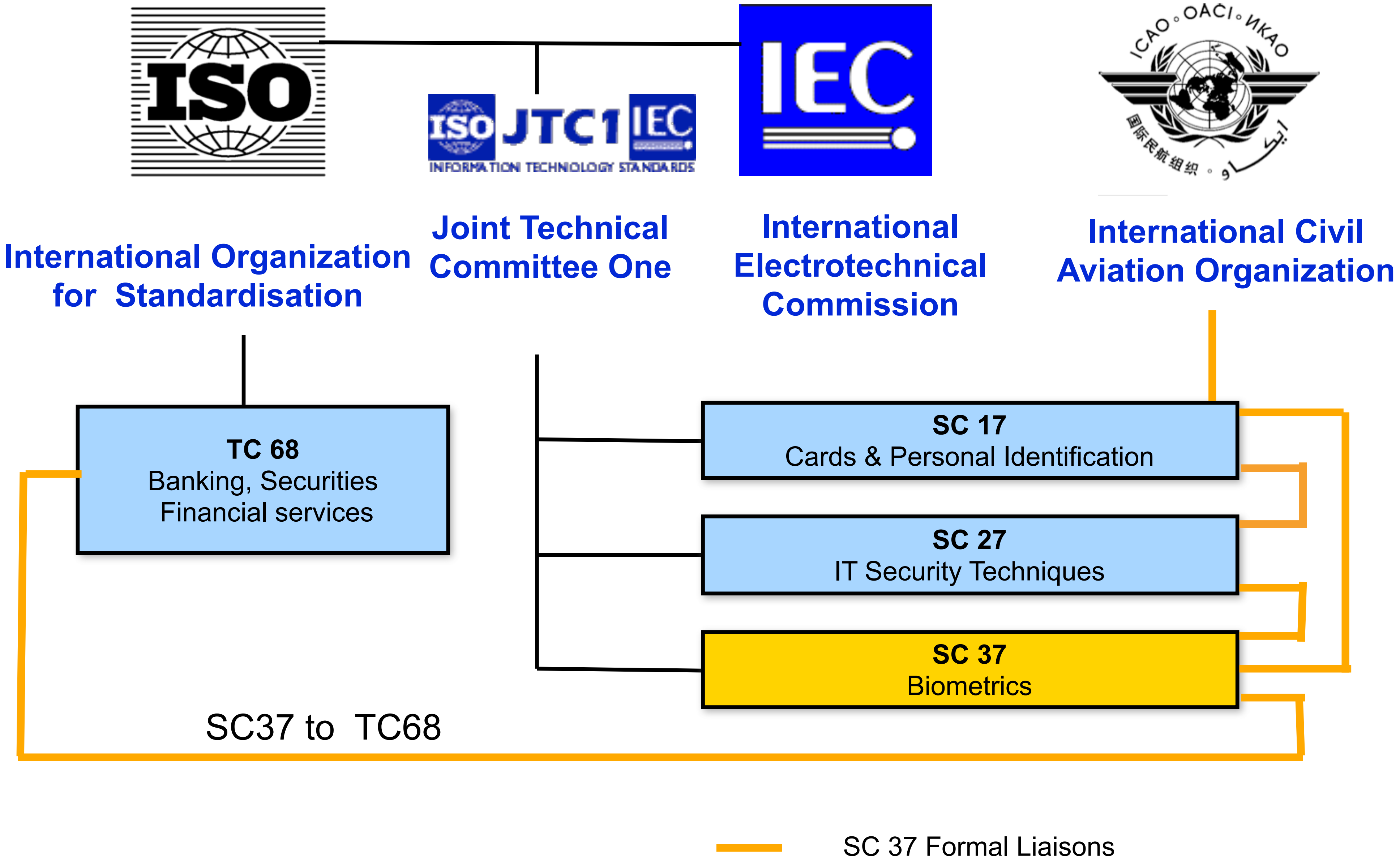
- Voice: current research topic

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

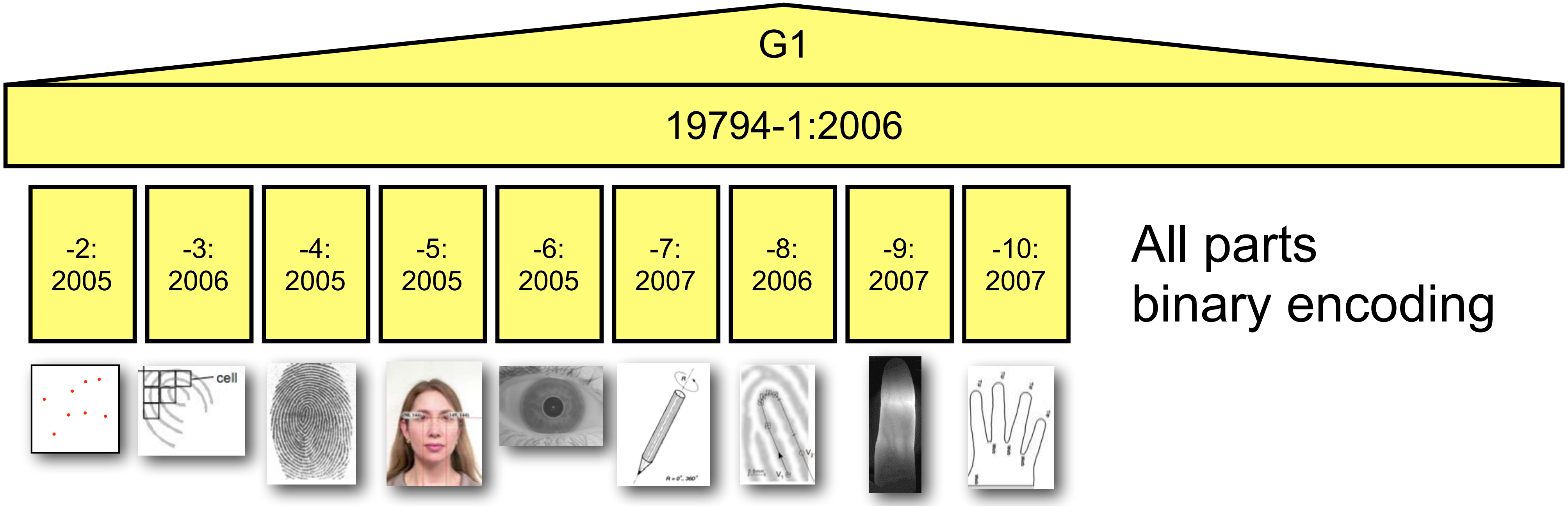
SC 27
IT Security Techniques

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

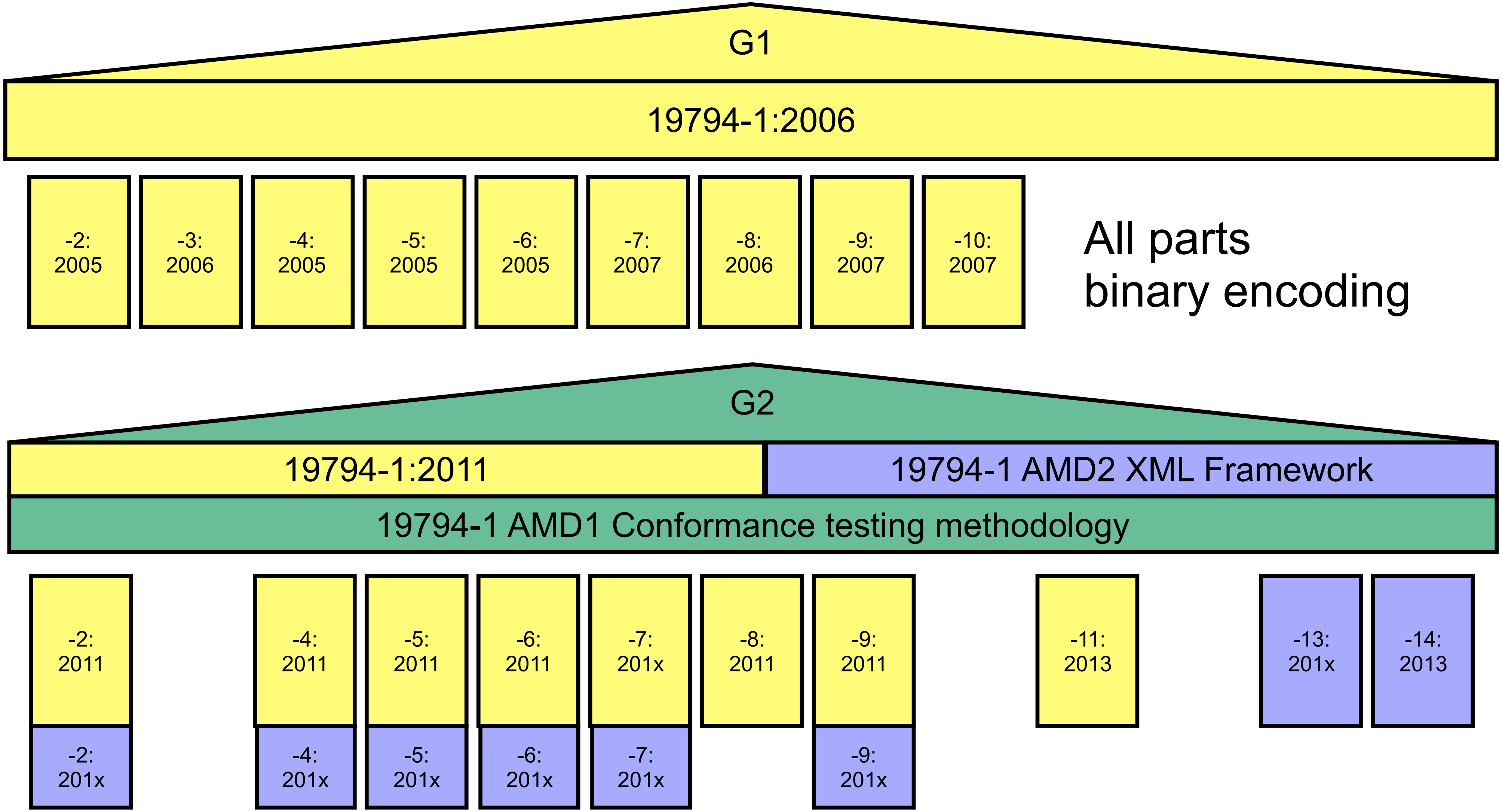
-9: 2007

-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 is equivalent for binary encoded and XML encoded records

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 Access Control

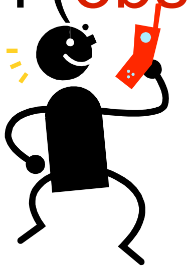
Foreground authentication (user interaction)

- 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 Speaker Recognition

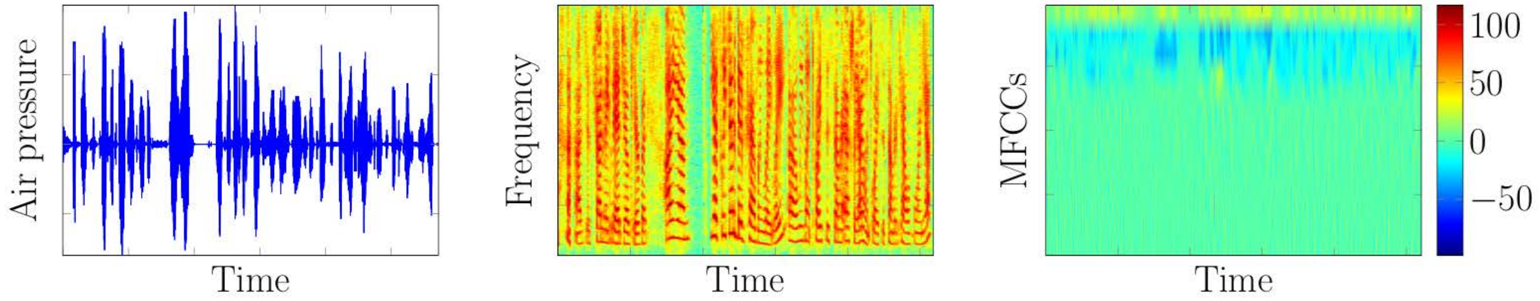
