

# Biometrisches Transaktions Authentisierungs Protokoll

Christoph Busch

Fraunhofer IGD / Gjøvik University College / Hochschule Darmstadt

12. Dezember 2011

# Risiken

## BSI: Warnt vor Gefahren im Online-Banking

The screenshot shows the BSI website interface. At the top, there is a navigation bar with links for 'Über das BSI', 'Service', 'Sitemap', and 'Kontakt & Impressum'. Below this is a banner image of a family and a cartoon dog with the slogan 'Ins Internet - mit Sicherheit!'. The main navigation area contains four buttons: 'Welche Gefahren begegnen mir im Netz?', 'Wie mache ich meinen PC sicher?', 'Wie bewege ich mich sicher im Netz?' (highlighted in blue), and 'Wie bewege ich mich sicher im mobilen Netz?'. A breadcrumb trail indicates the current path: 'Sie sind hier: > Startseite > Wie bewege ich mich sicher im Netz? > Online-Banking > Gefahren und Sicherheitsrisiken'. A search bar is located on the right. The left sidebar contains a menu with items like 'So kommen Sie in's Internet', 'Kommunikation über das Internet', 'Der neue Personalausweis', 'Einkaufen im Internet', 'Online-Banking' (highlighted), 'So funktioniert das Online-Banking', 'Gefahren und Sicherheitsrisiken' (highlighted), 'Sicherheitstipps', 'Was tun im Ernstfall?', and 'Der Staat online'. The main content area features the title 'Online-Banking - Gefahren und Sicherheitsrisiken' and an introductory paragraph about internet criminals. It lists several risks: Phishing with E-Mails, Phishing with Trojans, Datendiebstahl in Internetcafés, Angriffe auf das WLAN, and Angriffe auf das Mobile Banking.

Über das BSI | Service | Sitemap | Kontakt & Impressum

Ins Internet - mit Sicherheit!

Welche Gefahren begegnen mir im Netz? | Wie mache ich meinen PC sicher? | **Wie bewege ich mich sicher im Netz?** | Wie bewege ich mich sicher im mobilen Netz?

Sie sind hier: > [Startseite](#) > [Wie bewege ich mich sicher im Netz?](#) > [Online-Banking](#) > Gefahren und Sicherheitsrisiken

Suchbegriff eingeben

### Wie bewege ich mich sicher im Netz?

- So kommen Sie in's Internet
- Kommunikation über das Internet
- Der neue Personalausweis
- Einkaufen im Internet
- Online-Banking**
- So funktioniert das Online-Banking
- Gefahren und Sicherheitsrisiken**
- Sicherheitstipps
- Was tun im Ernstfall?
- Der Staat online

### Online-Banking - Gefahren und Sicherheitsrisiken

Betrüger sind leider oft sehr kreativ – gerade, wenn es um Bankgeschäfte geht. Mit unterschiedlichen Methoden versuchen Internet-Kriminelle, an Ihre Bankdaten heranzukommen, um Transaktionen auf eigene Konten umzuleiten. Hier stellen wir Ihnen einige weitverbreitete Angriffsmethoden vor.

- **Phishing mit E-Mails:** Ziel des Phishings ist es, Ihre Kontodaten, die PIN und TANs auszuspionieren. Dafür verschicken die Kriminellen gefälschte E-Mails von Banken, in denen die Kunden aufgefordert werden, ihre Kontonummer, PIN und einige TANs zum Beispiel per E-Mail oder über eine Webseite zu übermitteln. Mit diesen Daten können die Kriminellen dann Transaktionen vornehmen. Deshalb denken Sie immer daran: Ihre Bank wird niemals per E-Mail Ihre PIN und TANs erfragen.
- **Phishing mit Trojanern:** Hierbei infizieren die Kriminellen den Computer ihres Opfers mit einem Schadprogramm (Trojaner), das unbemerkt den Datenverkehr ins Internet überwacht. Erkennt das Schadprogramm eine Banktransaktion, manipuliert es den Betrag und die Kontonummer des Empfängers und leitet das Geld so zu den Angreifern um. Der Bankkunde merkt davon zunächst nichts, weil der Trojaner ihm eine ordnungsgemäß durchgeführte Transaktion vorgaukelt. Erst auf dem ausgedruckten Kontoauszug wird der Schaden sichtbar.
- **Datendiebstahl in Internetcafés:** Internet-Browser speichern Daten der letzten Verbindungen in ihrem „→ Cache“ – einer Art Zwischenspeicher – ab. Wer Bankgeschäfte im Internetcafé abwickelt, riskiert also, dass Kriminelle diese Informationen im Cache auslesen. Darum gilt: Wickeln Sie möglichst keine Bankgeschäfte auf fremden PCs ab – und wenn es sich doch mal nicht vermeiden lässt, löschen Sie den Cache unbedingt.
- **Angriffe auf das WLAN:** WLAN-Schnittstellen bieten Angriffsflächen, etwa für das Einschleusen von Schadprogrammen. Falls Sie Ihre Bankgeschäfte über eine WLAN-Schnittstelle abwickeln, achten Sie deshalb darauf, dass diese ausreichend abgesichert ist.
- **Angriffe auf das Mobile Banking:** Alle Gefahren, die Sie vom Online-Banking mit dem Computer kennen

# Warum Biometrie?

Personen-Authentisierung durch:

