Willkommen zur Vorlesung

Modellbasierte Softwaretechniken für sichere Systeme

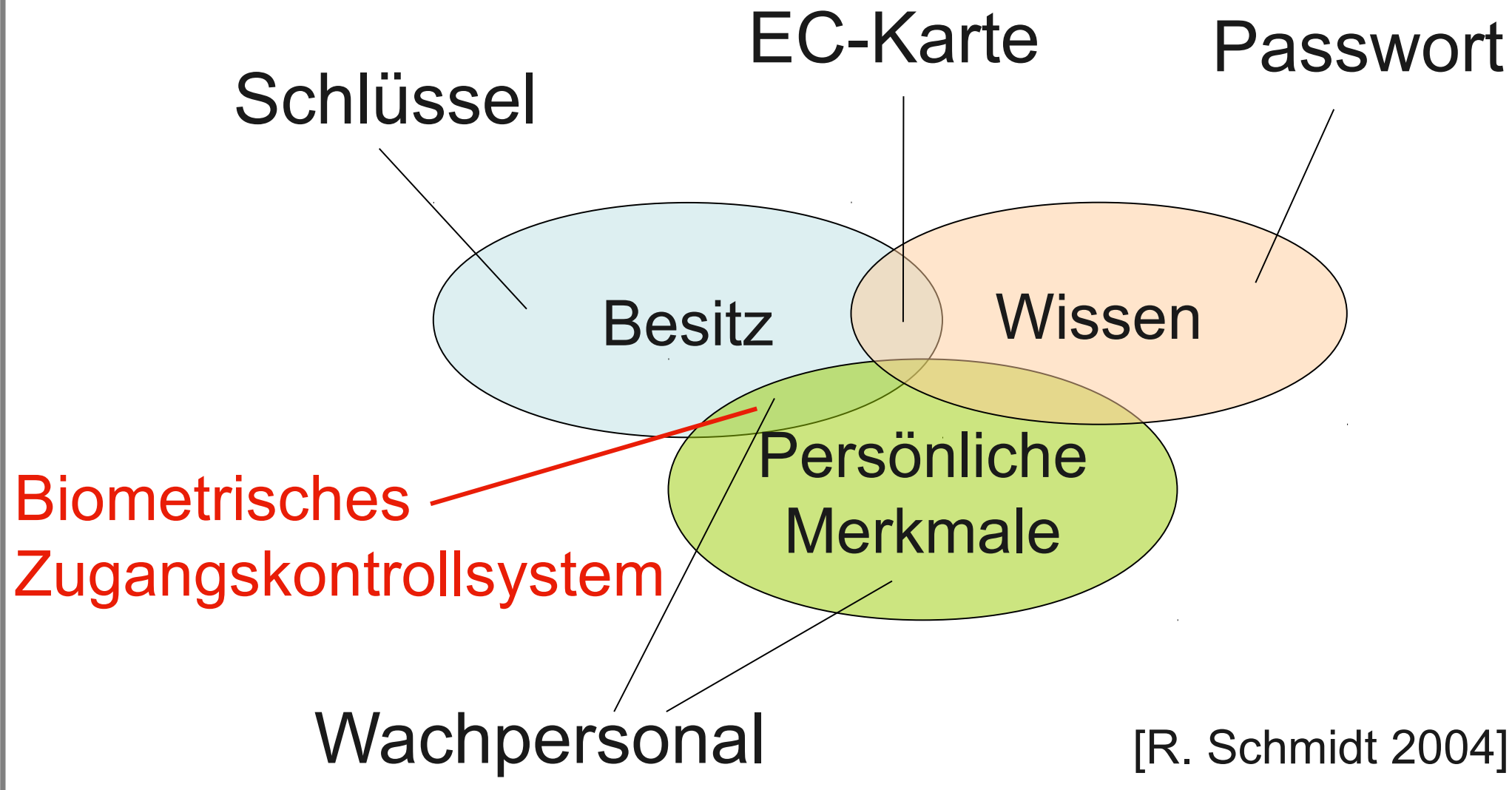
im Sommersemester 2012

Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

8. Biometrische Authentisierung

Zugangskontrollmechanismen



[R. Schmidt 2004]

Zugangskontrolle: Beispiele

Ziel: Sicherer Schutz vor unberechtigtem Zugang / Zutritt

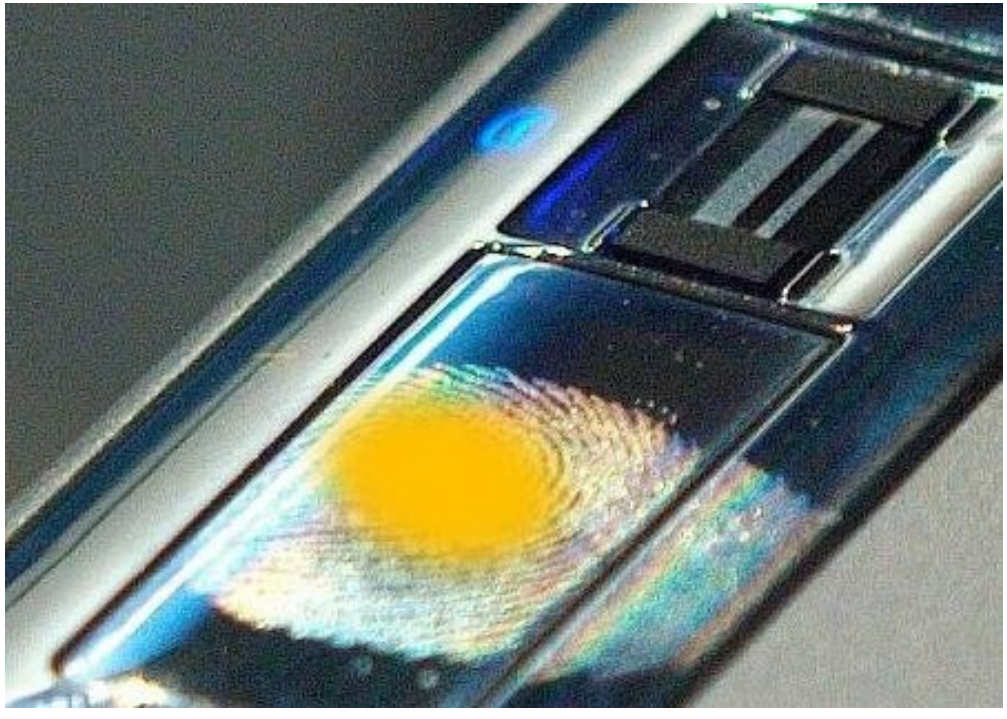
Beispiele:

Gegenstand	Schutzmaßnahme	Kategorie
Raum / Tür	Schlüssel Wachmann	Besitz Persönliche Merkmale
Computer	Passwort	Wissen
Konto	Karte mit PIN	Besitz + Wissen

Zugangskontrolle: Probleme I

[B. Schneier 2009]

Zugangskontrolle: Probleme II



[K. Cameron 2008]

Schwachstellen

Schutzmaßnahme	Problem
Schlüssel Wachmann	Kann verloren / gestohlen werden Bestechlich / 24 h Einsatz?
Passwort	Am Arbeitsplatz notiert, schlechte Wahl, Social Engineering
Karte mit PIN	PIN auf Karte notiert

Biometrische Authentisierung

Auf Basis von persönlichen Merkmalen:

Handgeometrie, Augennetzhaut, Augeniris, Venen, Unterschrift, Fingerabdruck, Stimmen, Gesicht, DNA, Geruch...

