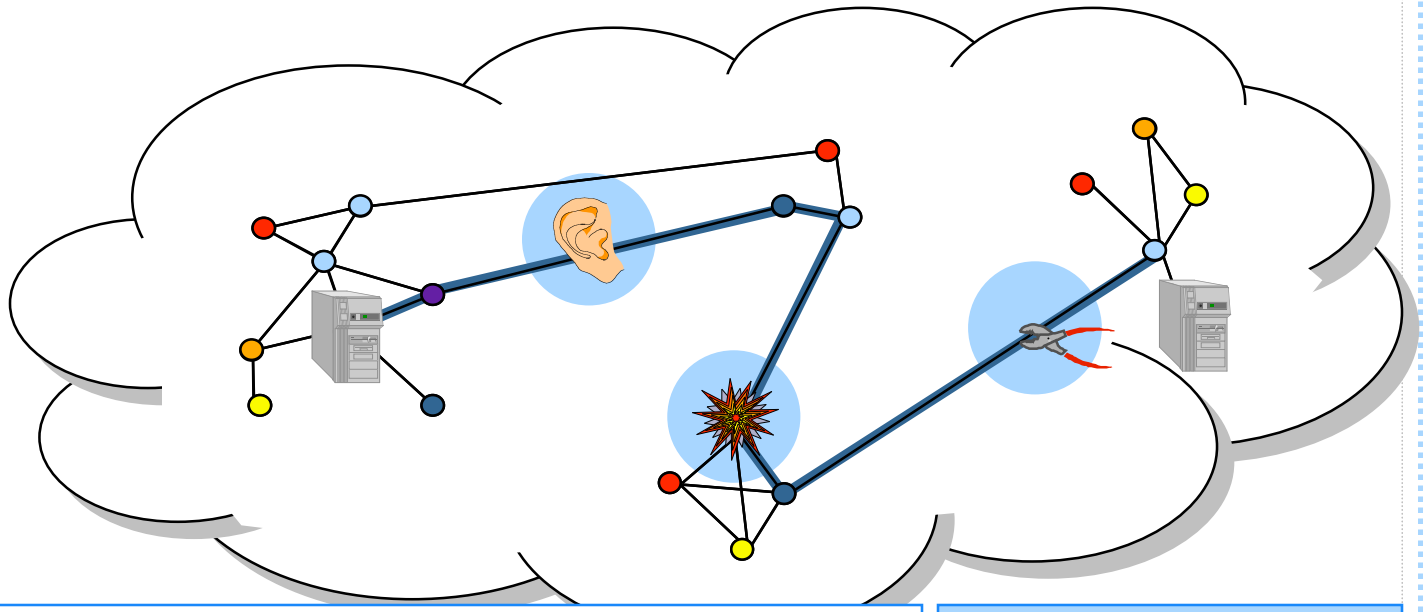
Technischer Schutz von Bezahlinhalten

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

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

Schutzziele



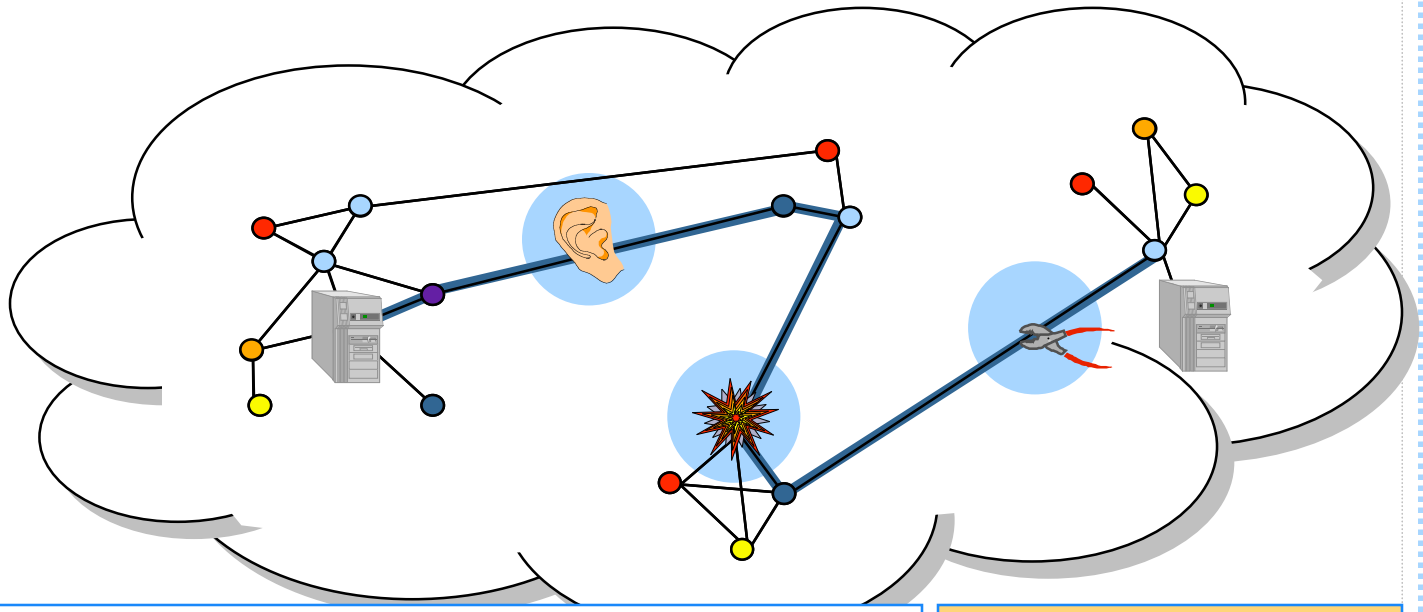
Bedrohungen

- unbefugter Informationsgewinn
- unbefugte Modifikation
