Technischer Datenschutz im Internet

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit · Uni Regensburg

http://www-sec.uni-regensburg.de/

Was ist Sicherheit?

Techniken zum Schutz?

Stand der Technik?

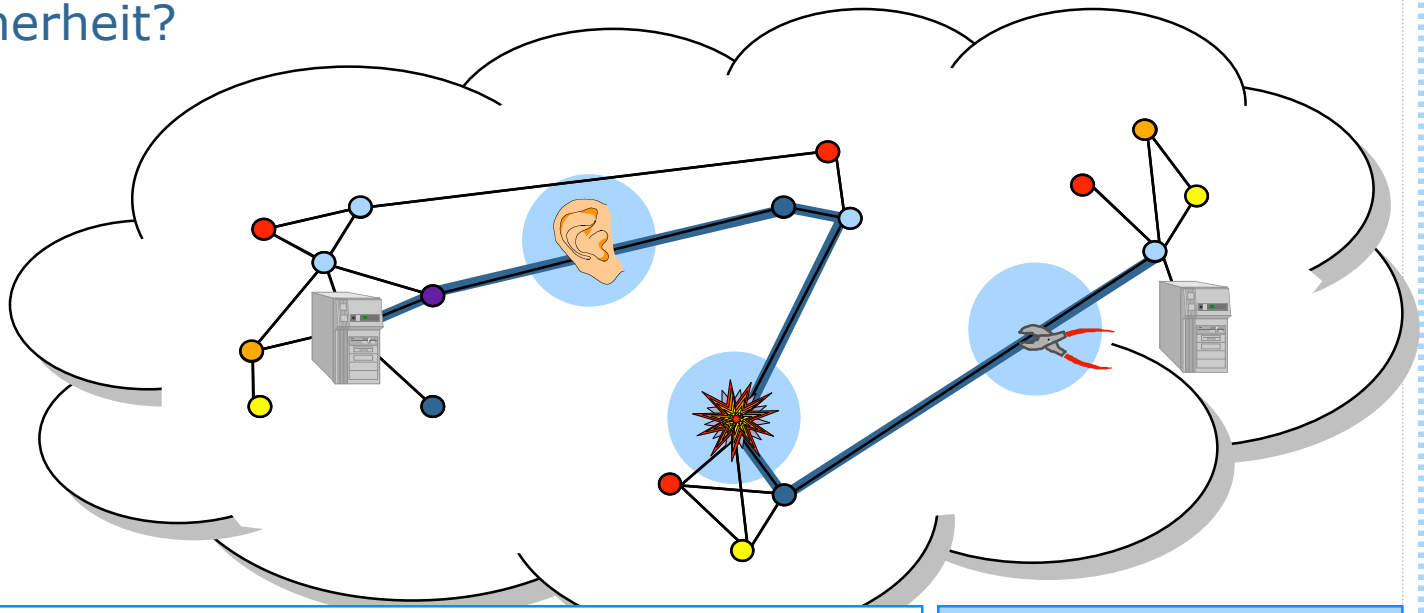
Management der Informationssicherheit

IT-Sicherheitsmanagement versucht, die mit Hilfe von Informationstechnik (IT) realisierten Produktions- und Geschäftsprozesse in Unternehmen und Organisationen systematisch gegen beabsichtigte Angriffe (Security) und unbeabsichtigte Ereignisse (Safety) zu schützen.

- Themen, die am Lehrstuhl bearbeitet werden:
  - Sicherheit in verteilten Systemen und Mehrseitige Sicherheit
  - Datenschutzfreundliche Techniken
  - Sicherheit im Internet
  - Digital Rights Management Systeme
  - Sicherheit im E-Commerce und in mobilen Systemen
- Weitere Informationen:
  - http://www-sec.uni-regensburg.de

Problemstellung

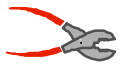
- Was ist Sicherheit?



Bedrohungen


unbefugter Informationsgewinn


unbefugte Modifikation


unbefugte Beeinträchtigung der Funktionalität

Schutz der

Vertraulichkeit

Integrität

Verfügbarkeit

Schutzziele: Einordnung

Kommunikationsgegenstand WAS?		Kommunikationsumstände WANN?, WO?, WER?
Vertraulichkeit **Verdecktheit**	Inhalte	**Anonymität** **Unbeobachtbarkeit** Sender, Ort, Empfänger
Integrität	Inhalte	**Zurechenbarkeit** **Rechtsverbindlichkeit** Absender, Bezahlung, Empfänger
Verfügbarkeit	Inhalte	**Erreichbarkeit** Nutzer, Rechner

Datenschutz

Kommunikationsgegenstand **WAS?**	**Kommunikationsumstände** **WANN?, WO?, WER?**
Vertraulichkeit **Verdecktheit**	**Anonymität** **Unbeobachtbarkeit**
	Zurechenbarkeit **Rechtsverbindlichkeit**