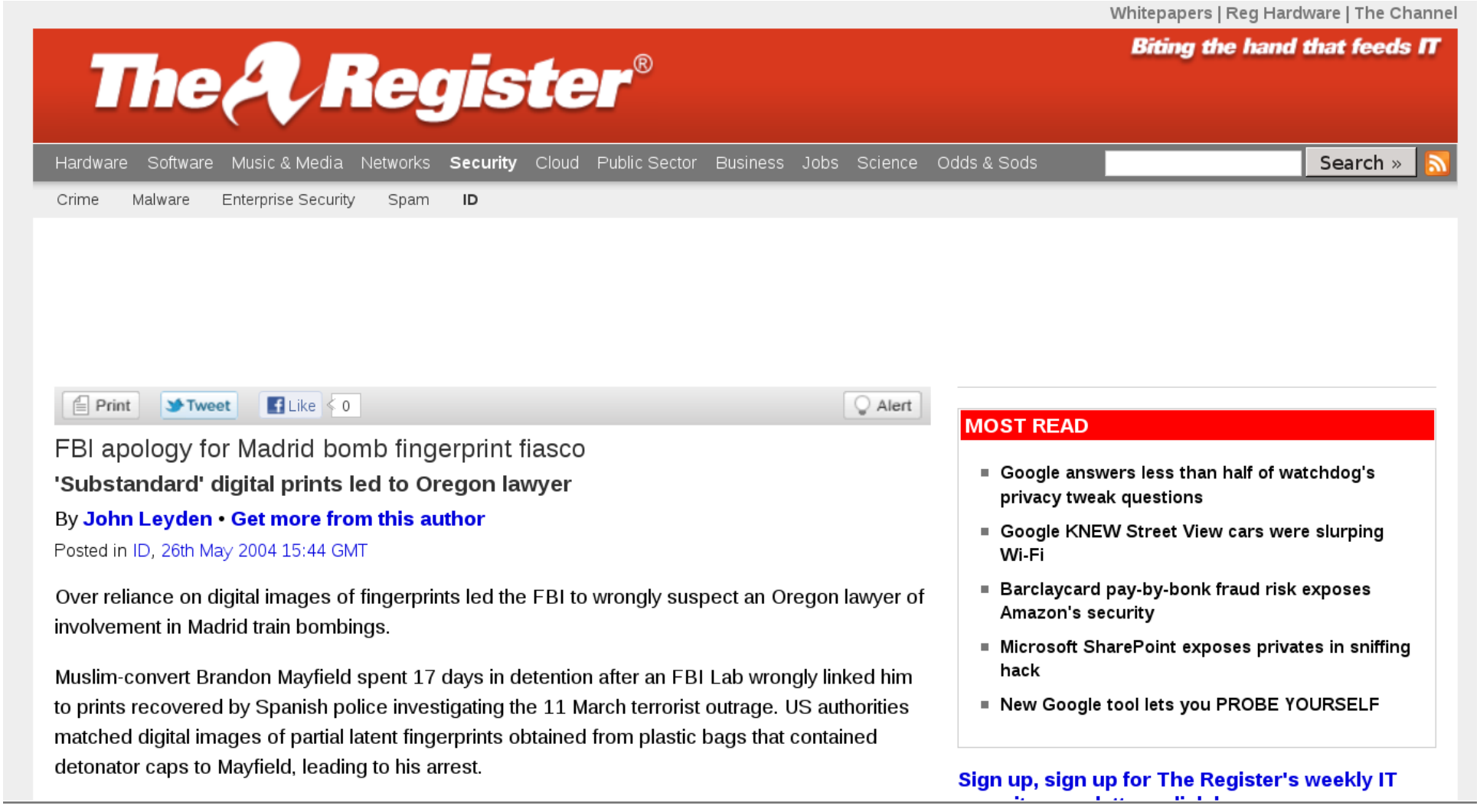
Aktuell: USA-Einreise; Reisepass; Flughafen (Vielflieger)

Soft Biometrics: Haut-, Augen- und Haarfarbe, Gang, Tastenanschlag, Verhalten

- Identifikation
  - Wer bist du?
  - Suche in einer Menge von bekannten Profilen nach aktuell erfasstem Profil
  - Problem:
    - Trennschärfe der Profile
      - Zu genau: Aktuell erfasste Person wird häufig nicht gefunden, obwohl bekannt
      - Zu weich: Aktuell erfasste Person wird mit Personen verwechselt, deren Profil ähnlich ist

- Verifikation
  - Bist du der, der du vorgibst zu sein?
  - Stimmen erfasstes Profil und Authentifizierungsprofil überein?
  - Potentiell einfacher als Identifikation
  - Aber:
    - Ablehnung von Berechtigten beeinträchtigen sehr schnell die Akzeptanz
    - Erfolgreiche Verifikation eines nicht Berechtigten ist meist direkt ein Sicherheitsrisiko

Beispiel: False Positive I



Whitepapers | Reg Hardware | The Channel

The Register®

Biting the hand that feeds IT

Hardware Software Music & Media Networks **Security** Cloud Public Sector Business Jobs Science Odds & Sods Search »

Crime Malware Enterprise Security Spam **ID**

Print Tweet Like 0 Alert

FBI apology for Madrid bomb fingerprint fiasco

'Substandard' digital prints led to Oregon lawyer

By **John Leyden** • **Get more from this author**

Posted in ID, 26th May 2004 15:44 GMT

Over reliance on digital images of fingerprints led the FBI to wrongly suspect an Oregon lawyer of involvement in Madrid train bombings.

Muslim-convert Brandon Mayfield spent 17 days in detention after an FBI Lab wrongly linked him to prints recovered by Spanish police investigating the 11 March terrorist outrage. US authorities matched digital images of partial latent fingerprints obtained from plastic bags that contained detonator caps to Mayfield, leading to his arrest.

MOST READ

- Google answers less than half of watchdog's privacy tweak questions
- Google KNEW Street View cars were slurping Wi-Fi
- Barclaycard pay-by-bonk fraud risk exposes Amazon's security
- Microsoft SharePoint exposes privates in sniffing hack
- New Google tool lets you PROBE YOURSELF

Sign up, sign up for The Register's weekly IT

Biometrische Authentisierung

Identifikation: 1 : n Vergleich

Verifikation: 1 : 1 Vergleich

Biometrisches System führt biometrische Verifikation / Identifikation durch.

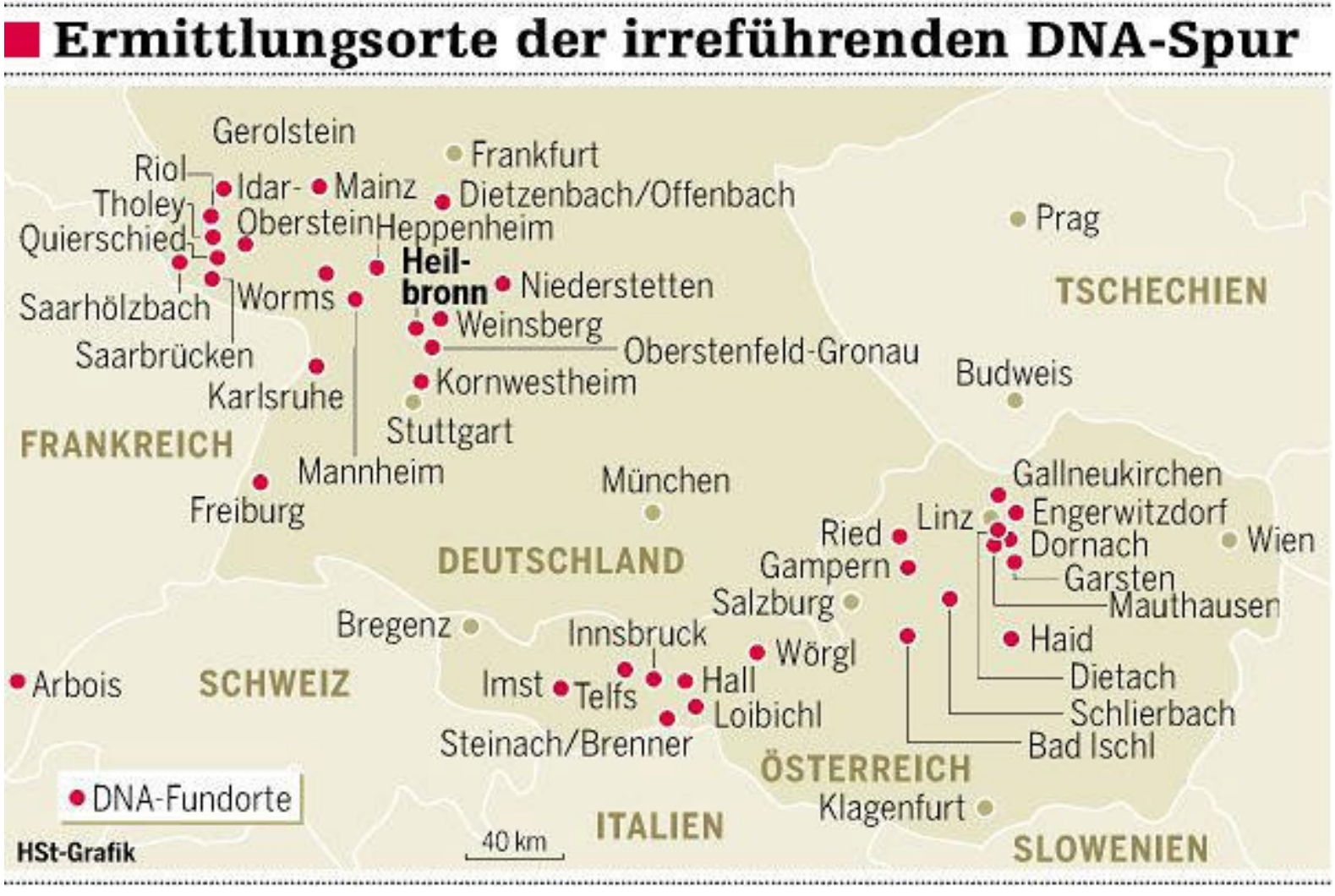
Unterschiedliche Verfahren, aber unterschiedlich geeignet bzw. problembehaftet

Probleme bei Biometrischer Authentisierung

False Positive, False Accept/Match Rate (FAR/FMR): Das Biometrische System ordnet ein Sample fälschlicherweise einem Template zu.