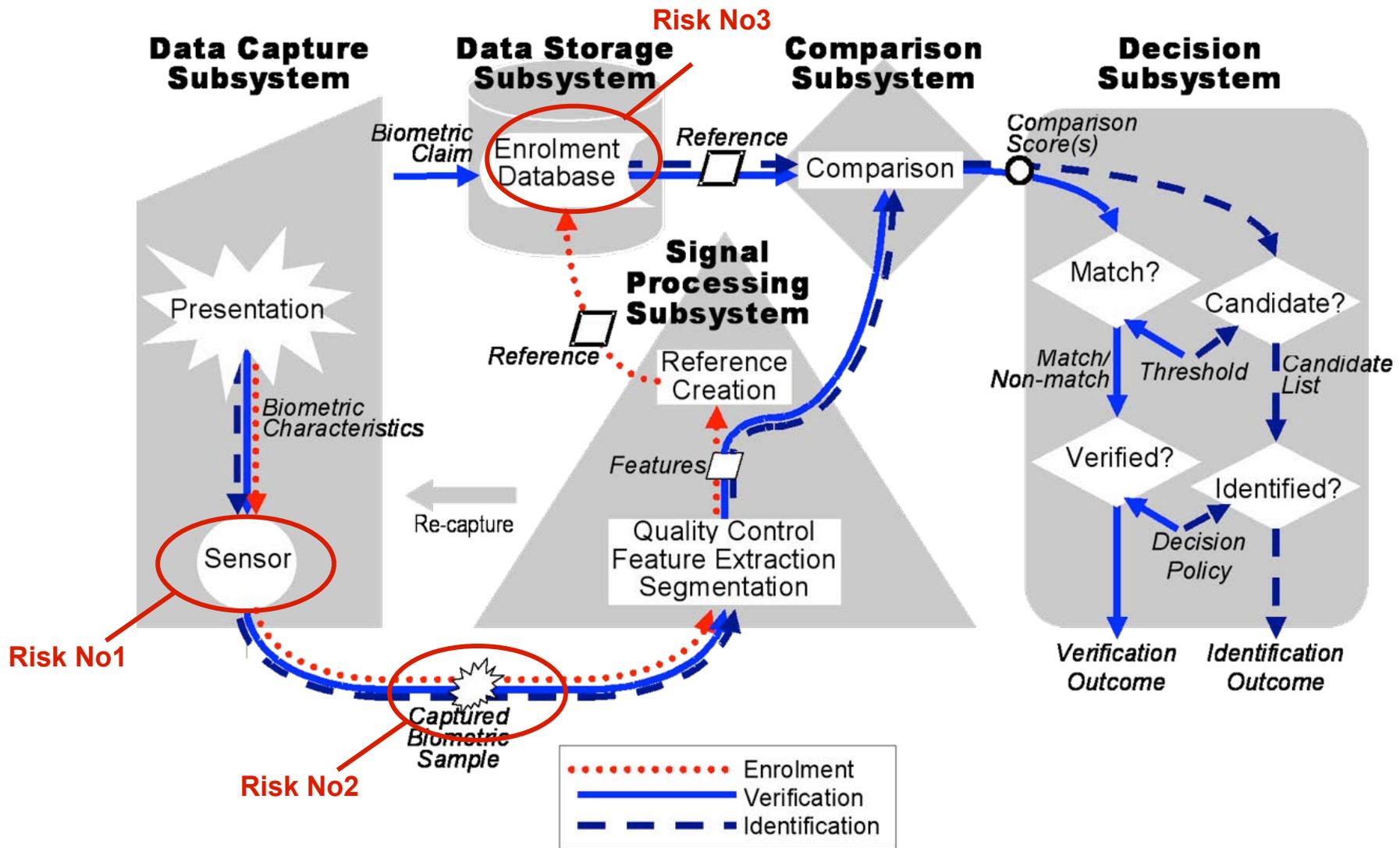
- Wissen: Passwort, PIN, sonstiges Geheimnis
- Besitz: Magnet- oder Chipkarte, Schlüssel
- Kennzeichen: biometrische Charakteristik

Wissen oder Besitz kann man leicht **verlieren, vergessen** oder **weitergeben**,  
biometrische Charakteristika nicht ohne weiteres.

Vorteile

- Sicherheitspolitik kann nicht durch Delegation umgangen werden!
- Eine Transaktion kann nicht abgestritten werden
  - „das muss *Igor Popov* mit meiner Karte gewesen sein ...“

# Risiken in Biometrischen Systemen



Source: ISO/IEC JTC1 SC37 SD11 Reference Architecture

# Replikate von Biometrischen Charakteristiken und Fake Finger Attacks

# Angriffe durch Replikate

## Gummi-Finger

**SKorean fools finger printing system at Japan airport: reports** 

Thu Jan 1, 2:57 pm ET  Buzz Up |  Send |  Share |  Print



TOKYO (AFP) – A South Korean woman barred from entering Japan last year passed through its immigration screening system by using tape on her fingers to fool a fingerprint reading machine, reports said Thursday.

The biometric system was installed in 30 airports in 2007 to improve security and prevent terrorists from entering into Japan, the [Yomiuri Shimbun](#) said.

The woman, who has a deportation record, told investigators that she placed special tapes on her fingers to pass through a [fingerprint reader](#), according to [Kyodo News](#).

Japan spent more than four billion yen (44 million dollars) to install the system, which reads the index fingerprints of visitors and instantly cross-checks them with a database of international fugitives and foreigners with deportation records, the Yomiuri Shimbun said.

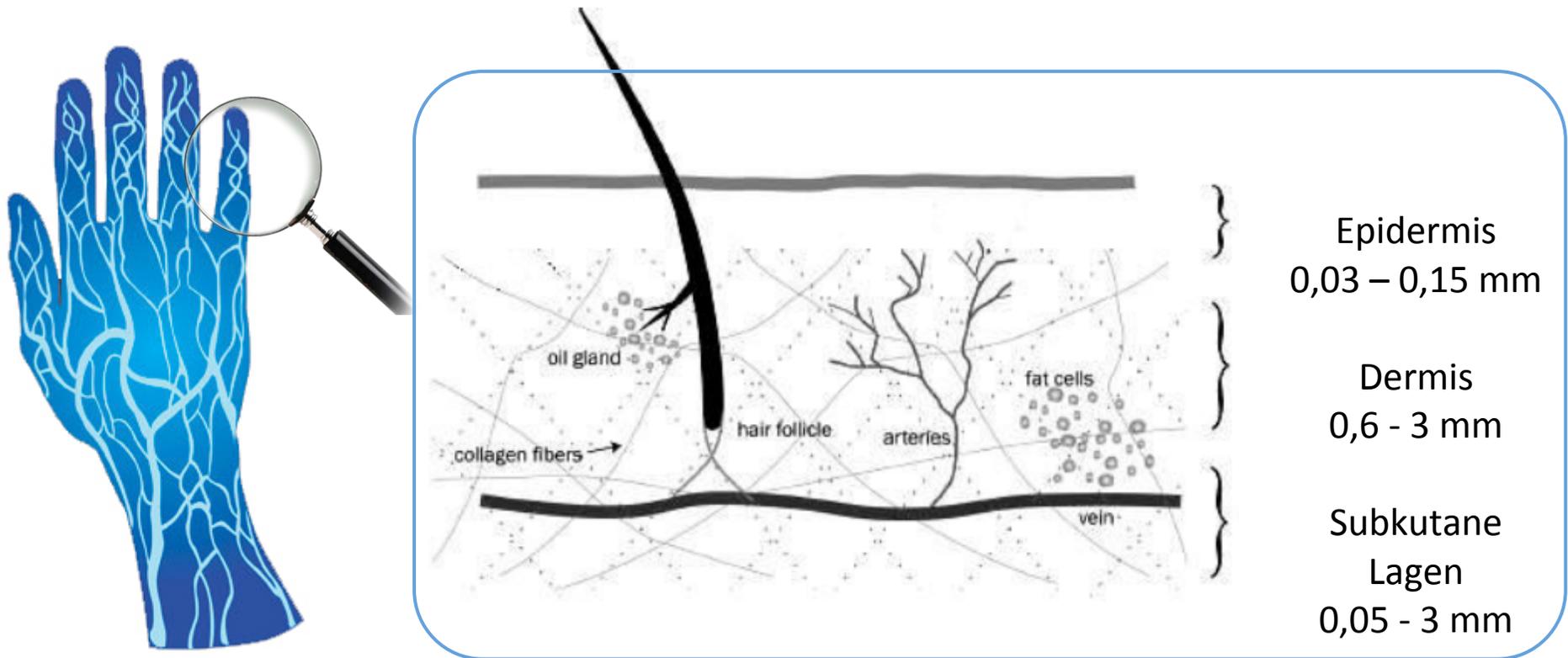
AFP/File – A woman uses a biometric scanner at an airport. A South Korean woman barred from entering Japan last ...

