

# Wie sicher können PKI sein?

Hannes Federrath

<http://www.inf.tu-dresden.de/~hf2/>

## **Grundlagen**

Grundaufbau eines Signatursystems

Schlüsselgenerierung durch Teilnehmergeräte

## **Public Key Infrastrukturen**

Web of Trust

Hierarchische Zertifizierung

## **Sichere Endgeräte**

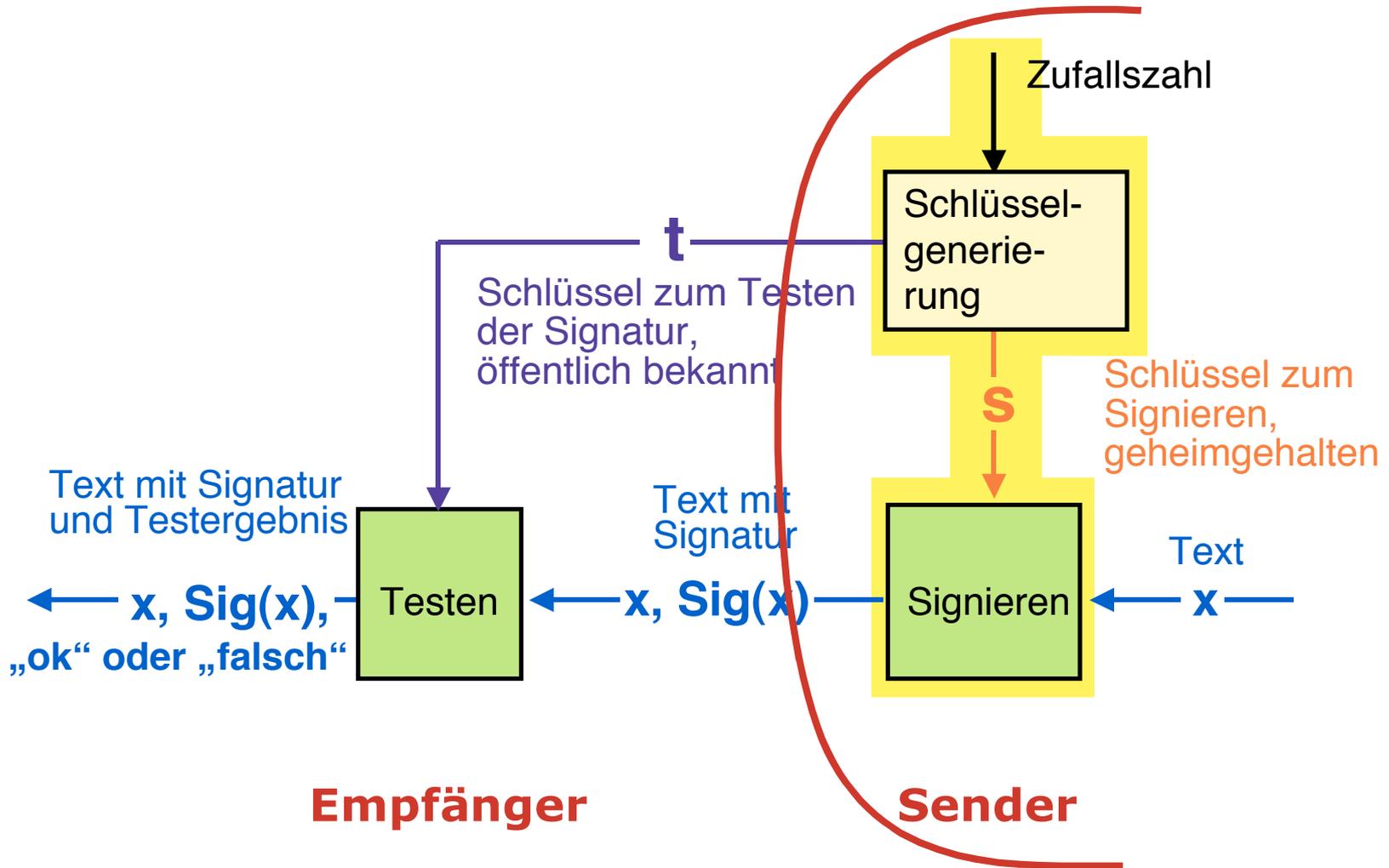
Vertrauenswürdige Kommunikation mit Signierkomponente