- unbefugte Beeinträchtigung der Funktionalität

Schutz der

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Technischer Schutz von Bezahlinhalten



Anforderung

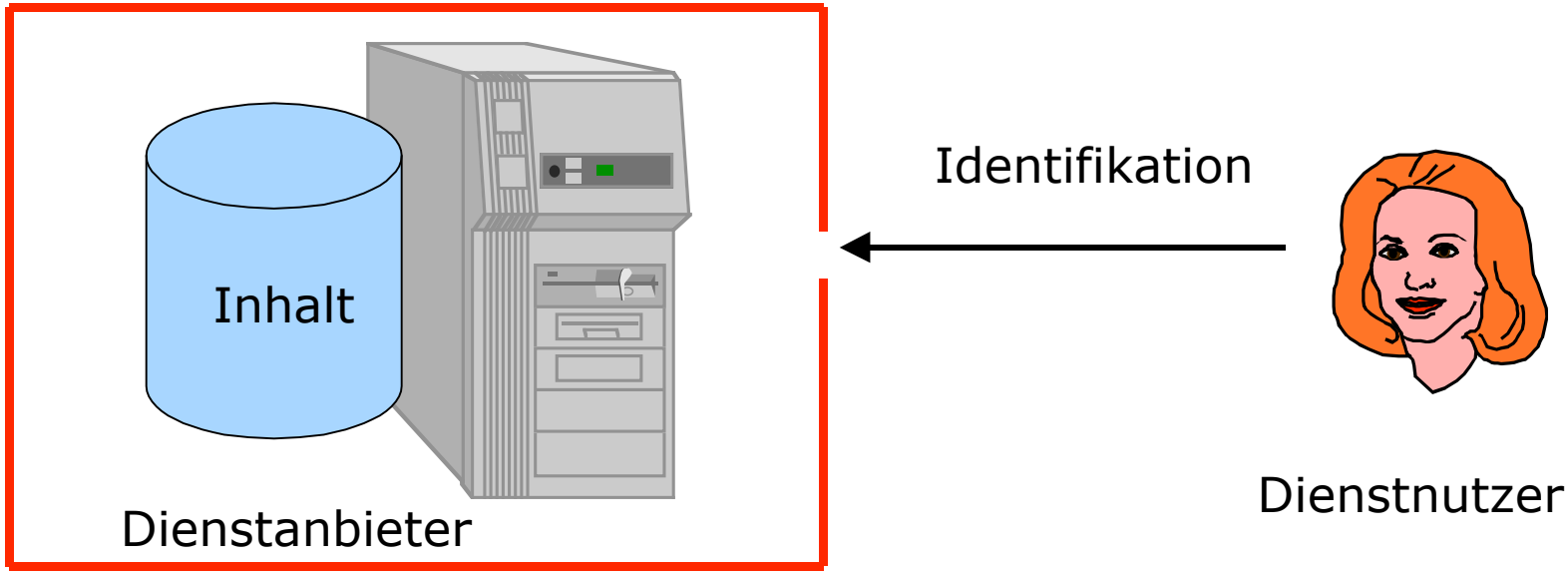
Inhalte sollen nur von Berechtigten genutzt werden können und somit vor Unberechtigten geschützt sein