Offer an unobtrusive or explicit authentication method

- Use embedded microphone in mobile device to record the voice signal
  - unobtrusive or
  - apply willful act for explicit transaction authorization
  - No extra hardware is necessary

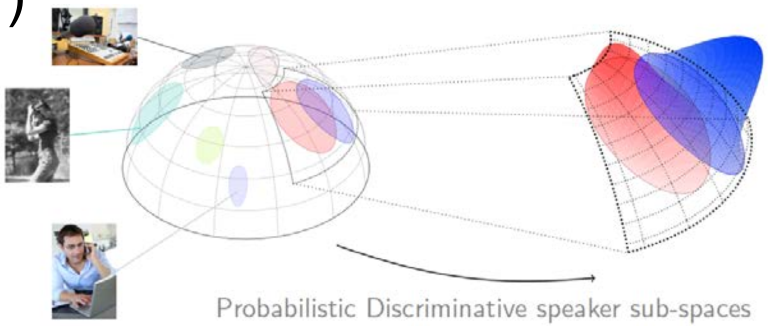
Biometric Speaker Recognition

State of the art

- Psychoacoustic spectrum analysis
  - 60 Mel-Frequency Cepstrum Coefficients (MFCCs)



- MFCC Clustering with Gaussian Mixture Models (GMMs)
  - 2048 × 60 free parameter per sample
- Total Variability Analysis: intermediate-sized vectors
  - 400-dimensional identity vectors (i-vector)
- Linear Discrimination Analysis (LDA)
  - 200-dimensional i-vector
- Projection into spherical space