Chipkarten bieten nur begrenzte Sicherheit

Angriff „Unterschieben eines gefälschten Dokuments“

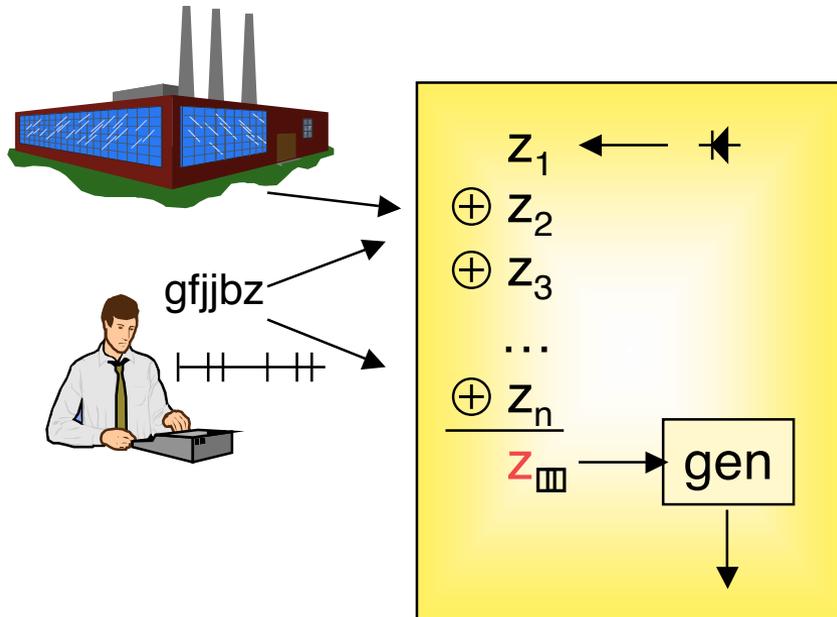
## **Zusammenfassung**

# Digitales Signatursystem



Glasvitrine mit Schloß, es gibt nur einen Schlüssel

# Schlüsselgenerierung

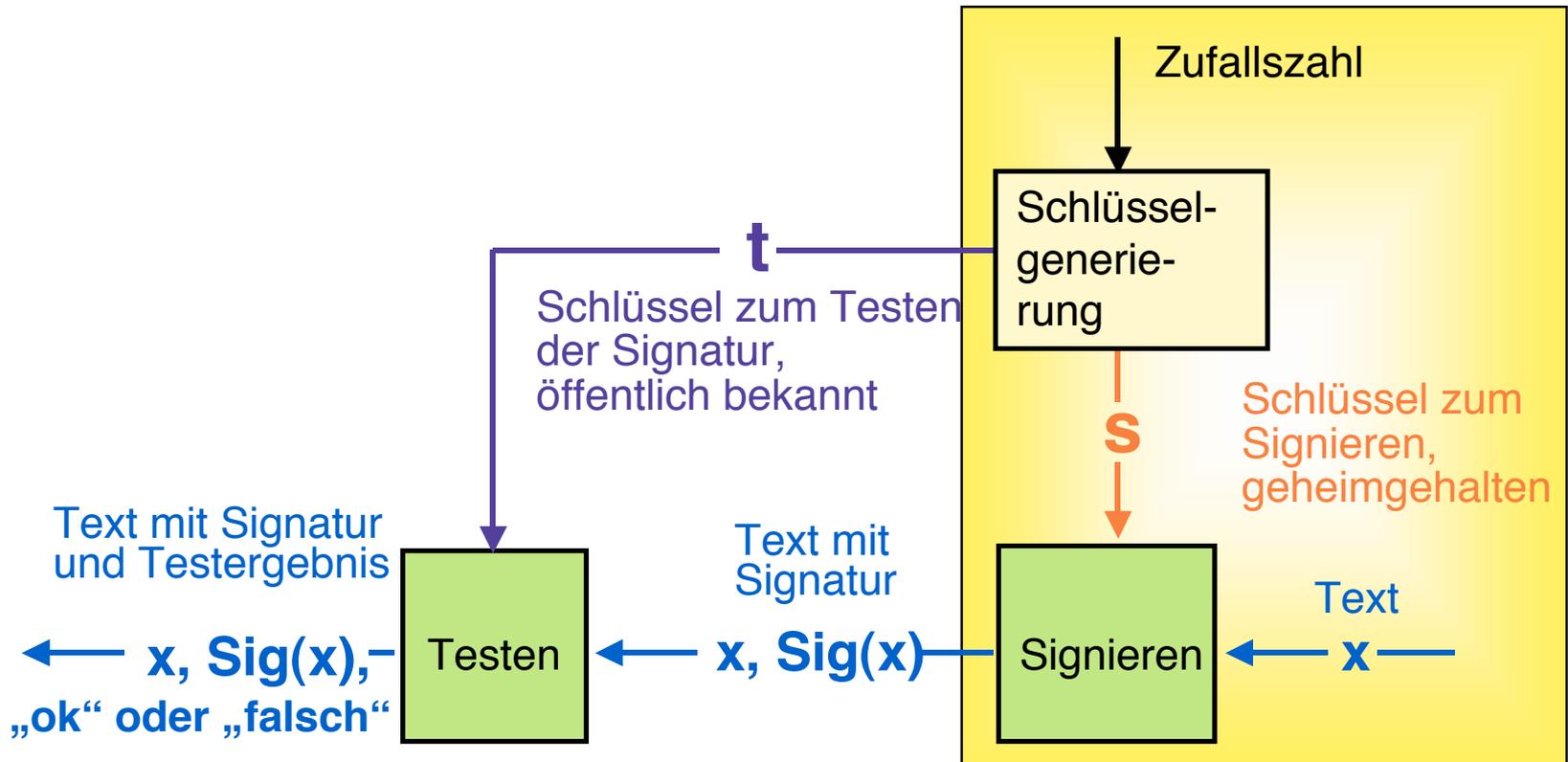


## Erzeugung einer Zufallszahl $z$ für die Schlüsselgenerierung:

XOR aus

- $z_1$ , einer im Gerät erzeugten,
- $z_2$ , einer vom Hersteller gelieferten,
- $z_3$ , einer vom Benutzer gelieferten,
- $z_n$ , einer aus Zeitabständen errechneten.