False Negative, False Reject/Non-Match Rate (FRR/FNMR): Ein „richtiges Template“ wird vom System nicht erkannt.

Beispiel: False Positive II



Characteristica Biometrischer Authentisierung I

Universalität: Wie viele Personen besitzen dieses Merkmal?

Einmaligkeit: Wie unterschiedlich ist das Merkmal bei unterschiedlichen Personen ausgeprägt?

Konstanz: Ändert sich das Merkmal im Laufe der Zeit?

Messbarkeit: Wie gut ist das Merkmal durch Sensoren messbar?

Characteristica Biometrischer Authentisierung II

Performanz: Wie schnell, genau und robust arbeiten die Sensoren mit denen das Merkmal erfasst wird?

Akzeptanz: Wie stehen die Personen zum erfassen des Merkmals?

Fälschungssicherheit: Wie schwer lässt sich das Merkmal imitieren?

Kosten, ...

Kein Merkmal ist bei allen Punkten optimal!

Kein Merkmal ist bei allen Punkten optimal!

Biometrische Merkmale...

- sind in der Regel nicht änderbar
- sind in der Regel nicht geheim

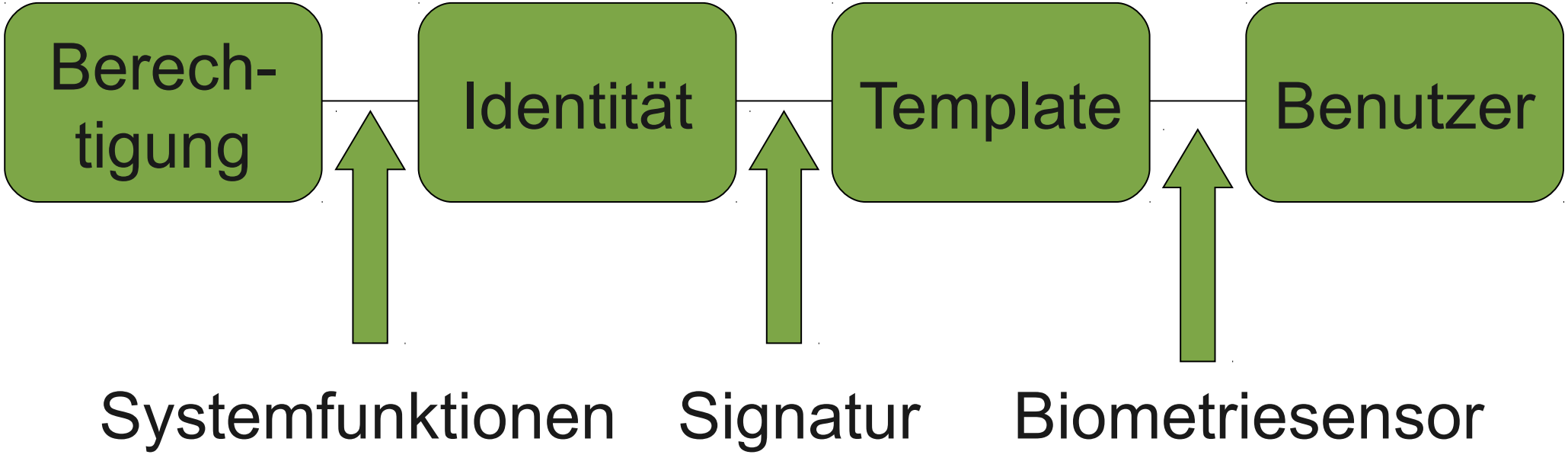
Überblick: Stärken / Schwächen biometrischer Verfahren

[Liu, Silverman, 2001]

	Usability	Kosten	Geschwindig.	Genauigkeit	Sicherheitsanf.	Akzeptanz
Gesichtserkenn.	o	--	--	+	o	o
Fingerabdruck	+	+	o	+	-	+
Handgeometrie	+	-	-	+	o	o
Iris-Scan	o	--	--	++	--	o
Sprache	+	++	+	+	o	+
Untersch.	+	++	+	+	o	o

Biometrisches System realisiert

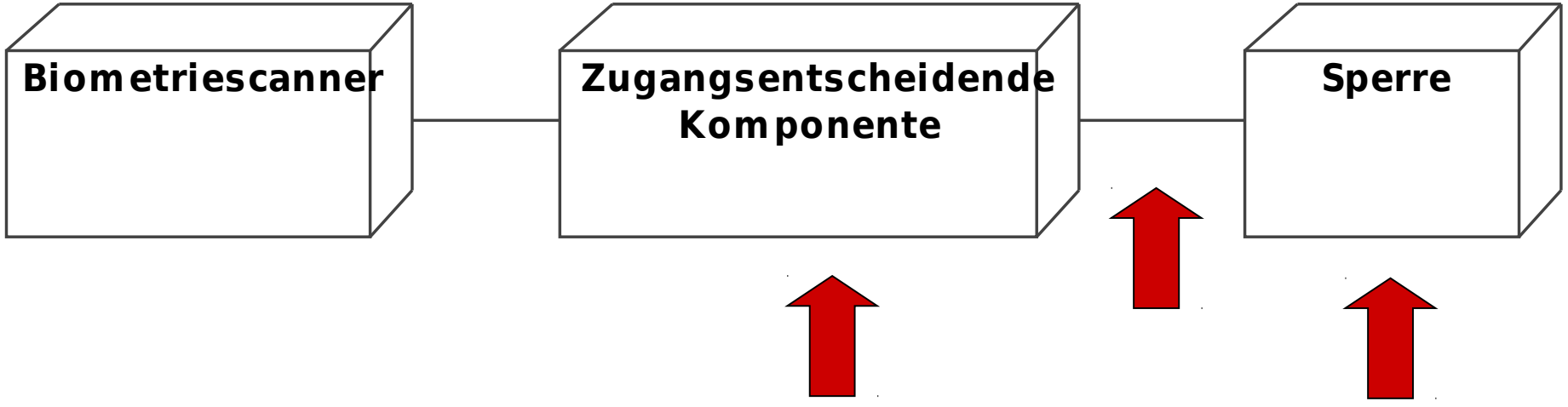
Verknüpfungskette:



Funktionsweise

- Scannen biometrischer Daten, Template extrahieren.
- Vergleich mit gespeichertem Referenztemplate.
- Bei ausreichender Übereinstimmung entsperren.

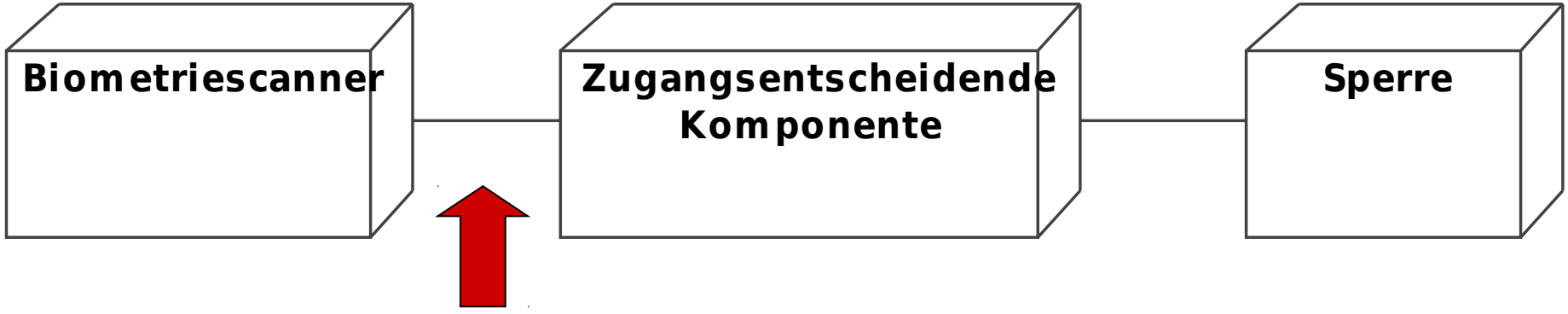
Angriffspunkte I



Angriff: Aufbrechen und / oder elektrisches Signal einspeisen.