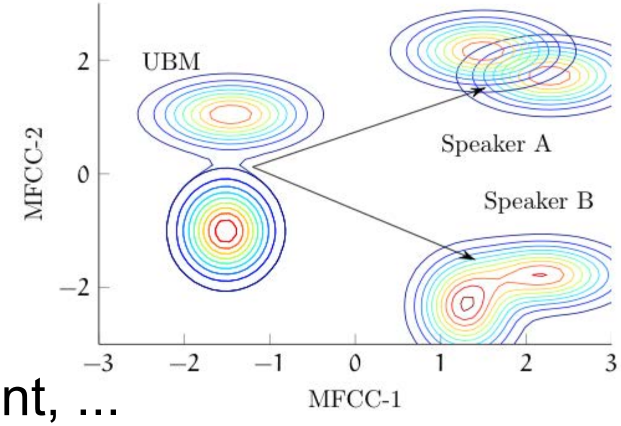


Probabilistic Discriminative speaker sub-spaces

Biometric Speaker Recognition

State of the art

- The i-vector approach represents a rather new approach which extracts adequate features within a speaker space.
  - 1.) Cepstral features
  - 2.) Supervector estimation
    - Estimateable by cepstral features
    - GMM-means as supervector
    - Variations due to:
      - ✦ noise, microphones, phonetic content, ...
      - ✦ Ageing, diseases, constitutional state, …
  - 3.) Total variability factor analysis:
    - Total variability matrix **T** - trained by the Universal Background Model (UBM)
    - Supervectors are mapped to i-vectors

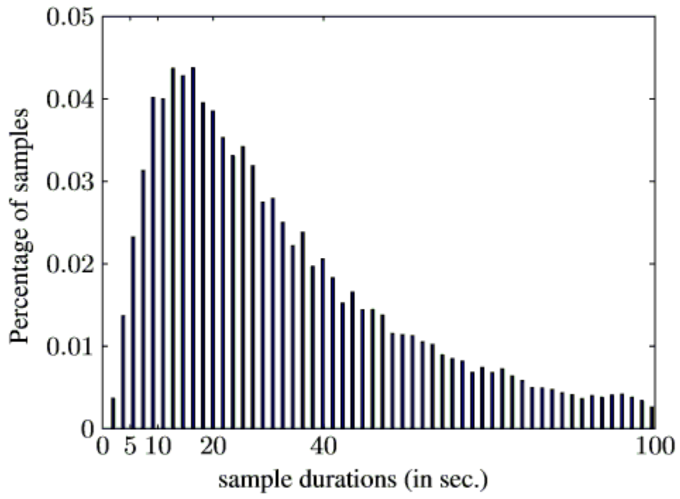


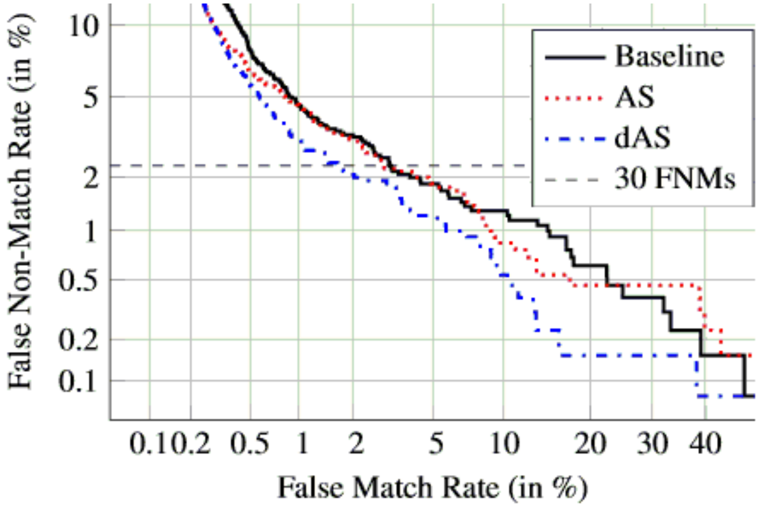
[Dehak2011] N. Dehak, P. J. Kenny, R. Dehak, P. Dumouchel, and P. Ouellet, “Front-End Factor Analysis for Speaker Verification,” in IEEE TASL, (2011)

Biometric Speaker Recognition

Challenges

- Within-Speaker variance
  (stress, health)
- Between-Sample variance
  (duration, noise, overlapping speakers)



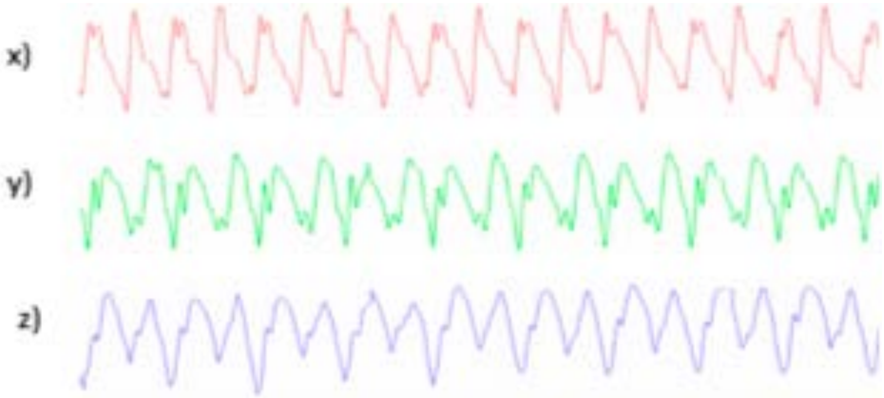


[Nautsch2014] A. Nautsch, C. Rathgeb, C. Busch, H. Reininger and K. Kasper: „Towards Duration Invariance of i-Vector-based Adaptive Score Normalization“, in Proceedings of Speaker and Language Recognition Workshop (Odyssey 2014), Finland, (2014)