Schutz personenbezogener Daten:
Verkehrsdaten
Interessensdaten

Vertraulichkeit

Verdecktheit

Anonymität
Unbeobachtbarkeit

Zurechenbarkeit
Rechtsverbindlichkeit

Verschlüsselungsverfahren

- **Symmetrische Verschlüsselung, z.B. DES, AES**
  - Kommunikationspartner teilen ein gemeinsames Geheimnis (symmetrischer Schlüssel)
  - Sicherheit basiert meist auf Chaos
  - Schlüssellänge ≥ 128 Bits
- **Asymmetrische Verschlüsselung, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Verschlüsselungsschlüssel
    - *Privaten* Entschlüsselungsschlüssel
  - Sicherheit basiert auf zahlentheoretischen Annahmen
  - Schlüssellänge ≥ 1024 Bit
  - Neuerdings: Elliptische Kurven: ca. 160 Bit

Vertraulichkeit

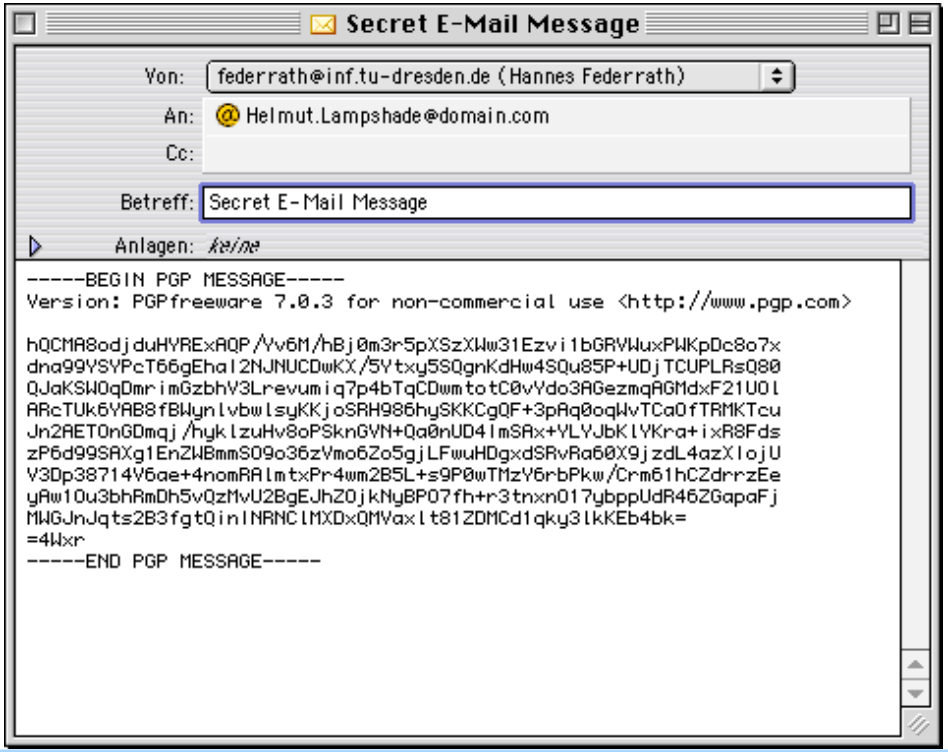
Verdecktheit

Anonymität
Unbeobachtbarkeit

Zurechenbarkeit
Rechtsverbindlichkeit

Verschlüsselungssoftware

- Pretty Good Privacy
  - http://www.pgp.com
  - http://www.pgpi.org
- Gnu Privacy Guard
  - http://www.gnupg.org



Vertraulichkeit

Verdecktheit

Anonymität

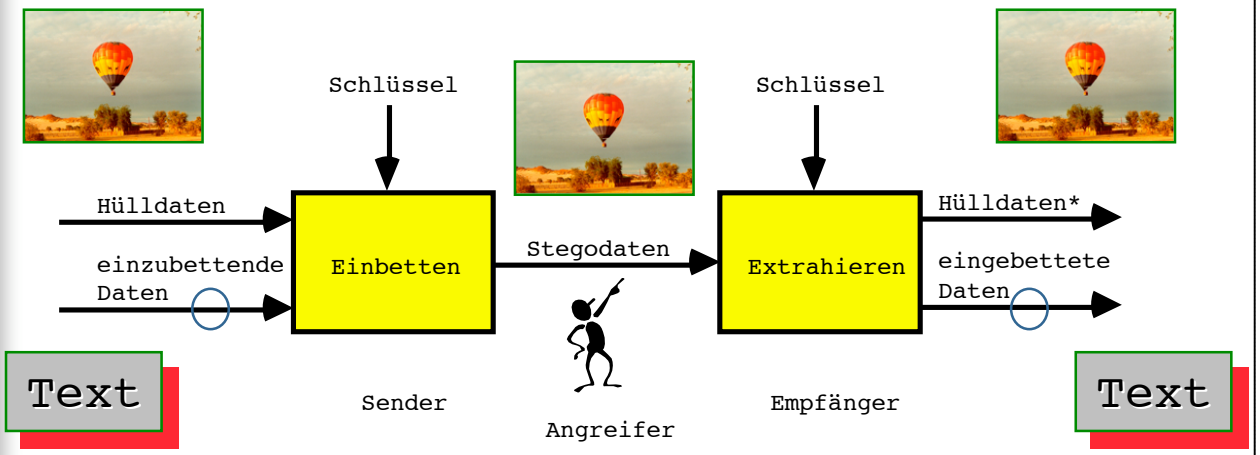
Unbeobachtbarkeit

Zurechenbarkeit

Rechtsverbindlichkeit

Steganographie

- **Verbergen der Existenz einer geheimen Nachricht**
  - geheimzuhaltende Nachricht wird in eine Hülle eingebettet
  - minimale Veränderungen kaum bzw. nicht erkennbar
  - Veränderungen nicht mit Messmethoden nachweisbar