Yahoo News am 1. Januar 2009

# Venenerkennung

## Aufnahme des Venenbildes

- Venen liegen unter der Haut
- Querprofil der Haut



# Venenerkennung

## Systeme

- Hitachi, Sony (Finger)
- Fujitsu, TechSphere (Handfläche)
- basierend auf "kontaktlosen" optischen Sensoren



Hitachi Fingervenen-Scanner



Sony Fingervenen-Scanner



Fujitsu Handflächen-Scanner



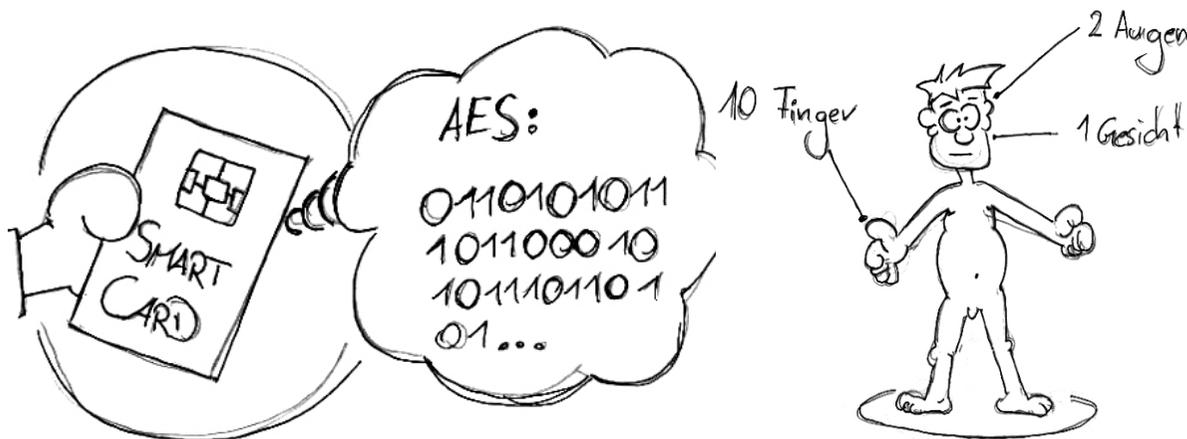
# Speicherung von Biometrischen Referenzen

# Risiken für Biometrische Daten

## Mögliche Angriffe auf Referenzdaten

- **Cross-Matching**: Identische Templates können ungewünschte Querverbindungen zwischen verschiedenen Datenbanken herstellen.
- **Renewability**: Die biometrische Charakteristik selbst kann nicht erneuert werden (Rückrufprinzip!)
- **Zusatzinformation**: über medizinischen Zustand

Kryptographische Verschlüsselung liefert keinen ausreichenden Schutz!



# Template Protection

Ansatz analog zur UNIX Password Authentisierung

- Öffentlich zugängliche Datei: /etc/passwd

`id:<login_name>:hash(password)`

- Authentisierung:

`hash(input) == hash(password) ?`

- Kollisionsarme Einwegfunktion:



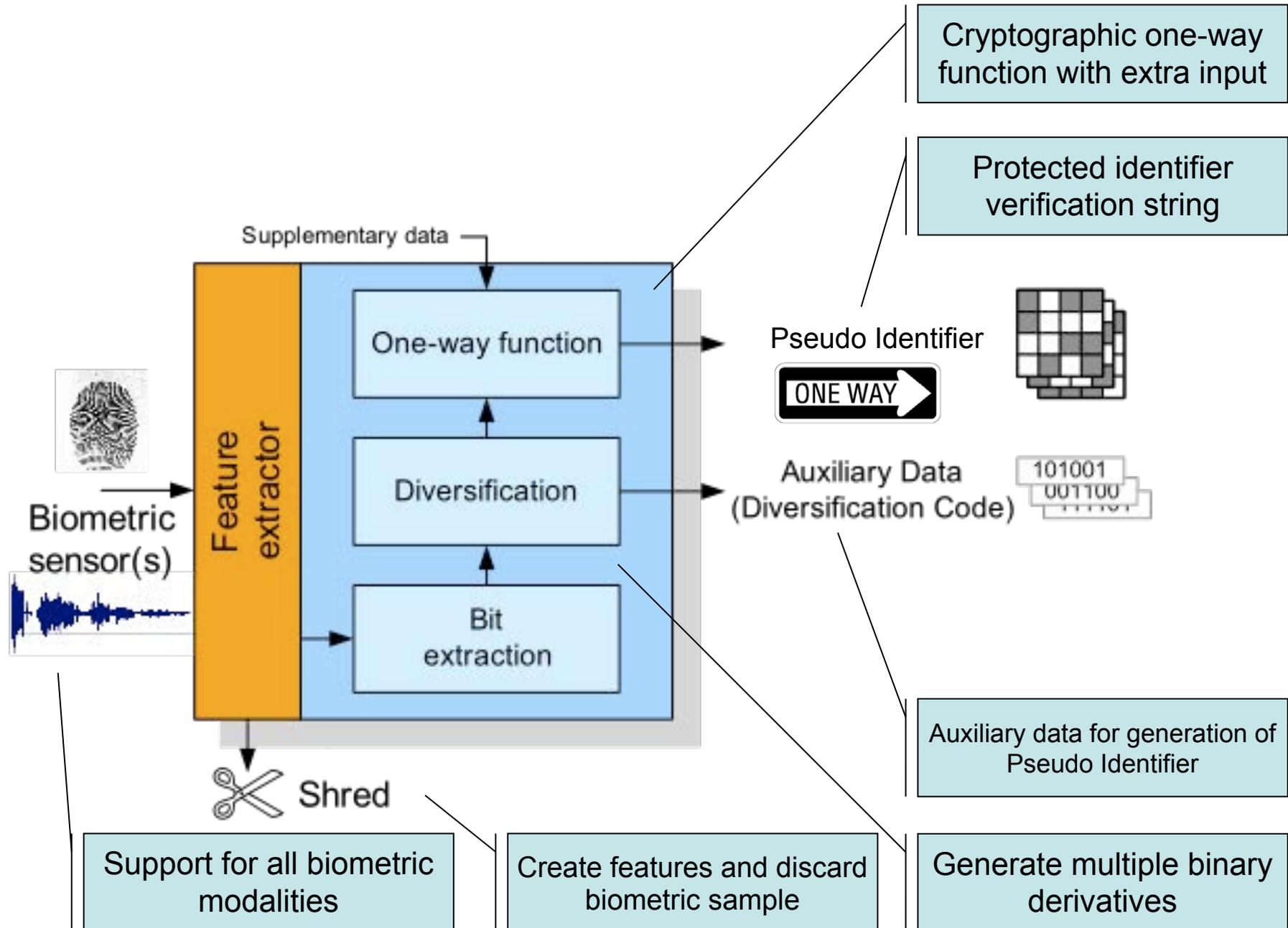
# Herausforderung

## Unterschied zwischen Passwörtern und biometrischen Samples

- Biometrische Messungen sind von Rauschen beeinflusst
- Kryptographische Einwegfunktionen sind extrem **sensitiv** gegenüber kleinsten Änderungen in den Eingabedaten