# Digitales Signatursystem



Schlüsselgenerierung in  
Signierkomponente für  
optimalen Schutz von  $s$

# Signierte Nachricht und Zertifikat

-----BEGIN SIGNED MESSAGE-----

Hiermit bestelle ich beim Lebensmittelversandhaus  
www.web-lebensmittel.de folgende Waren:

10 Eier	Euro	2,00
1 Flasche Milch	Euro	1,50
1 Kasten Bier	Euro	10,00
-----		
Gesamtbetrag	Euro	13,50

Die Zahlung erfolgt bei Lieferung.

Hannes Federrath

-----BEGIN SIGNATURE-----

iQA/AwUBOi9/VLoBzbJXQK0fgCg4CYo1rMKCKrdhezgAn2Rs  
amogkkm+Off90LOW5RxUubFS  
=eXuv

-----END SIGNATURE-----

-----BEGIN CERTIFICATE-----

Name: Hannes Federrath

Public key:

h833hd38dddajscbicme098k236egfkW74h5445  
84hdbscldmrtpofjrkt0jedagaszw12geb3u4b=

Date: 19.11.2001

Valid until: 18.11.2002

Issuer: Einwohnermeldeamt Dresden

Signature of Issuer:

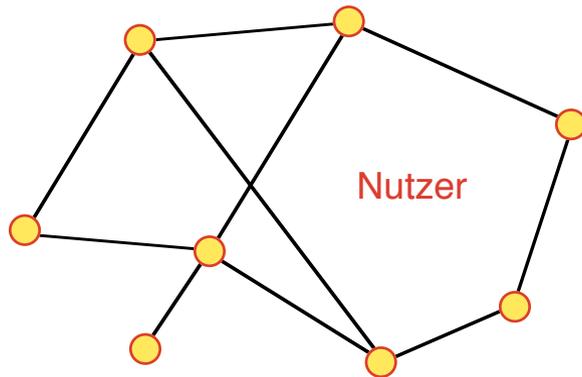
23j423vdsaz345kj435ekj4z2983734ijo23i72  
kj867wdbez2o074j5lkdmc1237t3rgbdvbwj=

-----END CERTIFICATE-----

# Zweck der Schlüsselzertifizierung

- ⌘ Betrifft öffentlichen Testschlüssel für die digitale Signatur
- ⌘ Zertifikat:
  - ⊗ bestätigt die **Zusammengehörigkeit von Testschlüssel und Benutzeridentität** bzw. Testschlüssel und Pseudonym.
  - ⊗ Enthält selbst die **Signatur des Zertifizierers**
- ⌘ Ohne Zertifikate:
  - ⊗ Angreifer kann ein Schlüsselpaar generieren und einfach behaupten, daß dieser Schlüssel jmd. gehört.
  - ⊗ Testschlüssel sind wertlos ohne Zertifikat (zumindest in einer offenen Welt)

## ⌘ Web of Trust (*Dezentral*)



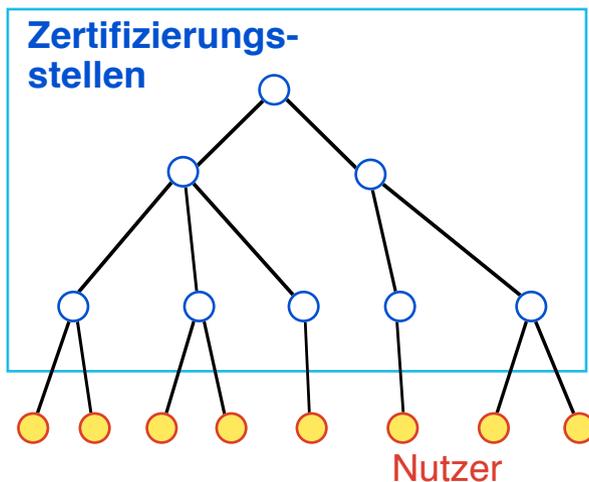
### Vorteile:

- ⊗ einfache, flexible Nutzung
- ⊗ viele potentielle Zertifikatsketten

### Nachteile:

- ⊗ keine oder nur schwer erreichbare Beweisführung im Streitfall
- ⊗ finden eines vertrauenswürdigen Pfades aufwendiger

## ⌘ Hierarchische Zertifizierung (*hierarchisch-zentral*)



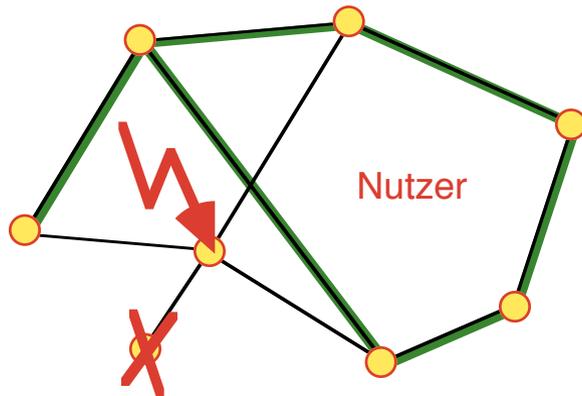
### Vorteile:

- ⊗ klare Strukturen und Zurechenbarkeiten (wichtig im Streitfall)

