Willkommen zur Vorlesung

Methodische Grundlagen des Software-Engineering

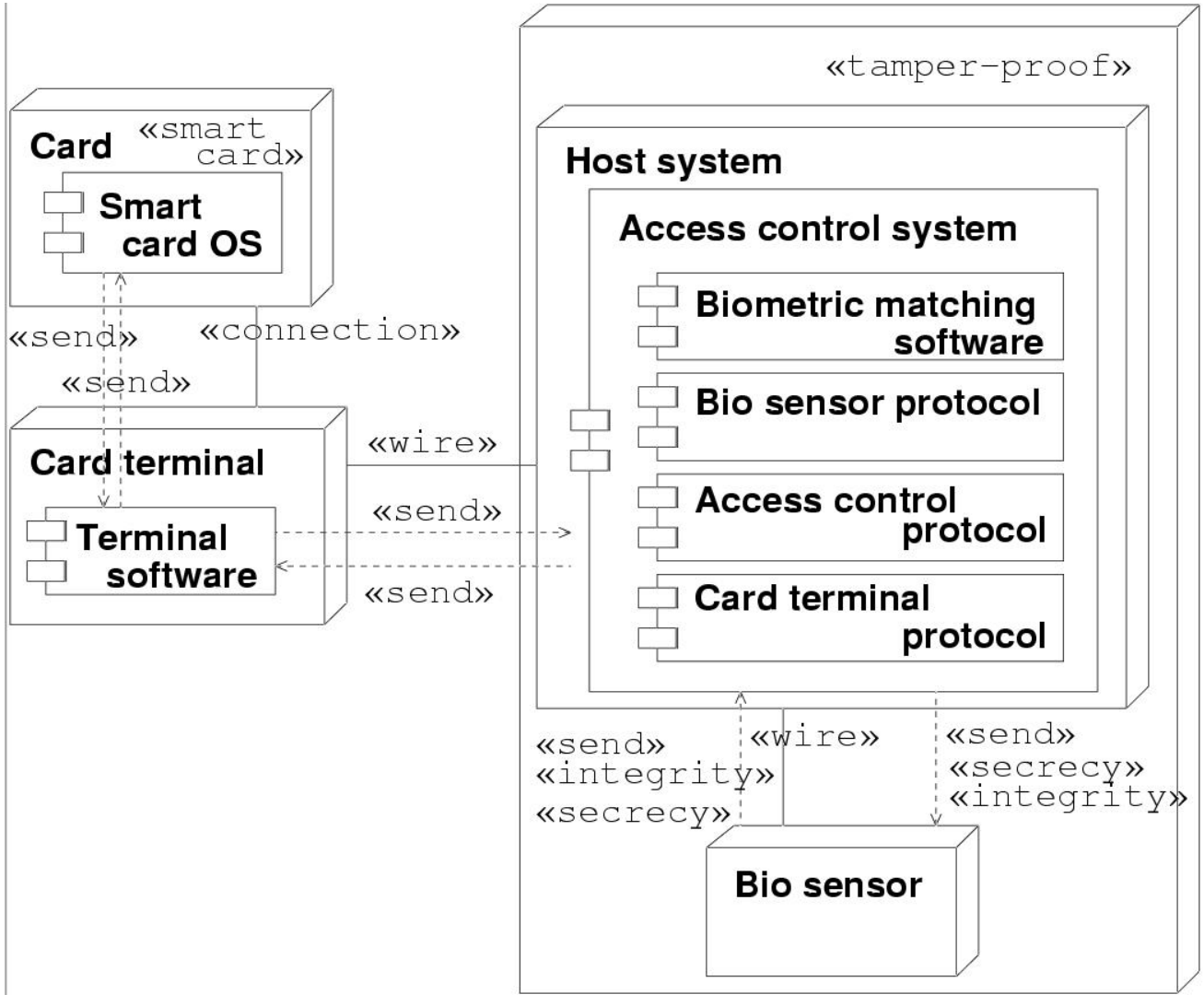
im Sommersemester 2011

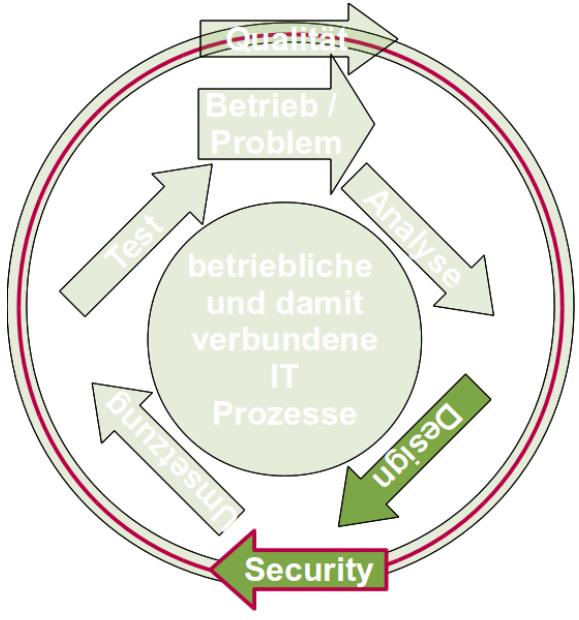
Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

