# BTAP: Secure Authentication of Banking Transaction data using biometric Identifiers

Christoph Busch

European Association for Biometrics / Fraunhofer IGD
http://www.christoph-busch.de/about-talks-slides.html

Biometrics in Banking and Payments

London - October 16, 2015

European Association for Biometrics
eab
Human Identity in Europe

Fraunhofer IGD

# Agenda

- Mobile biometrics
- Requirements for secure and reliable biometrics
- Biometric Transaction Authentication Protocol (BTAP)
  - a proposal for a „European derivate of Apple Pay“

# 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

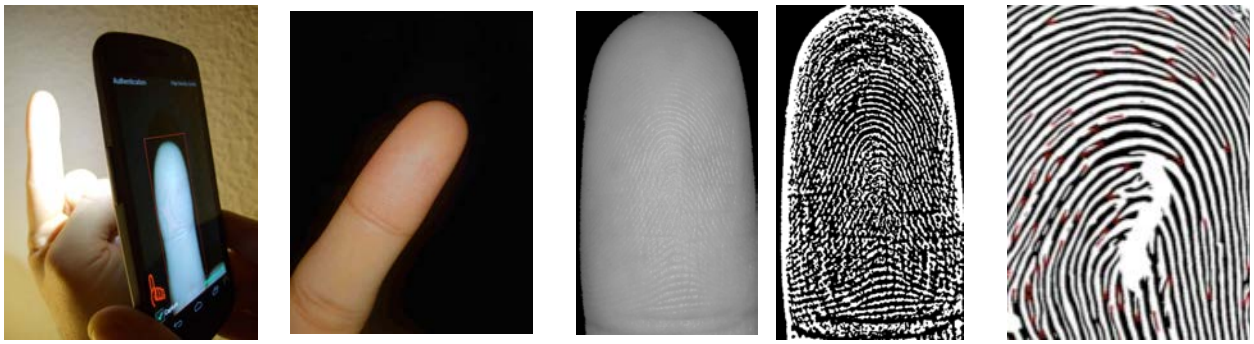
# Smartphone Access Control

## Capture process

- Camera operating in macro modus

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

- LED permanent on



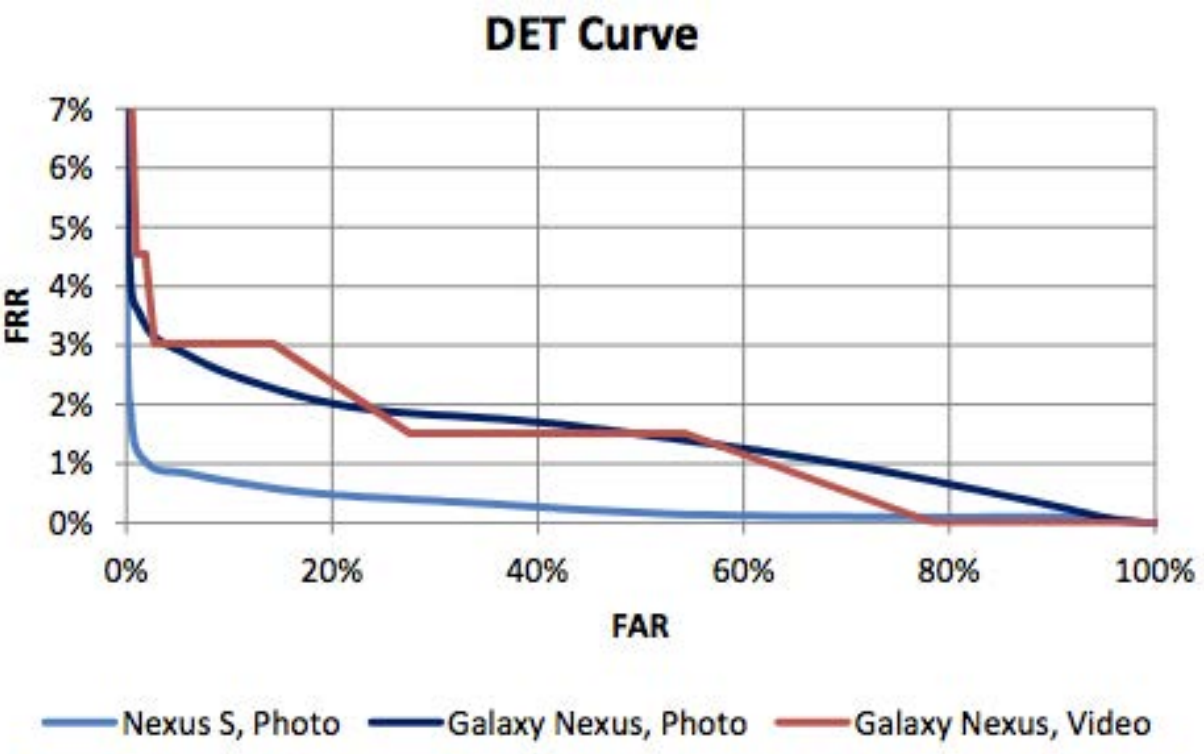
Finger illuminated

[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



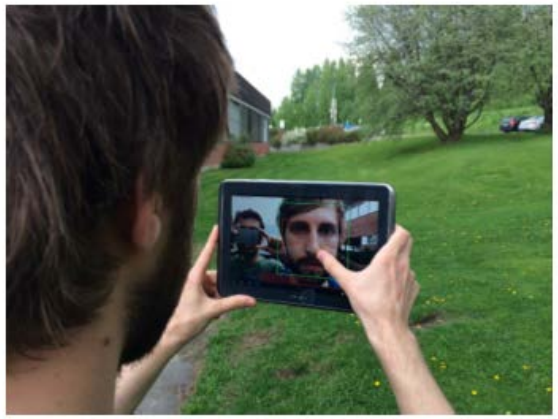

| Capture Method and Device | EER from [SC-2012] | EER | FRR (FAR=0.1%) |
|---|---|---|---|
| Photo, Nexus S | 22.3% | 1.2% | 2.7% |
| Photo, Galaxy Nexus | 19.1% | 3.1% | 6.7% |
| Video, Galaxy Nexus | - | 3.0% | 12.1% |