➔ Physikalischer Schutz notwendig.

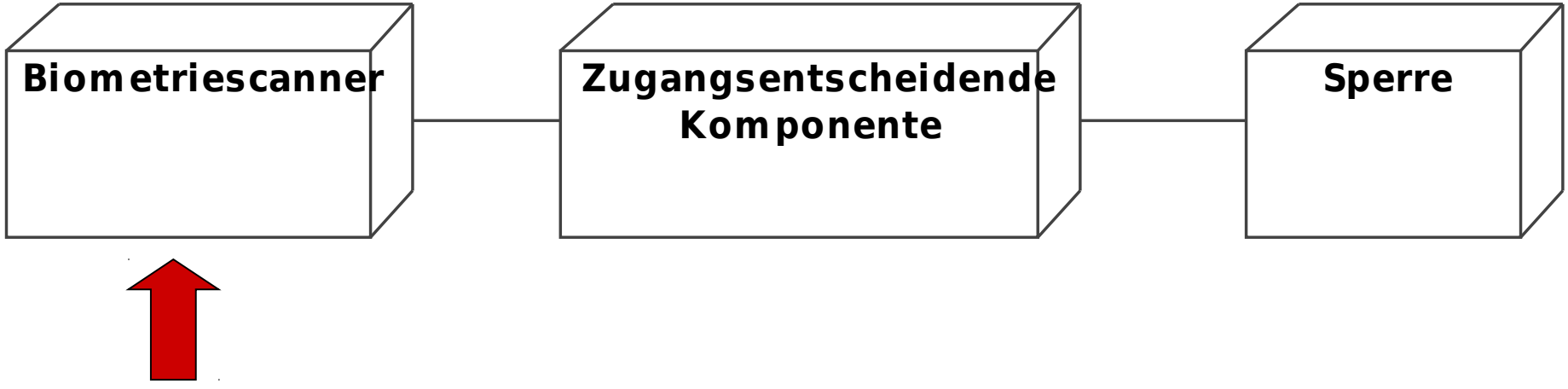
Angriffspunkte II



Angriff: Zugangsberechtigtes Template ablauschen und einspeisen.

➔ Physikalischer Schutz, oder Schutz durch Kryptographie.

Angriffspunkte III



Angriff: Imitation von Körperteilen, zum Beispiel Silikonfinger.

➔ Qualität des Biometriescanners erhöhen (Lebenderkennung).

Problem: Ewiger Wettlauf ?

Gefahren Biometrischer Authentisierung I

[CCC 2008]

[Wikimedia 2006]

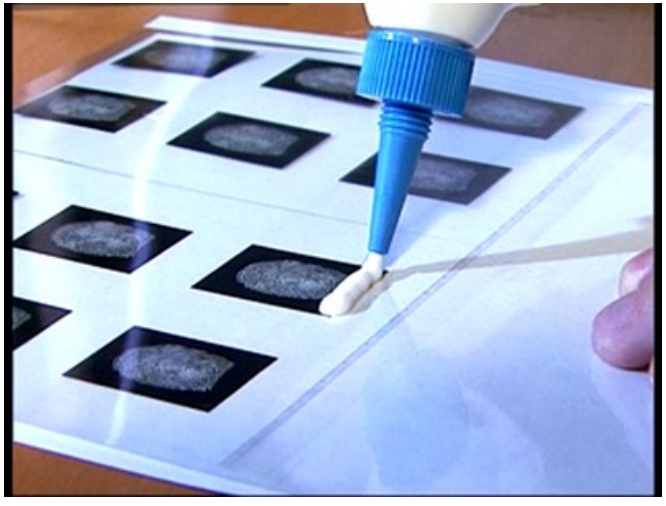
Gefahren Biometrischer Authentisierung II

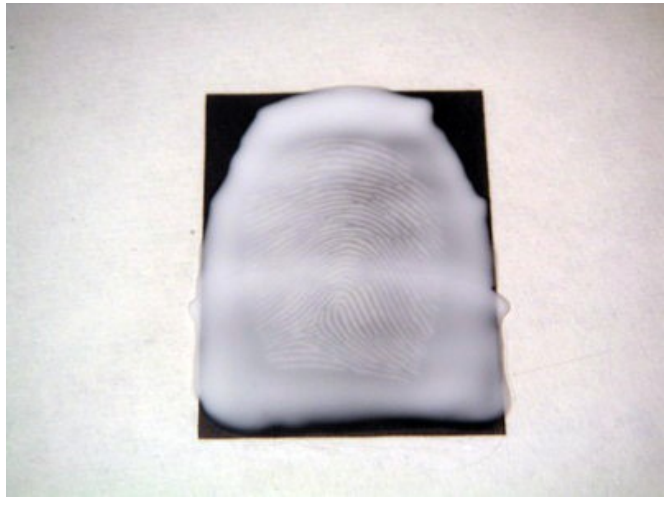


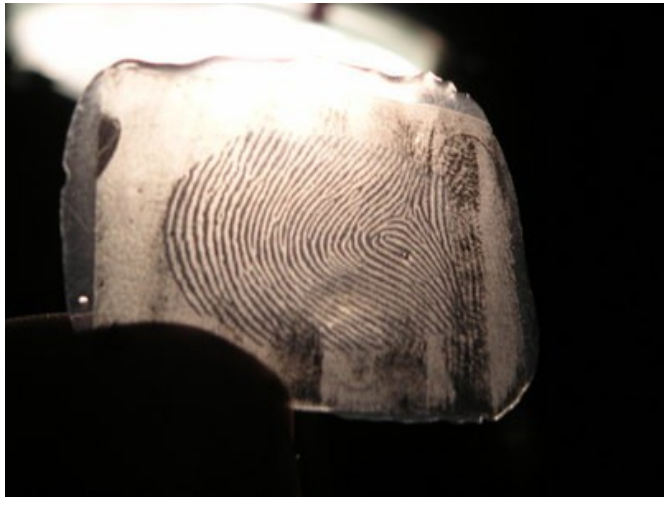



[CCC 2004]

Gefahren Biometrischer Authentisierung III








[CCC 2004]

BBC Home News Sport Radio TV Weather Languages Search

[an error occurred while processing this directive]

Low graphics | Accessibility help

BBC NEWS

Watch One-Minute World News

News services
Your news when you want it

News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment

Last Updated: Thursday, 31 March, 2005, 10:37 GMT 11:37 UK

E-mail this to a friend Printable version

Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

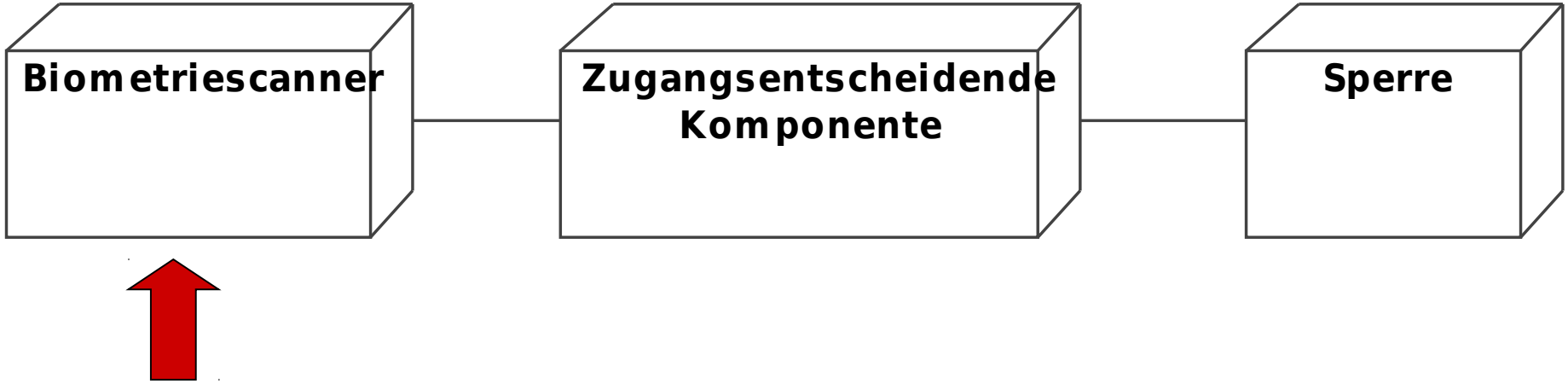
Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.

