Technologien zum Identitätsnachweis und zum Schutz der Identität

... und alles was dazwischen ist

Hannes Federrath

DFG-Netzwerk »Der digitale Bürger und seine Identität«
Berlin 12.3.2011

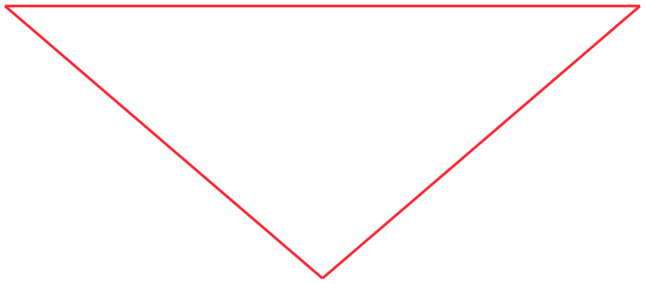
Identifizierung vs. Anonymität

- Identität: Menge von ggf. über die Zeit veränderlichen Attributen eines Individuums
- Identifikation: Übereinstimmung zweier Dinge hinsichtlich eines vorgegebenen Attributvektors

Identifizierung

gewollt:

Biometrie
Wissen
Besitz



Anonymität

ungewollt:

Strafverfolgung
Fingerprinting
Marketing

Pseudonymität

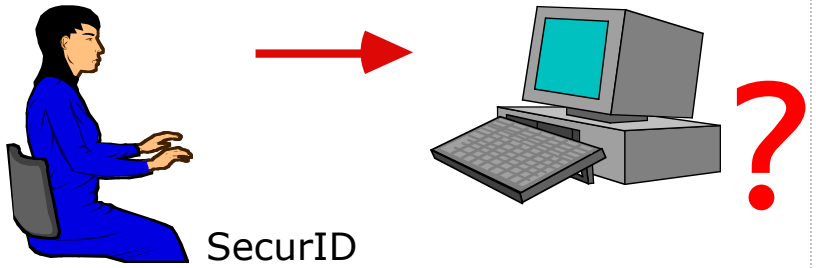
»Wiedererkennung«

Handlungen auch ohne Identifizierung verkettbar machen

Identifikation von Menschen durch IT-Systeme

- Was der MENSCH IST:
  - Handgeometrie
  - Fingerabdruck
  - Aussehen*
  - eigenhändige Unterschrift*
  - Retina-Muster
  - Stimme
  - Tipp-Charakteristik
  - DNA-Muster
- Was der MENSCH HAT:
  - Papierdokument*
  - Metallschlüssel
  - Magnetstreifenkarte
  - Chipkarte
  - Taschenrechner
- Was der MENSCH WEIß:
  - Passwort
  - Antworten auf Fragen
  - Rechenergebnisse für Zahlen

*=Ausweis



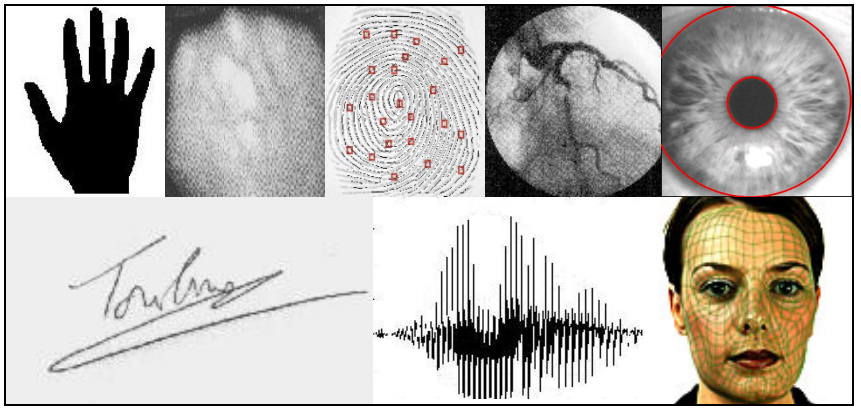
SecurID

Bild:
http://www.rasesecurity.com

Bild: ntz, Heft 3-4/2006, S. 35

Biometrische Merkmale

- Physiologische
  - Handgeometrie
  - Handvenenmuster
  - Fingerabdruck
  - Retina
  - Iris
  - Gesicht
  - DNA
  - Ohrmuscheln



Bilder:
http://biometrics.cse.msu.edu/
http://www.atica.pm.gouv.fr/dossiers/documents/biometrie.shtml
http://www.br-online.de/wissen-bildung/thema/biometrie/koerper.shtml

- Verhaltensbasierte
  - Handschrift
  - Stimme
  - Lippenbewegung
  - Tipp-Charakteristik
  - Gang