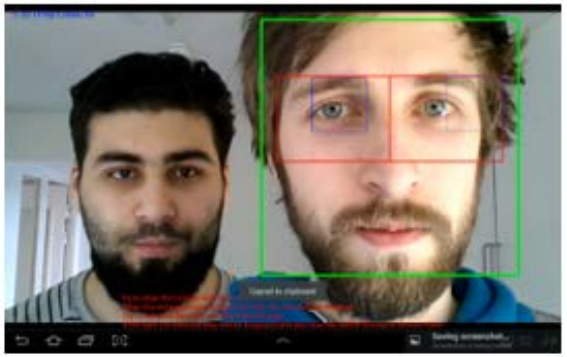
[SBB2013] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

# Biometric Eye Recognition

Images captured with either front or back camera

- Challenges
  - face and eye localization
  - feature extraction with SURF, SIFT und Binarized Statistical Image Features (BSIF)



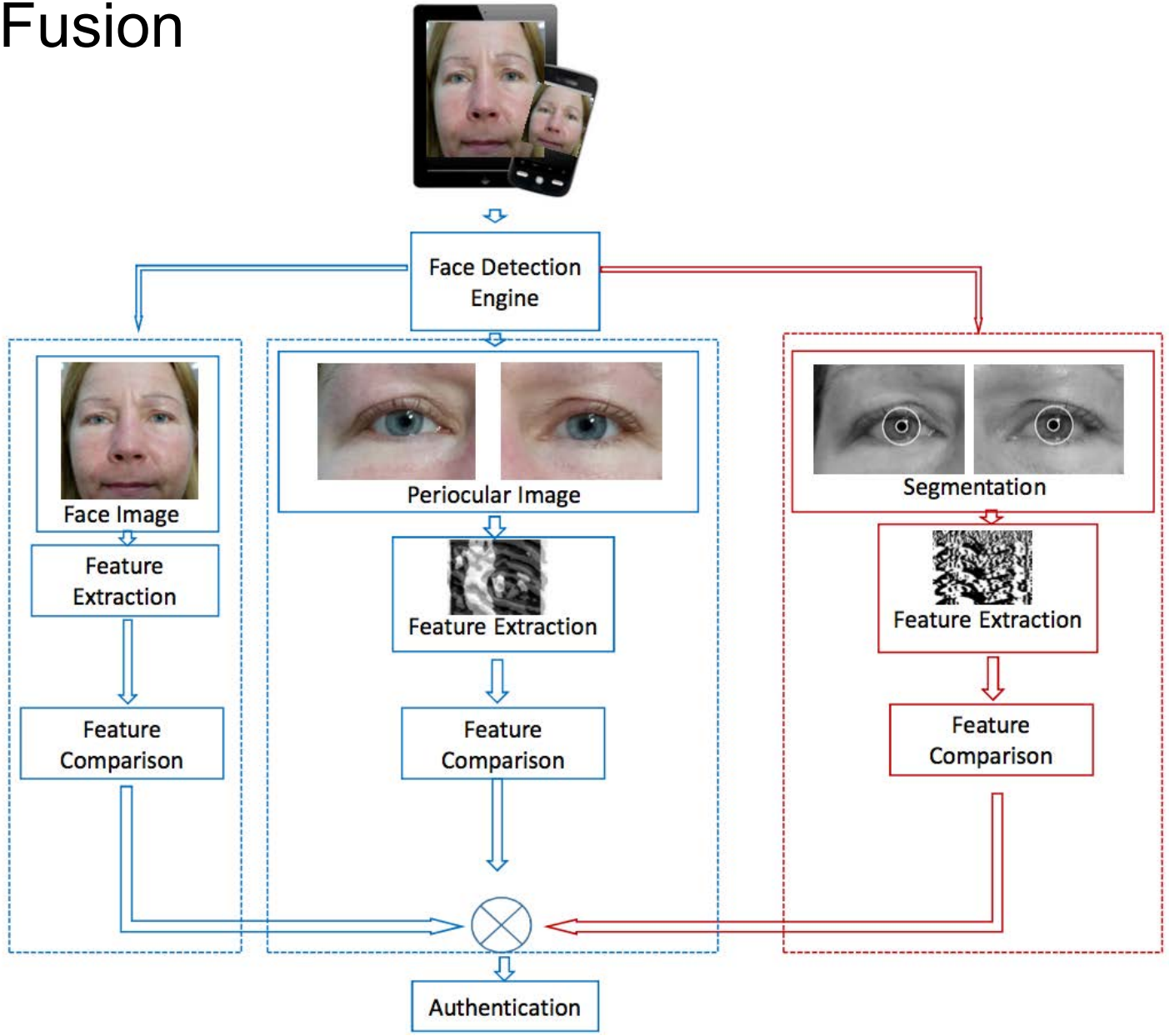


[KR12] J. Kannala and E. Rahtu. BSIF: „Binarized statistical image features“. ICPR conference, (2012)