Biometric Gait Recognition

Offer an unobtrusive authentication method

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

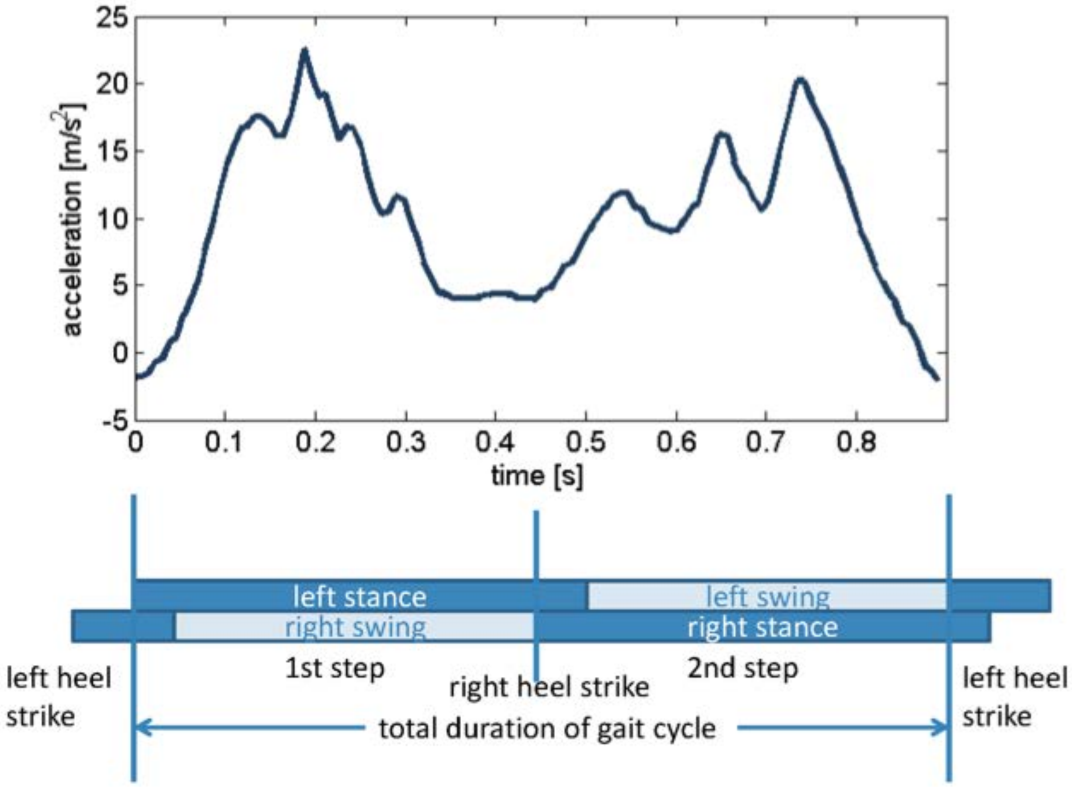


- First paper on this topic:
  [DNBB10] M. Derawi, C. Nickel, P. Bours, C. Busch: „Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition“, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2010)