23. Biometrische Authentisierung

Einordnung
Biometrische Authentifizierung mit UMLsec

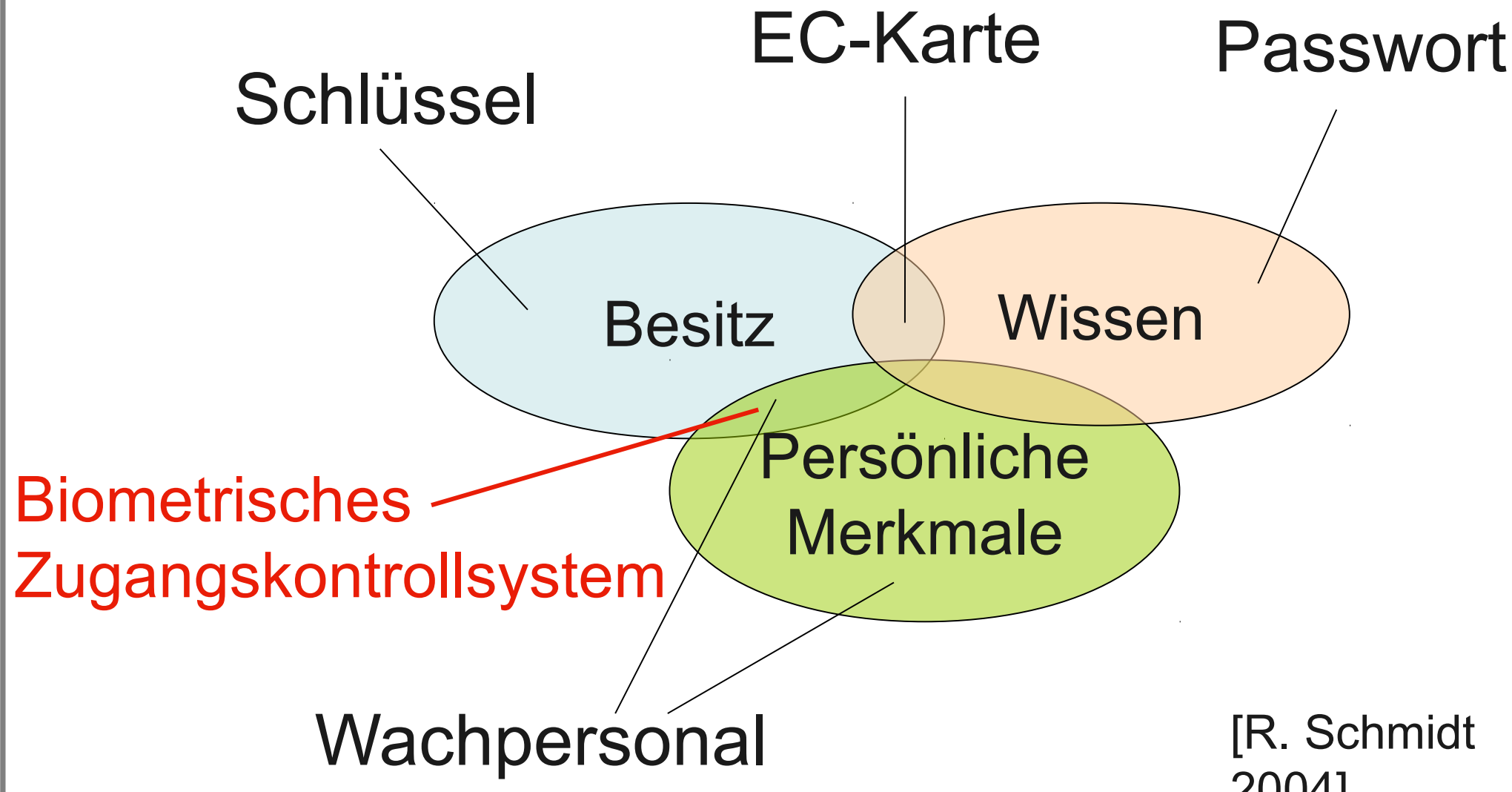




Einordnung
Einführung UML / UMLsec

- Business Prozesse
- Qualitätsmanagement
- Testen
- Sicherheit
- Sicheres Software Design
  - Einführung UML / UMLsec
  - Kryptographische Protokolle
  - Biometrische Authentifizierung
  - Elektronische Geldbörse
  - Weitere Anwendungsbeispiele

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

Schwachstellen

Schutzmaßnahme	Problem
Schlüssel Wachmann	Kann verloren / gestohlen werden Bestechlich / 24 h Einsatz?
Passwort	Am Arbeitsplatz notiert, an „Administrator“ verraten
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.

- 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

Biometrische Authentisierung

Identifikation: 1 : n Vergleich

Verifikation: 1 : 1 Vergleich

Biometrisches System führt biometrische Verifikation / Identifikation durch.