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

# Biometric Face and Eye Recognition

## Multimodal Fusion



# Biometric Face and Eye Recognition

## Multimodal Fusion - Biometric Performance

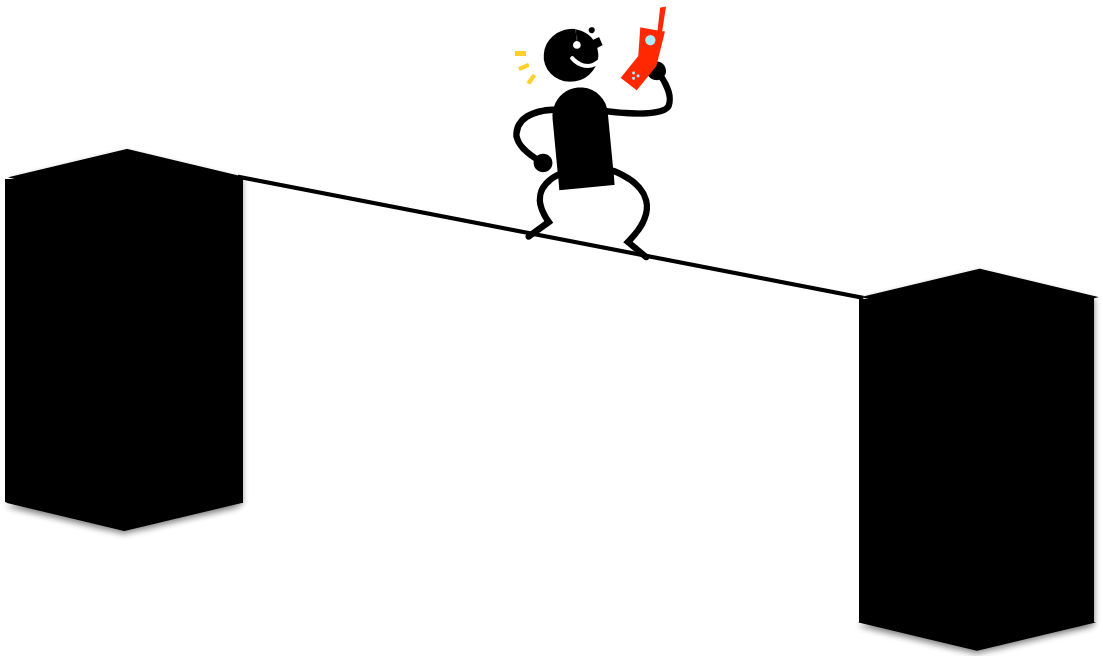
| Fusion Scheme | Camera | Samsung S5 | | Samsung Note | |
|---|---|---|---|---|---|
| | | GMR@FMR=0.01% | EER | GMR@FMR=0.01% | EER |
| Min Rule | Back Assisted | 99.17 | 0.43 | 88.57 | 3.43 |
| | Back | 97.12 | 0.93 | 88.13 | 4.34 |
| Max Rule | Back Assisted | 50.78 | 10.71 | 11.65 | 25.93 |
| | Back | 52.94 | 12.10 | 17.74 | 22.59 |
| Product | Back Assisted | 84.13 | 15.34 | 50.65 | 47.96 |
| | Back | 84.81 | 14.37 | 44.61 | 48.08 |
| Weighted Fusion | Back Assisted | **99.13** | **0.43** | **95.52** | **2.39** |
| | Back | **97.98** | **0.68** | **93.52** | **2.69** |

[RRB15] K. Raja, R. Raghavendra, C. Busch: " Multi-modal Authentication System for Smartphones", in Proceedings of the 8th IAPR International Conference on Biometrics (ICB), 19-22 May 2015, Phuket, Thailand, (2015)