Bild: Acer

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

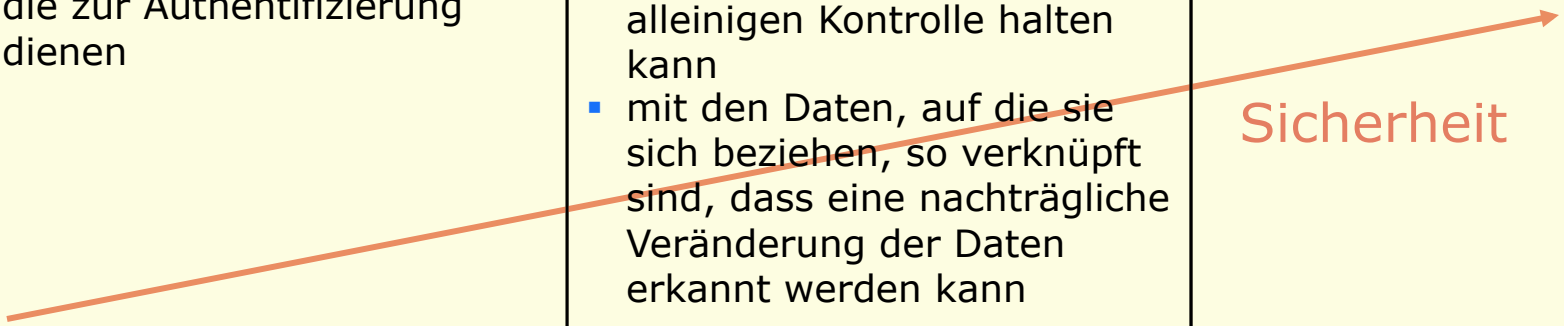
Daten in elektronischer Form, die

- 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/
AwUBP6wDdOFAIGFJ7x2EEQK9VgCg2Q4eQAzt
VIHP0HNFQ10eaXte96sAnR2p
53T/SdevjXIuX6WOF5IXA44S
=K3TO
-----END PGP SIGNATURE-----
```

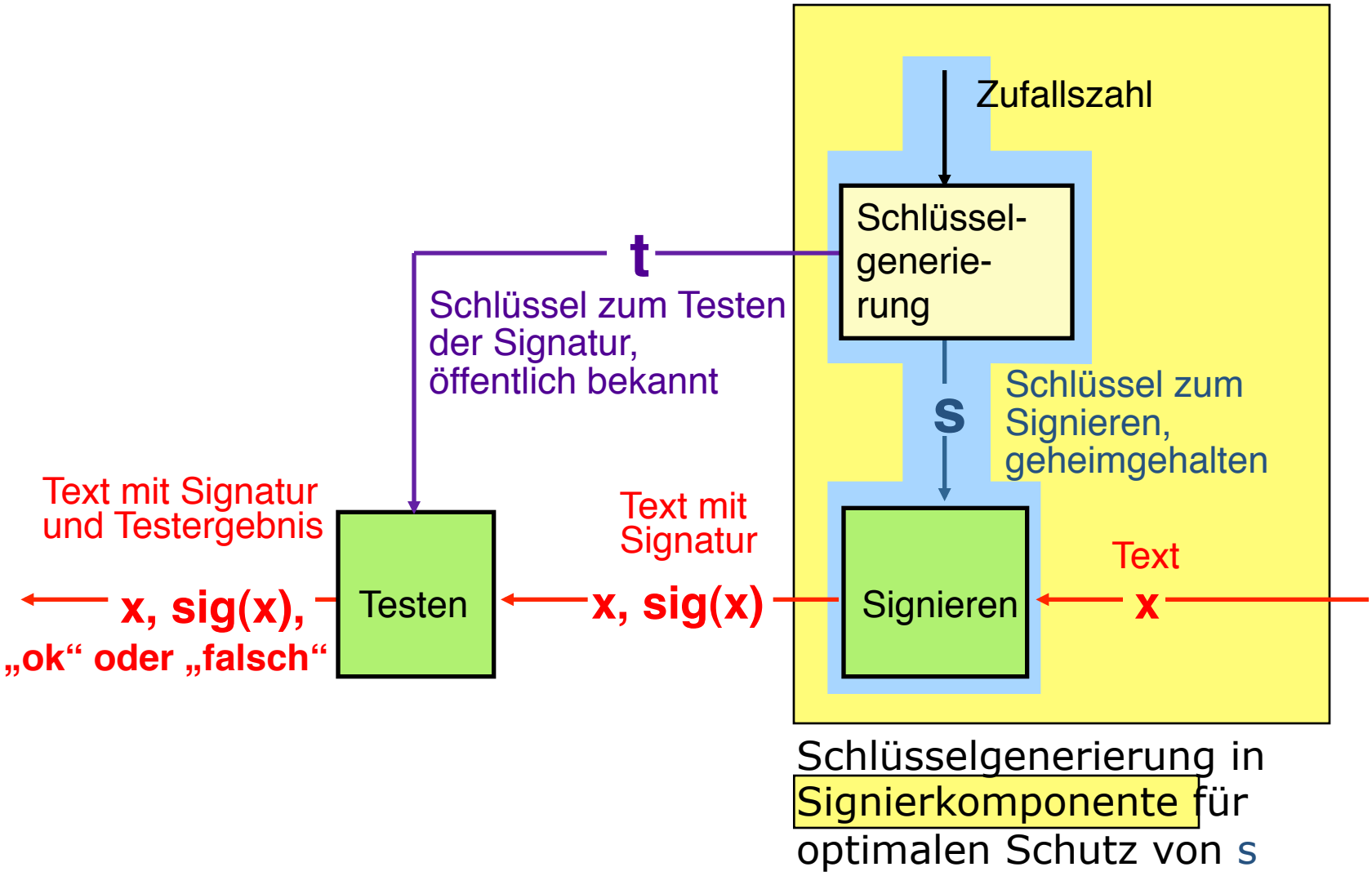
Qualifizierte Signatur

Zertifikatausstellung nach Identitätsüberprüfung

sichere Signaturerstellungseinheit

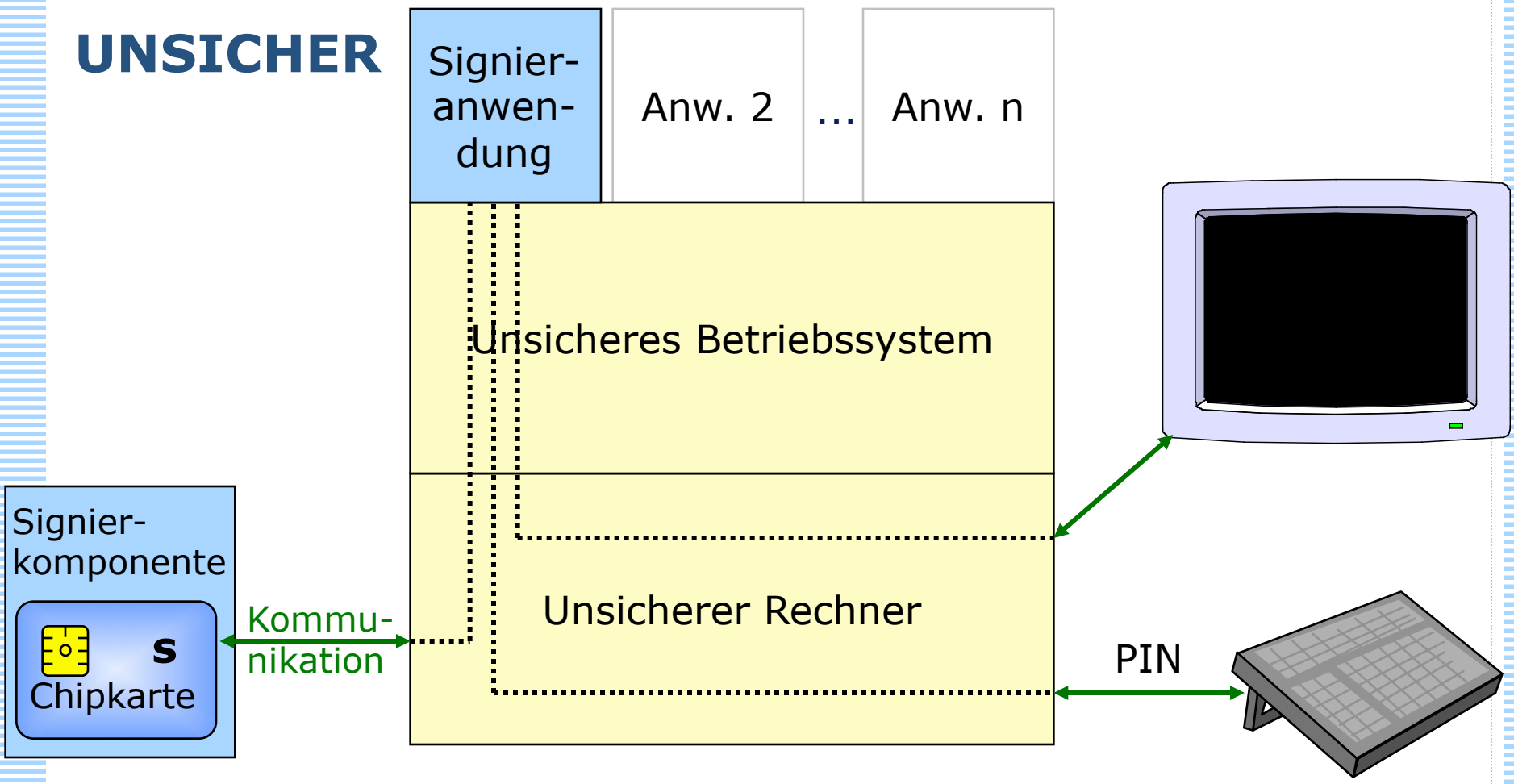
Sicherheit

Digitales Signatursystem



Standard-PC mit Chipkarte

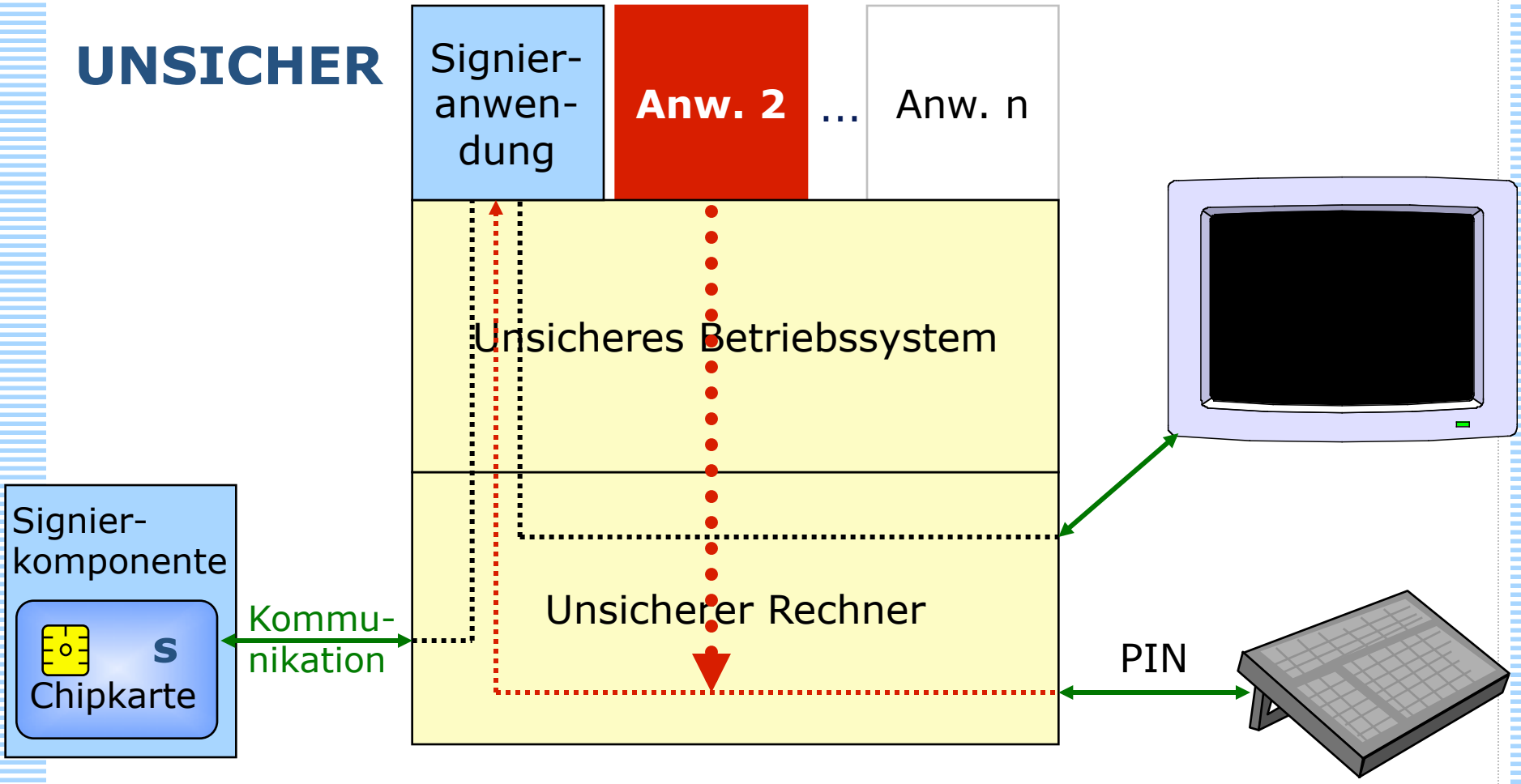
- Sichere Geräte sind eine Voraussetzung für sichere Signaturen



Standard-PC mit Chipkarte

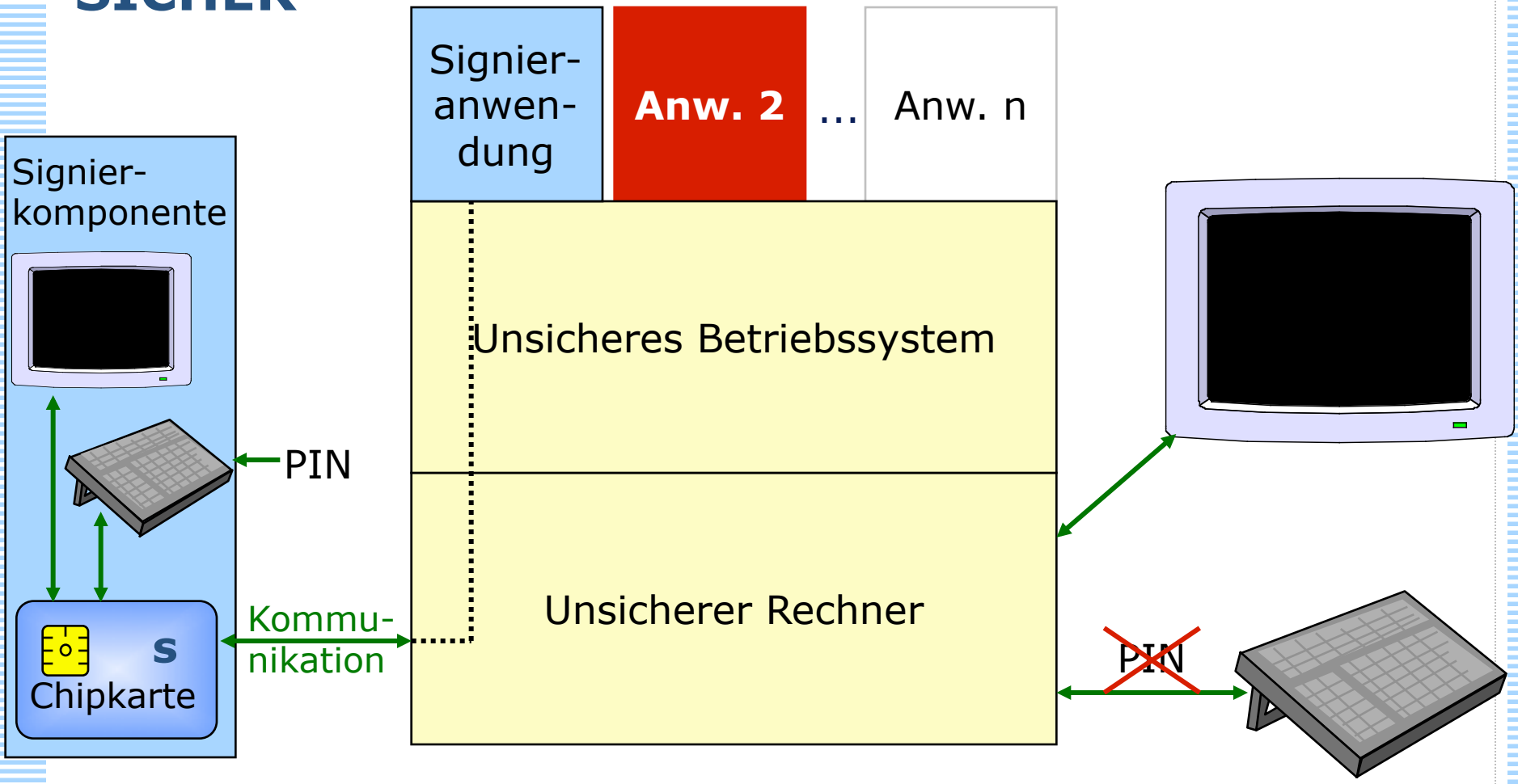
Bösartige Anwendung könnte z.B. PIN abfangen oder Text nach Anschauen und vor Senden an Signierkomponente heimlich ersetzen

UNSICHER

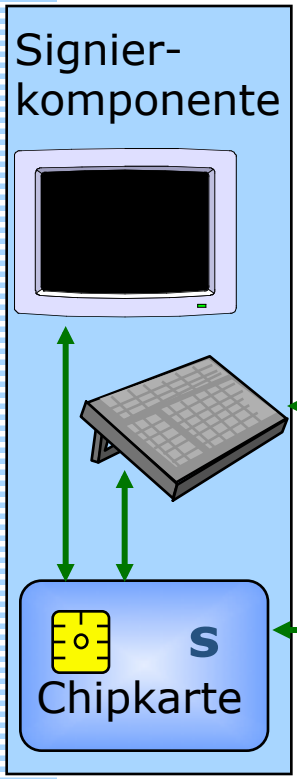


Sichere Signierkomponente mit Standard-PC

SICHER



Sichere Signierkomponente



=

- Display
- Tastatur
- Physischer Schutz: Manipulationserkennung