Unterschiedliche Verfahren, aber unterschiedlich geeignet bzw. problembehaftet

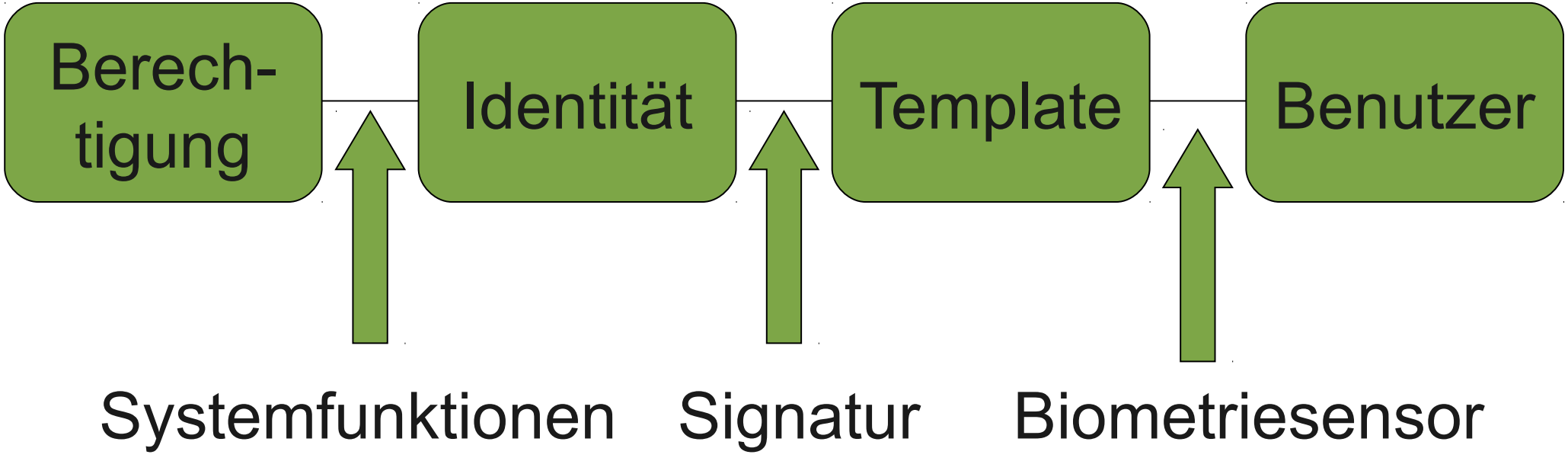
Überblick: Stärken / Schwächen biometrischer Verfahren

[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

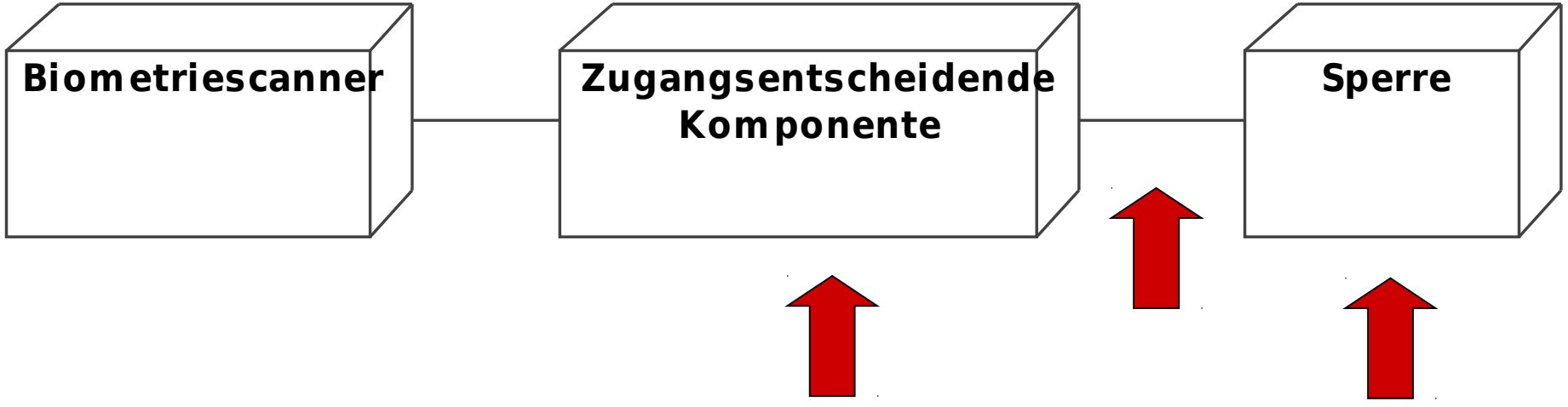
Verknüpfungskette:



Funktionsweise

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

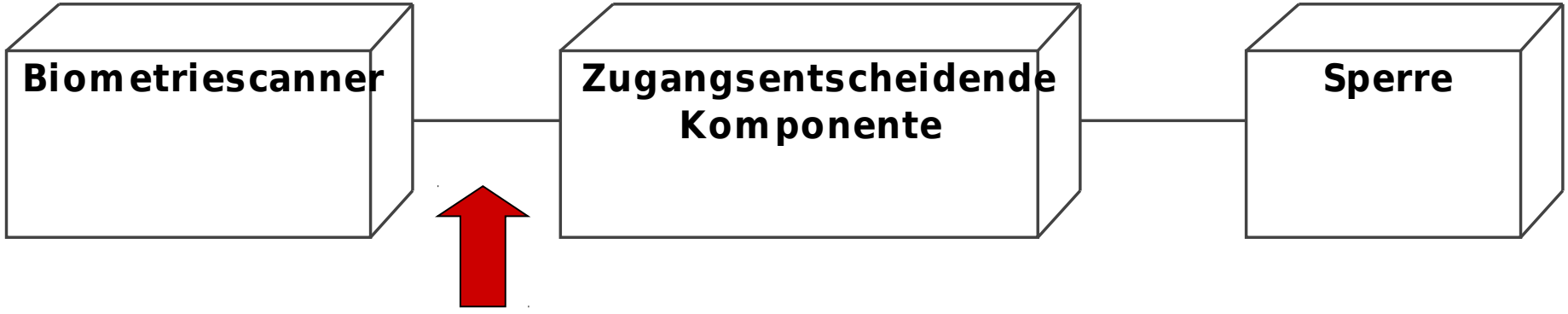
Angriffspunkte I



Angriff: Aufbrechen und / oder elektrisches Signal einspeisen.