SEE ALSO:
Malaysia to act against pirates
16 Mar 05 | Asia-Pacific

RELATED INTERNET LINKS:
Malaysian police

The BBC is not responsible for the content of external internet sites

Angriffspunkte III



Angriff: Imitation von Körperteilen, zum Beispiel Silikonfinger.

➔ Qualität des Biometriescanners erhöhen (Lebenderkennung).

Problem: Ewiger Wettlauf ?

Einschränkungen

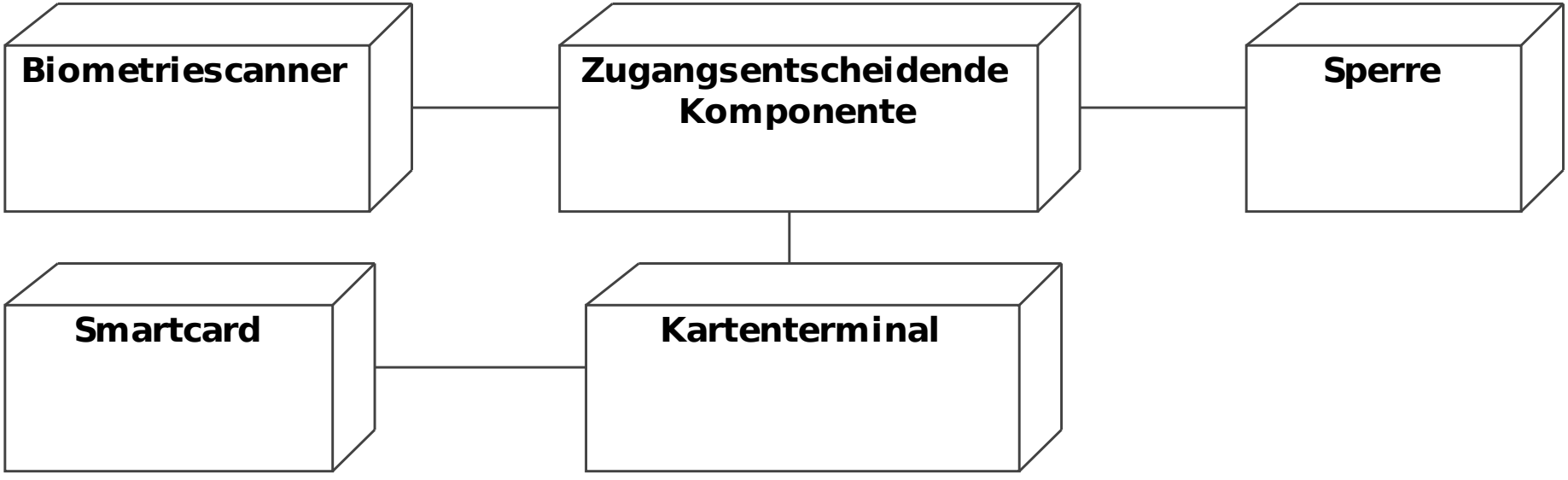
Realisierbarer Modus: Identifikation (1:n)

Notwendig: zentrale Speicherung biometrischer Datensätze.

Probleme:

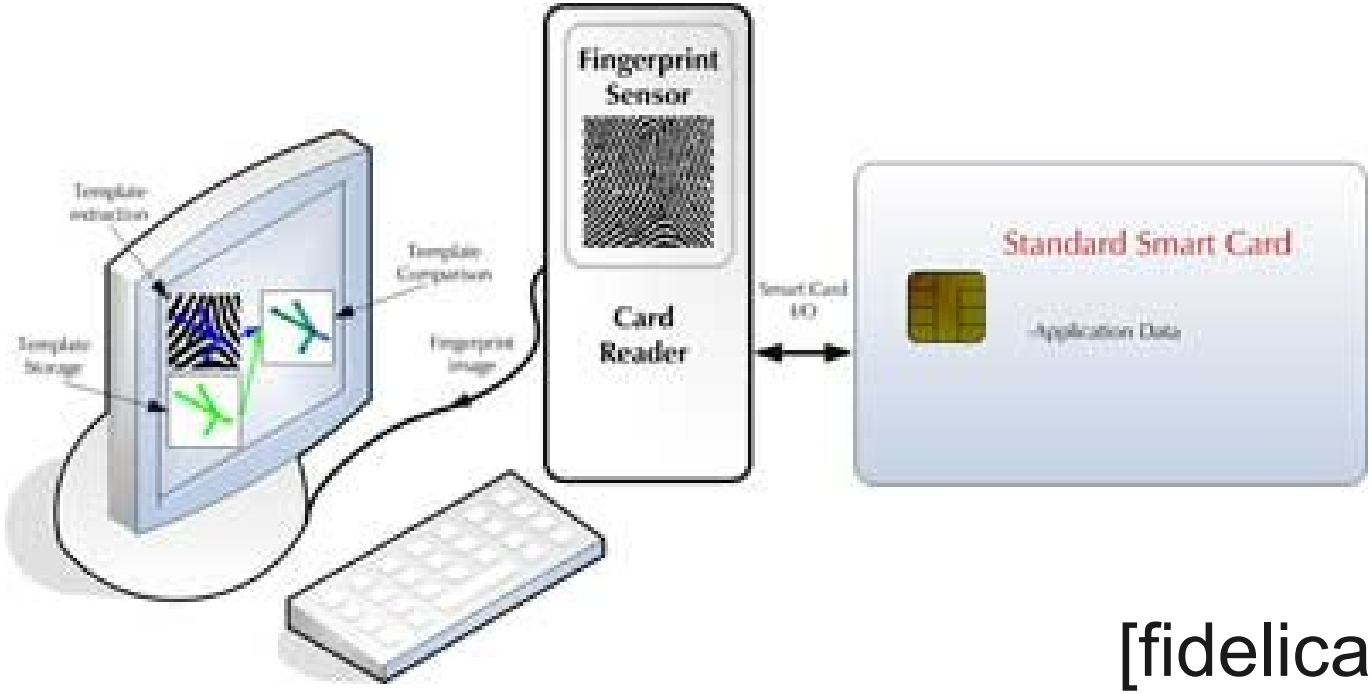
- mehrere Referenzdatensätze betrachten
- Speicherung persönlicher Merkmale unterliegt Datenschutz

System mit personifizierter Smartcard



- Referenztemplate auf Smartcard gespeichert.
- Besitzer der Smartcard trägt Verantwortung für seine biometrischen Daten: Datenschutz.
- Realisierbarer Modus: Verifikation (1:1).

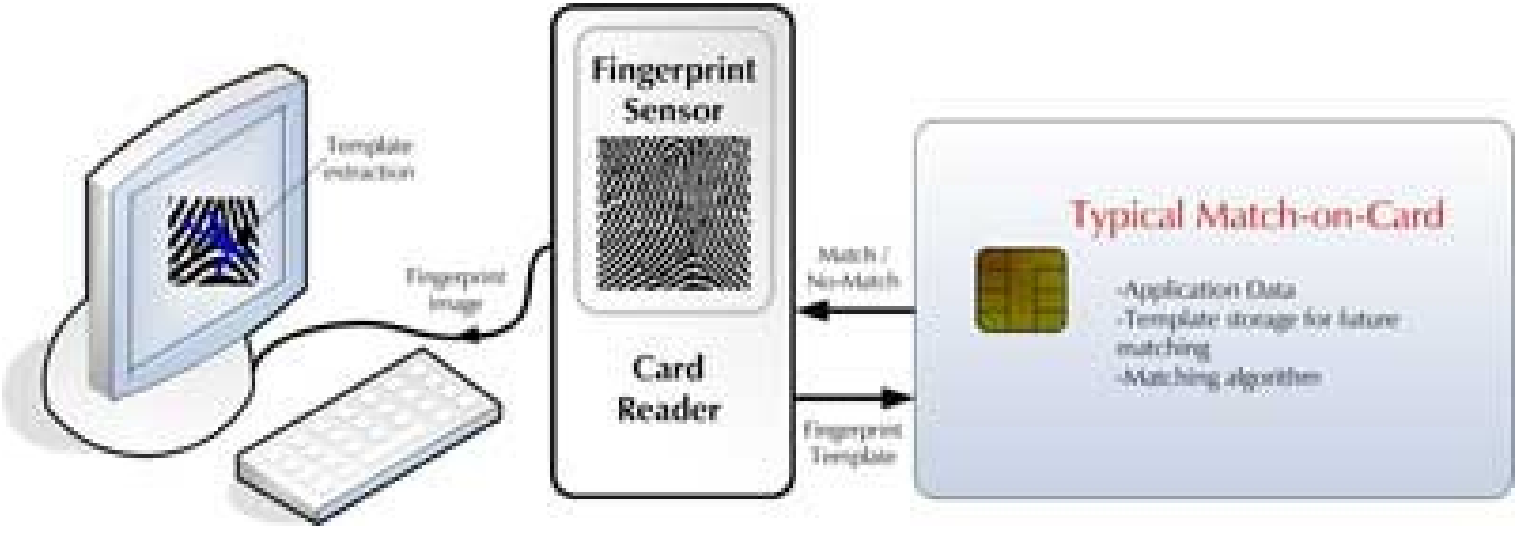
Standard Smart Card



[fidelica.com 2006]