- Entwurf offengelegt (keine versteckten Trojanischen Pferde)

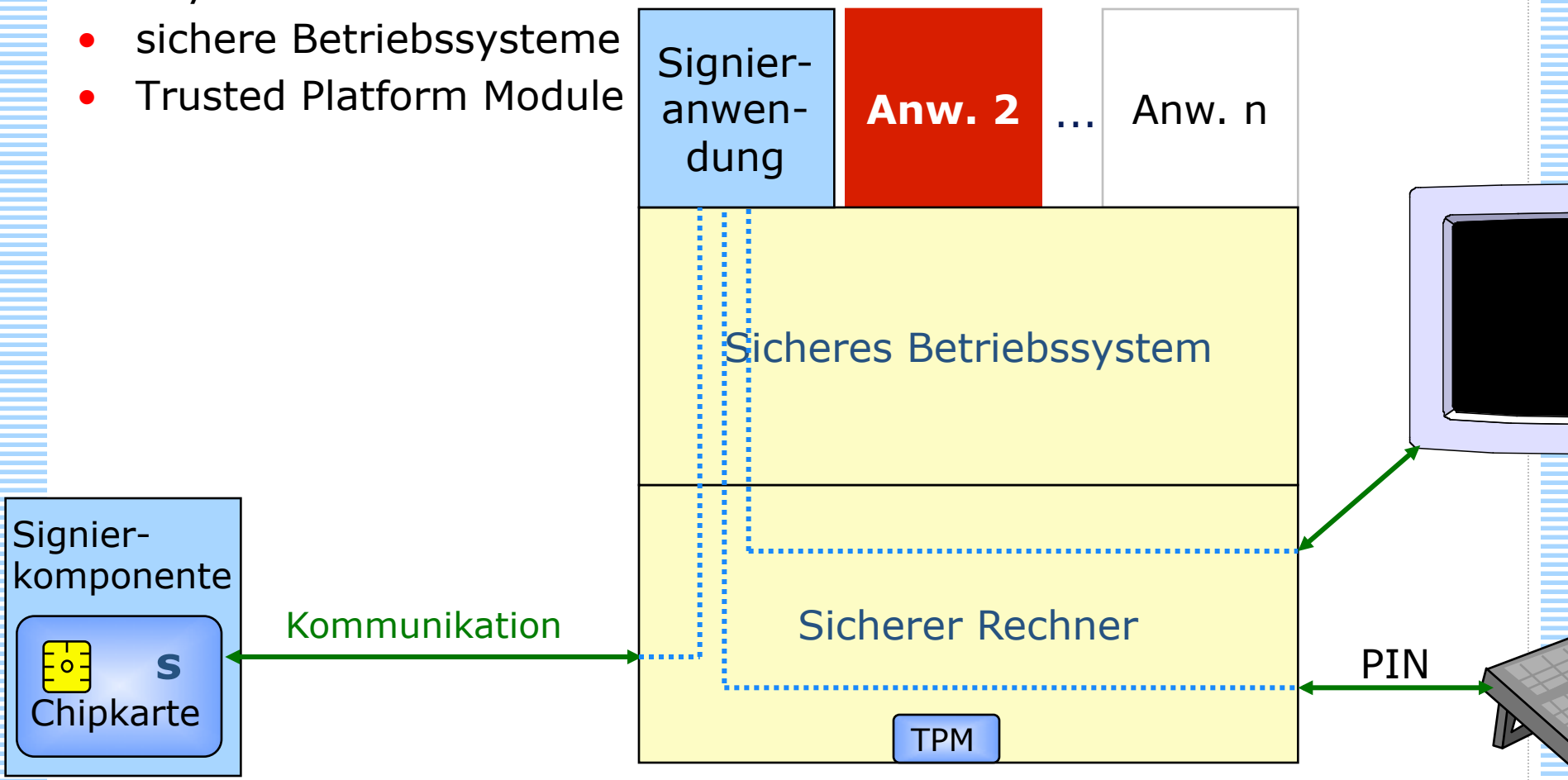
Chipkartenleser: Sicherheitsklassen

- 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

Physisch sichere Geräte und sichere Betriebssysteme

SICHER, wenn

- Physisch sichere Geräte
- sichere Betriebssysteme
- Trusted Platform Module



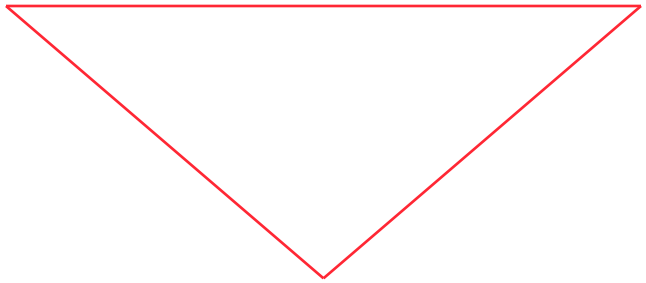
Identifizierung vs. Anonymität

- Unverkettbarkeit: Ereignisse werden vom Angreifer bzgl. des Senders und/oder Empfängers als unabhängig erkannt

Identifizierung

gewollt:

Biometrie
Wissen
Besitz



Pseudonymität

»Wiedererkennung«

Handlungen auch ohne Identifizierung verkettbar machen

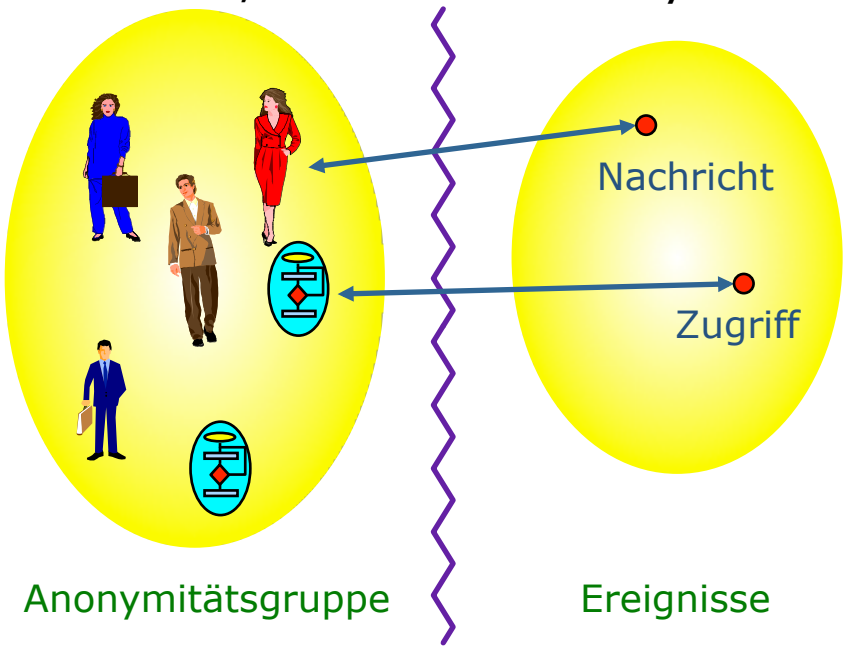
Anonymität

ungewollt:

Strafverfolgung
Fingerprinting
Marketing

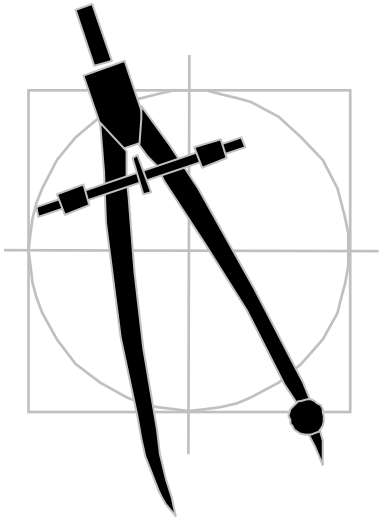
Anonymitätsgruppe

- Ein einzelnes Ereignis, das durch eine einzelne Person hervorgerufen wurde, kann nicht anonym oder unbeobachtbar sein.
- Wir benötigen eine Gruppe von Personen, die sich alle gleich verhalten: *Anonymitätsgruppe*