# Requirements

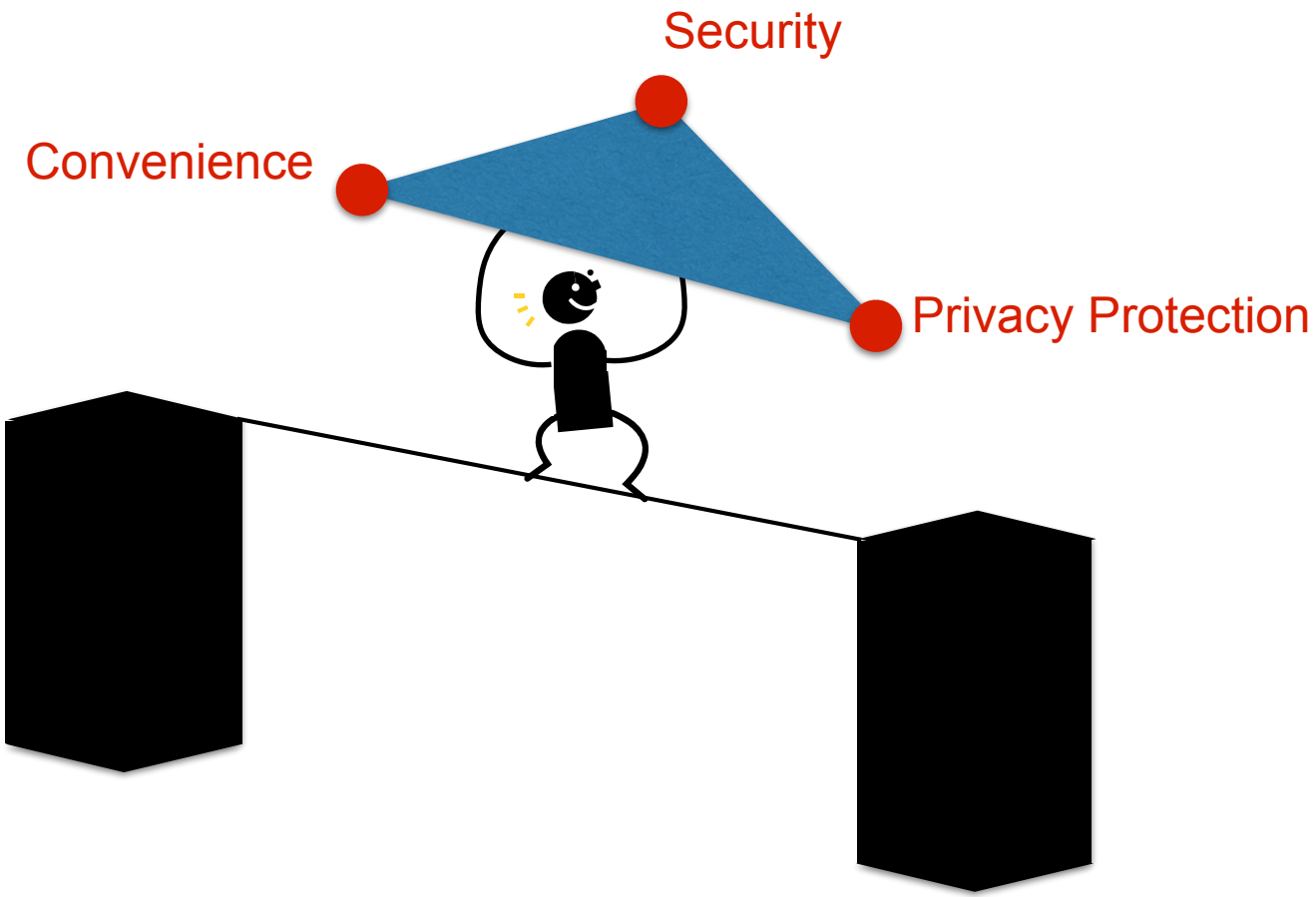
# Balance the Requirements

The requirements from operators / end-user



# Balance the Requirements

The requirements from operators / end-user



# Convenience ?

Operators will think:

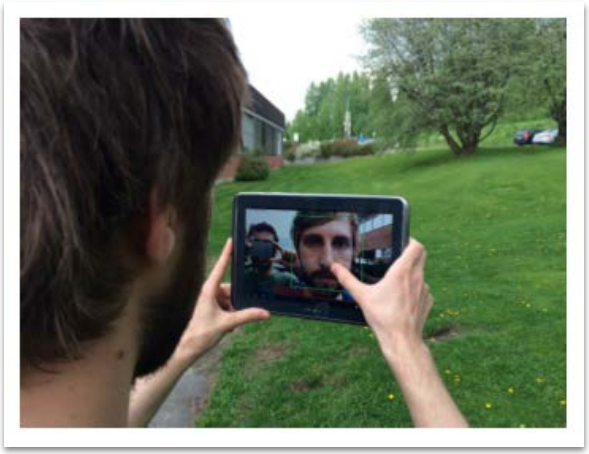
„*The biometric transactions system must be convenient for the end-user*“

# Convenience

Establish biometrics in the known environment

- No extra costs
- No extra training


Image Source: Apple 2013



# Security ?

Operators will think:

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

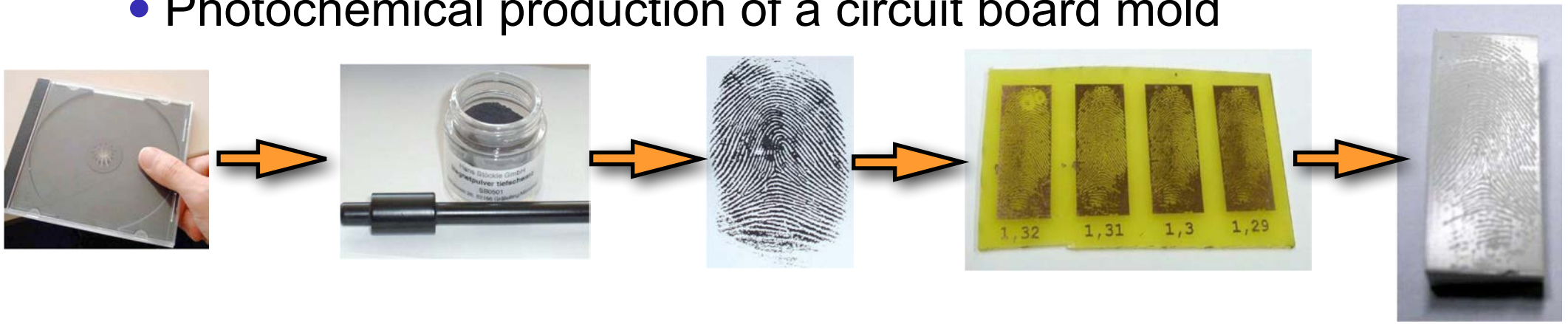
# Security ?

- Presentation Attacks

# Gummy Finger Production in 2000 !

Attack without support of an enroled individual

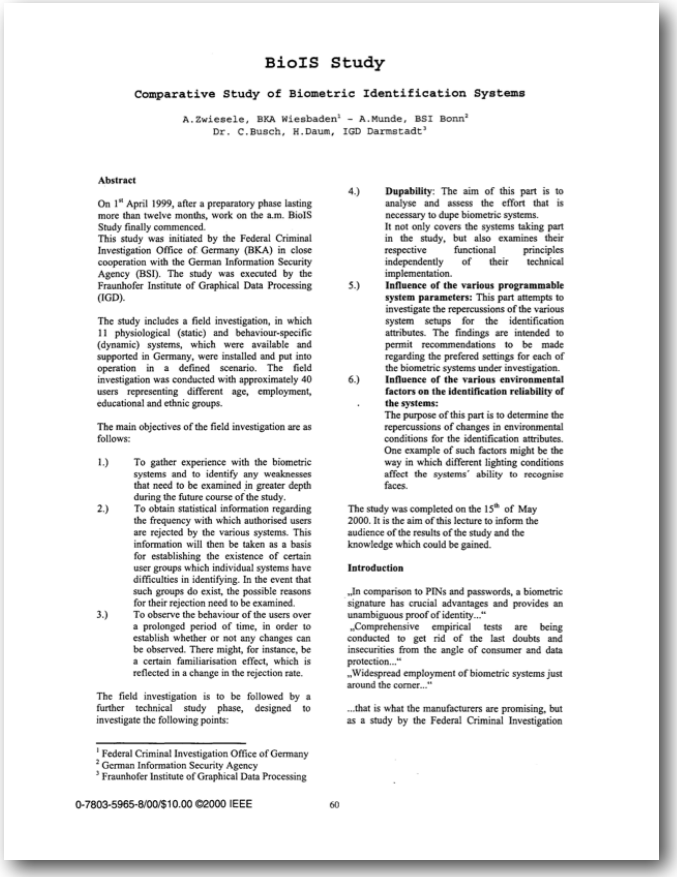
- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production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