Mechanismus

Zugangskontrolle

Zugangskontrolle

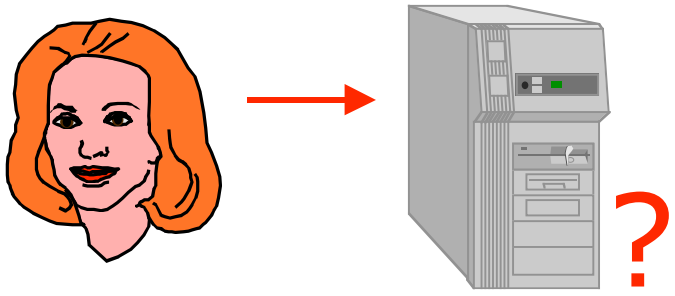
- IT-System erfragt die Identitäten seiner Kommunikationspartner
- Zweck
  - Nur mit berechtigten Partnern weiter kommunizieren
  - Verhindert unbefugte Inanspruchnahme von Betriebsmitteln



Identifikation von Menschen durch IT-Systeme

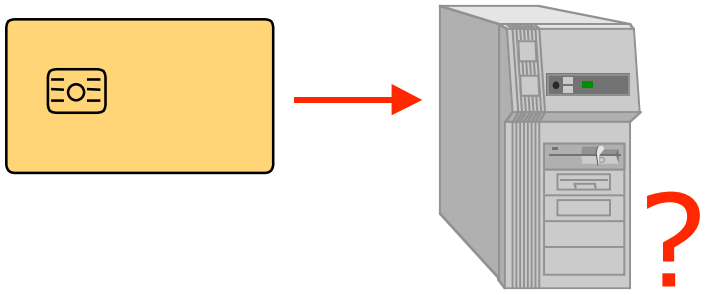
- Was der MENSCH IST:
  - Handgeometrie
  - Fingerabdruck
  - Aussehen*
  - eigenhändige Unterschrift*
  - Retina-Muster
  - Stimme
  - Tipp-Charakteristik
  - DNA-Muster
- Was der MENSCH HAT:
  - Papierdokument*
  - Metallschlüssel
  - Magnetstreifenkarte
  - Chipkarte
  - Taschenrechner
- Was der MENSCH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