  - Jedes Mitglied der Anonymitätsgruppe ist mit der gleichen Wahrscheinlichkeit der Urheber eines Ereignisses.
  - Eine öffentlich bekannte Eigenschaft, die alle Mitglieder der Anonymitätsgruppe erfüllen, kann nicht anonymisiert werden.



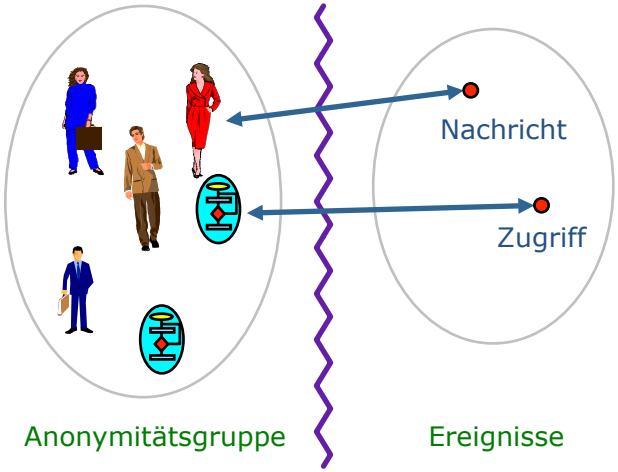
Technischer Datenschutz

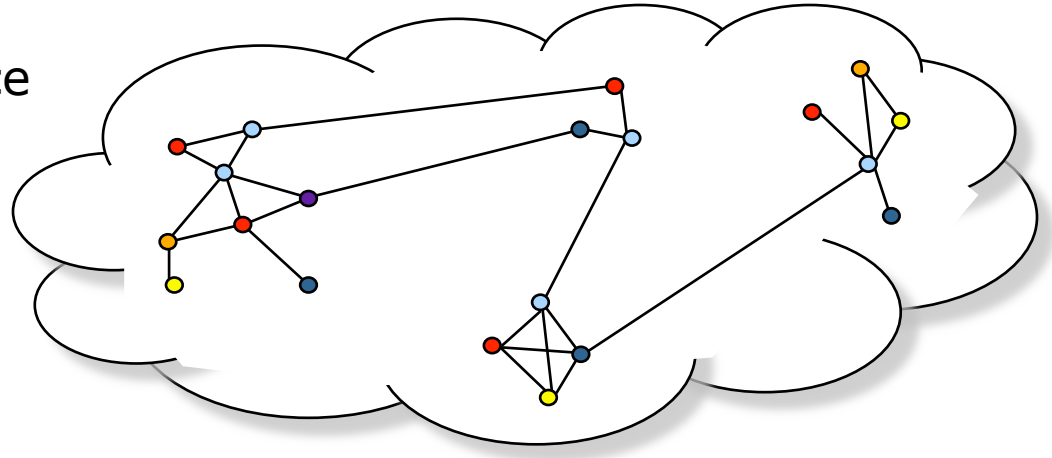
- Technischer Datenschutz
  - Systeme so konstruieren, dass unnötige Daten vermieden und nicht miteinander verkettet werden können.
- Zu verschleiern sind:
  - Adressen:
    - Sender, Empfänger, Kommunikationsbeziehung
  - Zeitliche Korrelationen:
    - Zeitpunkte, Dauer
  - Übertragenes Datenvolumen und inhaltliche Korrelationen
  - Orte:
    - Aufenthaltsorte, Bewegungsspuren



Verfahren zur unbeobachtbaren Kommunikation

- Wer ist zu schützen?
  - Schutz des Senders
  - Schutz des Empfängers
  - Schutz der Kommunikationsbeziehung
- Grundkonzepte:
  - Pseudonymität
  - Verteilung mit impliziter Adressierung
  - Dummy traffic
  - Proxies
  - DC-Netz
  - Blind-Message-Service
  - Mix-Netz
  - Steganographie

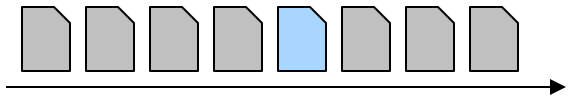