### Nachteile:

- ⊗ **Overhead durch Organisationsstruktur**
- ⊗
- ⊗

## ⌘ Web of Trust (*Dezentral*)



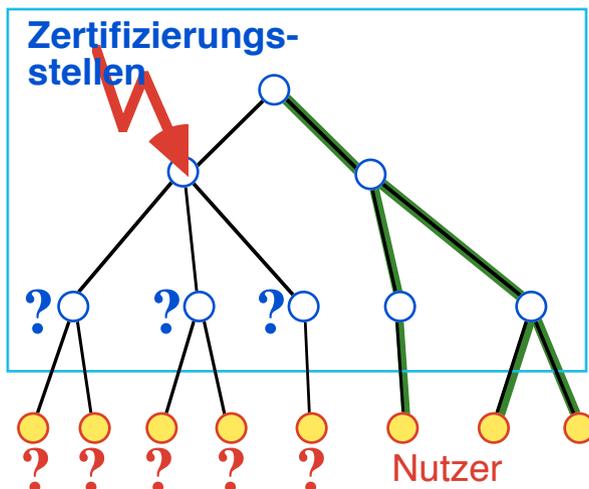
### Vorteile:

- ⊗ einfache, flexible Nutzung
- ⊗ viele potentielle Zertifikatsketten

### Nachteile:

- ⊗ keine oder nur schwer erreichbare Beweisführung im Streitfall
- ⊗ finden eines vertrauenswürdigen Pfades aufwendiger

## ⌘ Hierarchische Zertifizierung (*hierarchisch-zentral*)



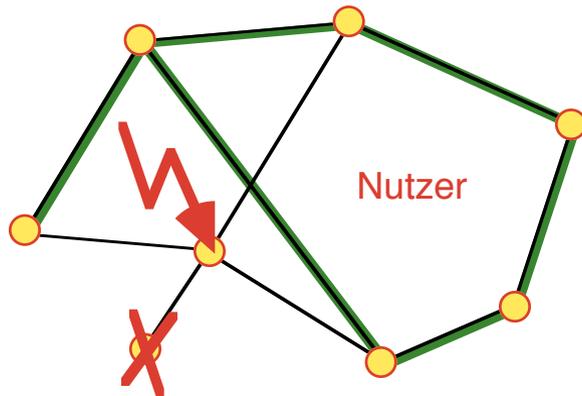
### Vorteile:

- ⊗ klare Strukturen und Zurechenbarkeiten (wichtig im Streitfall)

### Nachteile:

- ⊗ Overhead durch Organisationsstruktur
- ⊗ **anfällig gegen Fehlverhalten**
- ⊗

## ⌘ Web of Trust (*Dezentral*)



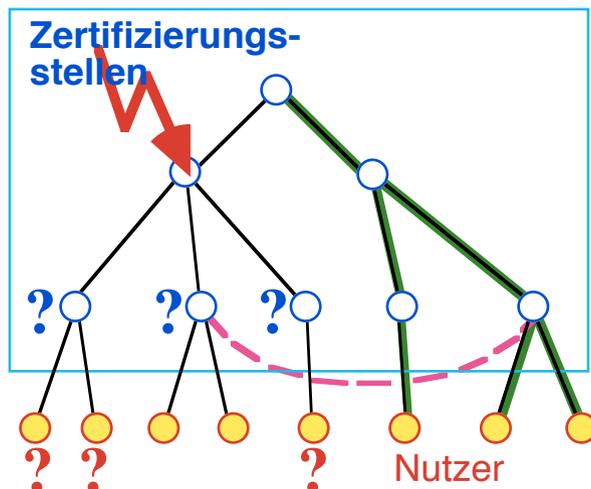
### Vorteile:

- ⊗ einfache, flexible Nutzung
- ⊗ viele potentielle Zertifikatsketten

### Nachteile:

- ⊗ keine oder nur schwer erreichbare Beweisführung im Streitfall
- ⊗ finden eines vertrauenswürdigen Pfades aufwendiger

## ⌘ Hierarchische Zertifizierung (*hierarchisch-zentral*)



### Vorteile:

- ⊗ klare Strukturen und Zurechenbarkeiten (wichtig im Streitfall)

### Nachteile:

- ⊗ Overhead durch Organisationsstruktur
- ⊗ anfällig gegen Fehlverhalten
- ⊗ **Cross Certification reduziert Fehlermöglichkeiten**