Vertraulichkeit

Verdecktheit

Anonymität
Unbeobachtbarkeit

Zurechenbarkeit
Rechtsverbindlichkeit

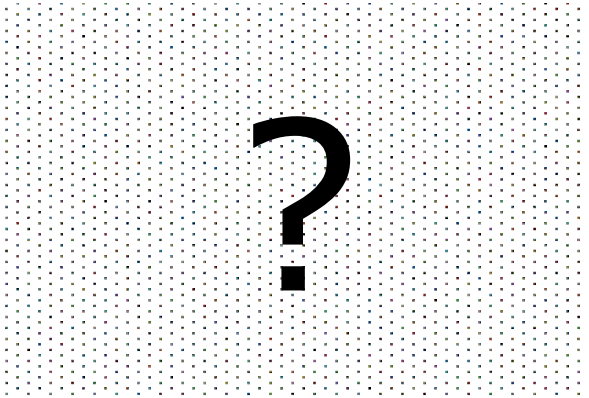
Steganographie

- **Verbergen der Existenz einer geheimen Nachricht**

Original

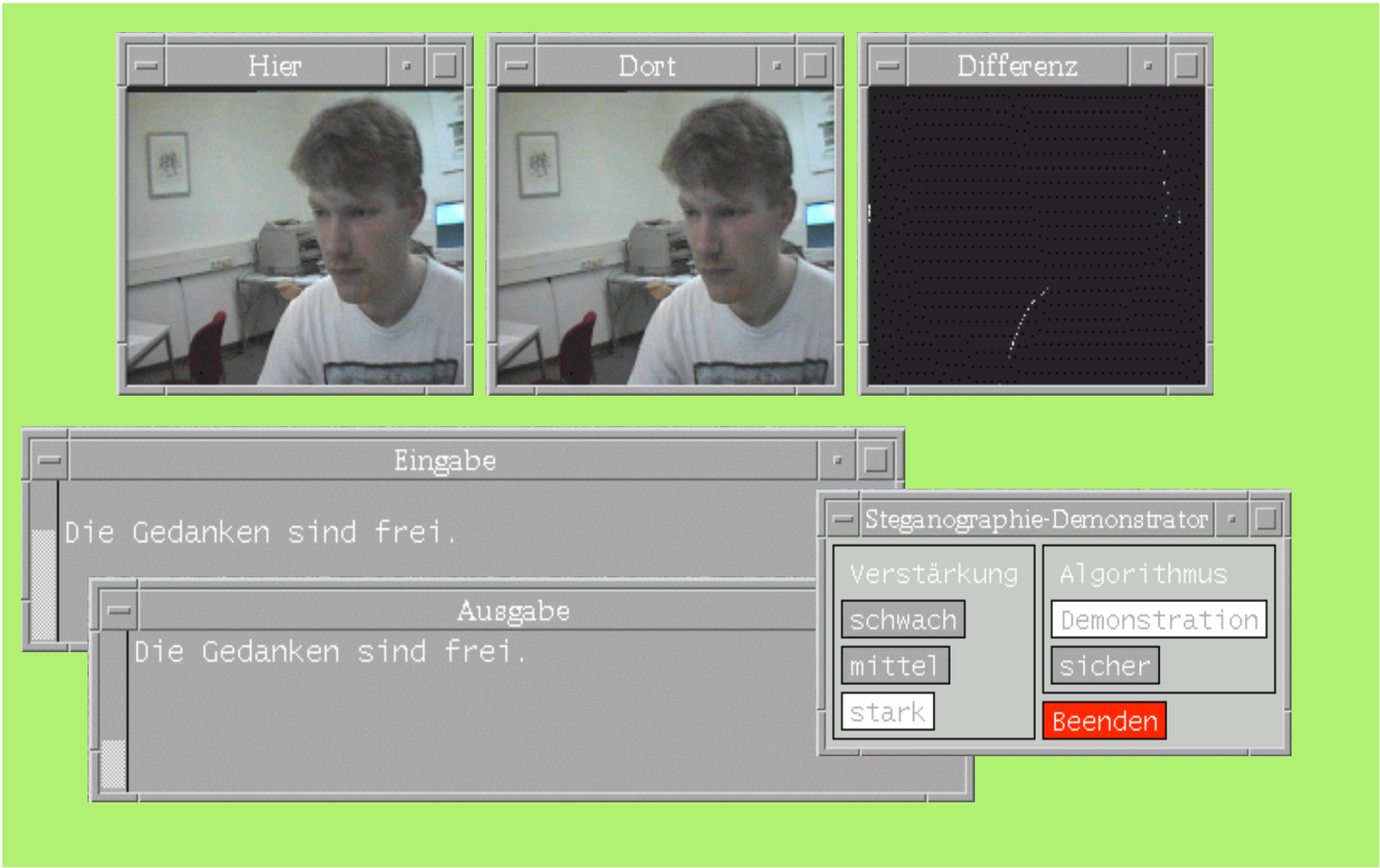
Verändert

Differenz



Prof. Dr.-Ing.
Hannes Federrath

Steganographie in Videokonferenzen



Vertraulichkeit
Verdecktheit

Anonymität
Unbeobachtbarkeit

Zurechenbarkeit
Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

- **Adressierungsinformationen können nicht verschlüsselt werden**
  - Problem Verkehrsdaten:
    - Wer mit wem, wann, wie lange, wo, wieviel Information?
  - Problem Interessensdaten:
    - Wer interessiert sich für was?