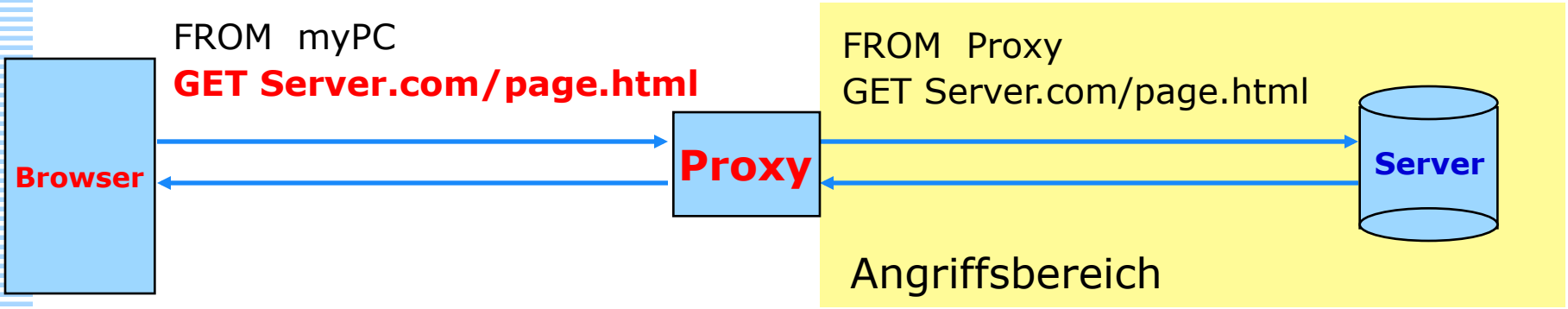
Grundsätzliche Techniken

- Verteilung (Broadcast) + implizite Adressierung
  - Schutz des Empfängers; alle erhalten alles
  - lokale Auswahl

- Dummy Traffic: Senden bedeutungsloser Nachrichten
  - Schutz des Senders



- Proxies zwischenschalten
  - Server erfährt nichts über Client, Proxy kann mitlesen



Grundsätzliche Techniken

- DC-Netz: kombiniert u.a. Broadcast, Kryptographie und Dummy Traffic
  - Schutz des Senders
- Blind-Message-Service: Unbeobachtbare Abfrage aus von unabhängigen Betreibern replizierten Datenbanken
  - Schutz des Clients
- MIX-Netz: kombiniert u.a. hintereinander geschaltete Proxies von unabhängigen Betreibern, Kryptographie und Dummy Traffic
  - Schutz der Kommunikationsbeziehung
  - Effizient in Vermittlungsnetzen
- Steganographie
  - Verbergen einer Nachricht in einer anderen

Website-Fingerprinting

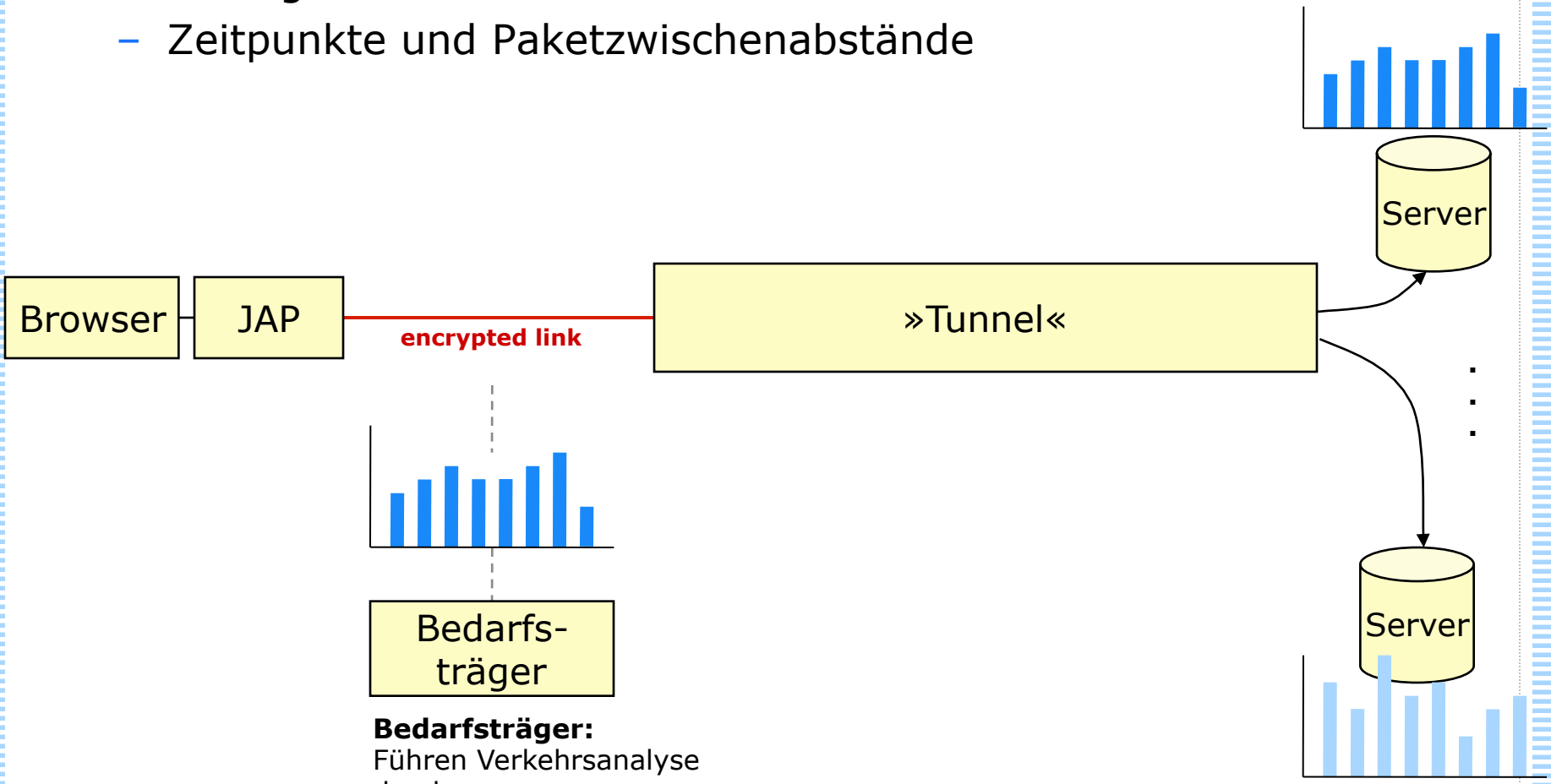
- Entschlüsselung des Datenstroms meist aussichtslos

- Alternativen:
  - Online-Durchsuchung: Direkter Zugriff auf Klartexte durch Installation einer Software auf dem Rechner eines Verdächtigen.