*=Ausweis

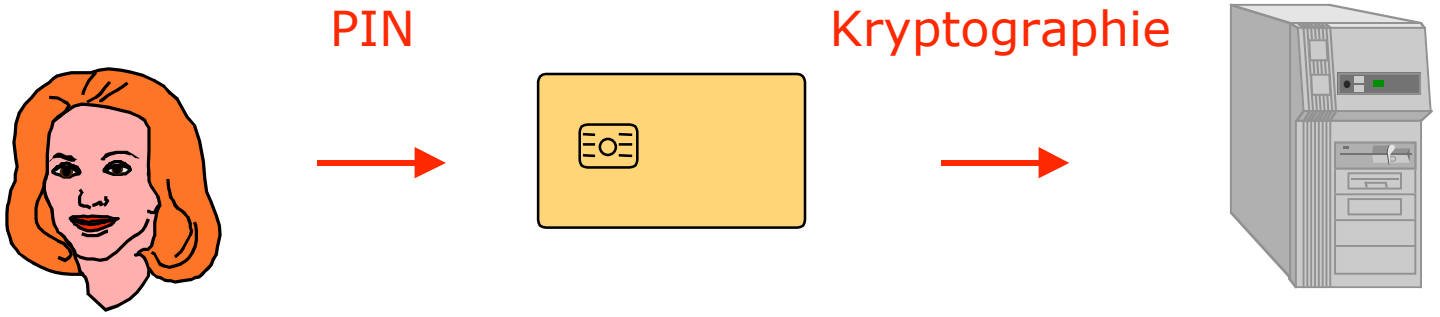


Identifikation von IT-Systemen durch IT-Systeme

- Wenn ein persönliches Gerät (Smartcard) eindeutig einem Berechtigten zugeordnet ist, kann dieses die Authentifizierung gegenüber dem IT-System übernehmen.



Zusammenspiel:



Passwort

- Identifizierung durch Wissen
- Unberechtigte Weitergabe des Passworts (Mehrfachnutzung) kann nicht verhindert werden
- Einmalpasswort in Kombination mit Besitz: SecurID