# Was geht mit Web of Trust?

## ⌘ Kommunikation in geschlossener Gruppe

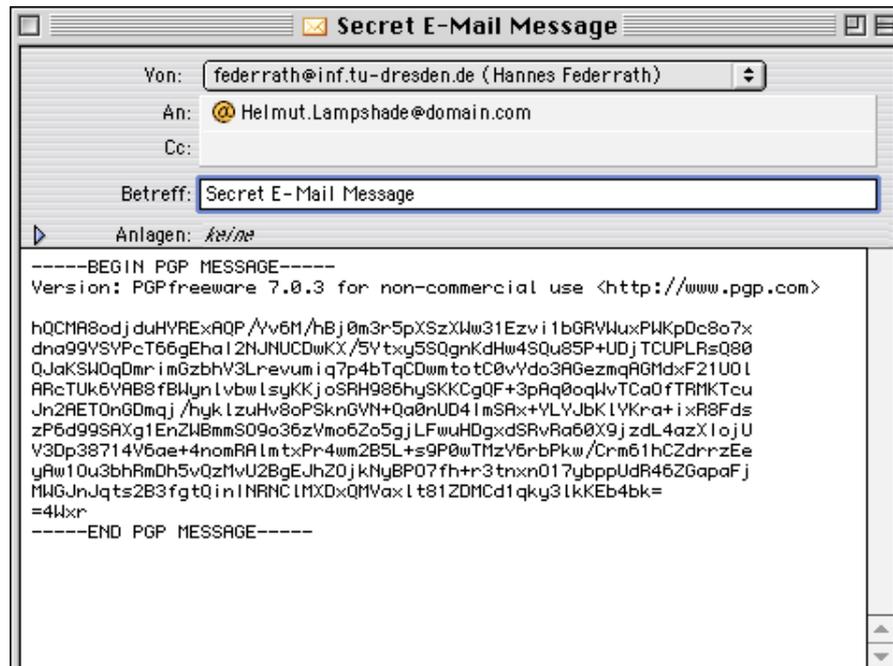
☒ mit festgelegter Policy: sehr gut

## ⌘ Offene Kommunikation

☒ zunächst ohne rechtliche Relevanz: sehr gut

☒ einfach nur vertraulicher und authentischer Nachrichtenaustausch zwischen den Kommunikationspartnern,

☒ eben Pretty Good Privacy



Pretty Good Privacy

<http://www.pgp.com>



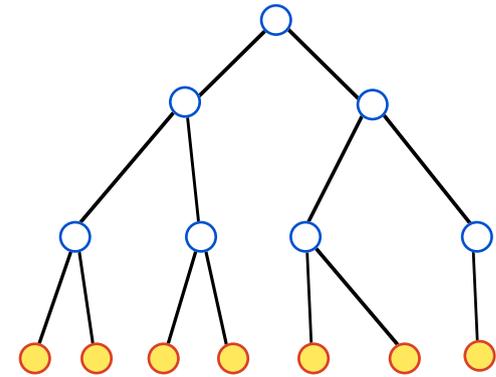
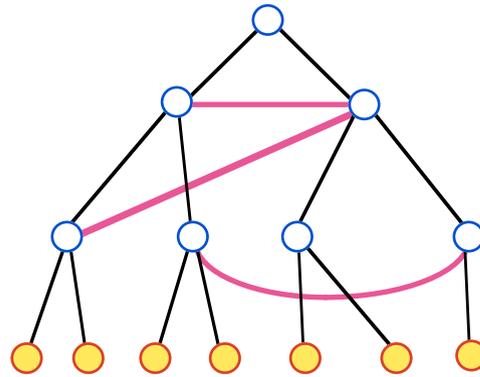
# Zertifizierungsmodelle

Haftung des  
Zertifizierers

Vermaschter  
Graph

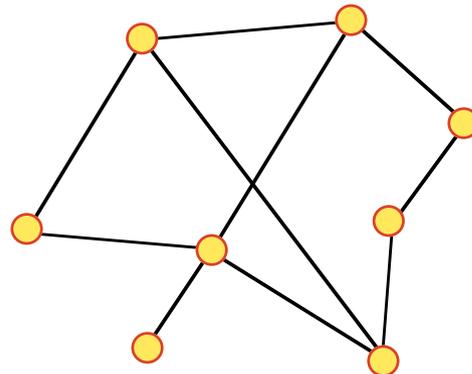
Baum  
(minimal zusammen-  
hängender Graph)