  - Traffic-Analyse: Durch Analyse charakteristischen Eigenschaften des Datenverkehrs kann ein passiver Beobachter auf Inhalts und/oder Adressdaten schließen.

- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände

Website-Fingerprinting

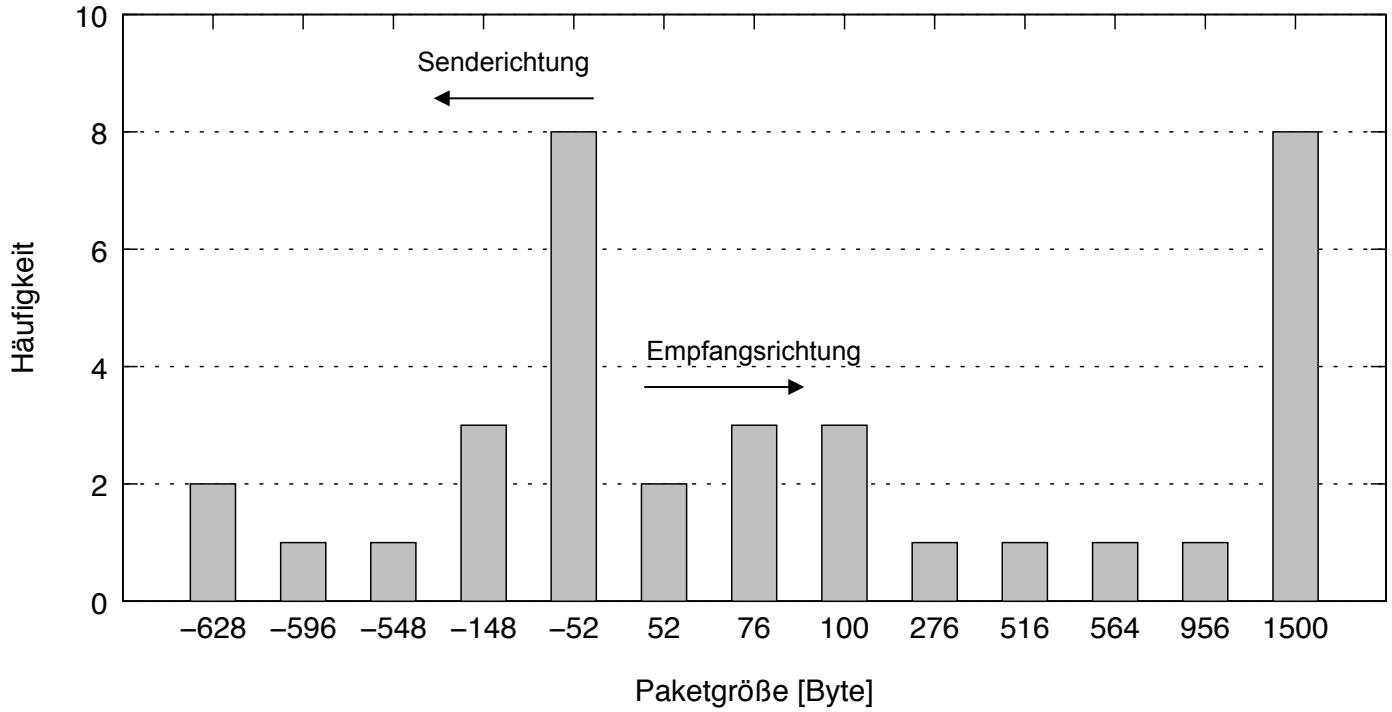
- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände



Bedarfsträger:
Führen Verkehrsanalyse durch

Verbessertes Website-Fingerprinting-Verfahren

- Analyse der charakteristischen Häufigkeitsverteilung der IP-Paketgrößen



- Schutz durch datenschutzfreundliche Systeme?
  - gering: SSH-Tunnel und VPNs; Erkennungsrate: 90-97%
  - moderat: Anonymisierer wie Tor und JAP/JonDonym; Erkennungsrate: < 20%

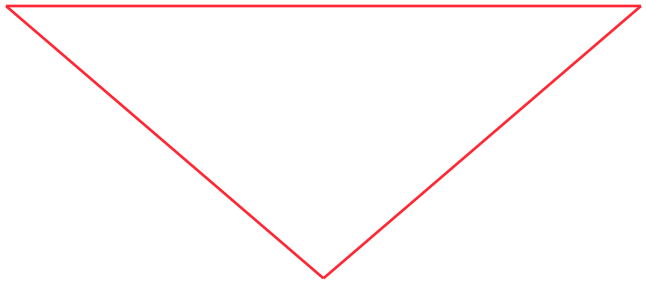
Identifizierung vs. Anonymität

- Pseudonymität bietet im Sinne der mehrseitigen Sicherheit einen Kompromiss zwischen Identifizierung und Anonymität
  - Berücksichtigung der Sicherheitsinteressen mehrerer Parteien

Identifizierung

gewollt:

Biometrie
Wissen
Besitz



Anonymität

ungewollt:

Strafverfolgung
Fingerprinting
Marketing