Biometric Gait Recognition

Data capture process

- periodical pattern in the recorded signal



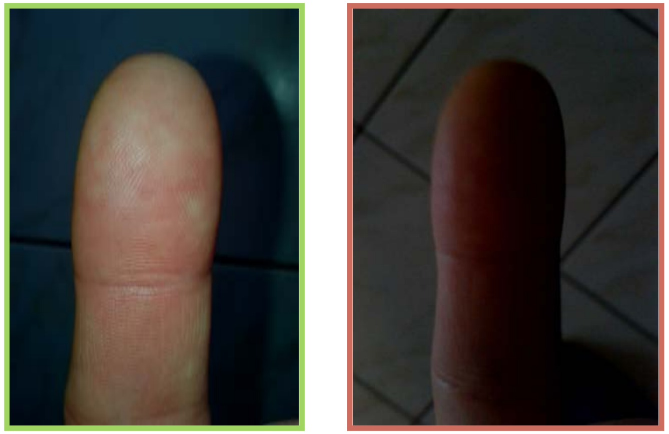
Best result

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

Smartphone Access Contol

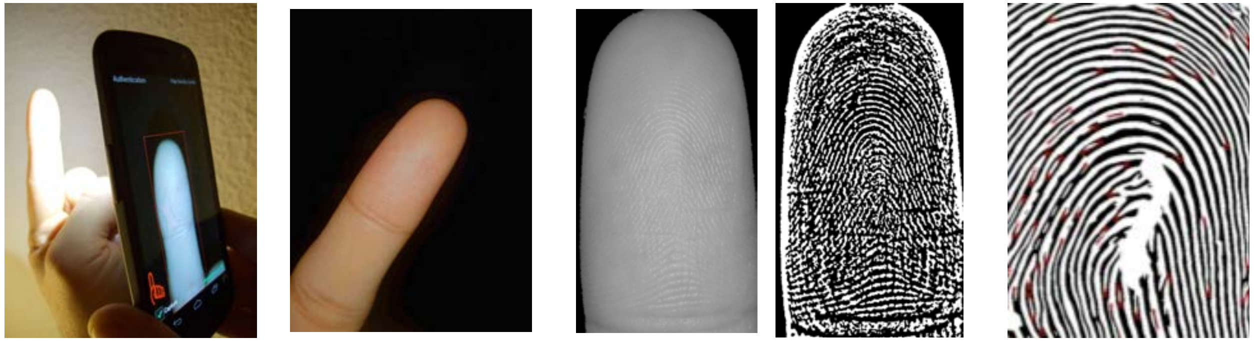
Capture process

- Camera operating in macro modus



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

- LED permanent on



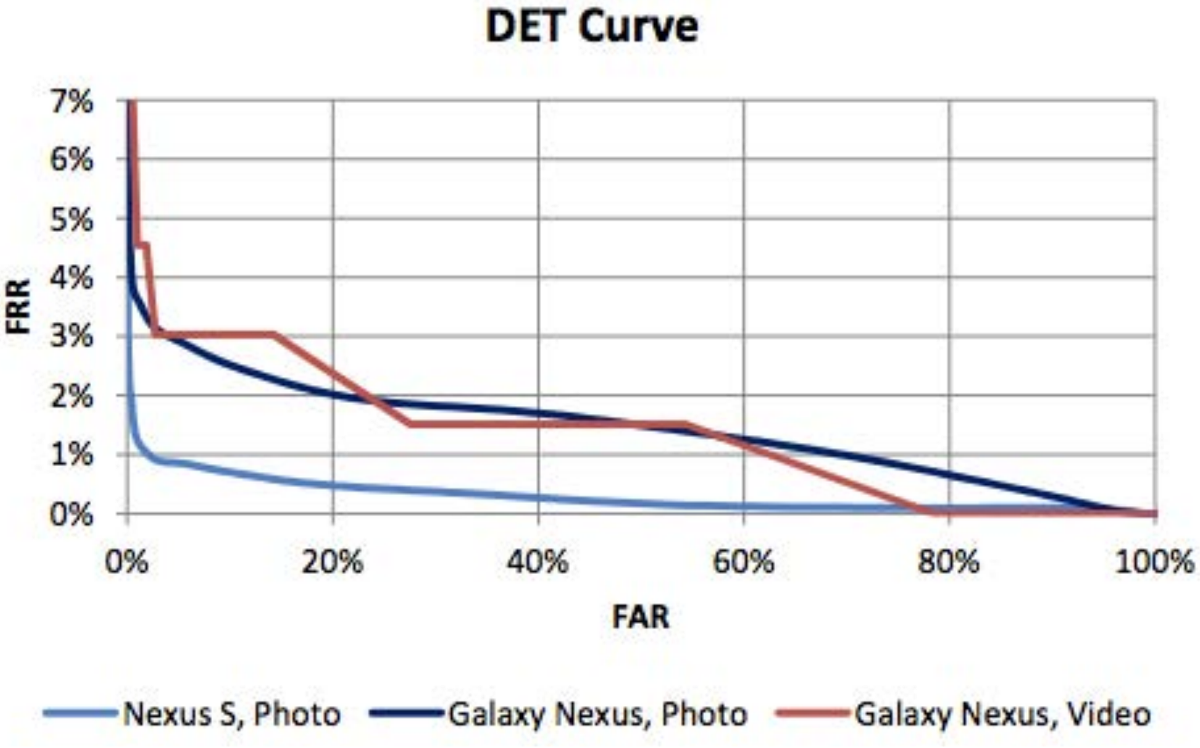
Finger illuminated

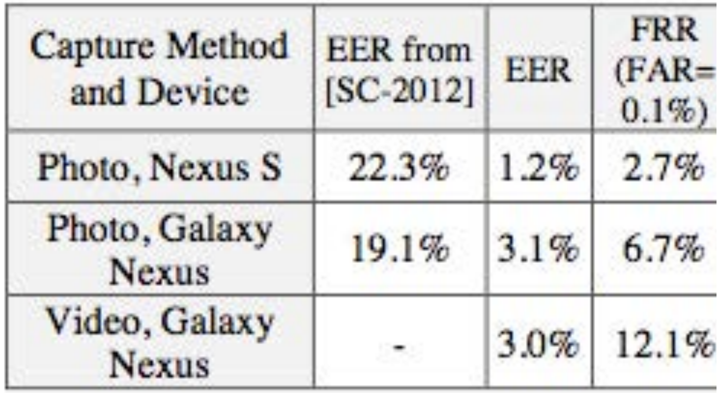
[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

Smart Phone Access Contol

Finger recognition study - 2012/2013

- Result: biometric performance at 1.2% EER





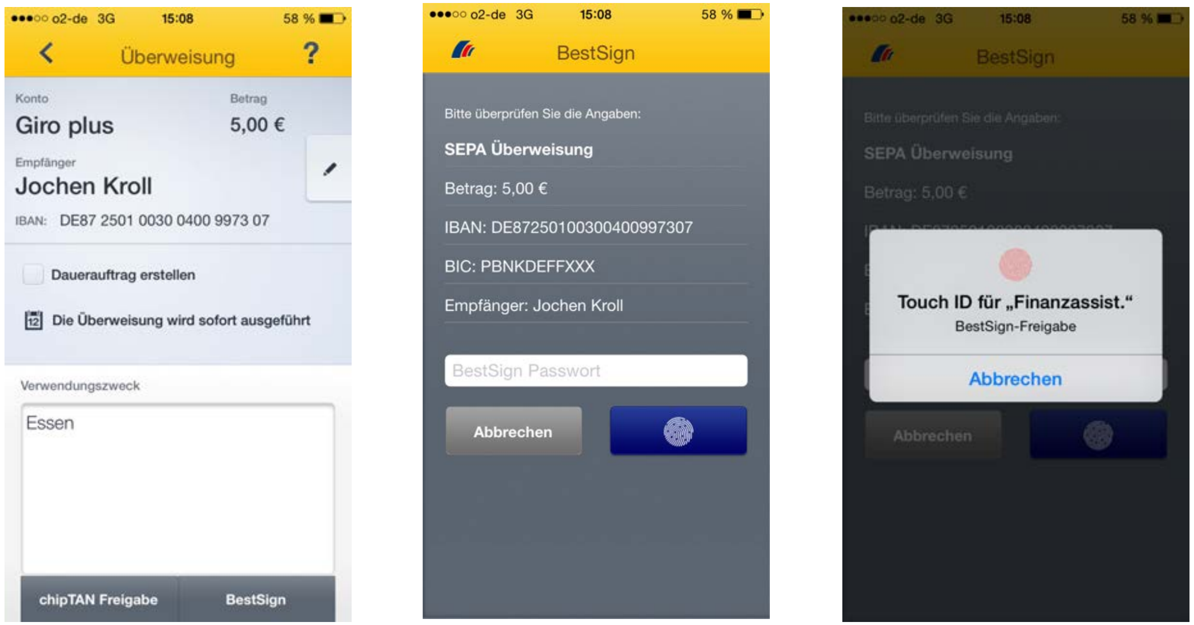
Capture Method and Device	EER from [SC-2012]	EER	FRR (FAR= 0.1%)
Photo, Nexus S	22.3%	1.2%	2.7%
Photo, Galaxy Nexus	19.1%	3.1%	6.7%
Video, Galaxy Nexus	-	3.0%	12.1%

[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)

Why for Mobile Phones multiple Modalities?

Financial Transactions

- Post bank’s solution with TouchID
  - presented in December 2014



Konto Giro plus

Betrag 5,00 €

Empfänger Jochen Kroll

IBAN: DE87 2501 0030 0400 9973 07

□ Dauerauftrag erstellen

Die Überweisung wird sofort ausgeführt

Verwendungszweck Essen

Bitte überprüfen Sie die Angaben:

SEPA Überweisung

Betrag: 5,00 €

IBAN: DE87250100300400997307

BIC: PBNKDEFFXXX

Empfänger: Jochen Kroll

Touch ID für „Finanzassist.“

BestSign-Freigabe

Image Source: Postbank 2014

- There will be solutions beyond ApplePay
  - for reasons to avoid vendor lock-in
  - for data privacy reasons
  - for reasons to scale biometrics to the transaction volume

Financial Transactions

- White paper Bundesverband Deutscher Banken (BdB)
  - number and strength of biometric factors should scale with transaction volume