- **Spezielle Verfahren:**
  - Proxies
  - Mix-Netz
  - DC-Netz
  - Dummy traffic
  - …

Verfahren zum Schutz von Verkehrdaten

- **Teledienstedatenschutzgesetz (TDDSG)**

§ 4 Absatz 6: Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

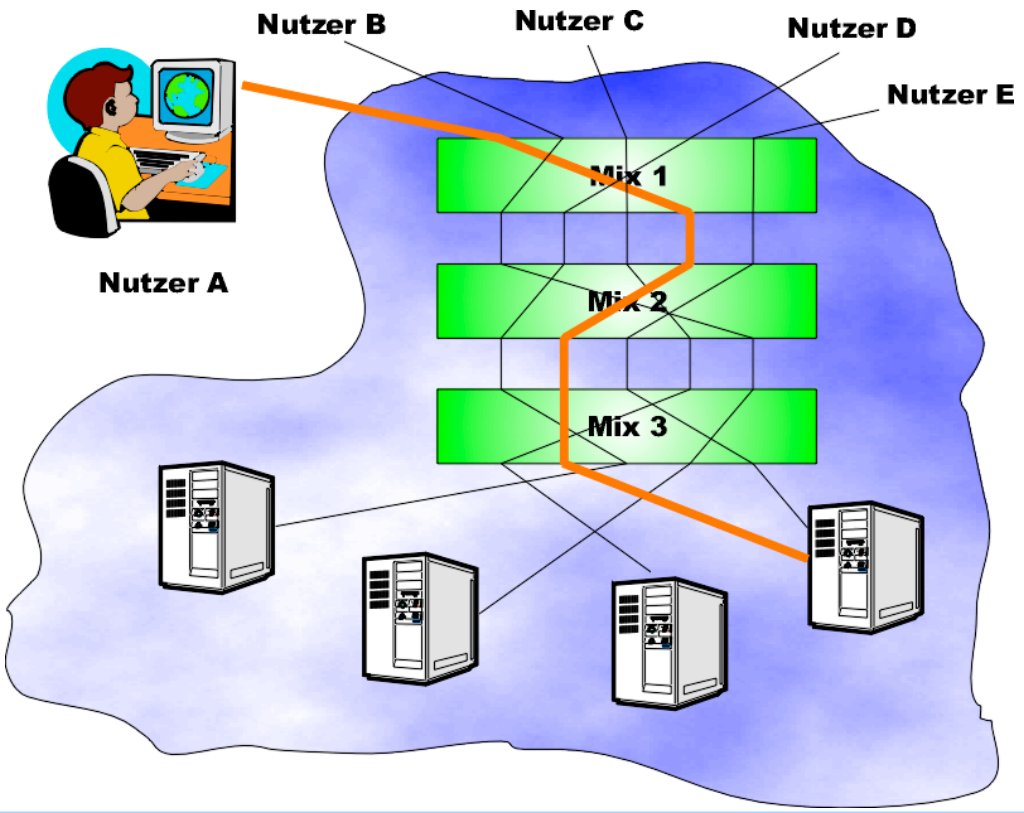
Vertraulichkeit
Verdecktheit

Anonymität
Unbeobachtbarkeit

Zurechenbarkeit
Rechtsverbindlichkeit

Verfahren zum Schutz von Verkehrdaten

- **Anonymisierung von Web-Zugriffen**
  - JAP-Software
  - http://www.anon-online.de



Vertraulichkeit
Verdecktheit

Anonymität
Unbeobachtbarkeit

Zurechenbarkeit
Rechtsverbindlichkeit

Digitale Signatur

- **Asymmetrisches Verfahren, z.B. RSA**
  - Jeder Nutzer generiert Schlüsselpaar:
    - *Öffentlichen* Testschlüssel
    - *Privaten* Sigierschlüssel
- **Nachweisbarkeit gegenüber Dritten**
- **Ebenfalls einsetzbar:**
  - Pretty Good Privacy
  - http://www.pgp.com
- **Rechtsverbindlichkeit der Digitalen Signatur**
  - Klare Regeln bzgl. Beweiswert
  - Zertifizierung von Schlüsseln (Public Key Infrastructure PKI)

Stand der Sicherheitstechnik

- Viele Verfahren sind theoretisch ausgereift und sichere Technik ist teilweise verfügbar:
  - meistens noch Detailprobleme
  - selten Grundsatzprobleme:
    - Beispiel: Wie realisiert man eine dauerhaft sichere, nicht ausforschbare Hardware (z.B. zur Aufbewahrung von kryptographischen Schlüsseln)?