$h(01000101)$  ist ungleich  $h(01010101)$

# Template Protection in ISO 24745



# Biometrisches-Transaktions-Authentisierungs- Protokoll (BTAP)

# Ziel

## Biometrische Transaktions Authentisierung

- für Online-Banking Szenarien

## Transaktions-Authentisierung

- **Personen** Authentisierung
  - Nachweis, dass ein registrierter Bank-Kunde und **nur** dieser eine Transaktion initiiert hat
- **Daten** Authentisierung
  - Der registrierte Bank-Kunde hat die **Transaktionsdaten** gesehen und die Transaktion **autorisiert**

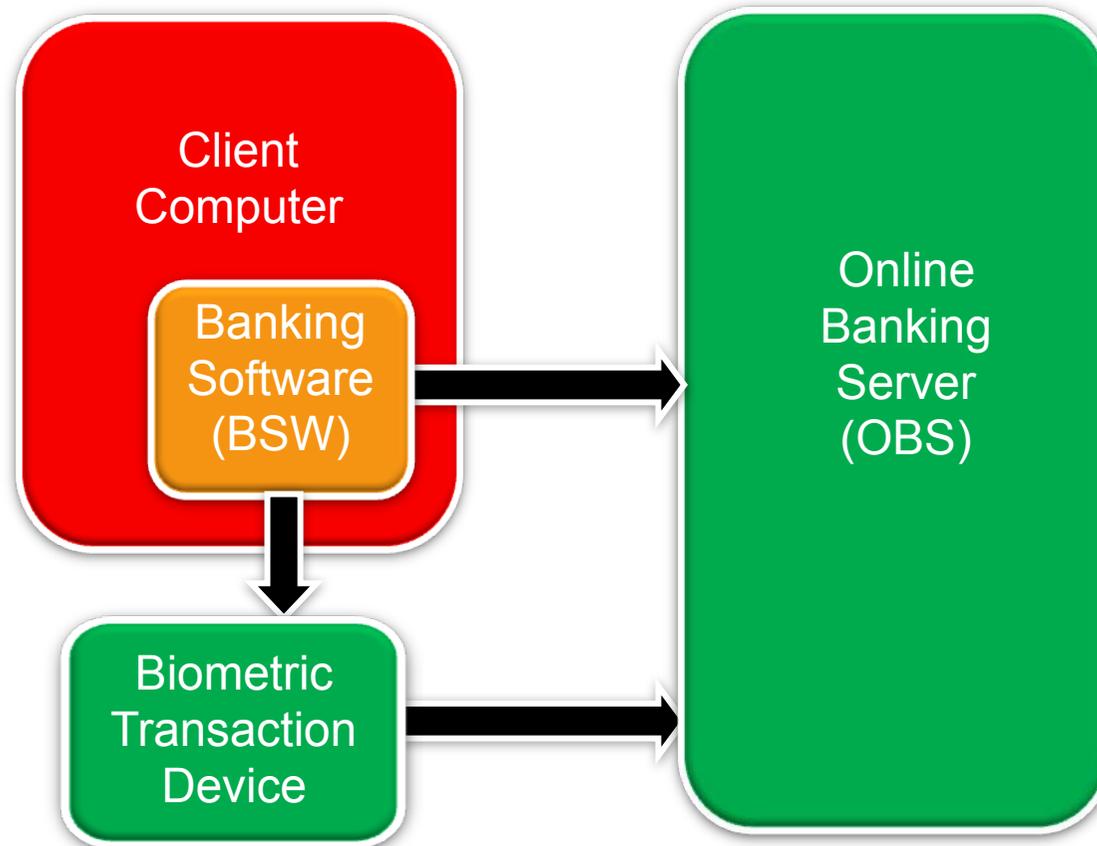
# Finanztransaktionen

Bei vielen Finanztransaktionen sind die relevanten Informationen:

- Welches Empfänger-Konto erhält eine Gutschrift?
  - Receiver-Account-Number (RAN)
- Welcher Betrag soll dem Empfänger gutgeschrieben werden?
  - Ordered Amount (ORA)
- Welches Sender-Konto erhält eine Belastung?
  - Sender-Account-Number (SAN)
- Welche natürliche Person hat die Transaktion initiiert und die Transaktionsdaten bestätigt?

# Online-Banking-Szenario

Für das Online-Banking existiert:

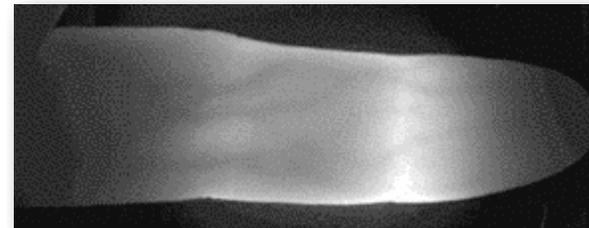


# Transaktions-Authentisierungs-Protokoll

## BTAP - Enrolment

### 1.) Enrolment im **Biometric Transaction Device** (BTD)

- Biometrische Samples des Kunden werden mit BTD erfasst



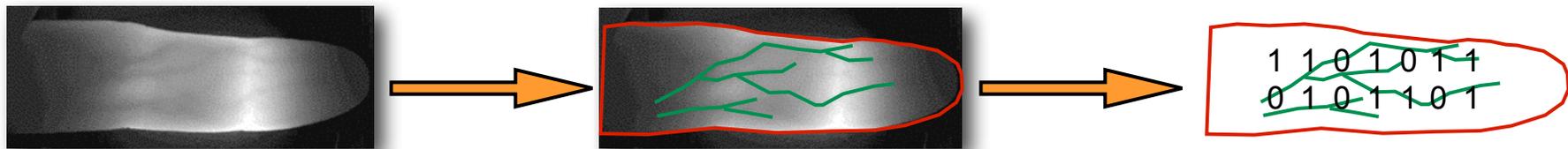
Source: [http://images.pennnet.com/articles/lfw/thm/th\\_121040.gif](http://images.pennnet.com/articles/lfw/thm/th_121040.gif)

# Transaktions-Authentisierungs-Protokoll

## BTAP - Enrolment

### 1.) Enrolment im Biometric Transaction Device (BTD)

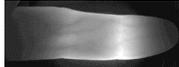
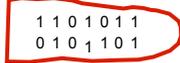
- Biometrische Samples  werden mit BTD erfasst
- Quantisierter Binärvektor wird aus den Merkmalen erzeugt