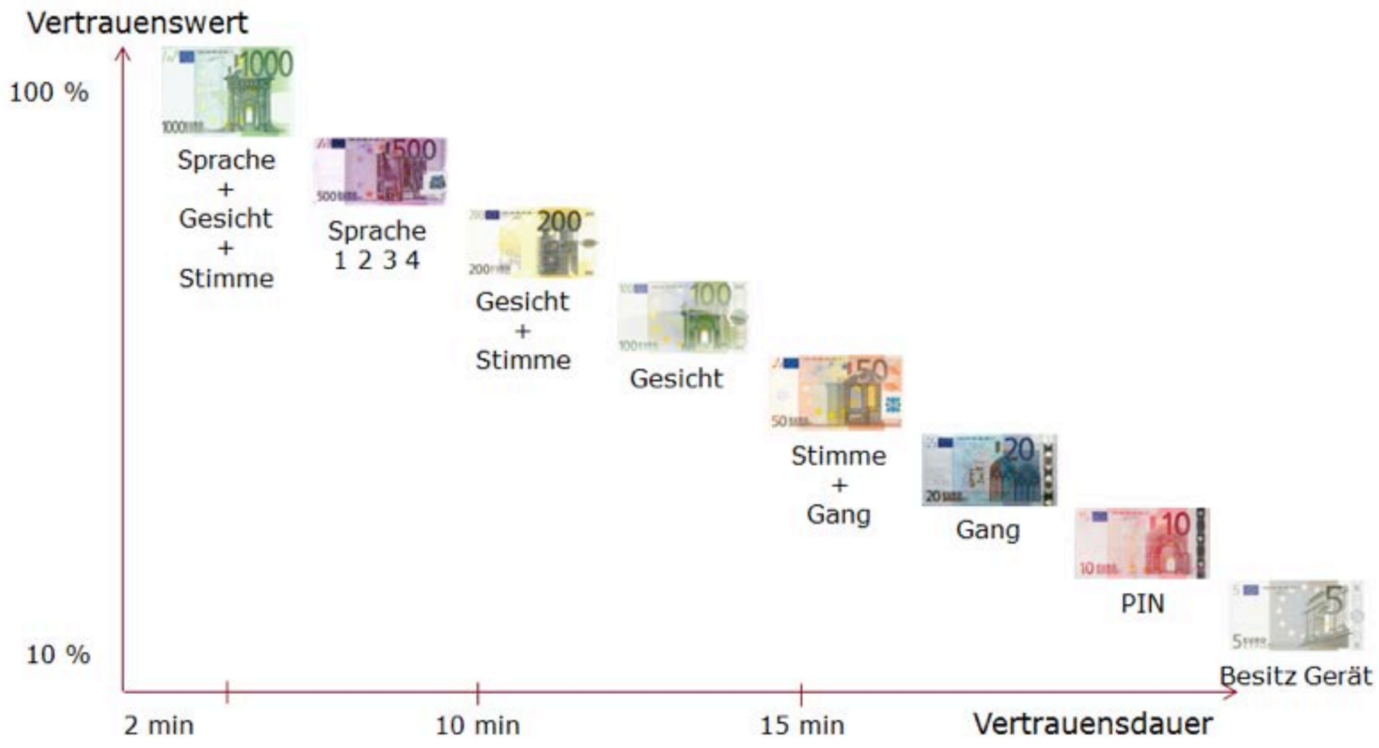


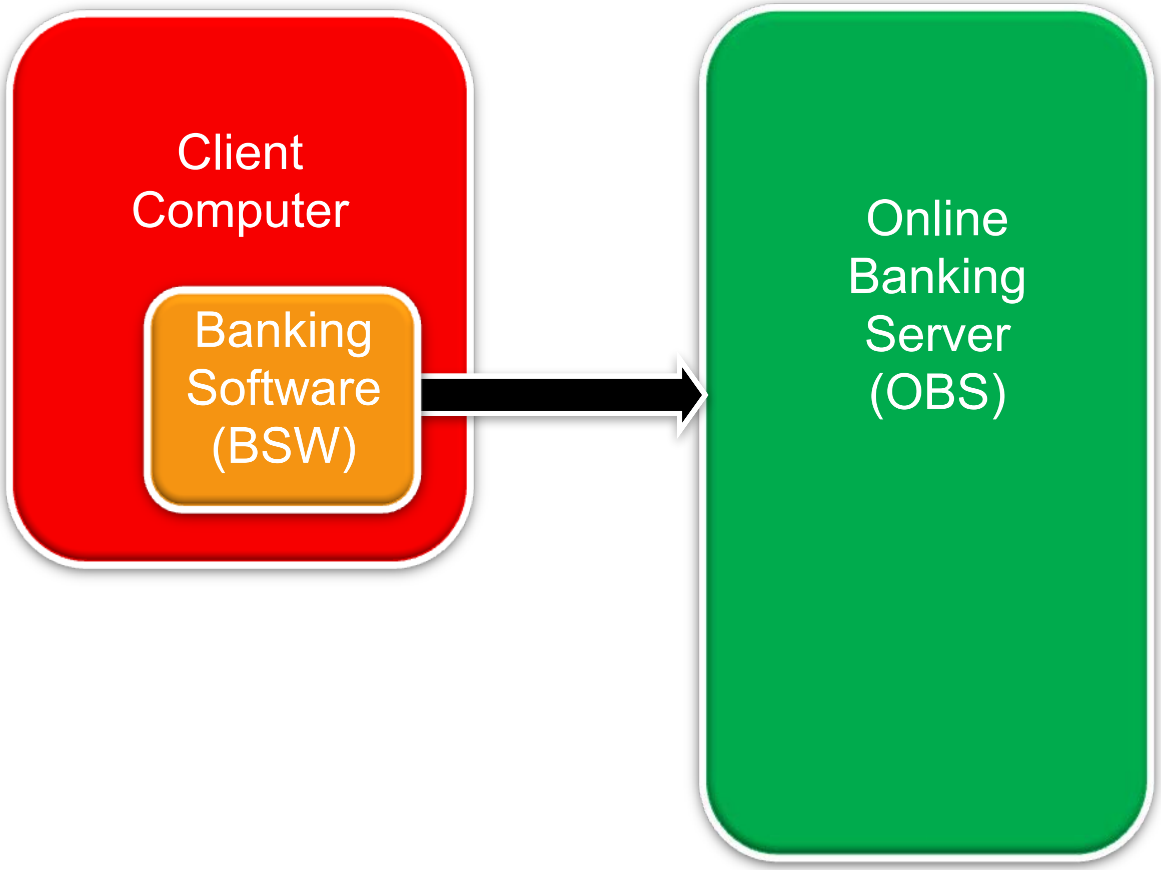
Image Source: BdB 2014

[Gru2014] W. Grudzien, „Synopse Biometrie – Update 2014"
Whitepaper Bundesverband Deutscher Banken, November 2014

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

Online-Banking-Scenario

Elements in the Online-Banking-Scenario:



Client Computer

Banking Software (BSW)

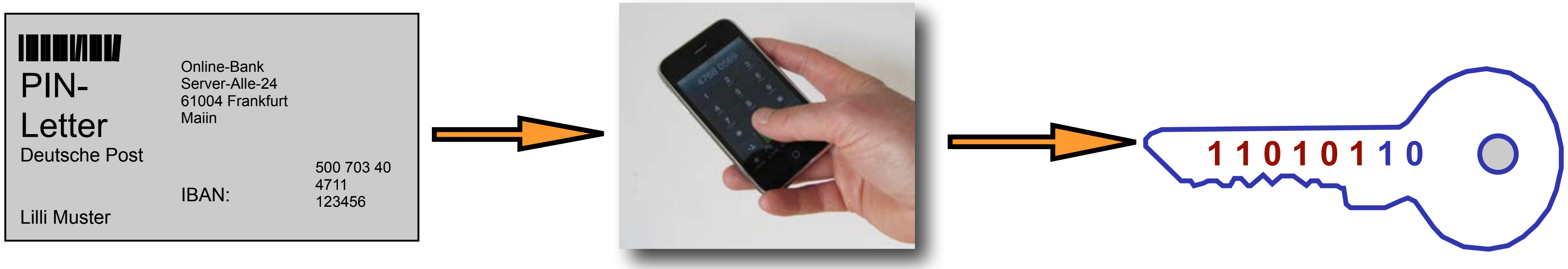
Online Banking Server (OBS)

Transaction-Authentication-Protocol

Biometric Transaction Authentication Protocol (BTAP)