- Defizite:
  - Integration von Sicherheitsfunktionen in existierende Systeme
    - Beispiel: Sicheres Betriebssystem
  - Mehrseitig sichere Technik: Beachtung von Sicherheit bereits beim Systemdesign berücksichtigen
    - Sicherheit der Betreiber und der Benutzer

Drei Arten von Signaturen nach SigG

- Signaturgesetz (SigG) vom 16. Mai 2001
  - schafft rechtliche Rahmenbedingungen für den Beweiswert digitaler Signaturen

Elektronische Signatur

Daten in elektronischer Form, die

- anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen

Fortgeschrittene Signatur

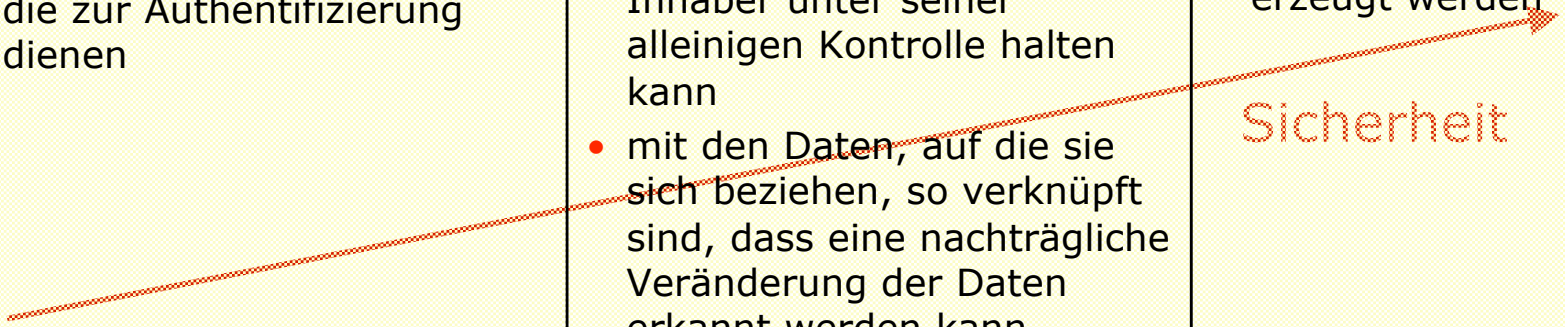
Daten in elektronischer Form, die

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann
- mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann

Qualifizierte Signatur

Daten in elektronischer Form, die

- die Anforderungen an eine fortgeschrittene Signatur erfüllen
- auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen
- mit einer sicheren Signaturerstellungseinheit erzeugt werden



Drei Arten von Signaturen nach SigG

- Signaturgesetz (SigG) vom 16. Mai 2001
  - schafft rechtliche Rahmenbedingungen für den Beweiswert digitaler Signaturen

Elektronische Signatur

Beispiel:

E-Mail mit "Signatur"

```
From: Hannes Federrath
Subject: Beispiel

Das ist der Text.
--
Hannes Federrath
Uni Regensburg
Sicherheitsmanagement
93040 Regensburg
```

Fortgeschrittene Signatur

Beispiel:

PGP-signierte E-Mail

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Das ist der Text.