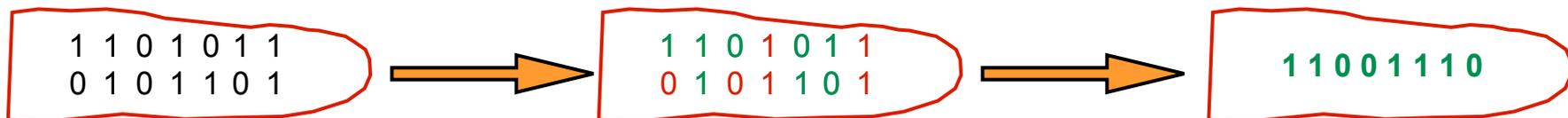


# Transaktions-Authentisierungs-Protokoll

## BTAP - Enrolment

### 1.) Enrolment im Biometric Transaction Device (BTD)

- Biometrische Samples  werden mit BTD erfasst
- Quantisierter Binärvektor  wird aus Merkmalen erzeugt
- Binärvektor wird auf stabile Merkmale reduziert (*RBV*) und die **relevanten Positionen** (AD1) gespeichert



Merke Auxilliary Data (AD1): Bit-Indices = 0,1,2,4,5,8,11,12

# Transaktions-Authentisierungs-Protokoll

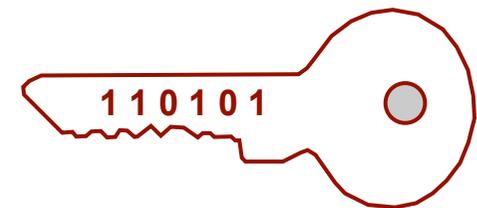
## BTAP - Enrolment

### 1.) Enrolment im Biometric Transaction Device (BTD)

- Biometrische Samples  werden mit BTD erfasst
- Quantisierter Binärvektor  wird aus Merkmalen erzeugt
- Binärvektor wird auf stabile Merkmale reduziert (*RBV*)  und die relevanten Positionen (*ADI*) gespeichert {0,1,2,4,5,8,11,12}
- Kunde bekommt Postbrief mit PIN und gibt diese **einmalig** ein



PIN = 4768 0569



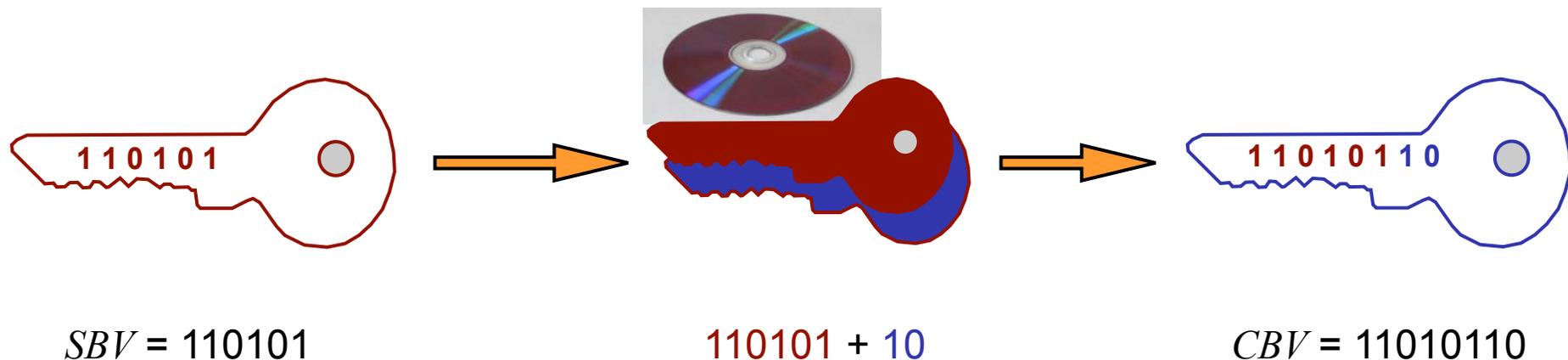
*SBV* = 110101

# Transaktions-Authentisierungs-Protokoll

## BTAP - Enrolment

### 1.) Enrolment im Biometric Transaction Device (BTD)

- Biometrische Samples  werden mit BTD erfasst
- Quantisierter Binärvektor  wird aus Merkmalen erzeugt
- Binärvektor wird auf stabile Merkmale reduziert (*RBV*)  und die relevanten Positionen (*ADI*) gespeichert  $\{0,1,2,4,5,8,11,12\}$
- Postbrief mit PIN liefert einen Schlüssel 
- Geheimvektor *CBV* wird aus dem Schlüssel durch Fehlerkorrekturverfahren ermittelt

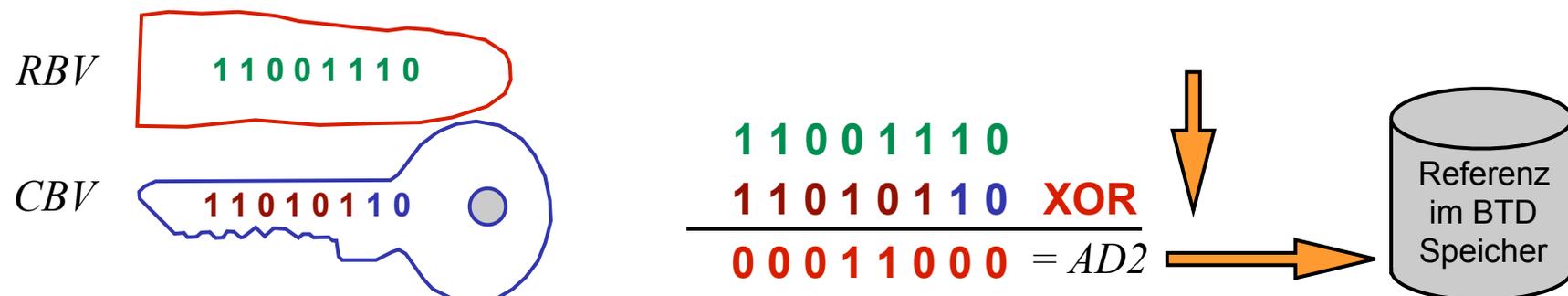


# Transaktions-Authentisierungs-Protokoll

## BTAP - Enrolment

### 1.) Enrolment im **Biometric Transaction Device** (BTD)

- Biometrische Samples  werden mit BTD erfasst
- Quantisierter Binärvektor  wird aus Merkmalen erzeugt
- Binärvektor wird auf stabile Merkmale reduziert (*RBV*)  und die relevanten Positionen (*ADI*) gespeichert  $\{0,1,2,4,5,8,11,12\}$
- Postbrief mit PIN liefert einen Schlüssel 
- Geheimvektor *CBV*  wird ermittelt
- Reduzierter Binärvektor *RBV* wird mit Geheimvektor *CBV* durch eine **XOR** Operation verknüpft