- Templates müssen nicht zentral gespeichert werden
- Templates / Biometrosche Merkmale werden im System verarbeitet

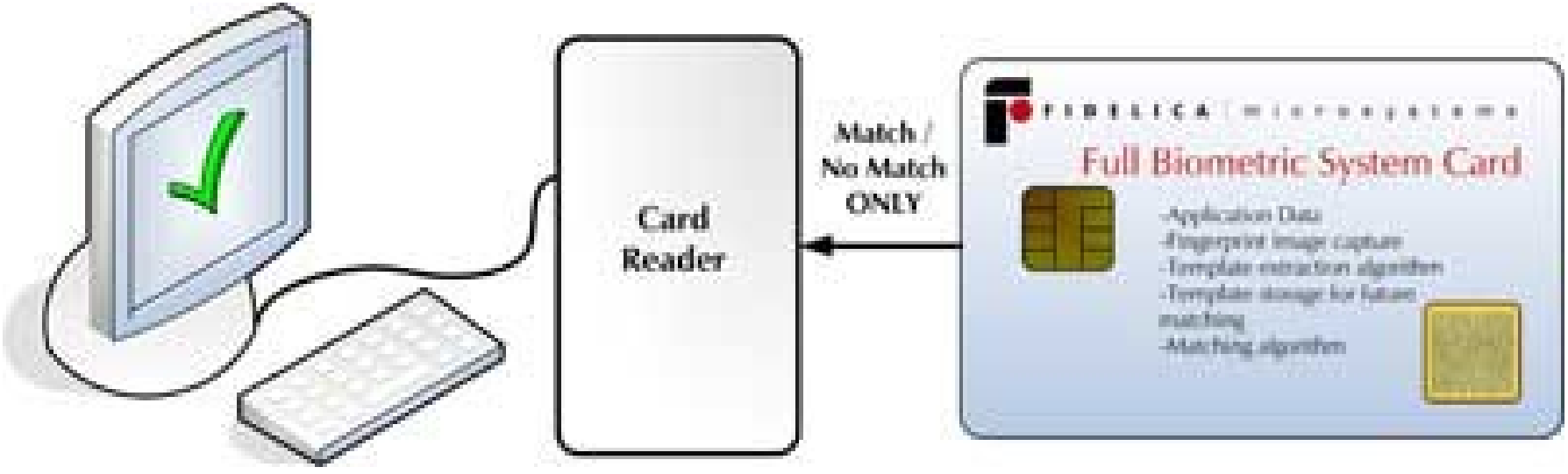
Match-on-Card



[fidelica.com 2006]

- Templates müssen nicht zentral gespeichert werden
- Templates / Biometrosche Merkmale sind nur im Terminal

Biometrische Smart Card

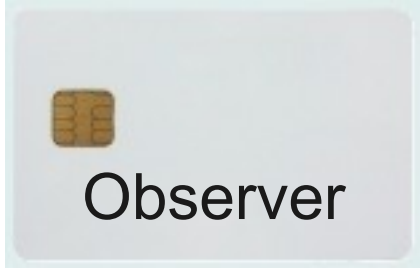


[fidelica.com 2006]

- Templates müssen nicht zentral gespeichert werden
- Templates / Biometrosche Merkmale verlassen die Karte nicht

Wallet with Observer

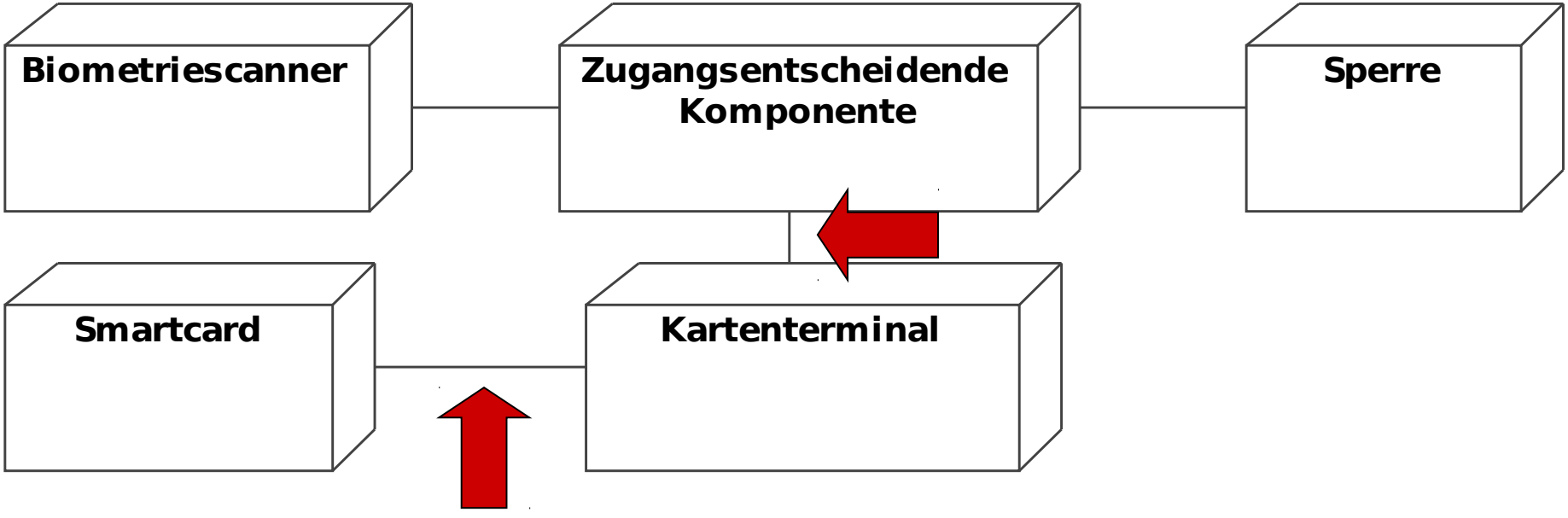
Verifier



[Impagliazzo & More 2003]

- Templates nicht zentral gespeichert
- Templates / Biometrosche Merkmale verlassen die Karte nicht
- Geringere Vertrauensannahmen notwendig

Angriffspunkte IV

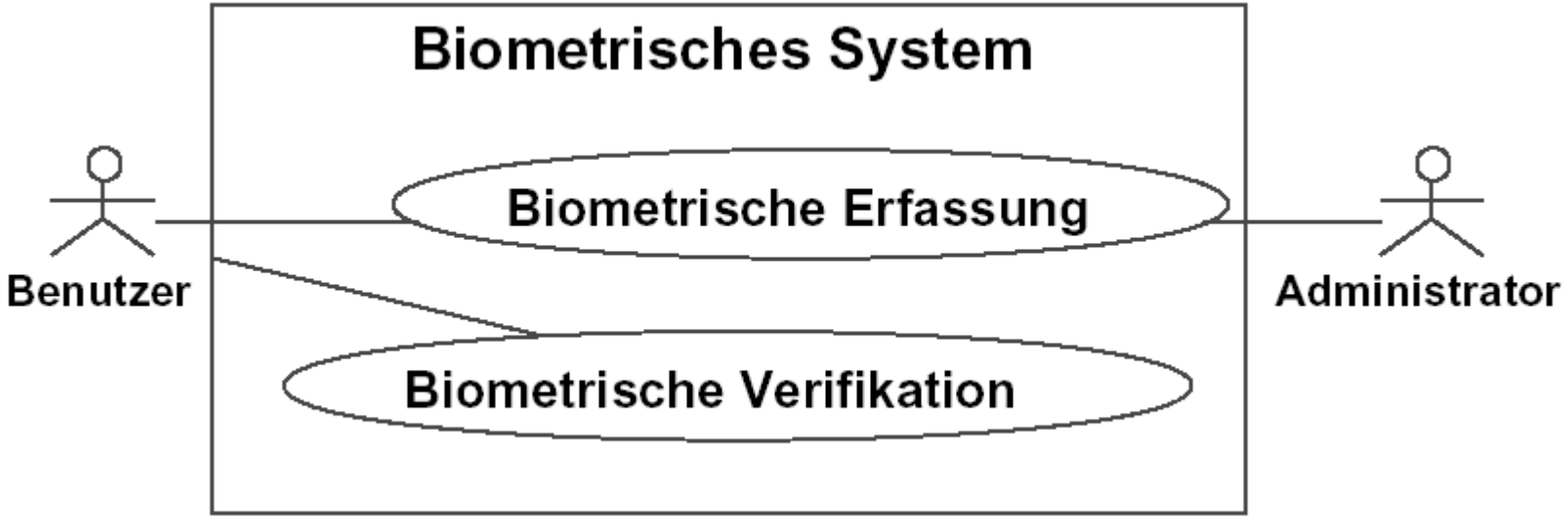


Angriff: Vergleich zwischen gespeichertem Referenztemplate und aktuellem Wert manipulieren.