-----BEGIN PGP SIGNATURE-----
Version: PGP 8.0.2

iQA/AwUBP6wDdOFAIGFJ7x2EEQK9VgCg2Q4e
QAztVIHP0HNFQ10eaXte96sAnR2p
53T/SdevjXIuX6WOF5IXA44S
=K3TO
-----END PGP SIGNATURE-----
```

Qualifizierte Signatur

Zertifikatausstellung nach Identitätsüberprüfung

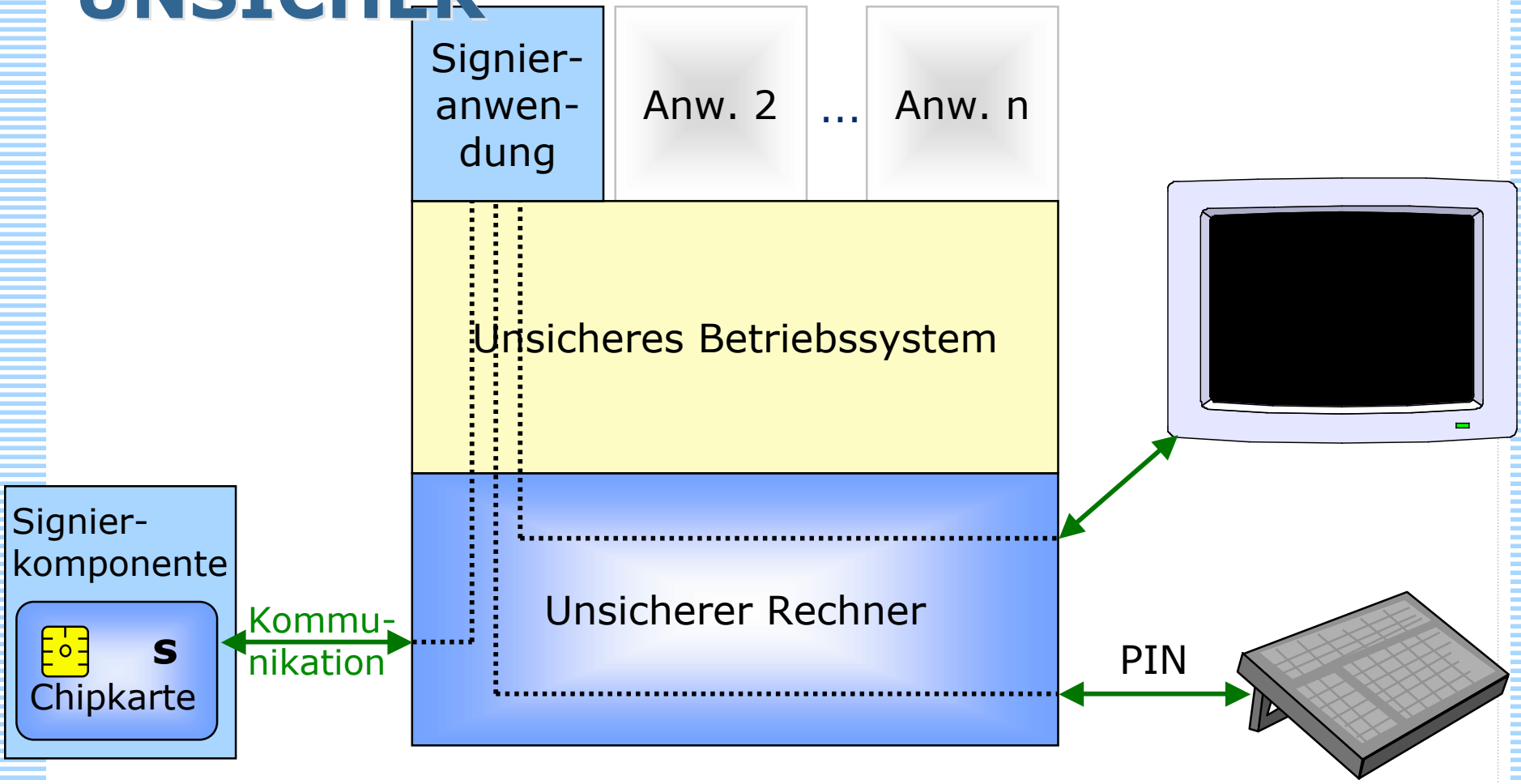
sichere Signaturerstellungseinheit

Sicherheit

Standard-PC mit Chipkarte

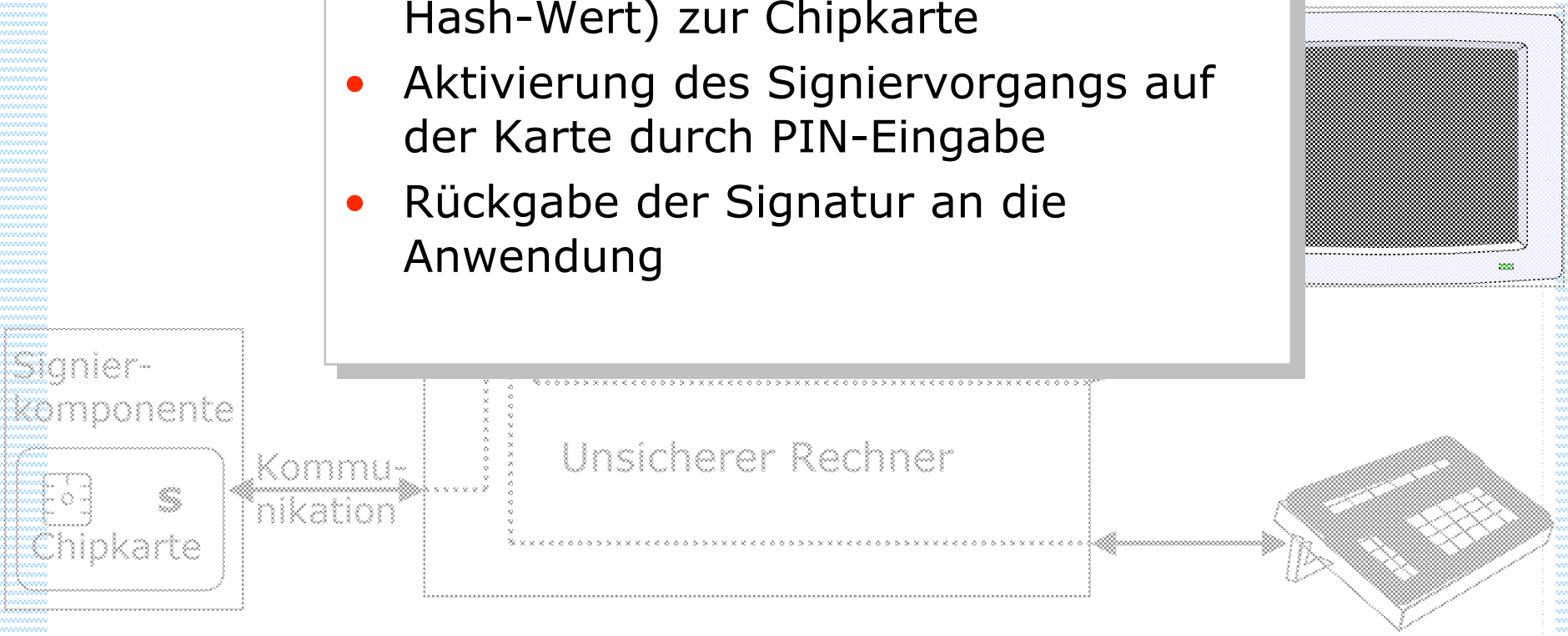
- Sichere Geräte sind eine Voraussetzung für sichere Signaturen

UNSICHER



Ablauf auf Standard-PC mit Chipkarte

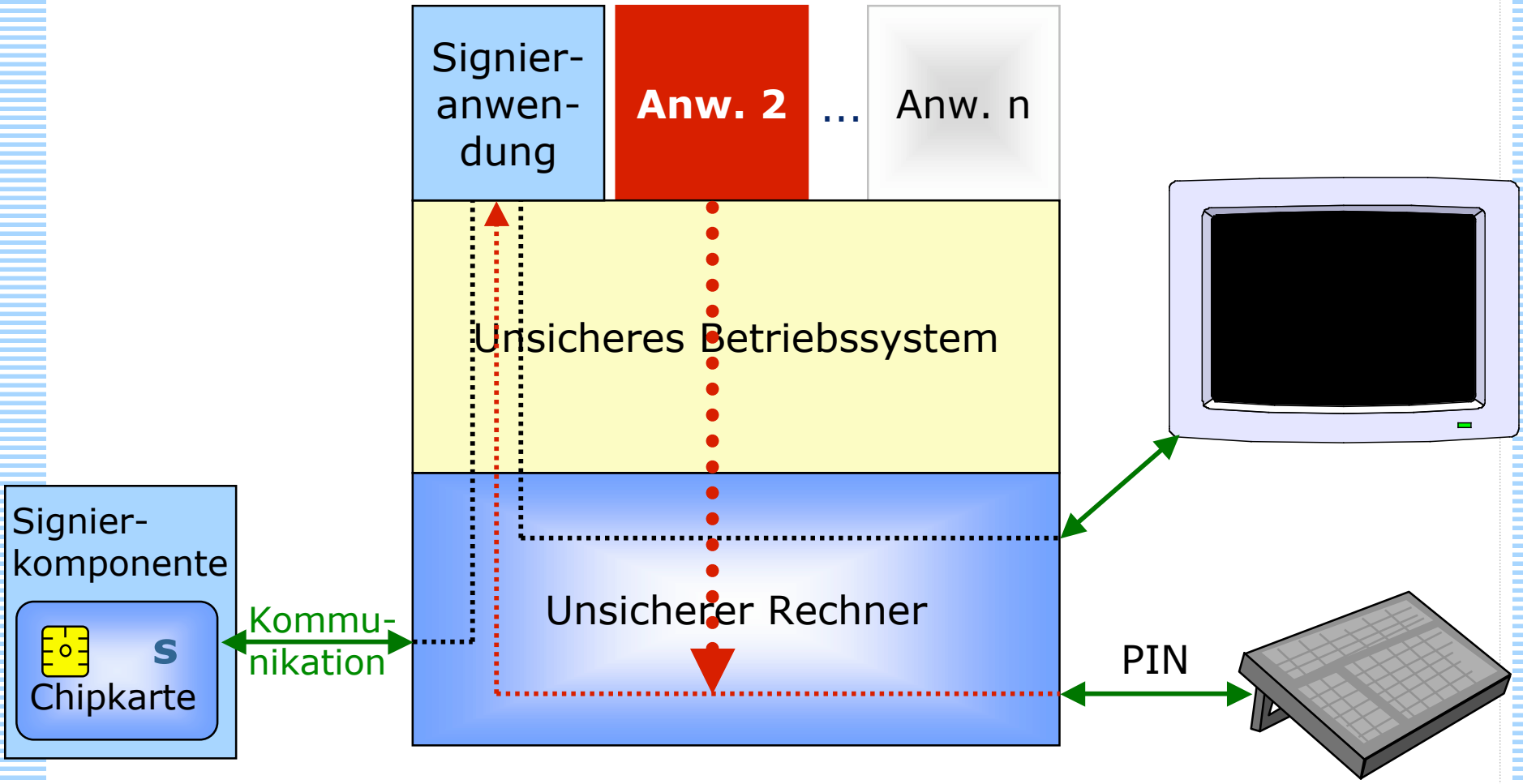
- Anzeige des Dokuments auf dem externem Monitor
- Senden des Dokuments (bzw. dessen Hash-Wert) zur Chipkarte