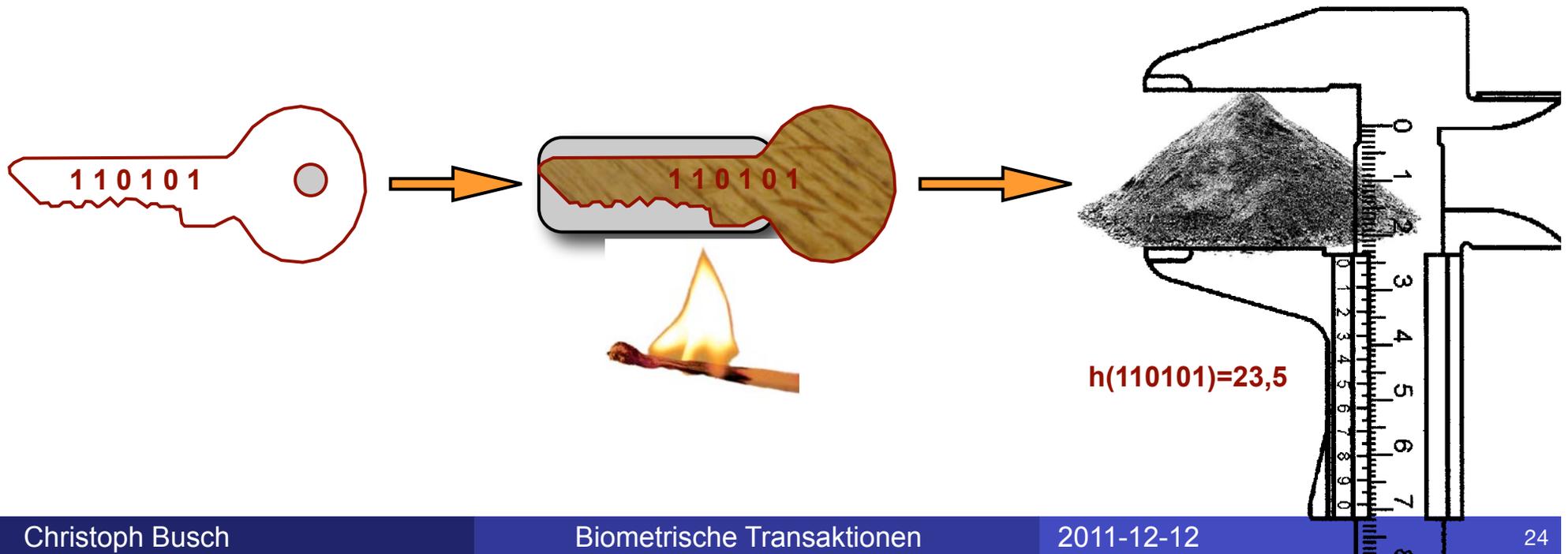
- Hilfsdaten *ADI* und Referenz *AD2* werden im BTD gespeichert

# Biometric Transaction Authentication

## BTAP - Enrolment

### 2.) Enrolment im **Online-Banking-Server** (OBS)

- Anlegen eines Kundenrecords mit Account-Number (AN)
- Hash-Wert vom geheimen Schlüssel *SBV* wird mit Kundenrecord in der OBS-Datenbank abgelegt
  - Hash-Wert entspricht einem Pseudo-Identifizier nach ISO 24745



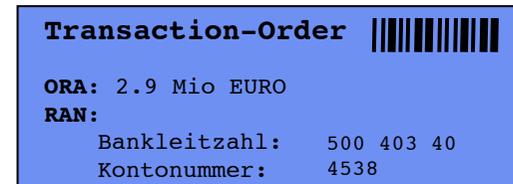
# Die biometrische und sichere Transaktion

# Transaktions-Verifikation

## BTAP - Transaktion

### 1. ) Operationen der **Online-Banking-Software** (BSW)

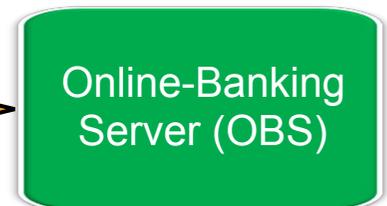
- Kunden erstellt durch Interaktion mit der BSW-Software einen Transaction-Order-Record (TOR)



Dieser TOR beinhaltet:

- Transaktionsidentifikator (TID), Sender-Account-Number (SAN)  
**Receiver-Account-Number** (RAN), **Ordered Amount** (ORA)

- BSW überträgt den TOR an den Online-Banking-Server (OBS)



- BSW überträgt den TOR an das mit dem Kunden-Rechner verbundene Biometric-Transaction-Device (BTD)

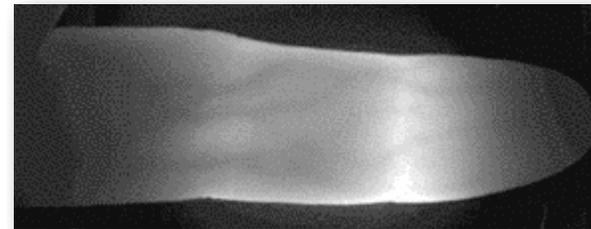


# Transaktions-Verifikation

## BTAP - Transaktion

### 2. ) Operationen des **Biometric-Transaction-Device** (BTD)

- Die relevante Information aus dem Transaction-Order-Record (TOR) wird im Display des BTD angezeigt:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Zur Bestätigung der gewünschten Transaktion
  - legt der Kunde den Finger auf und
  - dadurch wird ein Proben-Sample mit dem BTD erfasst

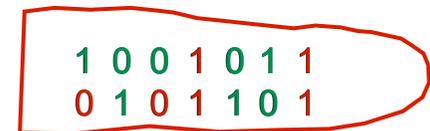
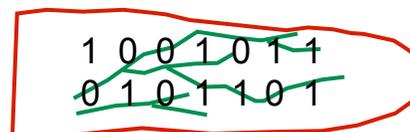
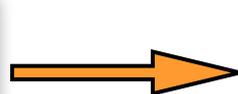
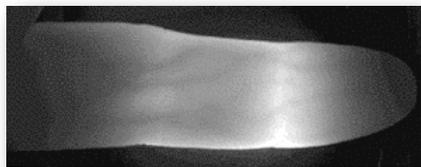


# Transaktions-Verifikation

## BTAP - Transaktion

### 2. ) Operationen des **Biometric-Transaction-Device** (BTD)

- Die relevante Information aus dem Transaction-Order-Record (TOR) wird im Display des BTD angezeigt:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Bestätigung der gewünschten Transaktion durch Proben Sample
- Auxilliary Data  $ADI_{\{0,1,2,4,5,8,11,12\}}$  wird aus dem BTD-Speicher abgerufen
- Ein binarisierter frischer Merkmalsvektor  $XBV$  ergibt sich aus der Probe  $XR_V$  und den Auxilliary Data  $ADI$