➔ Physikalischer Schutz notwendig.

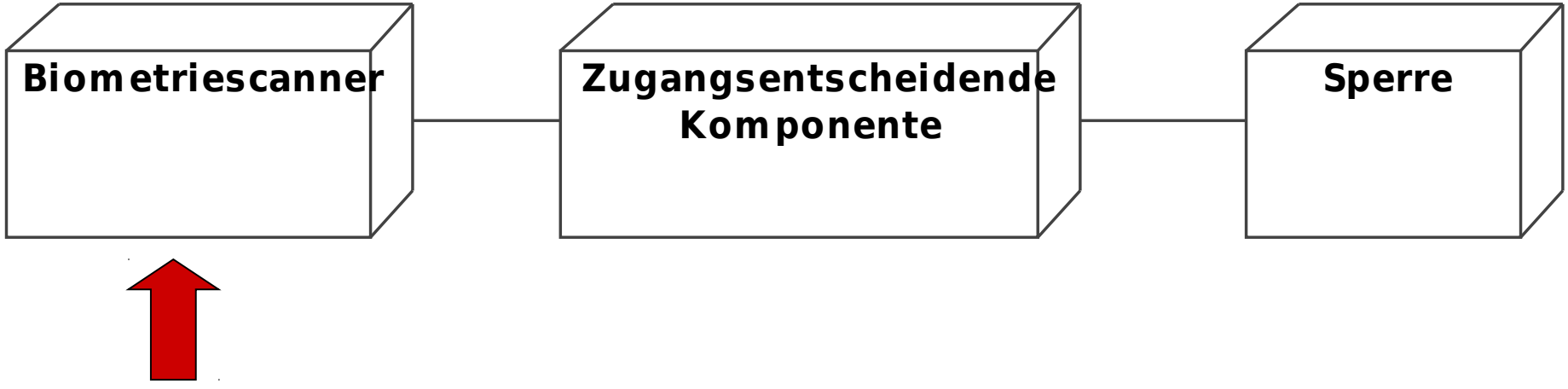
Angriffspunkte II



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 ?

Einschränkungen

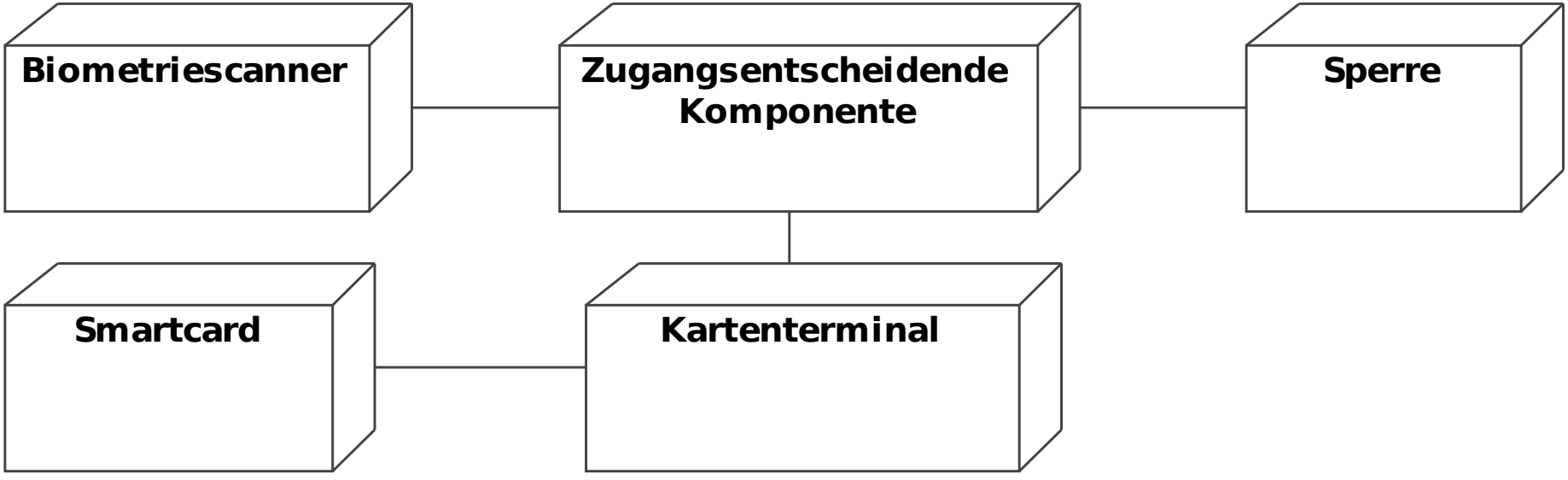
Realisierbarer Modus: Identifikation (1:n)

Notwendig: zentrale Speicherung biometrischer Datensätze.