Ja



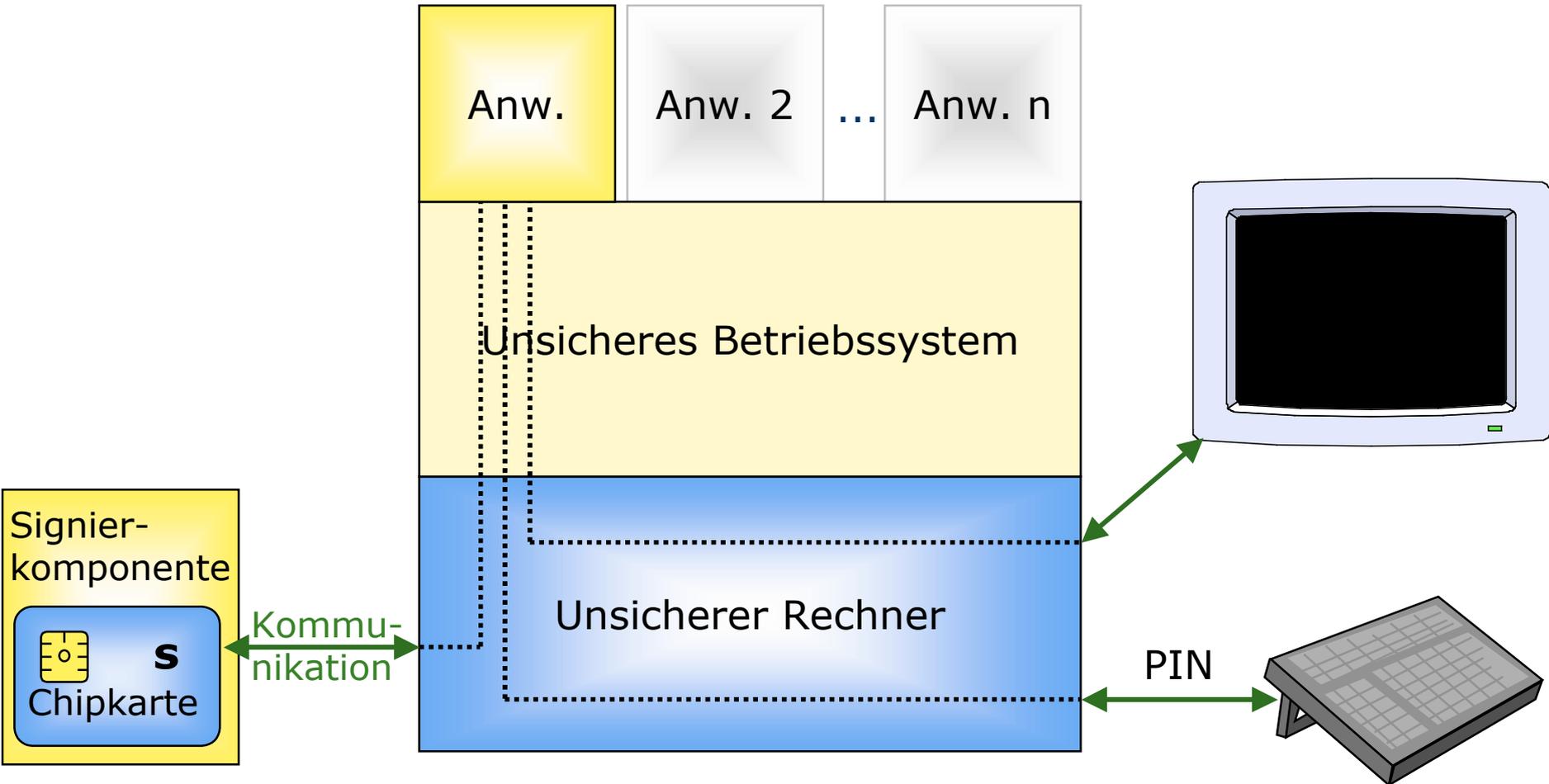
Reduzieren der  
Fehleranfälligkeit durch  
Cross Certification

Nein



—

## UNSICHER



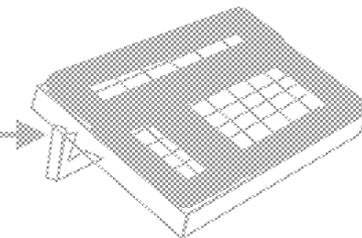
# Ablauf auf Standard-PC mit Chipkarte

- ⌘ Anzeige des Dokuments auf dem externem Monitor
- ⌘ Senden des Dokuments (bzw. dessen Hash-Wert) zur Chipkarte
- ⌘ Aktivierung des Signiervorgangs auf der Karte durch PIN-Eingabe
- ⌘ Rückgabe der Signatur an die Anwendung