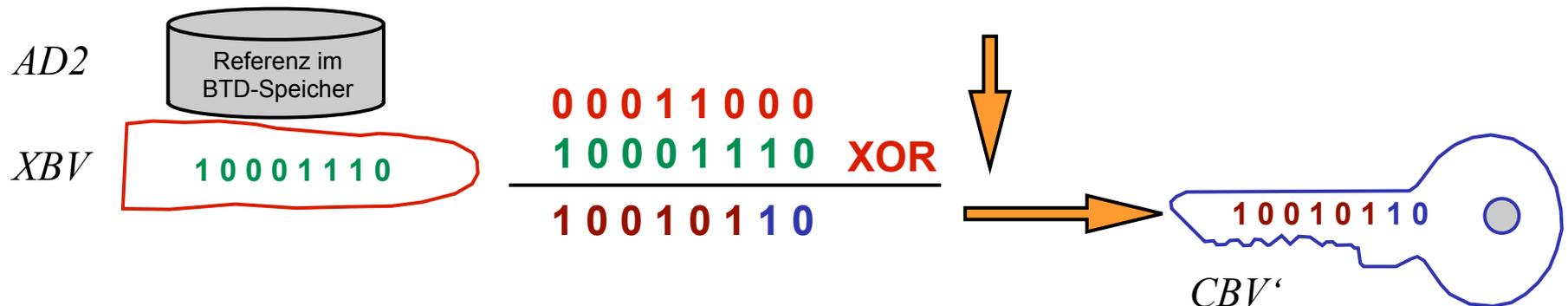
Auxilliary Data ( $ADI$ ): Bit-Indices = 0,1,2,4,5,8,11,12

# Transaktions-Verifikation

## BTAP - Transaktion

### 2. ) Operationen des **Biometric-Transaction-Device** (BTD)

- Die relevante Information aus dem Transaction-Order-Record (TOR) wird im Display des BTD angezeigt:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Bestätigung der gewünschten Transaktion durch Proben Sample
- Auxilliary Data  $ADI_{\{0,1,2,4,5,8,11,12\}}$  wird aus dem BTD-Speicher abgerufen
- Ein binarisierter Merkmalsvektor  $XBV$  10001110 ergibt sich
- Ein Geheimvektor  $CBV'$  wird durch **XOR** rekonstruiert aus im BTD gespeicherter Auxilliary Data  $AD2$  Referenz und dem binarisierten Proben Merkmals Vektor  $XBV$  10001110

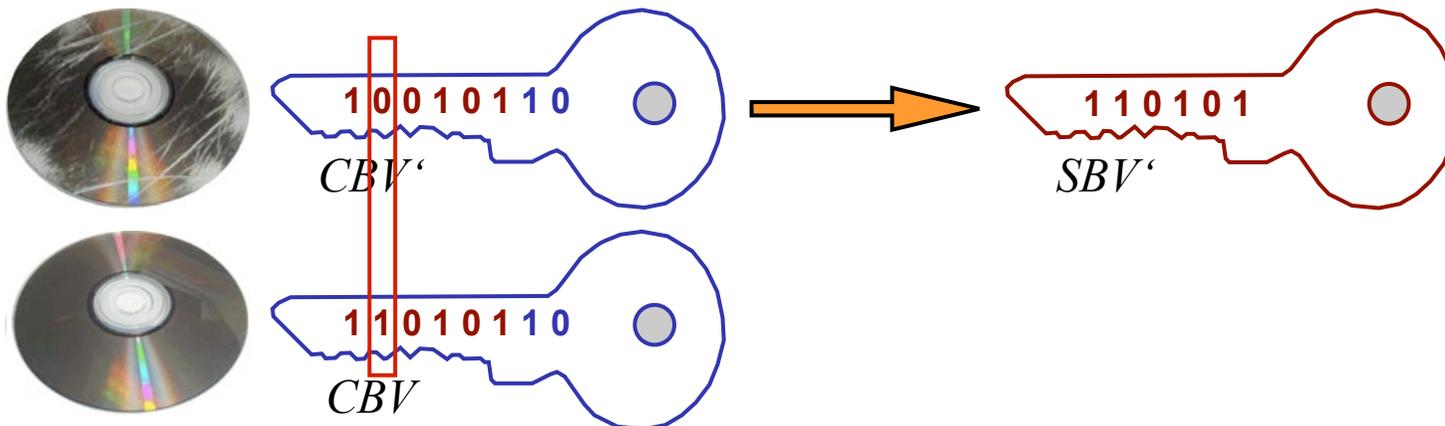


# Transaktions-Verifikation

## BTAP - Transaktion

### 2. ) Operationen des **Biometric-Transaction-Device** (BTD)

- Die relevante Information aus dem Transaction-Order-Record (TOR) wird im Display des BTD angezeigt:
  - Receiver-Account-Number (RAN), Ordered Amount (ORA)
- Bestätigung der gewünschten Transaktion durch Proben Sample
- Auxilliary Data  $ADI_{\{0,1,2,4,5,8,11,12\}}$  wird aus dem BTD-Speicher abgerufen
- Ein binarisierter Merkmalsvektor  $XBV$  10001110 ergibt sich
- Ein Geheimvektor  $CBV'$   wird rekonstruiert
- Der geheime Schlüssel  $SBV'$  wird aus  $CBV'$  neu berechnet  
 $SBV' = dec(CBV')$



# Transaktions-Verifikation

## BTAP - Transaktion

### 2.b ) Siegel-Operationen des BTD

- Ein Transaktions-Order-Siegel (TOS') wird gerechnet

- aus Transaction-Order-Record *TOR*

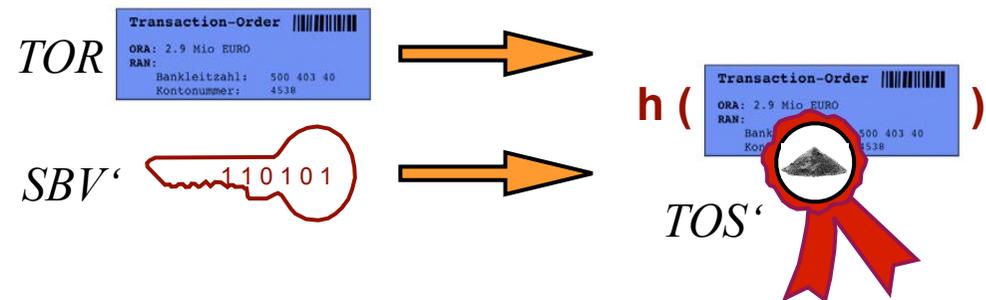


- und dem rekonstruiertem geheimen Schlüssel *SBV'*



$$TOS' = MAC(h(TOR), PI')$$

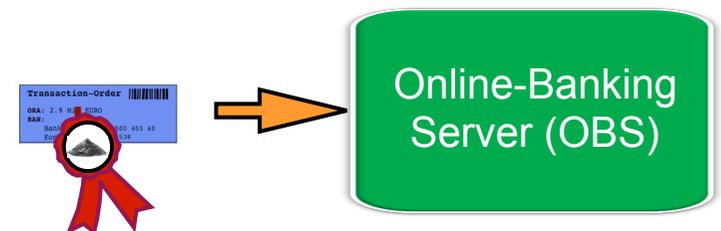
$$PI' = h(SBV')$$



- Umsetzungsmöglichkeit mit HMAC:

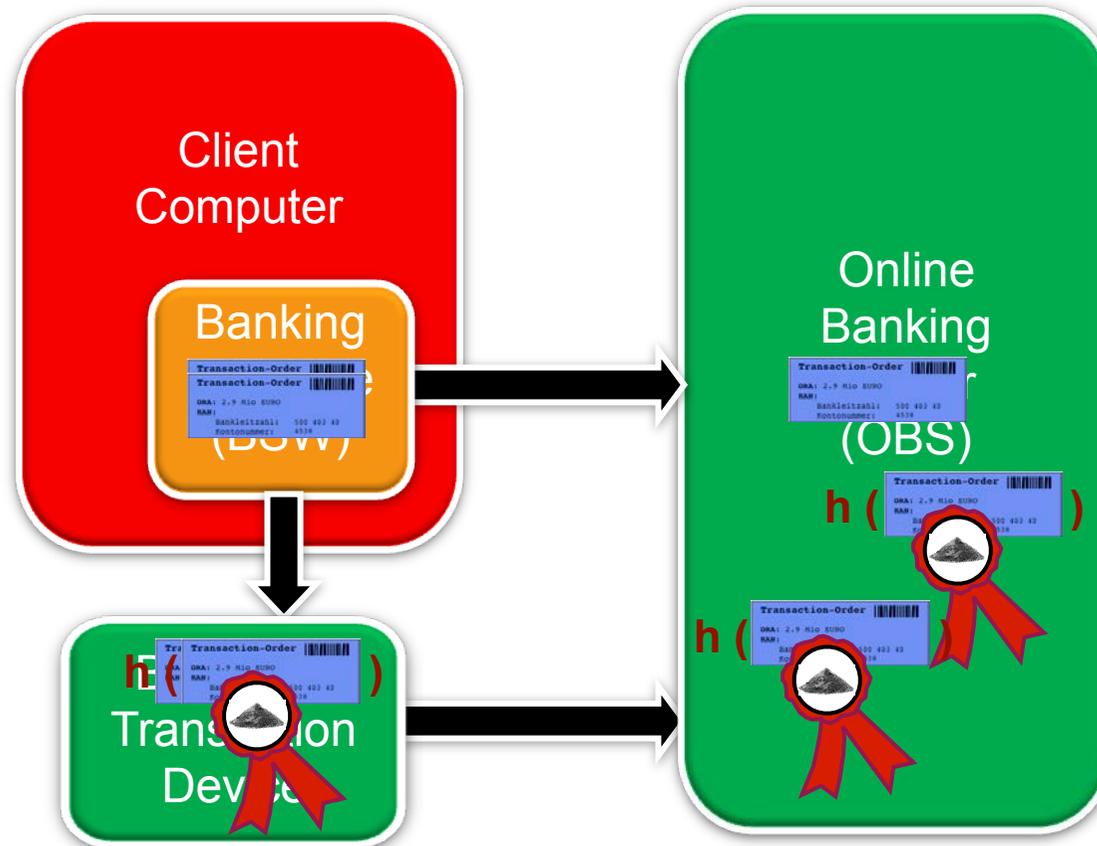
$$TOS' = h(PI' XOR OPAD, h(PI' XOR IPAD, TOR))$$

- Das Siegel (TOS') wird zum Online-Banking-Server übertragen



# Transaktions-Verifikation

Zwei unabhängige Kanäle

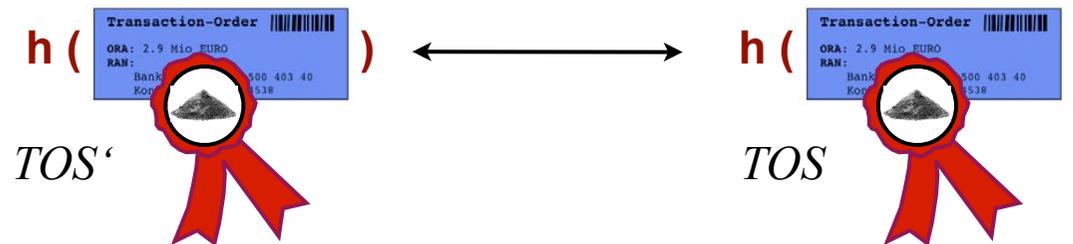


# Transaktions-Verifikation

## BTAP- Transaktion

### 3. ) Operationen des **Online-Banking-Server** (OBS)

- Vergleicht den rekonstruierten TOS mit dem vom BTD gelieferten TOS':  
 $TOS == TOS'$



- Die Transaktion ist personen- **und** datenauthentisch, wenn TOS und TOS' identisch sind.



# Zusammenfassung

In vielen derzeitig eingesetzten Protokollen sind die Informationen nur ungenügend geschützt.

- In keinem der derzeitigen Protokolle wird die Information über den Initiator nachweisbar gesichert

Das hier vorgeschlagene Biometrische-Transaktions-Authentisierungs-Protokoll realisiert

- eine **Daten**-Authentisierung und gleichzeitig eine **Personen**-Authentisierung.
  - Damit wird eine starke **Bindung** zwischen dem Kunden und den relevanten Informationen hergestellt
  - Somit wird für den Ausführenden der Transaktion gesichert **nachgewiesen**, dass tatsächlich eine (berechtigte) **natürliche Person** (der Bank-Kunde) die Transaktion initiiert und bestätigt hat.
- Umsetzungsperspektive durch starkes Interesse der Industrie

# Warum Biometrie im Online-Banking?

Die Gefahr liegt in der Automatisierung der Angriffe

- Ein biometrischer Authentisierungsfaktor kann nicht automatisiert im Angriff eingespeist werden..

Das liefert doch schon der TAN-Generator?

- TAN-Generatoren werden genauso häufig verloren oder gestohlen gehen wie Handys!
- Der TAN-Generator ist derzeit zwar das sicherste Verfahren....



...aber man sollte Immer noch einen weiteren Pfeil im Köcher haben

# Fachgremien



CAST-Forum

<http://www.cast-forum.de>



Gesellschaft für Informatik - BIOSIG

Fachgruppe Biometrie und Elektronische Signaturen

<http://www.biosig.org>



TeleTrust

Arbeitsgruppe Biometrie

<http://www.teletrust.de>



European Biometrics Forum

<http://www.eubiometricsforum.com>



Prof. Dr. Christoph Busch

Department  
Security Technology

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

# Kontakt



**Prof. Dr. Christoph Busch**  
Principal Investigator

CASED  
Mornewegstr. 32  
64293 Darmstadt/Germany  
[christoph.busch@cased.de](mailto:christoph.busch@cased.de)

Telefon +49 6151/16 9444  
Fax  
[www.cased.de](http://www.cased.de)

# Kontakt



**GJØVIK UNIVERSITY COLLEGE**  
FACULTY OF COMPUTER SCIENCE AND  
MEDIA TECHNOLOGY

**Christoph Busch, Dr.-Ing.**  
Professor

P.O. Box 191, N-2802 Gjøvik, Norway  
Phone: +47 61 13 51 94  
Fax: +47 61 13 52 40  
E-mail: [christoph.busch@hig.no](mailto:christoph.busch@hig.no)  
[www.hig.no](http://www.hig.no) | [www.nislab.no](http://www.nislab.no)