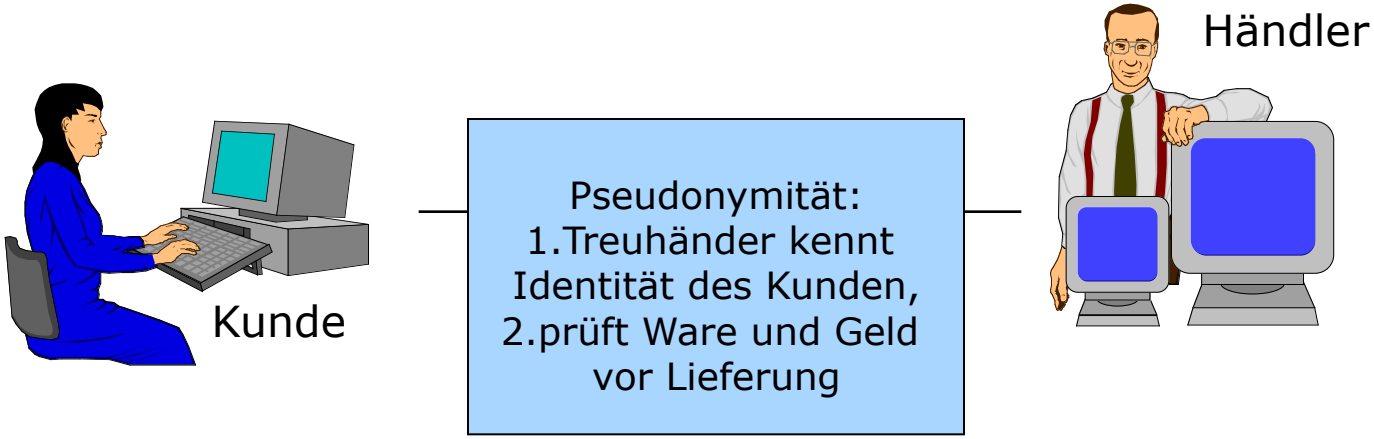
Pseudonymität

»Wiedererkennung«

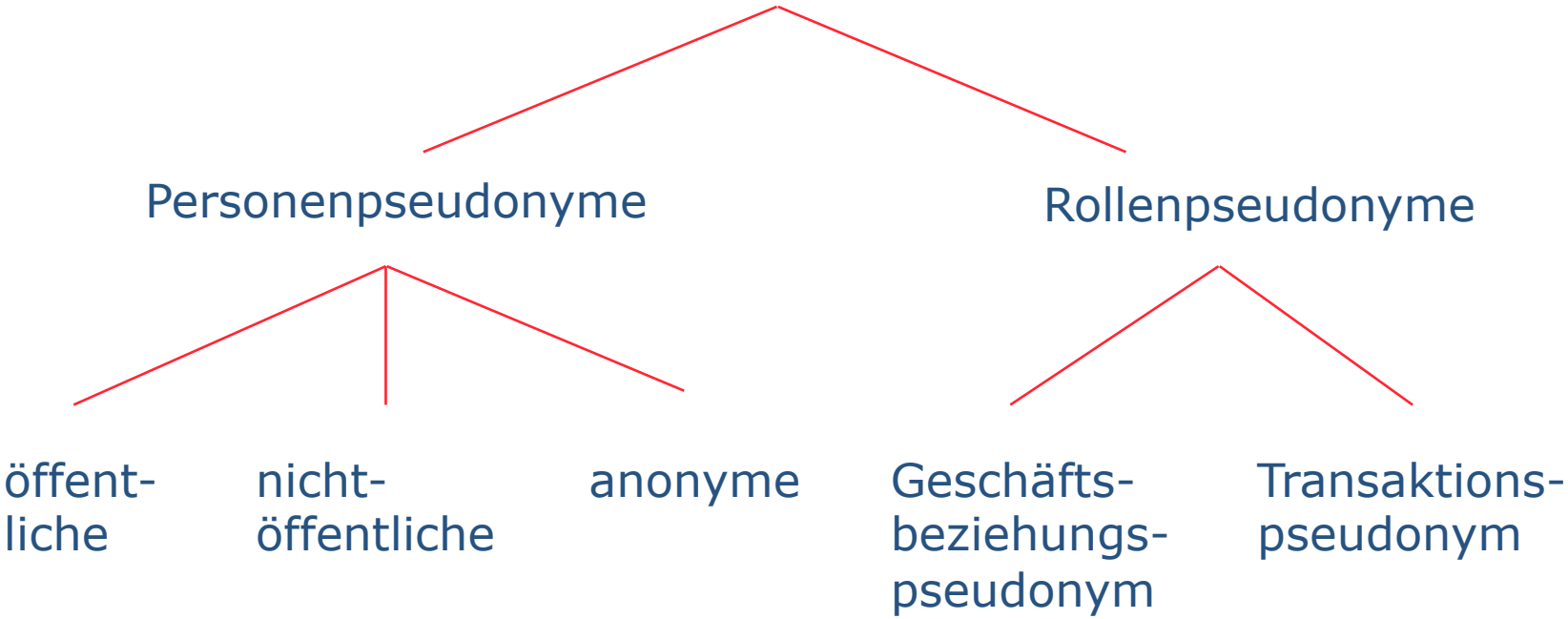
Handlungen auch ohne Identifizierung verkettbar machen

Grundverfahren für pseudonyme Transaktionen

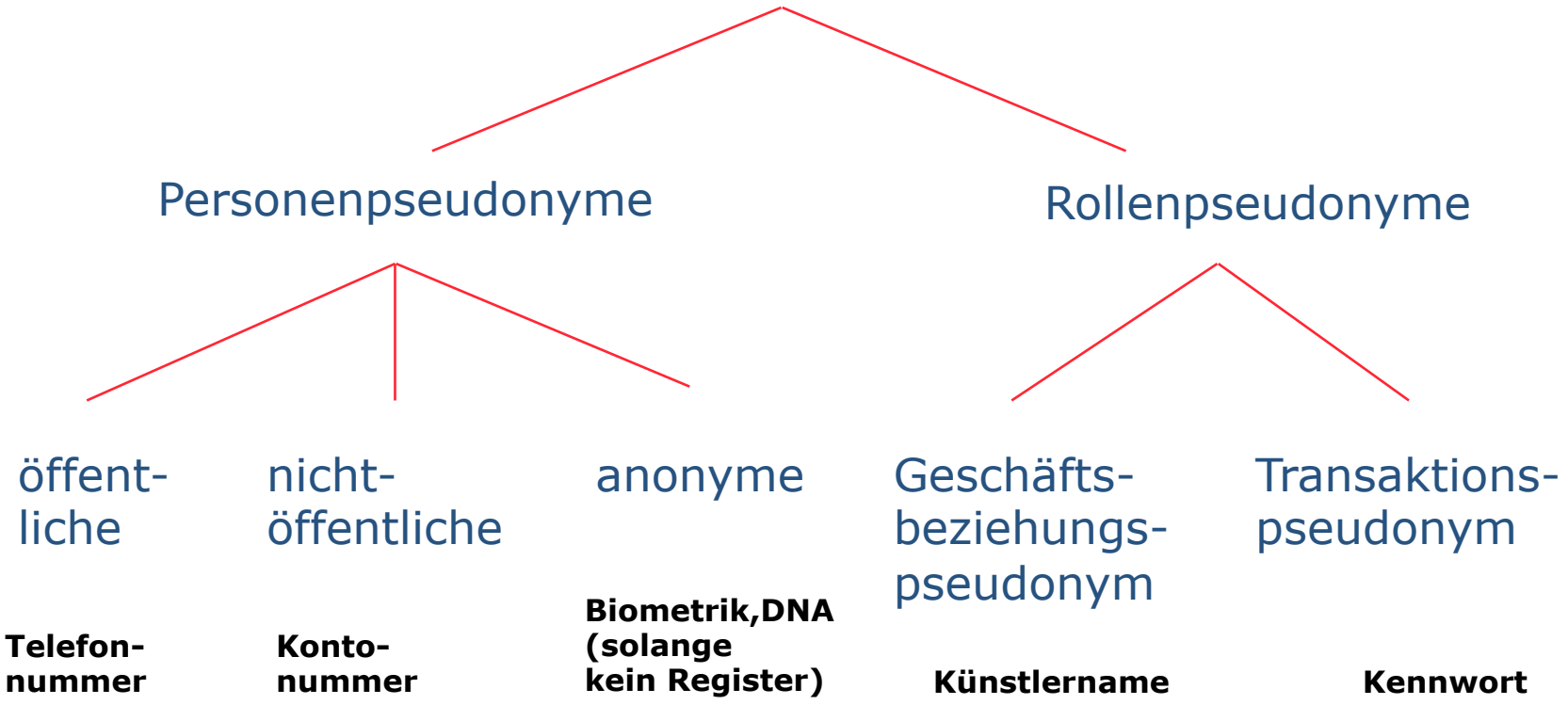
- Zwei Grundkonzepte unter Verwendung von Pseudonymen (öffentl. Testschlüssel):
  - Treuhänder kennt Identität des Kunden
    - passiver Treuhänder, deckt Identität im Streitfall auf, üblicherweise realisiert durch Zertifizierungsstelle
  - «aktiver Treuhänder», prüft Ware und Geld vor Lieferung
- Vertrauen in Treuhänder ist nötig



Pseudonyme: Systematik



Pseudonyme: Beispiele



Pseudonyme: Implementierungen

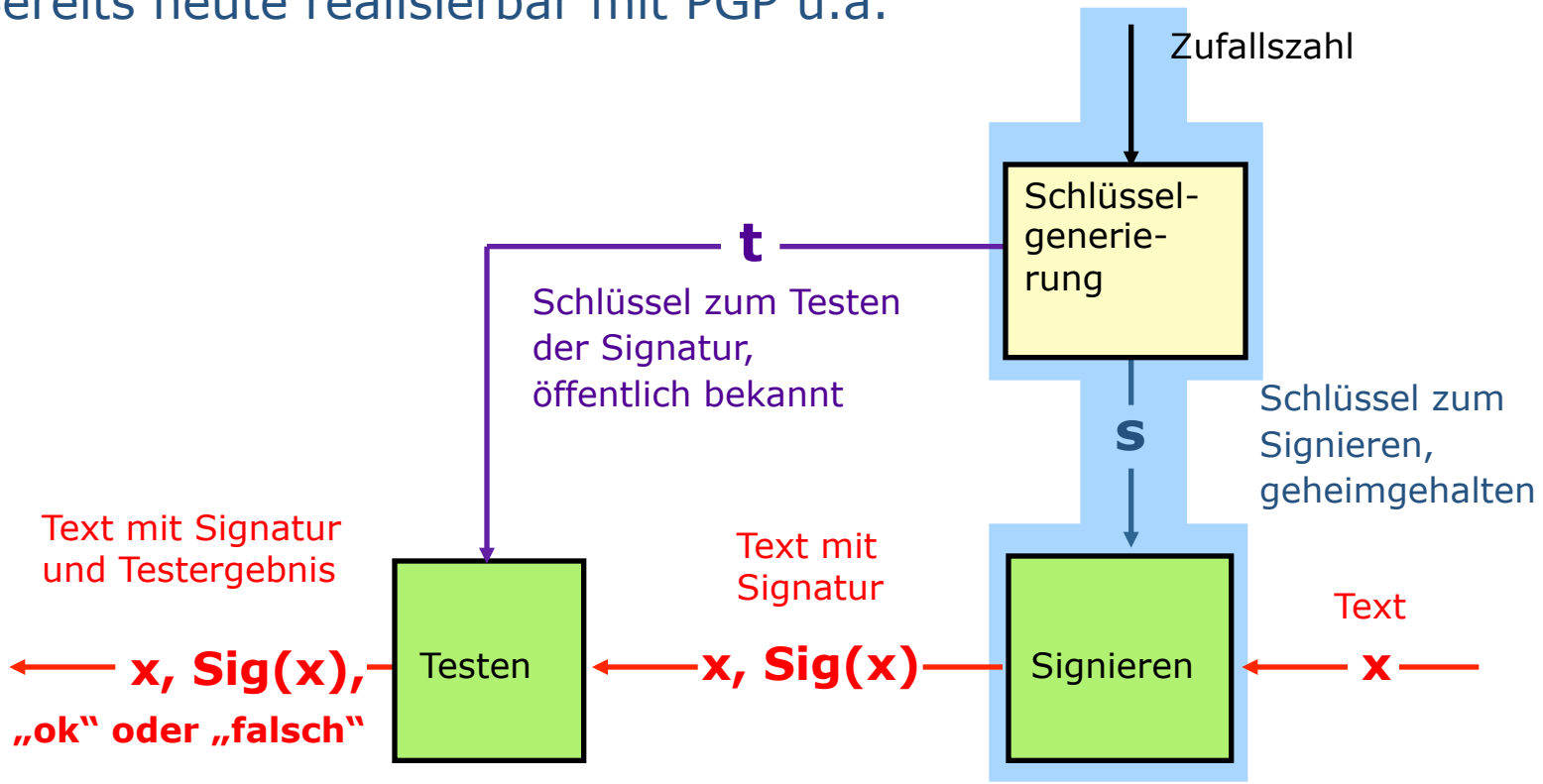
- Pseudonym-Arten
  - Vom Teilnehmer selbst gewählte Zeichenketten, die keinen Bezug zu seiner Identität besitzen
  - Große Zufallszahlen (etwa 45 Dezimalstellen)
  - Öffentliche Testschlüssel eines Signatursystems

- Pseudonyme zur Bestätigung von Eigenschaften
  - Einfaches »qualifizierendes Zertifikat«
  - Blenden des Pseudonyms vor dem Zertifizieren
  - Secret-key Zertifikate