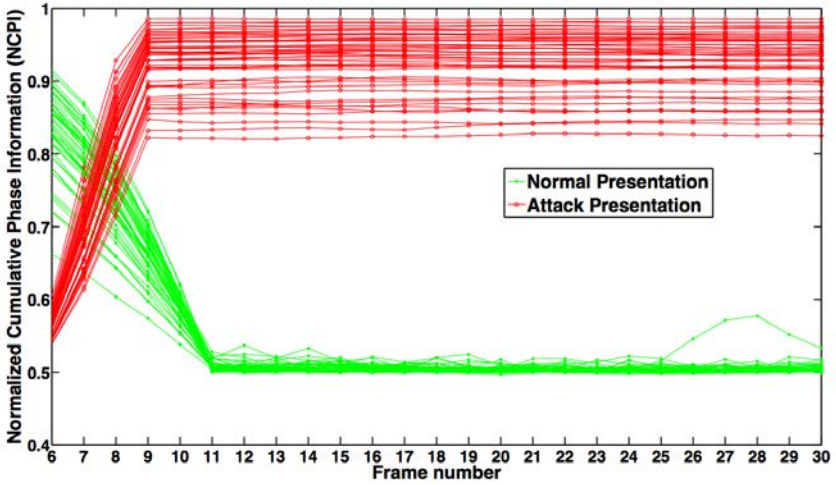
- **Normal presentation classification error rate (NPCER)**
  *proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario*

# 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




- 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 ?

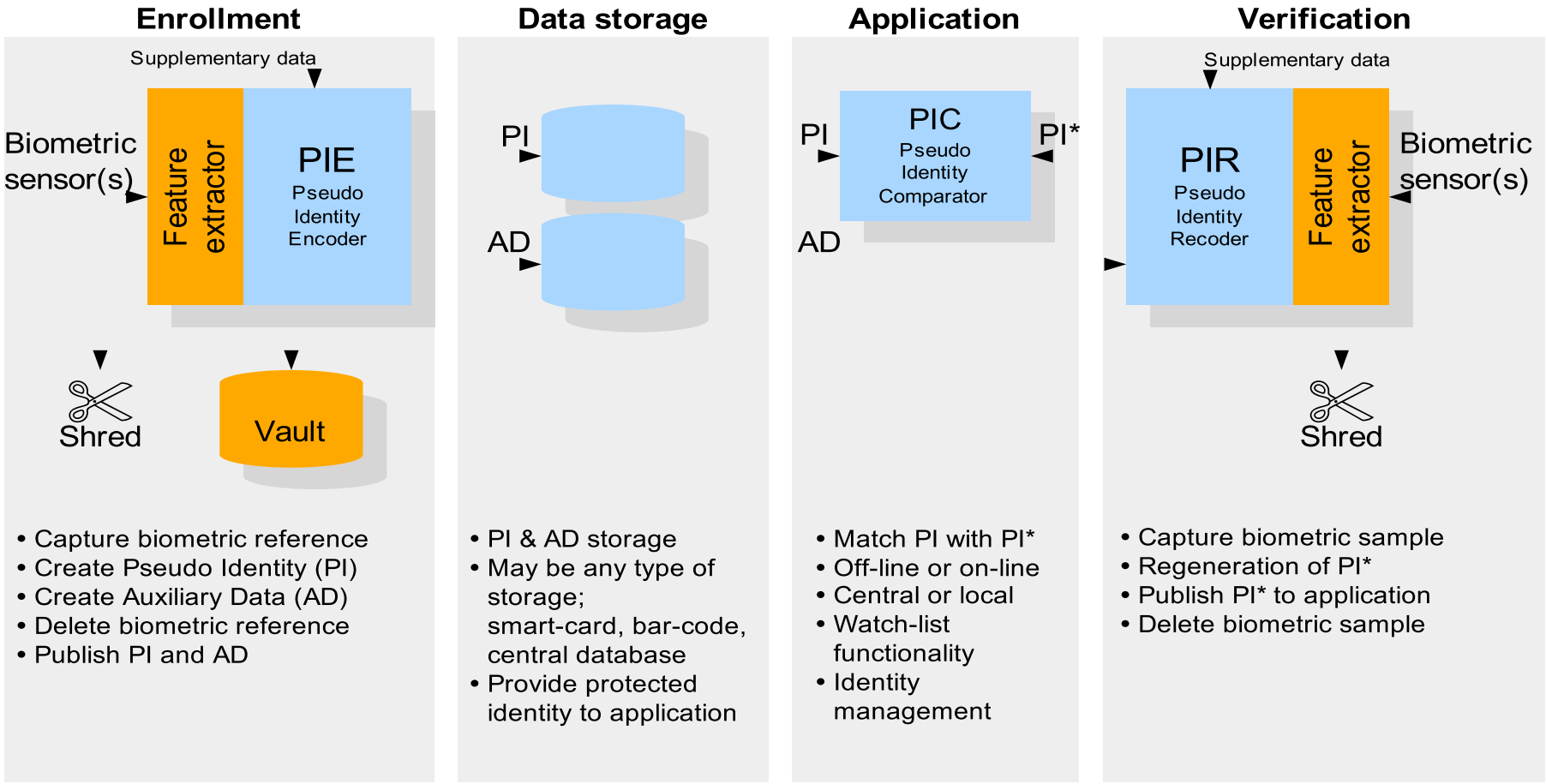
Operators will think:

*„Biometric systems must be compliant to data privacy and data protection principles“*