Probleme:

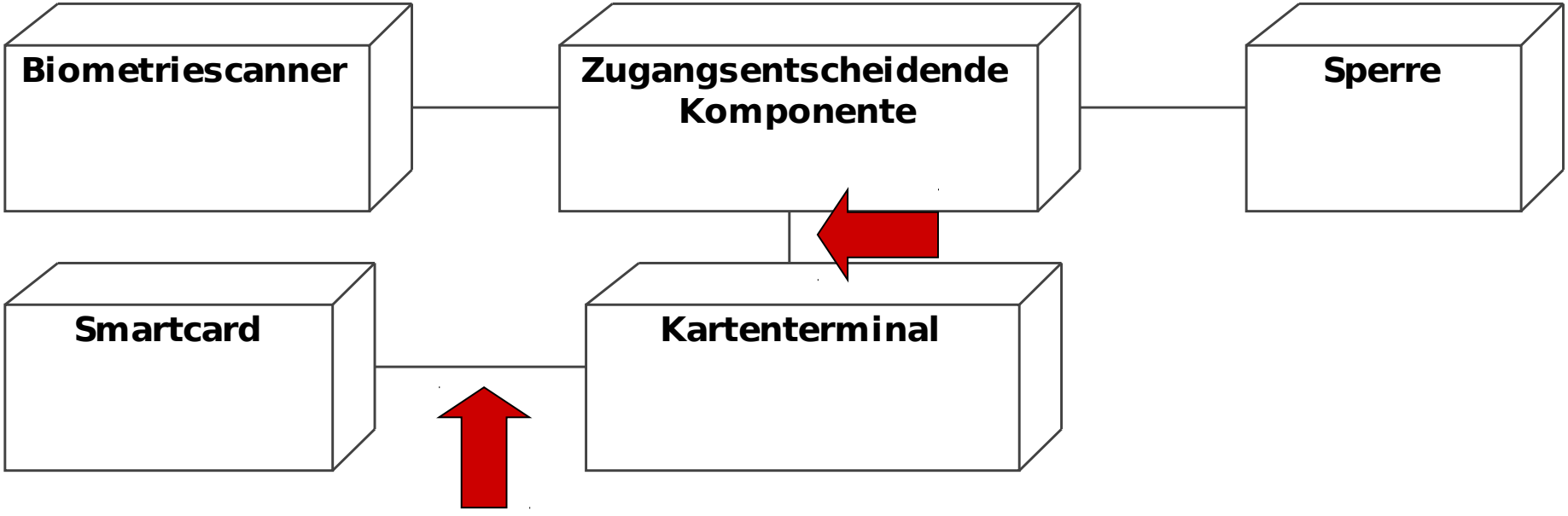
- mehrere Referenzdatensätze betrachten
- Speicherung persönlicher Merkmale unterliegt Datenschutz

System mit personifizierter Smartcard



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

Angriffspunkte IV

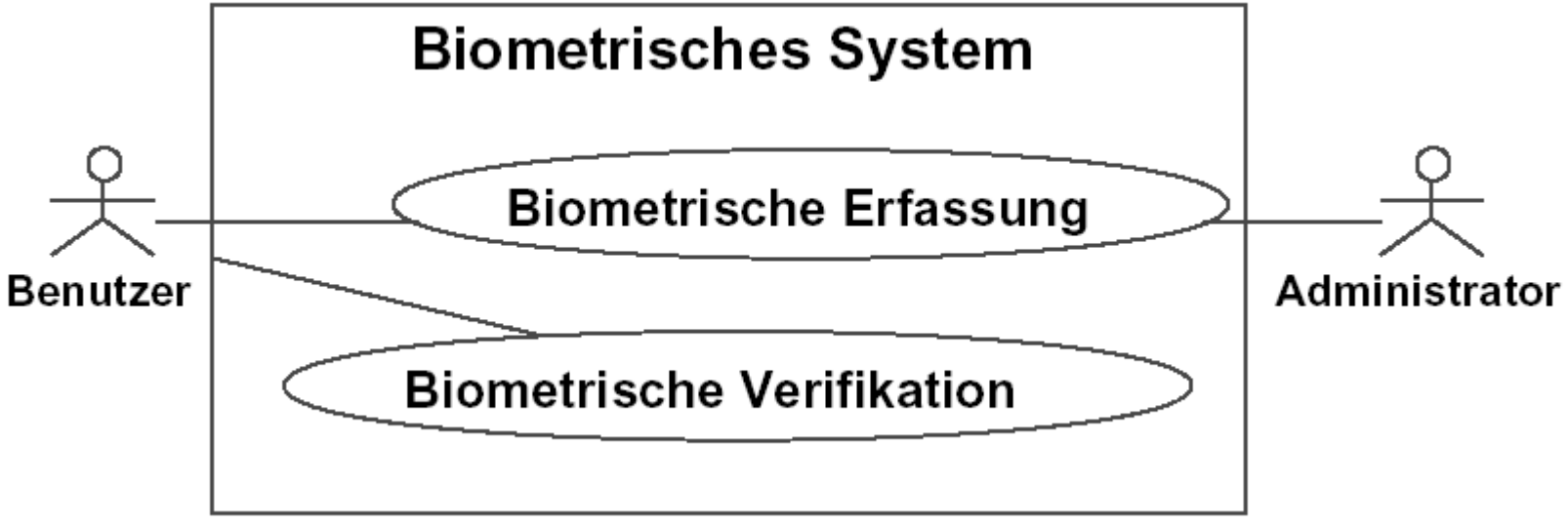


Angriff: Vergleich zwischen gespeichertem Referenztemplate und aktuellem Wert manipulieren.