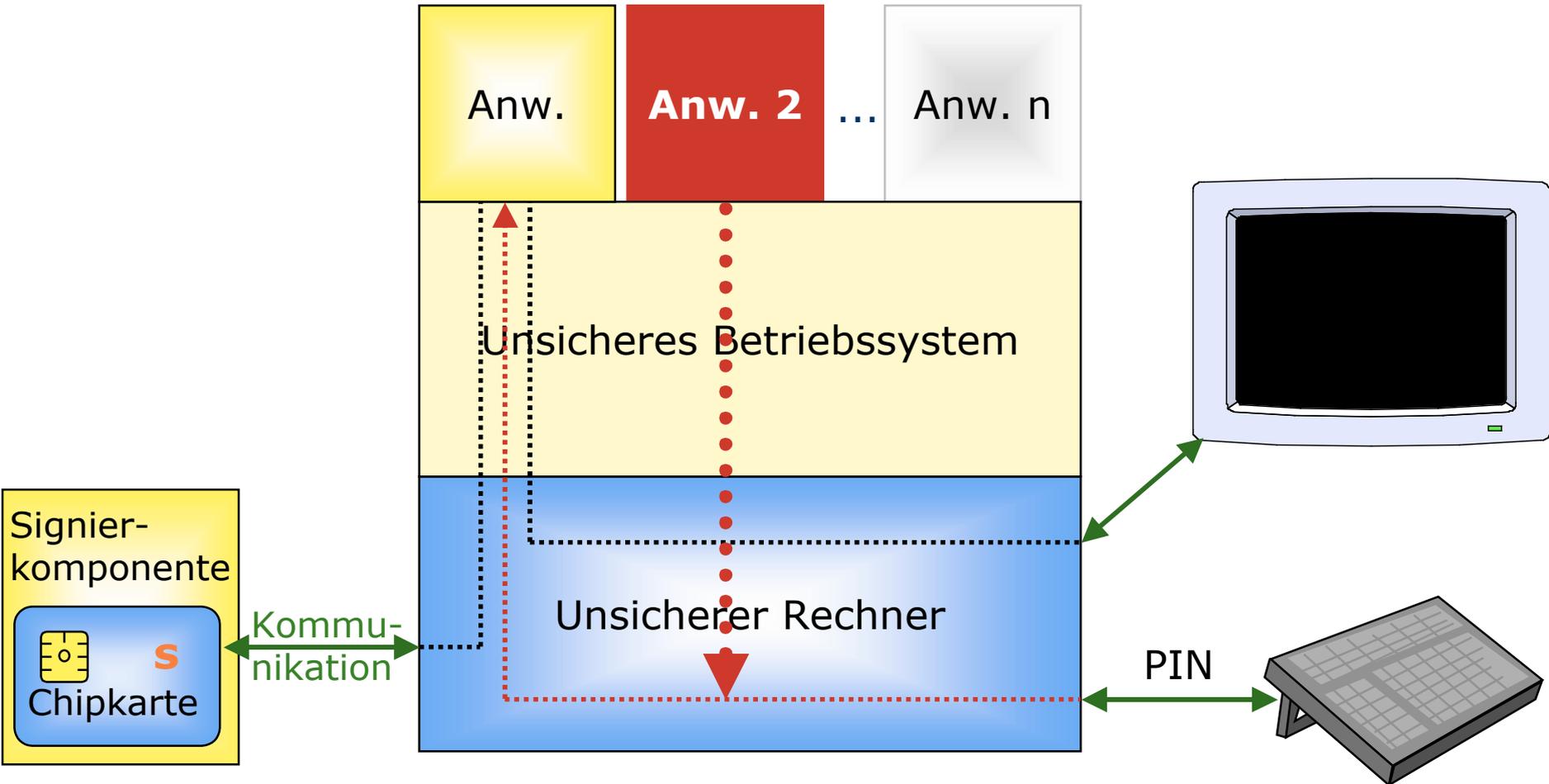
Kommunikation

Unsicherer Rechner



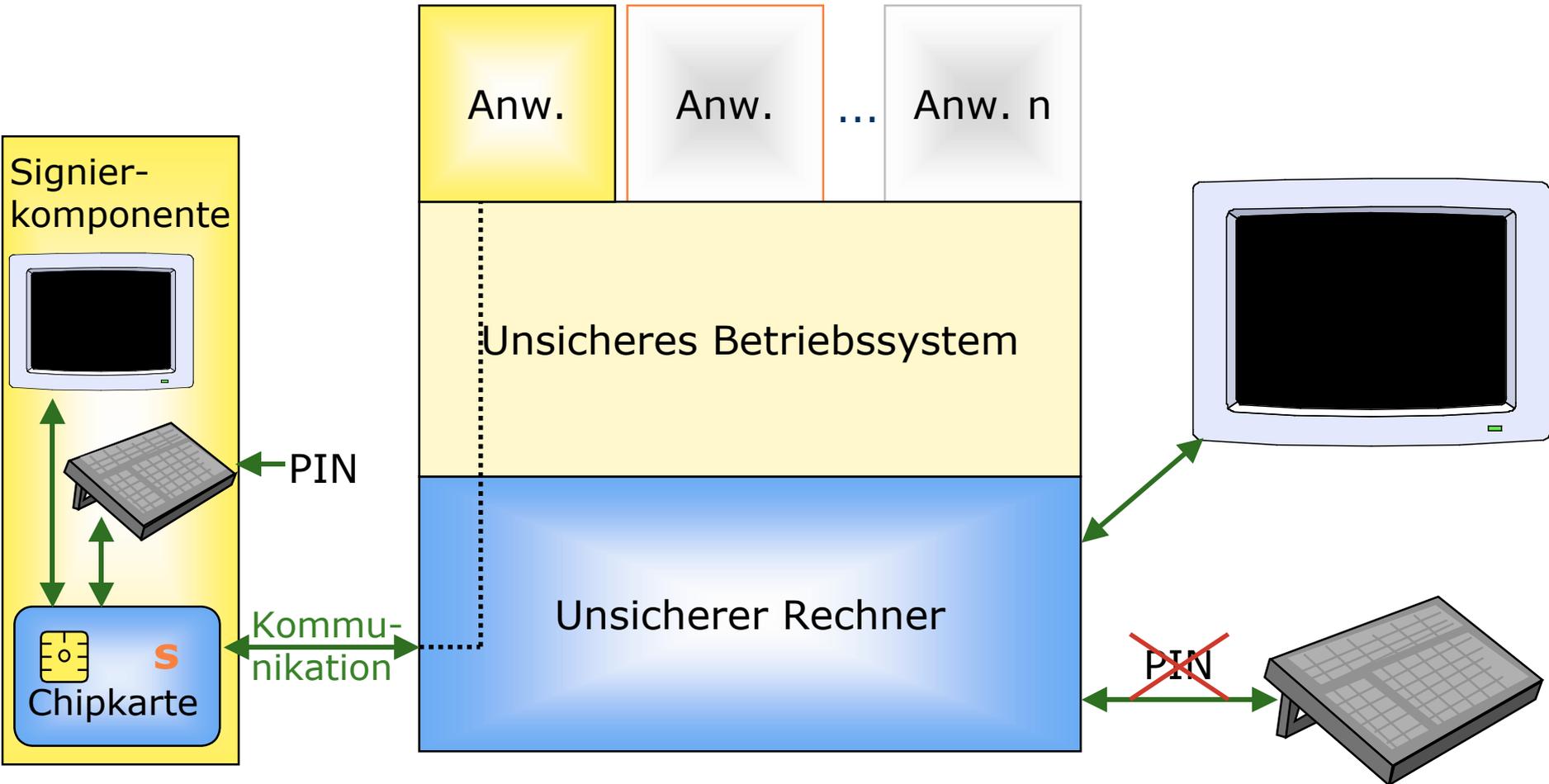
## UNSICHER

Bösartige Anwendung kann z.B. PIN abfangen



# Sichere Signierkomponente mit Standard-PC

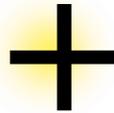
## SICHER



# Sichere (portable) Endgeräte



Entwurf offengelegt



Display

Tastatur

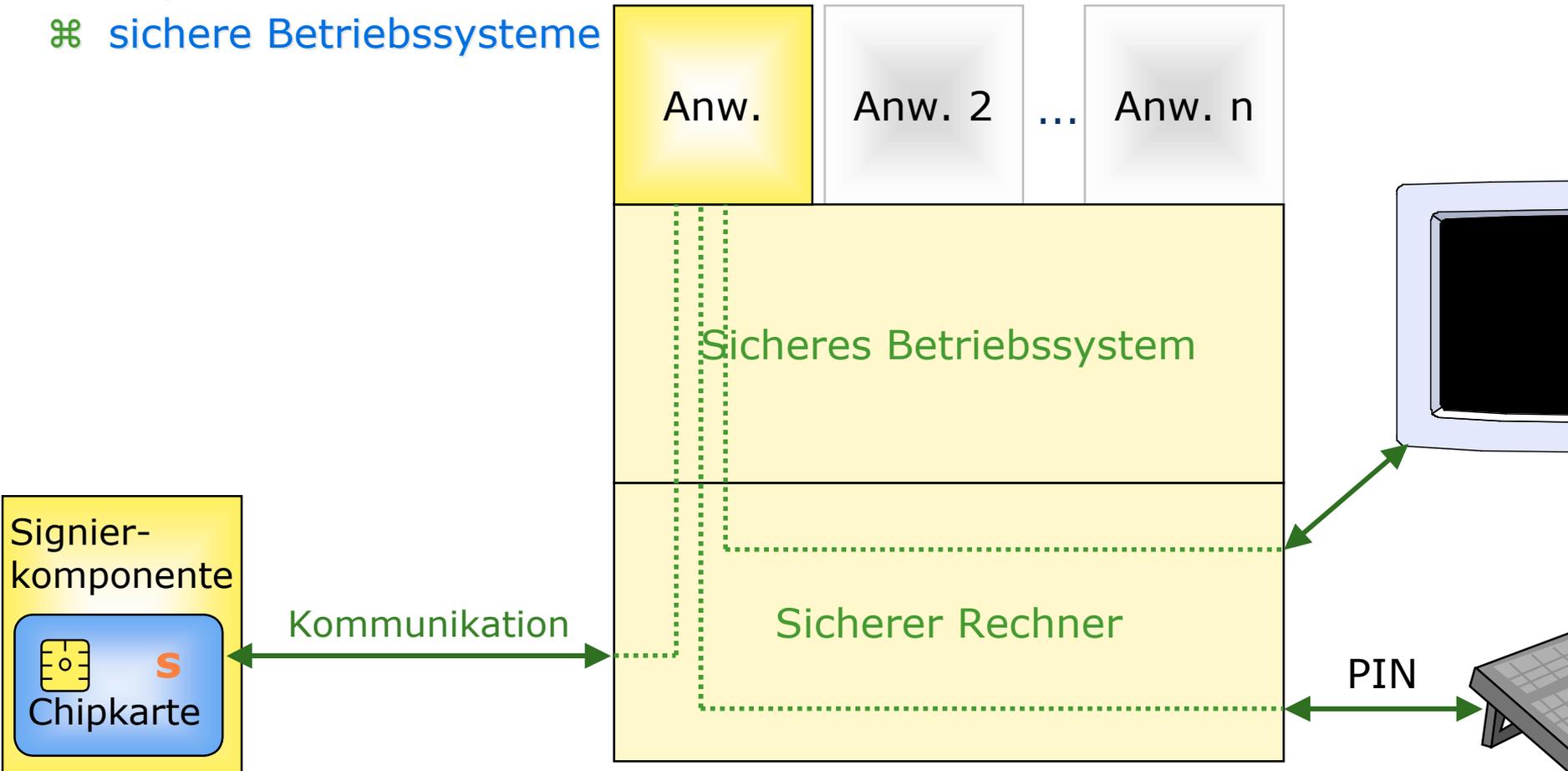
physischer  
Schutz:  
Manipulations-  
erkennung

**PDA oder Handy statt Chipkarte**

# Physisch sichere Geräte und sichere Betriebssysteme

## SICHER, wenn

- ⌘ Physisch sichere Geräte
- ⌘ sichere Betriebssysteme



## ⌘ Schlüsselgenerierung durch Teilnehmergeräte:

- ⊗ Erhöht Sicherheit
- ⊗ Erlaubt vielfältige Pseudonyme, dadurch weniger Profile

## ⌘ Vertrauenswürdige Zertifizierungsinfrastruktur:

- ⊗ Beglaubigung der öffentlichen Testschlüssel
- ⊗ Keine Hinterlegung von Schlüsseln
- ⊗ Kreuzzertifizierung

## ⌘ Vertrauenswürdige Kommunikation mit Signier- und Anzeigekomponente:

- ⊗ Sichere portable Endgeräte – PDA oder Handy statt Chipkarte
- ⊗ Sichere Betriebssysteme