# 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



# Why multiple Modalities?

# Financial Transactions

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

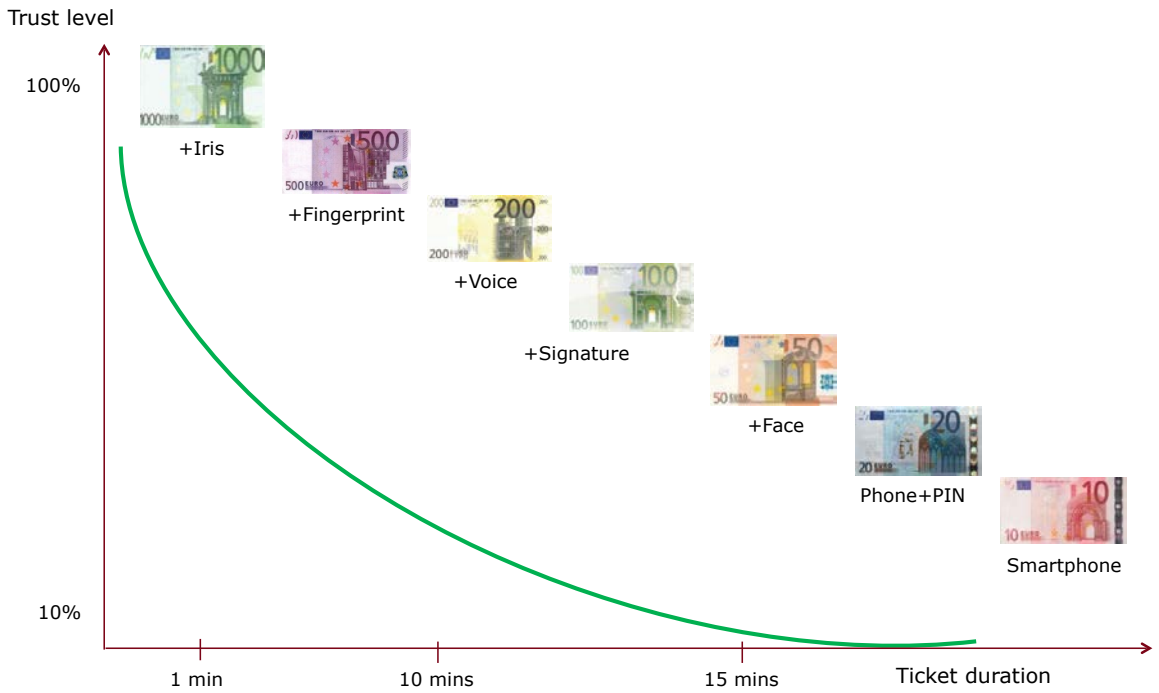



Image Source: BdB 2015

[Gru2015] W. Grudzien, „Current trends in the payments and transactions landscape" Bundesverband Deutscher Banken, October 2015

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

# Transaction-Authentication-Protocol

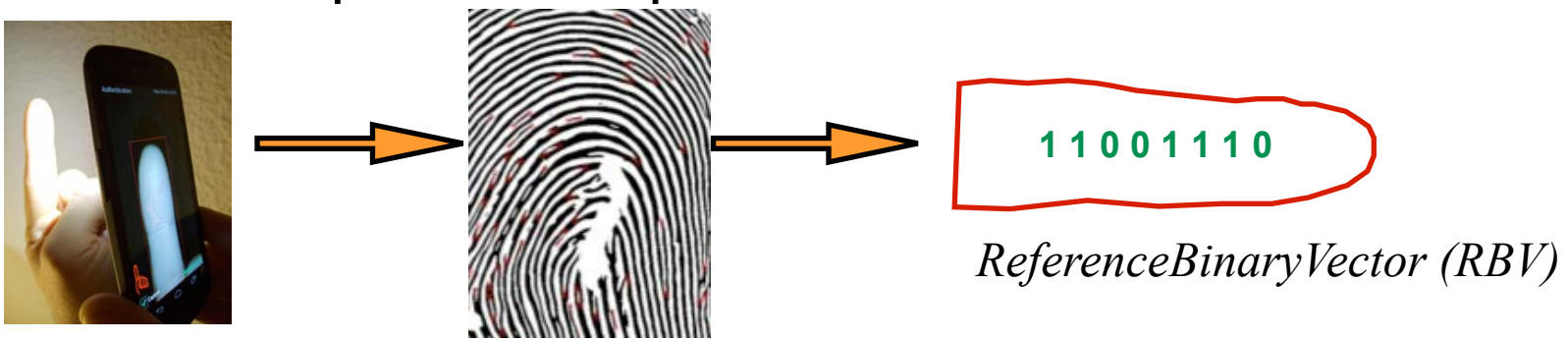
## Biometric Transaction Authentication Protocol (BTAP)

### 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

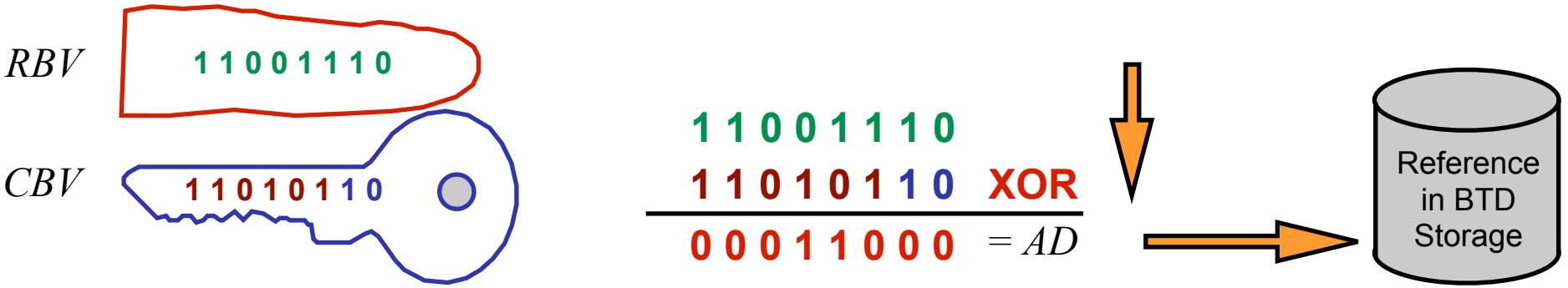


# Transaction-Authentication-Protocol

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



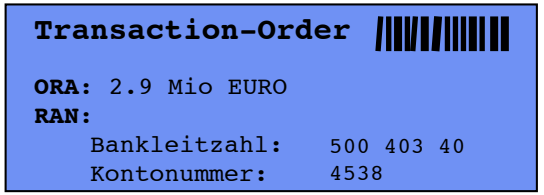

- Auxilliary data (AD) stored in the Smartphone
  - Biometric Transaction Device = FIDO Authenticator