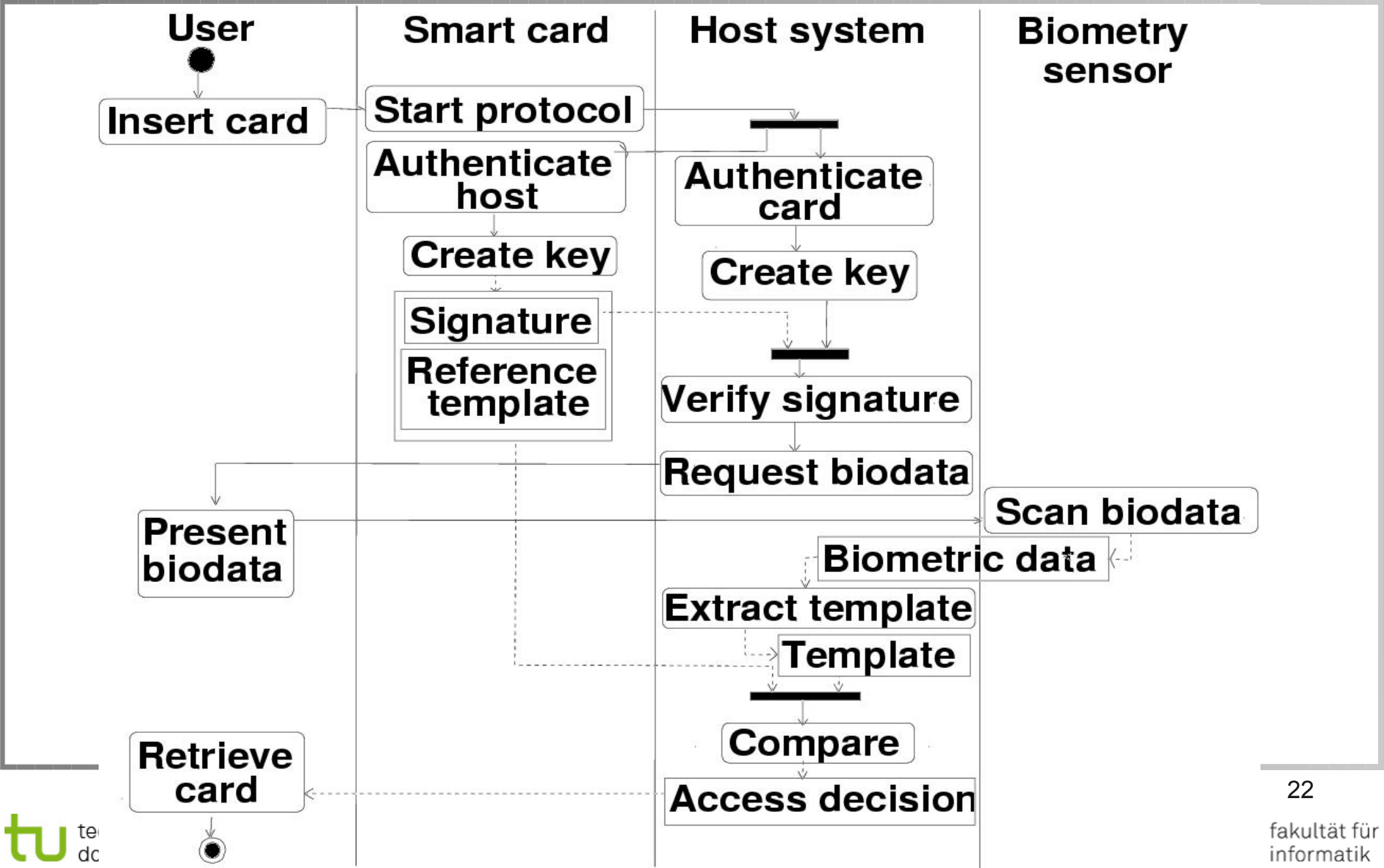
➔ Kryptographische Authentifikation.

Biometrisches Authentifikationssystem in industrieller Entwicklung.