- Aktivierung des Signiervorgangs auf der Karte durch PIN-Eingabe
- Rückgabe der Signatur an die Anwendung



Standard-PC mit Chipkarte

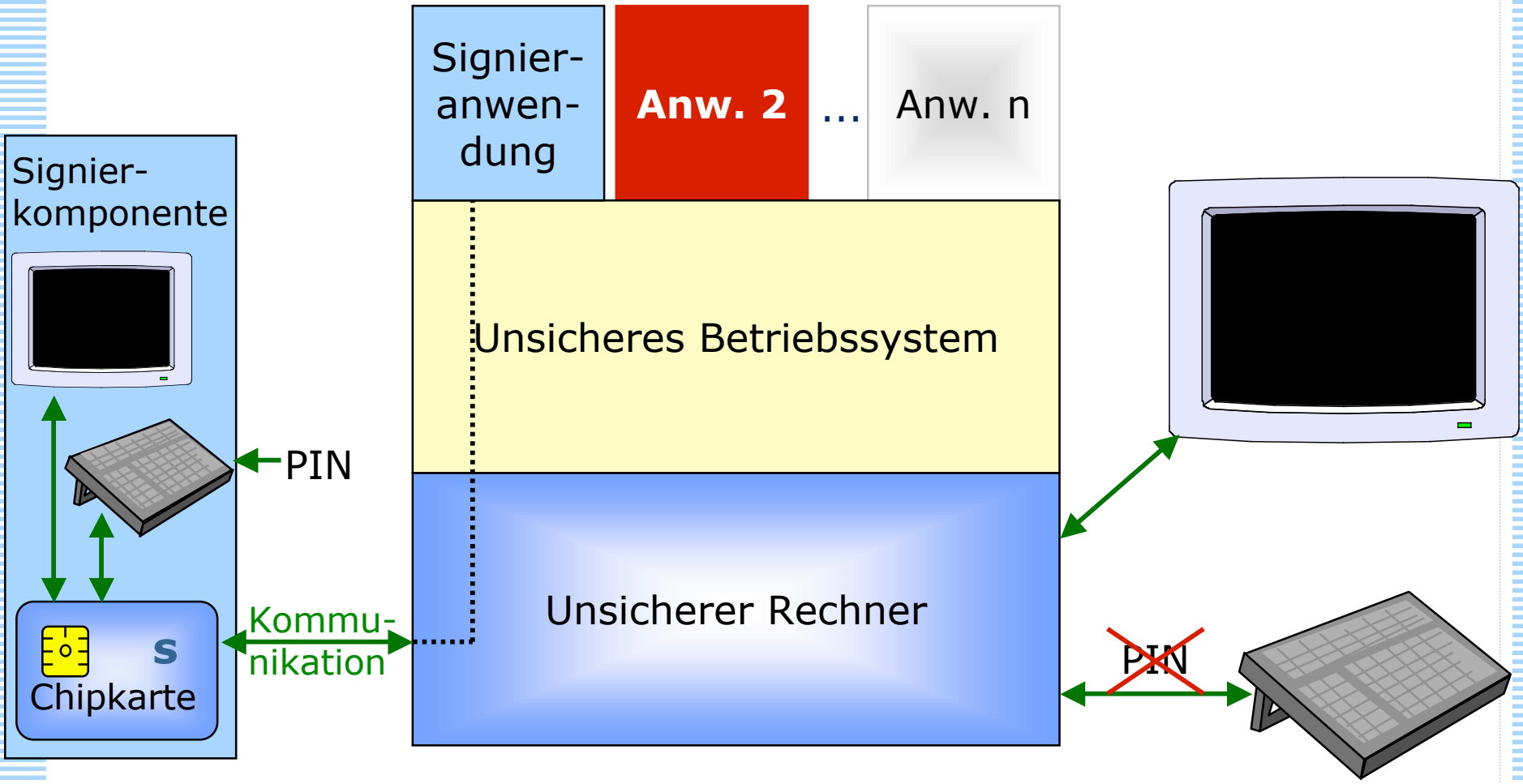
UNSICHER

Bösartige Anwendung könnte z.B. PIN abfangen oder Text nach Anschauen und vor Senden an Signierkomponente heimlich ersetzen



Sichere Signierkomponente mit Standard-PC

SICHER



Chipkartenleser: Sicherheitsklassen

- Klasse 1:
  - Keine Sicherheitsfunktionen
  - realisieren nur Kommunikation zwischen PC und Leser
- Klasse 2:
  - PIN-Eingabe kann nicht vom PC mitgeloggt werden
    - Variante 1: PC-Tastatur ist direkt mit Leser verbunden, Verbindung zu PC wird während PIN-Eingabe (physisch) unterbrochen
    - Variante 2: Eigene Tastatur im Leser
- Klasse 3:
  - eigene Tastatur und eigene Anzeige
  - PC ist nicht an der Kommunikation zwischen Karte, Tastatur und Anzeige beteiligt
- Klasse 4:
  - eigener Signaturschlüssel
  - kann später ermittelt werden, in welchem Lesegerät die Signatur geleistet wurde

Stand der Sicherheitstechnik

Schutzziel	Technik	Stand der Technik	Nutzbarkeit
Vertraulichkeit	Verschlüsselung	sehr gut	gut
Verdecktheit	Steganographie	mittel	schlecht
Anonymität Unbeobachtbarkeit	Remailer, Proxies, Mixe	mittel	mittel
Zurechenbarkeit Rechtsverbindlichkeit	Digitale Signatur	schlecht	schlecht