# Transaction-Verification

## BTAP - Transaction

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

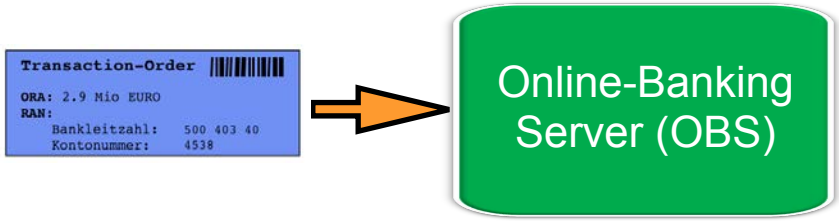
- Customer generates by interacting with the BSW-Software a new Transaction-Order-Record (TOR)



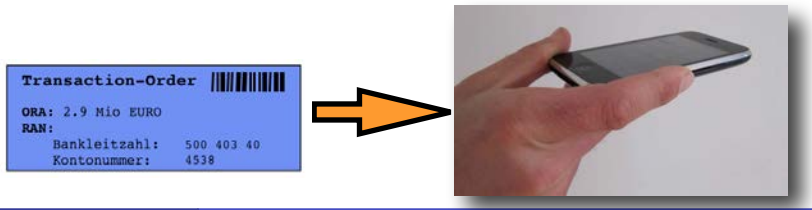

  This TOR consist of:

  - 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)

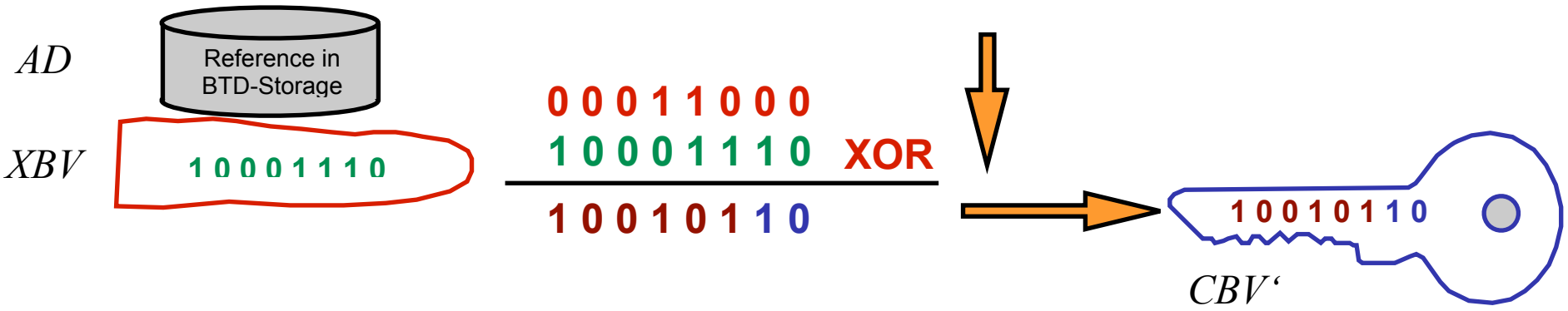


# Transaction-Verification

## 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 $XBV$



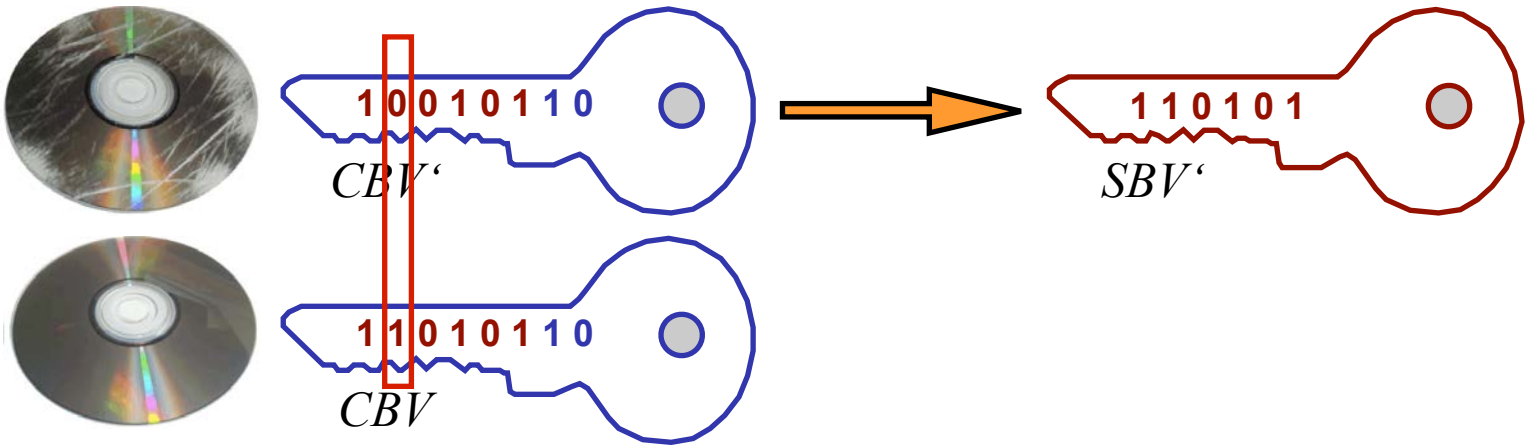
# Transaction-Verification

## 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 $CBV'$ 10010110 is reconstructed
- The secret key $SBV'$ is freshly re-computed from $CBV'$