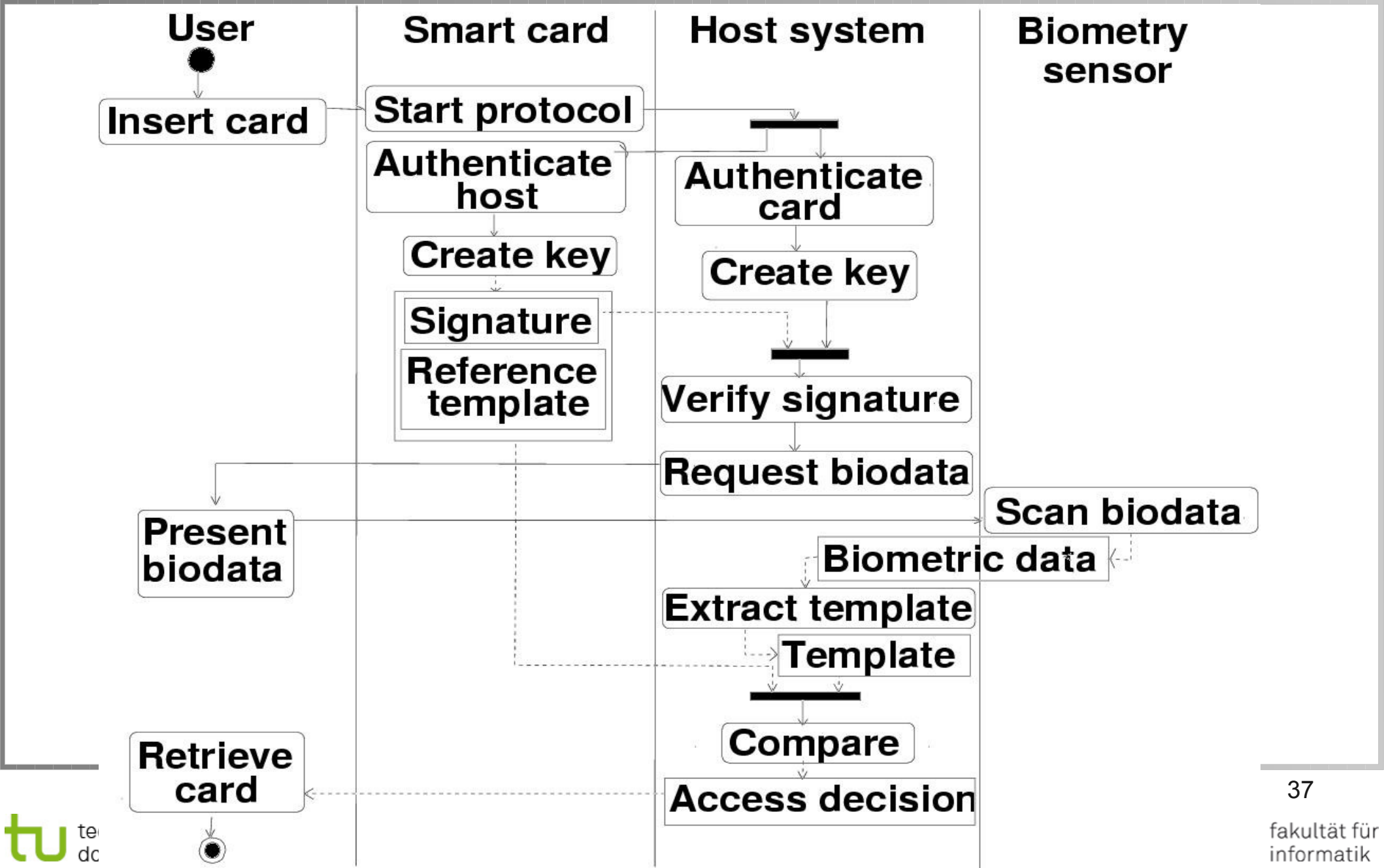
➔ Kryptographische Authentifikation.

Biometrisches Authentifikationssystem in industrieller Entwicklung.