BEGIN ZERTIFIKAT
Pseudonym: 30452634272346623424987241375
Öffentlicher Testschlüssel des Pseudonyms:
h833hd38dddajscbicme098342k236egfkw74h5445
84hdbscldmrtpofjrkt0jshuedagaszw12geb3u4b=
Bestätigte Eigenschaften:
Der Inhaber ist über 18 Jahre alt.
Der Inhaber ist deutscher Staatsbürger.
Datum: 19.03.2000
Gültig bis: 18.03.2001
Aussteller: Einwohnermeldeamt Dresden
Signatur des Ausstellers:
23j423vdsaz345kj435ekji3u4z2983734ijo23i72
kj867wdbez2o074j5lkdmcdkki1237t3rgbdvbwdj=
END ZERTIFIKAT

Signatursystem für Pseudonymität verwenden

- Testschlüssel t ist das Pseudonym
- Bereits heute realisierbar mit PGP u.ä.



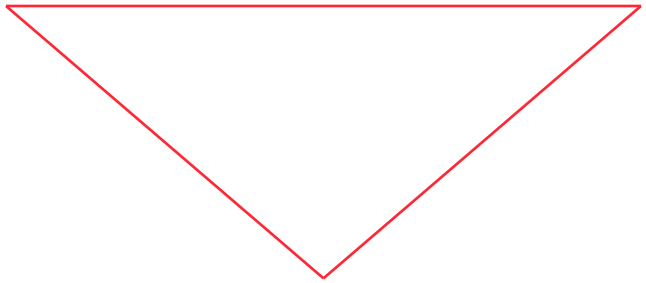
Identifizierung vs. Anonymität

- Pseudonymität bietet im Sinne der mehrseitigen Sicherheit einen Kompromiss zwischen Identifizierung und Anonymität
  - Berücksichtigung der Sicherheitsinteressen mehrerer Parteien

Identifizierung

gewollt:

Biometrie
Wissen
Besitz



Anonymität

ungewollt:

Strafverfolgung
Fingerprinting
Marketing

Pseudonymität

»Wiedererkennung«

Handlungen auch ohne Identifizierung verkettbar machen