$$SBV' = dec\,(CBV')$$



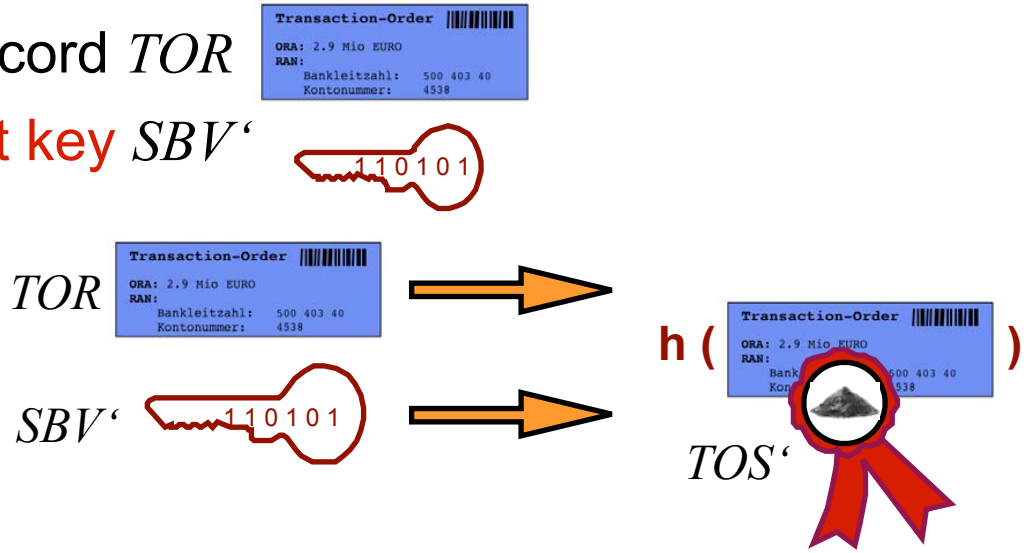
# Transaction-Verification

## BTAP - Transaction

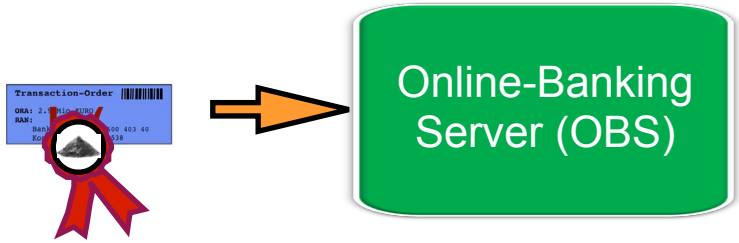
## 2.b ) Mirror-Operations of the BTD and the OBS

- 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‘) )*



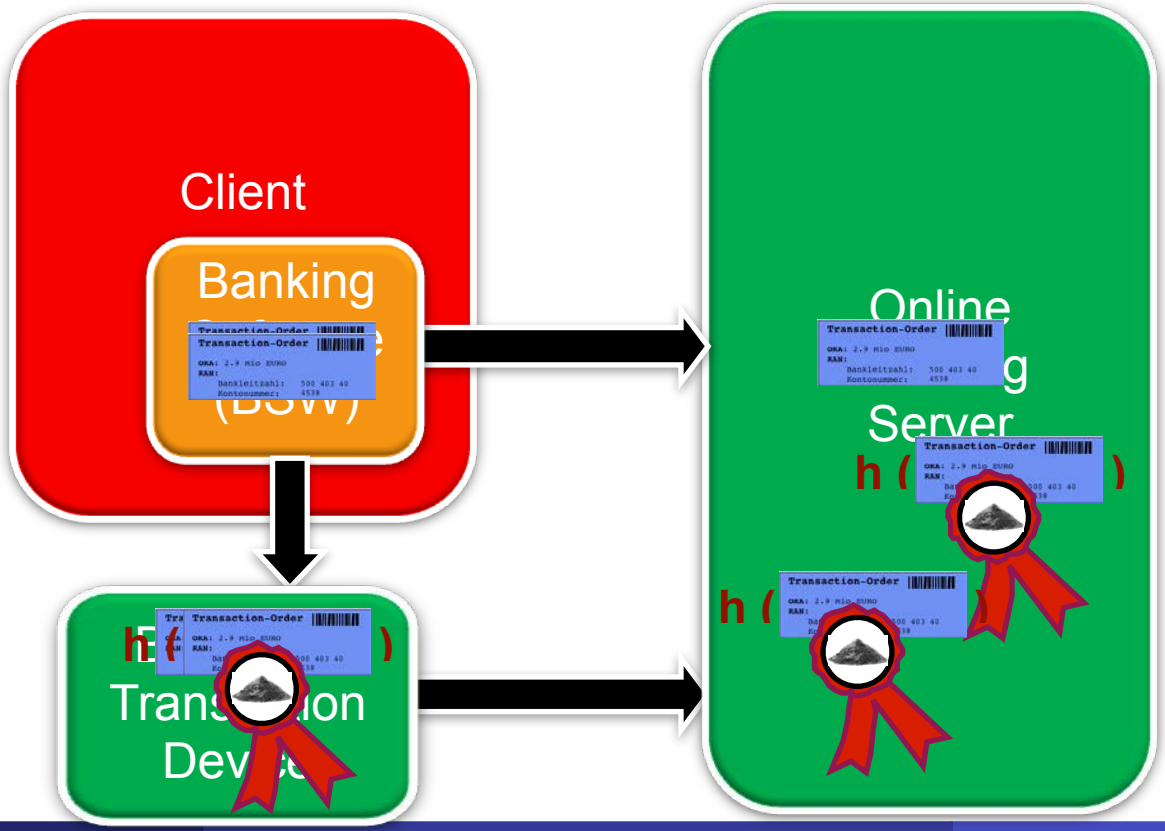

- The seal (TOS‘) is transferred to the Online-Banking-Server



# 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