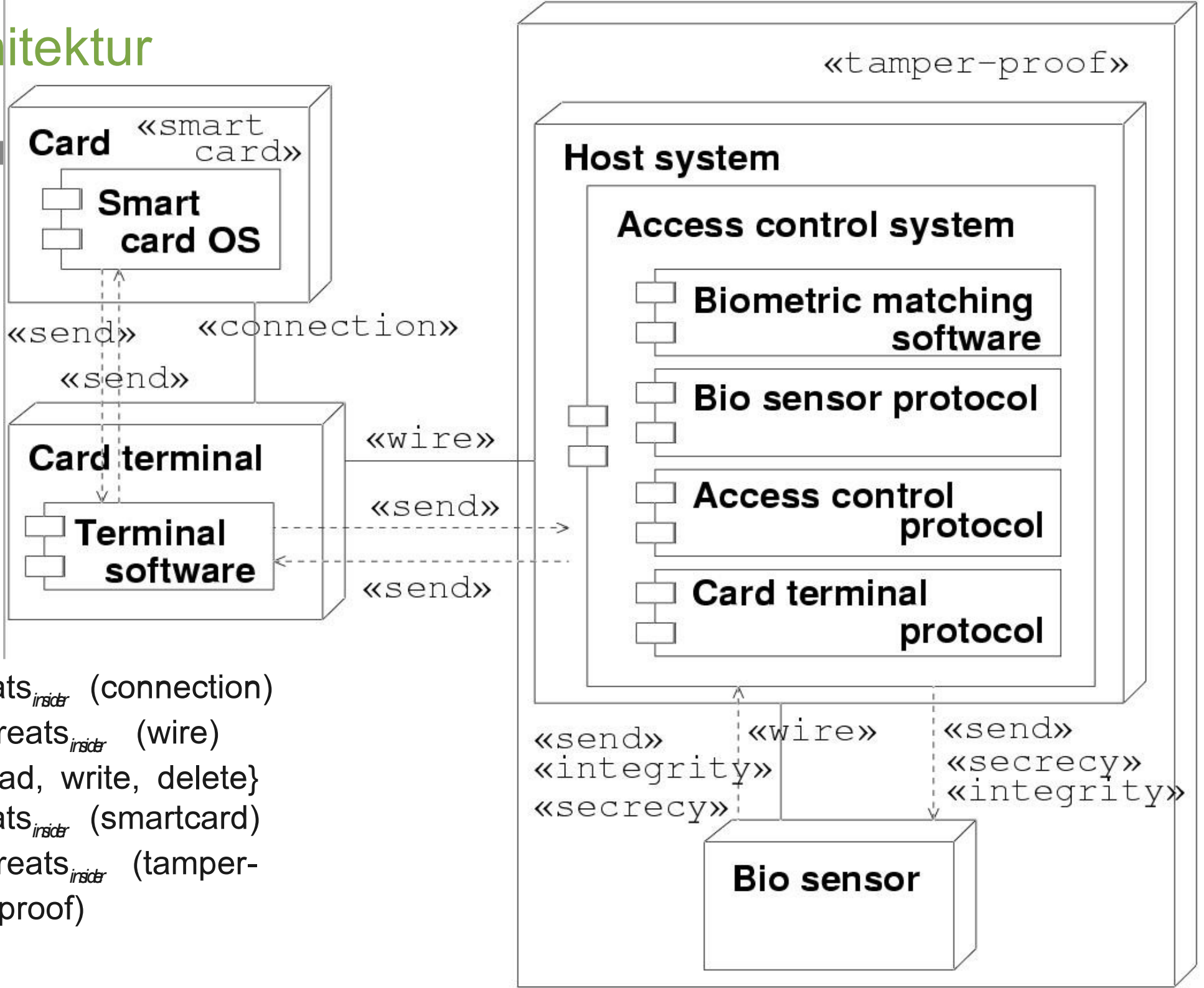
Anwendungsfälle



Anwendungsfall: Biometrische Verifikation

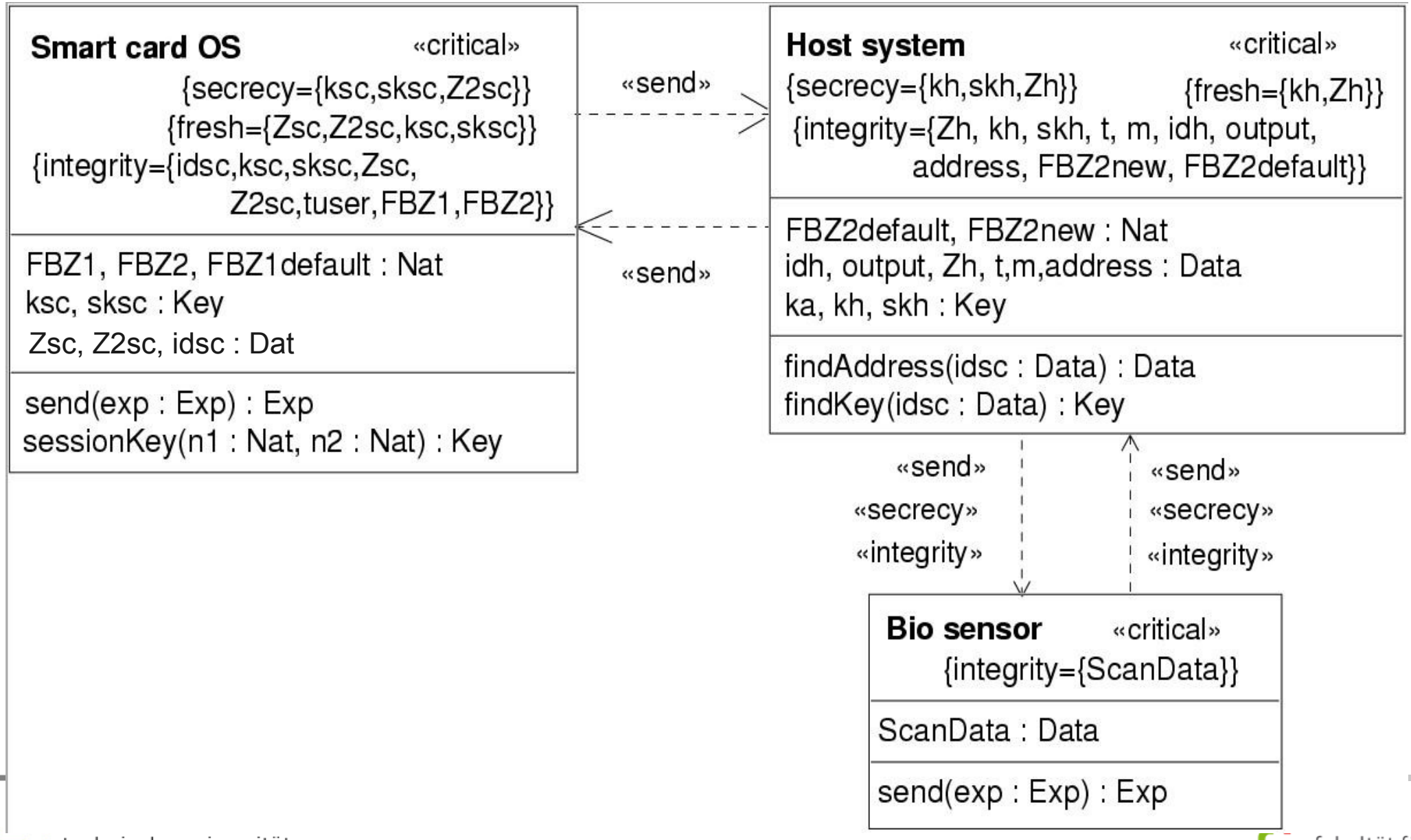


Architektur

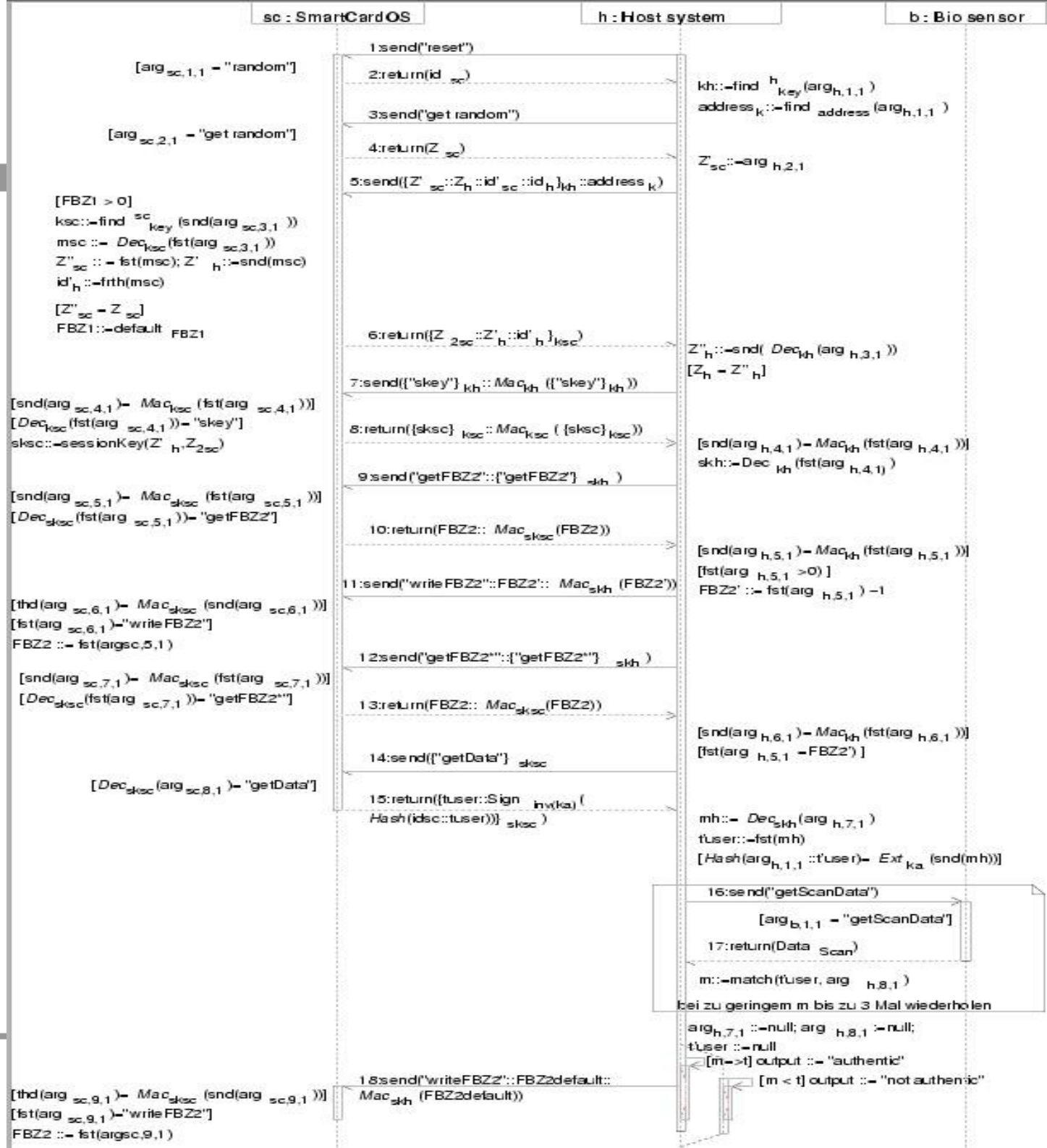


$Threats_{insider}$ (connection)
= $Threats_{insider}$ (wire)
= {read, write, delete}
$Threats_{insider}$ (smartcard)
= $Threats_{insider}$ (tamper-proof)
= Ø

Klassendiagramm



Protokoll (Vogel-Perspektive)



Zusammenfassung

- Grundlagen Biometrie
- Biometrieverfahren
- Biometriearchitektur und Angriffspunkte