1.) Shared secret

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



PIN-Letter
Deutsche Post
Lilli Muster

Online-Bank
Server-Alle-24
61004 Frankfurt
Maiin

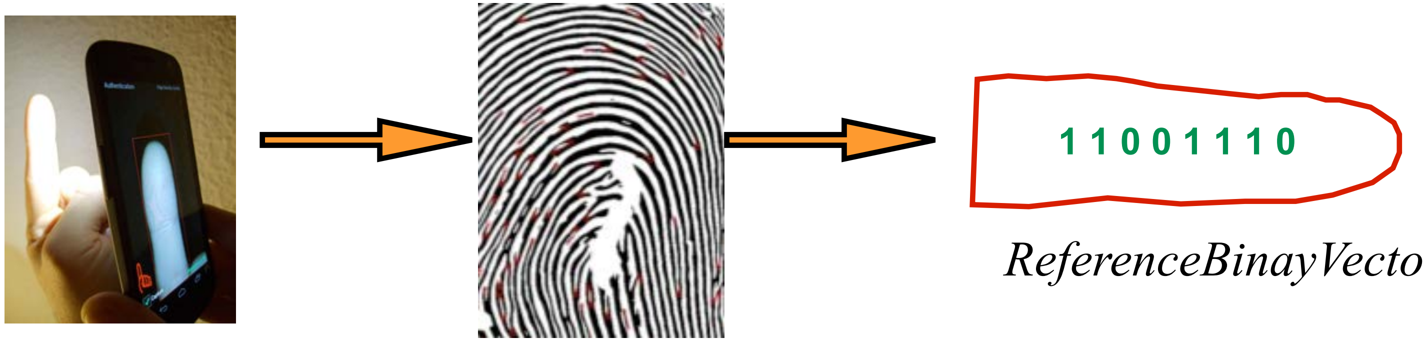
IBAN: 500 703 40
4711
123456

PIN = 4768

CodeBookVector (CBV)

2.) Biometric enrolment

- Biometric samples are captured



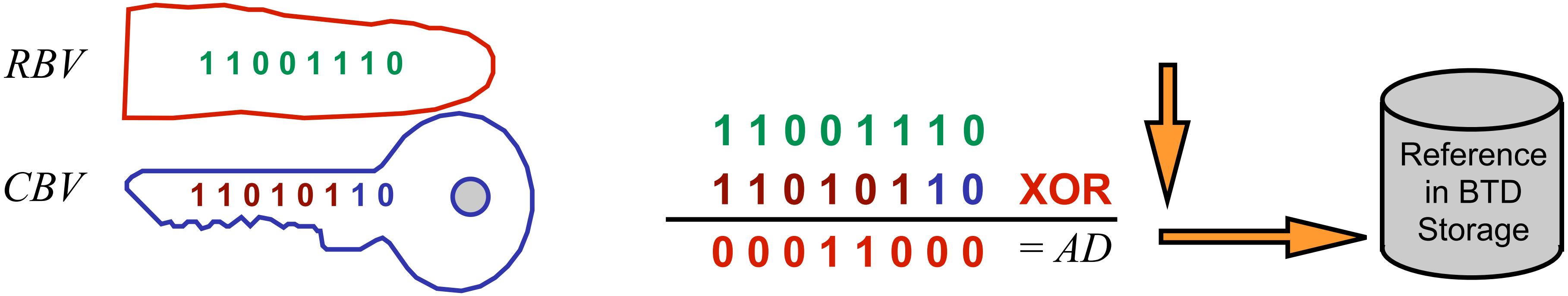
ReferenceBinayVector (RBV)

Transaction-Authentication-Protocol

Biometric Transaction Authentication Protocol (BTAP)

3.) Secure storage of auxilliary data

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



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

Transaction-Verification

BTAP - Transaction

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

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

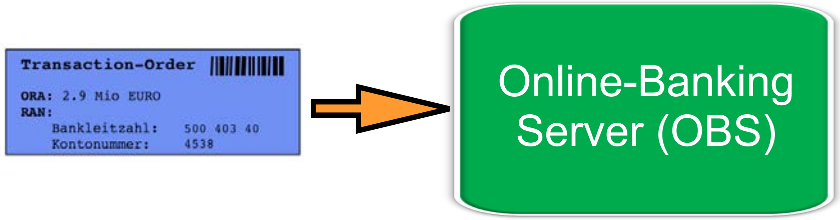
```
Transaction-Order

ORA: 2.9 Mio EURO
RAN:
    Bankleitzahl:    500 403 40
    Kontonummer:     4538
```

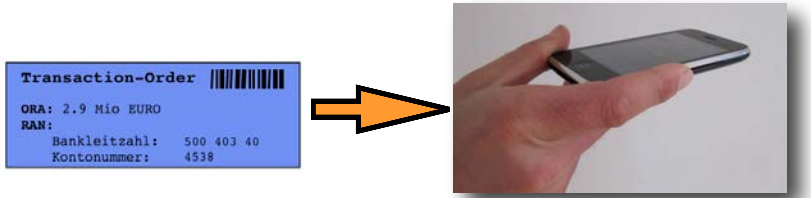
  This TOR consist of:

  - 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)

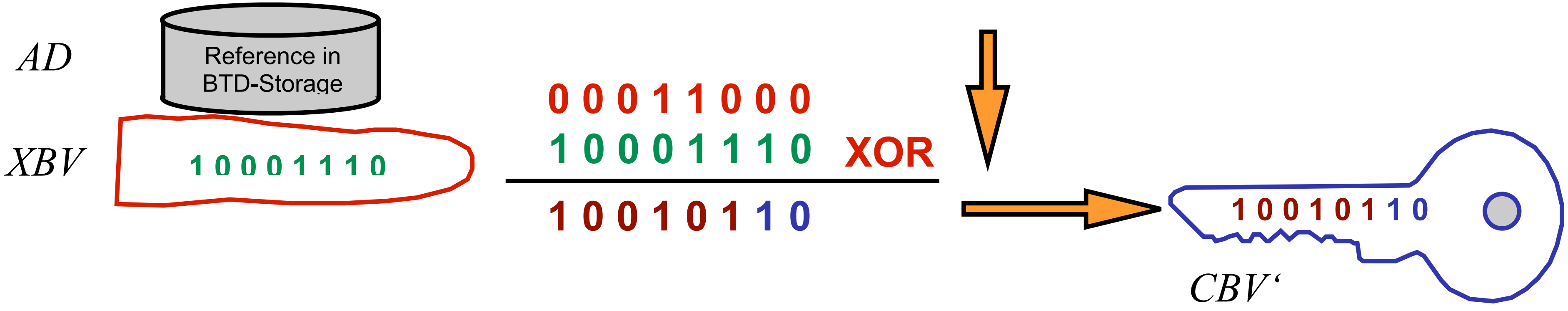


Transaction-Verification

BTAP - Transaction

2.) Operations on the Smartphone (BTD)