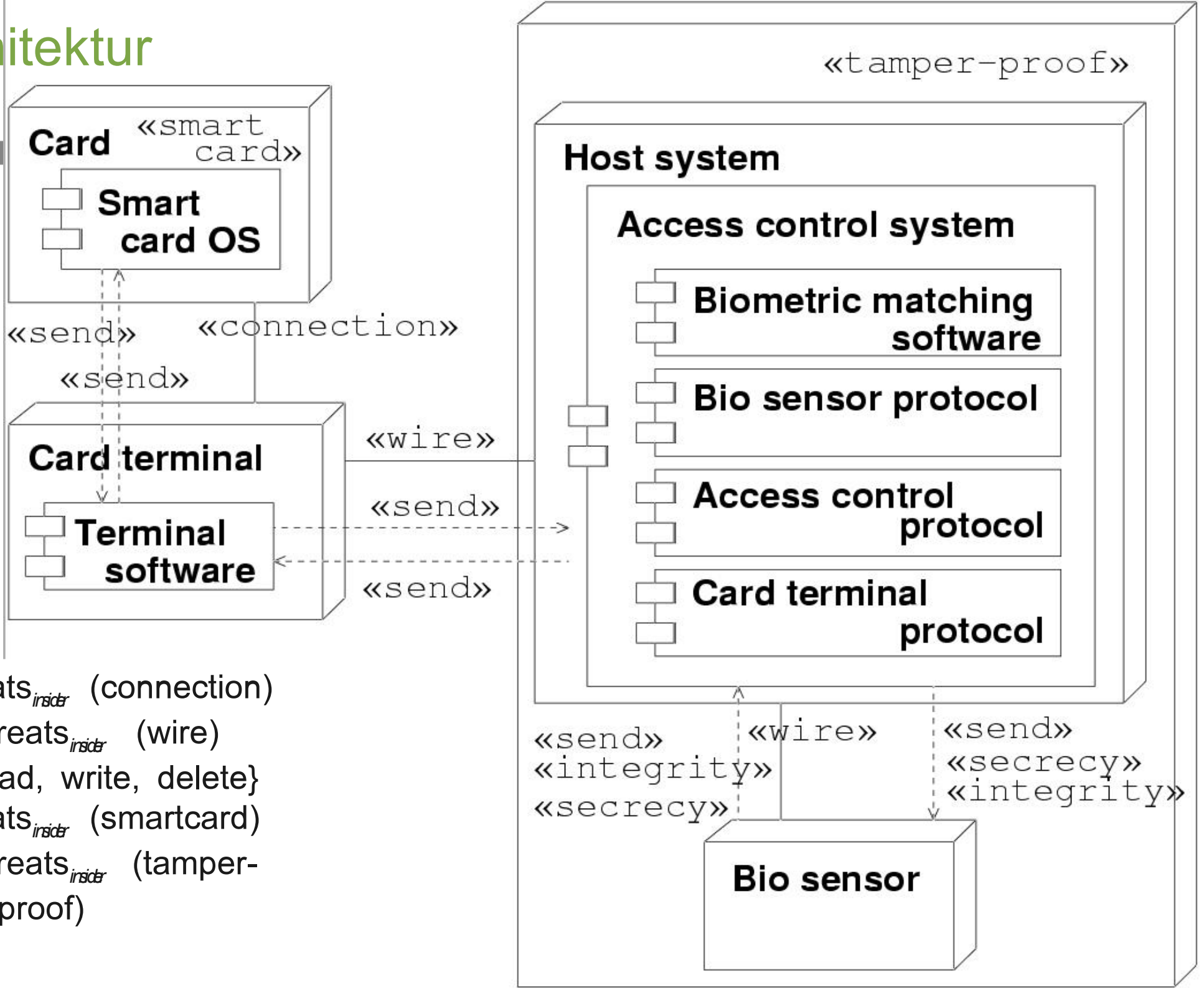
Anwendungsfälle



Anwendungsfall: Biometrische Verifikation

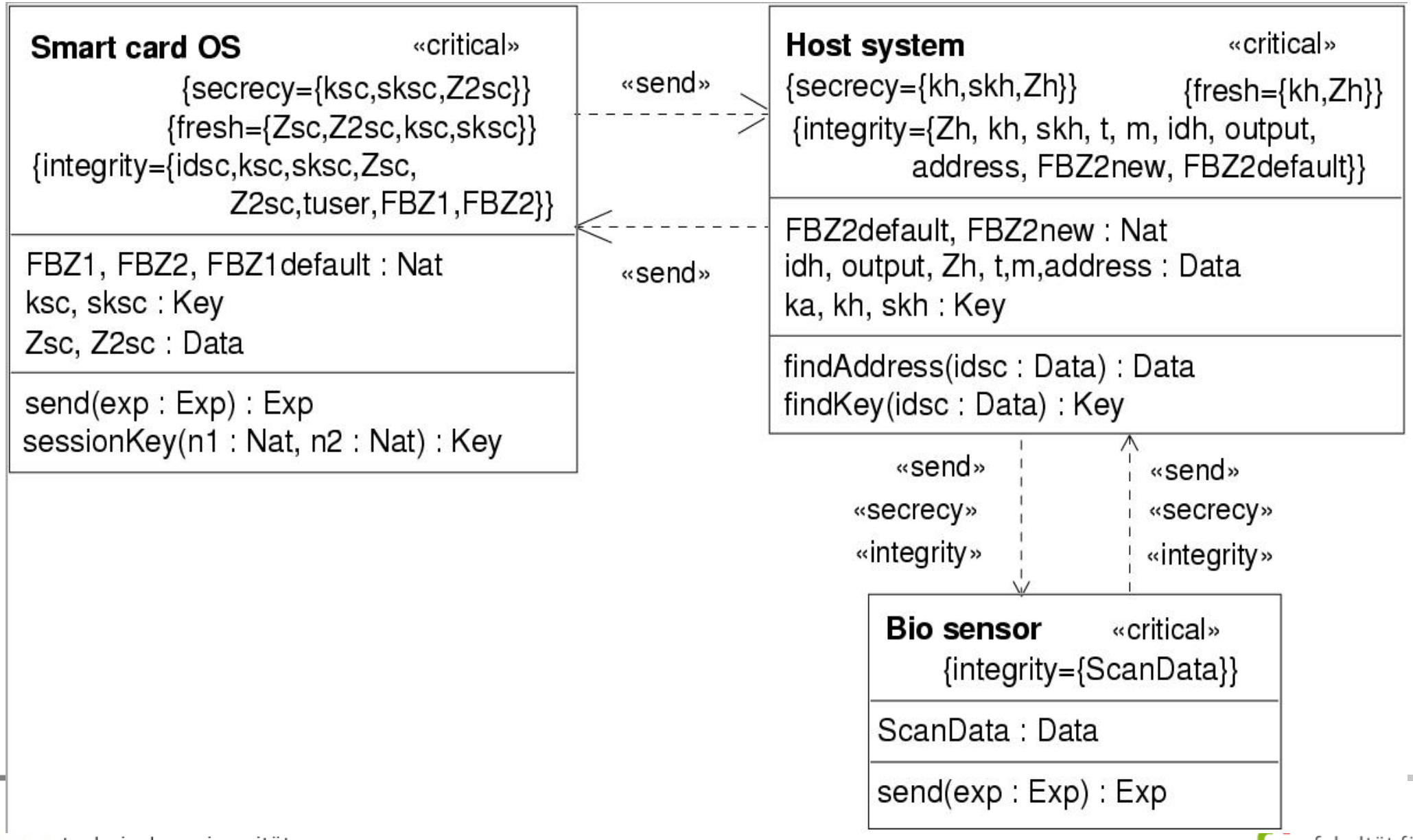


Architektur

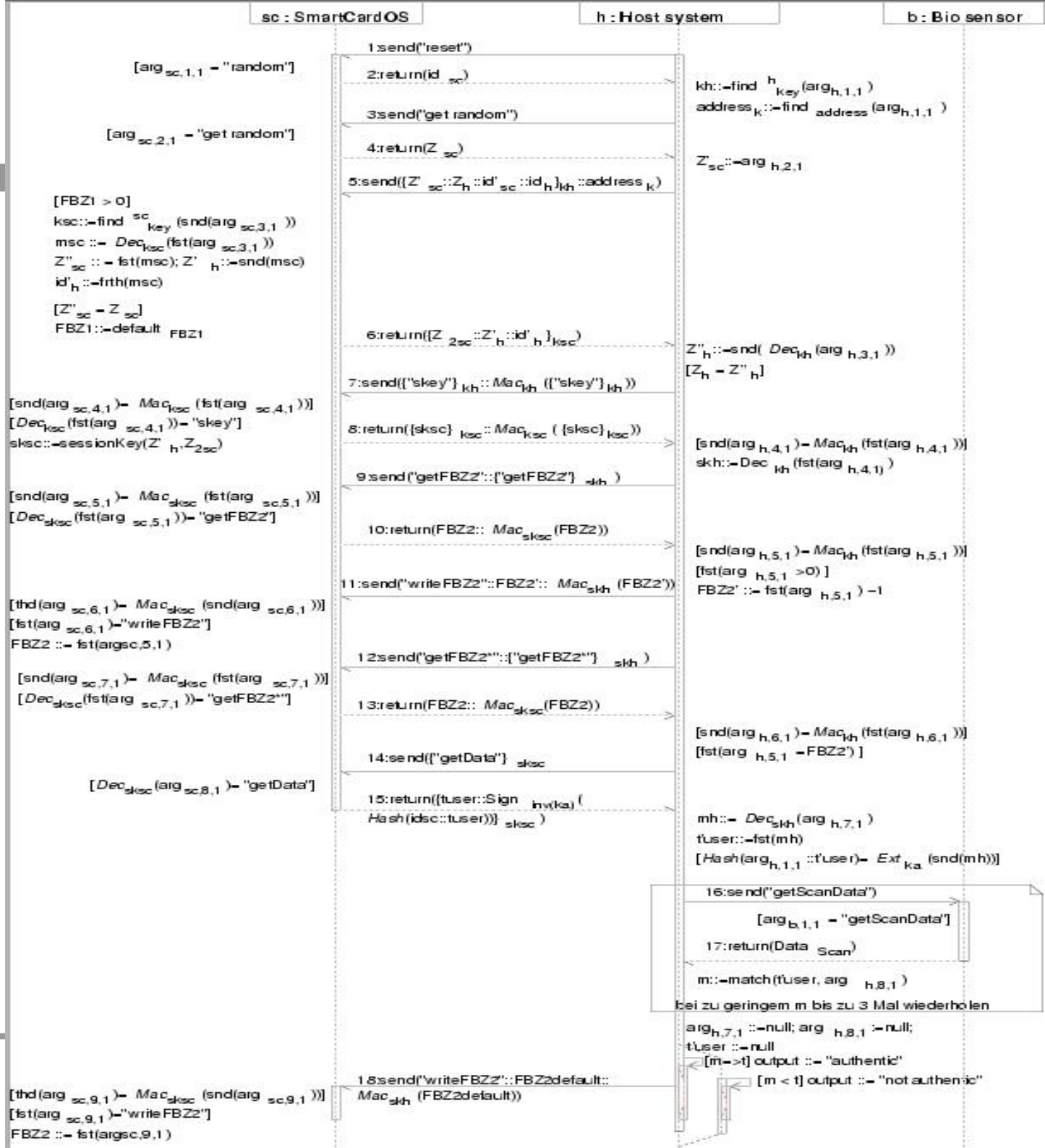


$Threats_{insider}$ (connection)
= $Threats_{insider}$ (wire)
= {read, write, delete}
$Threats_{insider}$ (smartcard)
= $Threats_{insider}$ (tamper-proof)
= Ø

Klassendiagramm



Protokoll (Vogel-Perspektive)



Zusammenfassung

- Grundlagen Biometrie
- Biometrieverfahren
- Biometriearchitektur und Angriffspunkte