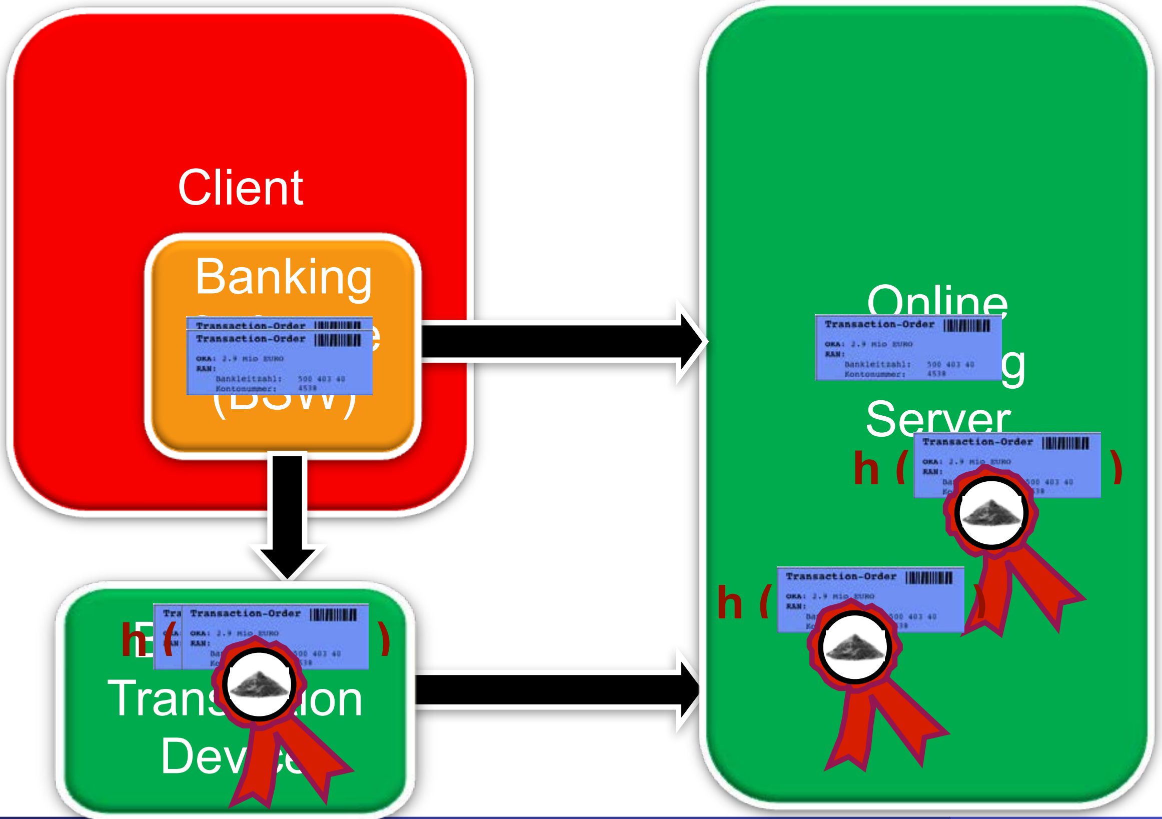
- Approval of the intended transaction by capturing a probe sample
- A secret vector *CBV‘* is reconstructed with XOR operation from the Auxilliary Data *AD* that was stored in the BTD and from the binarized feature vector *XBV*



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

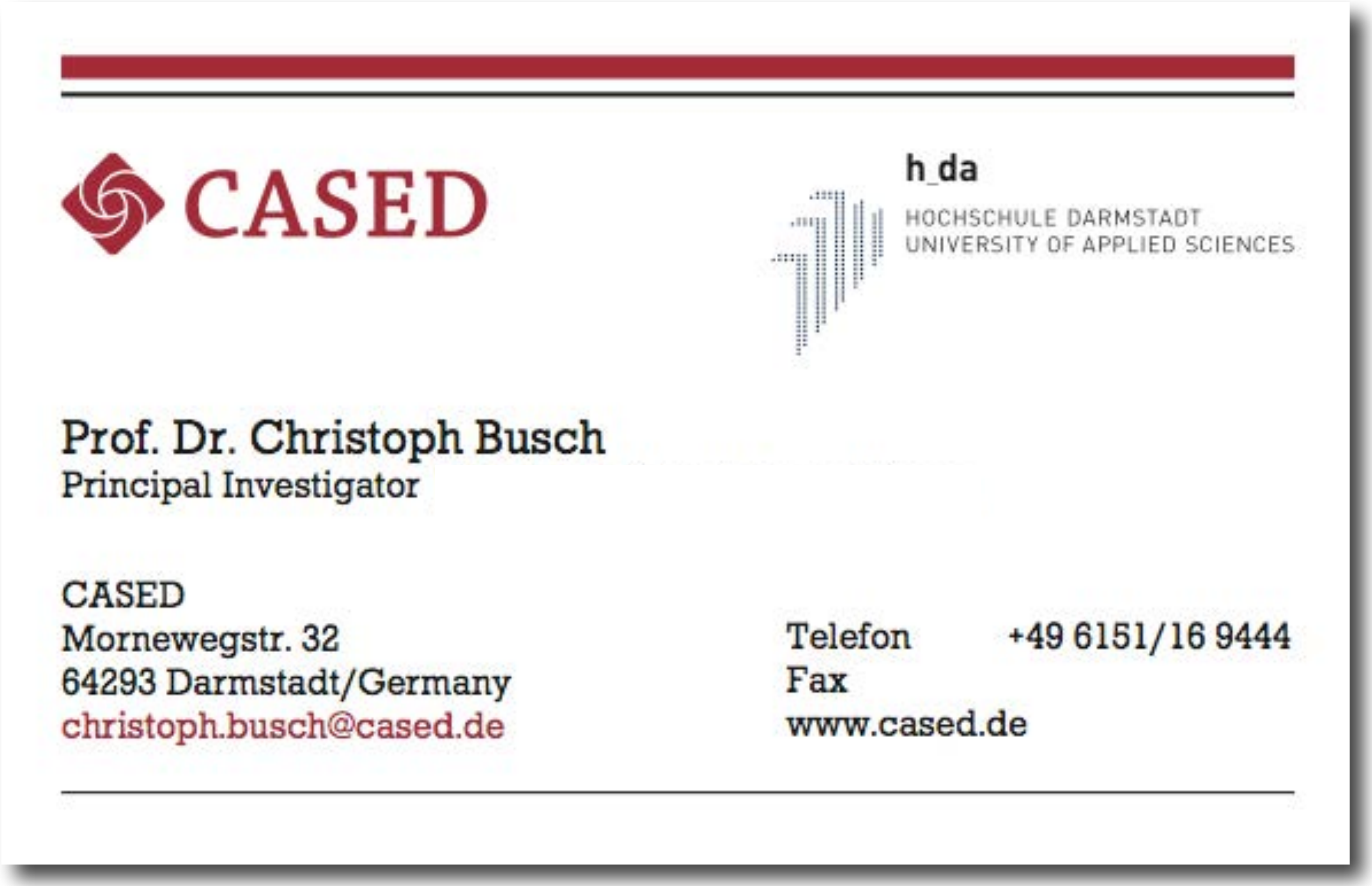
BTAP follows the two channel concept

- 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