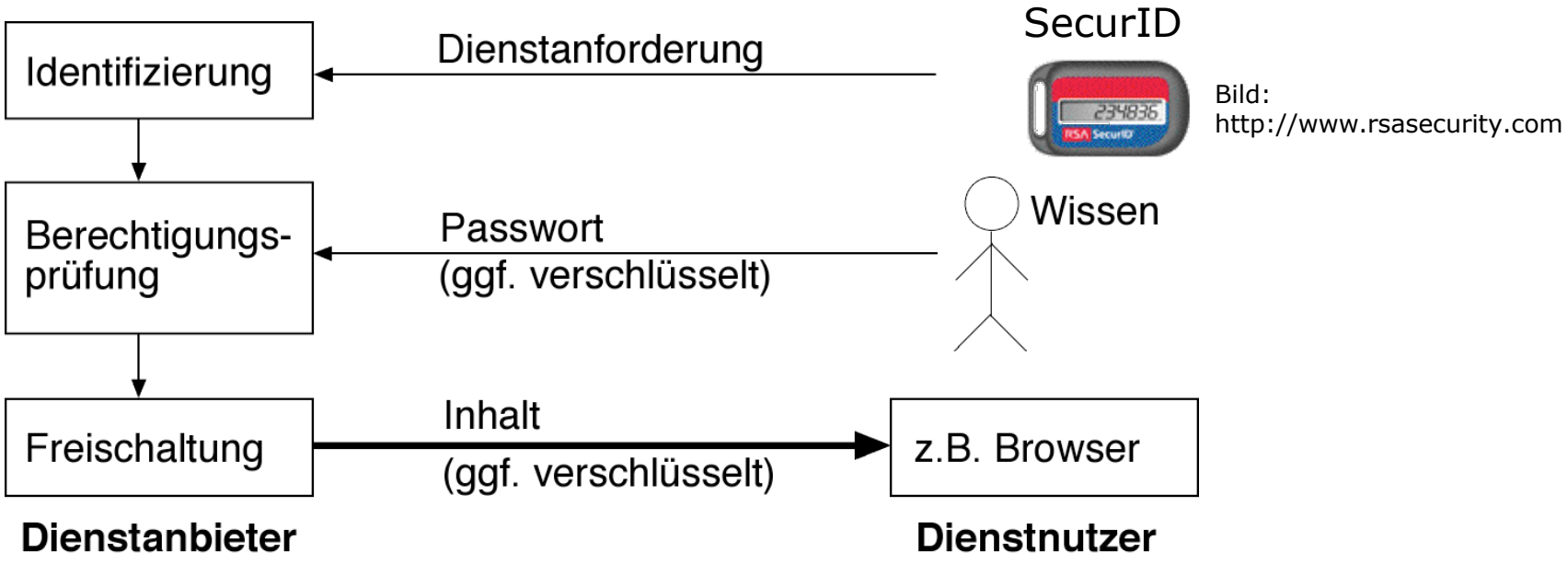
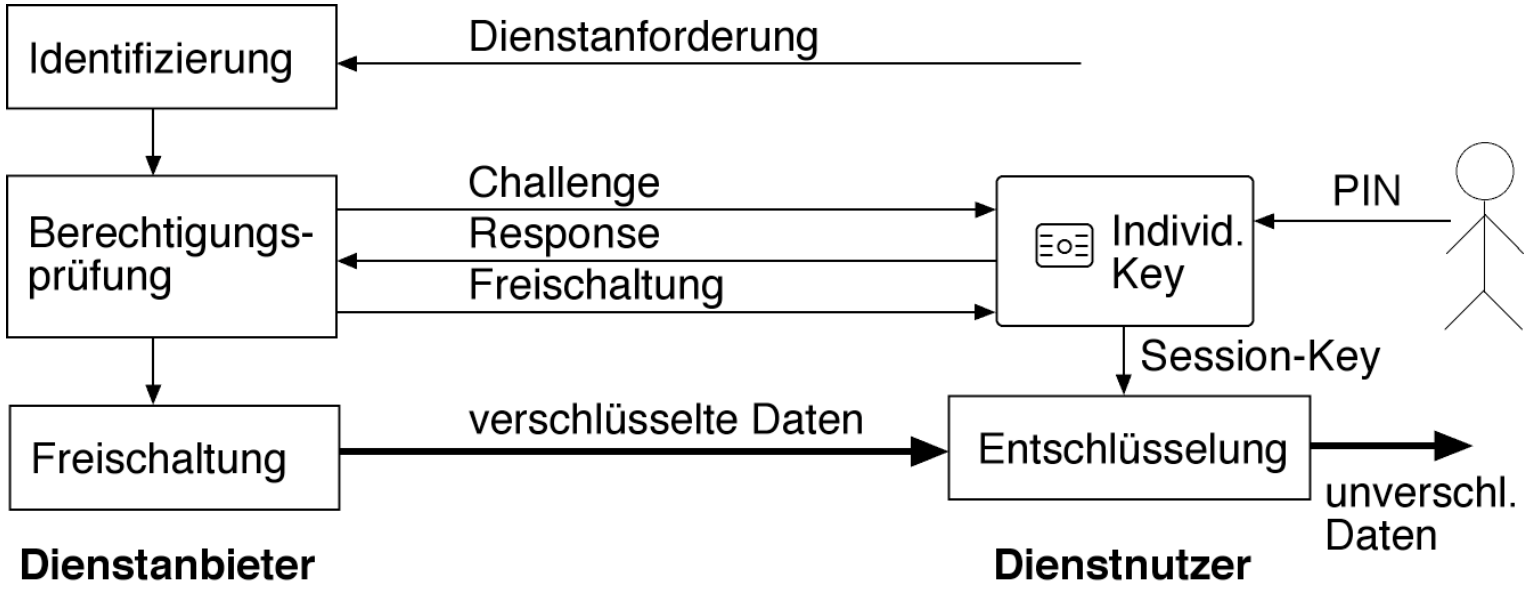


Bild:
http://www.rsasecurity.com

Challenge-Response-Authentikation

- Gebräuchlich im Mobilfunk
- geeignet für Punkt-zu-Punkt-Kommunikation
- nicht geeignet bei der Distribution

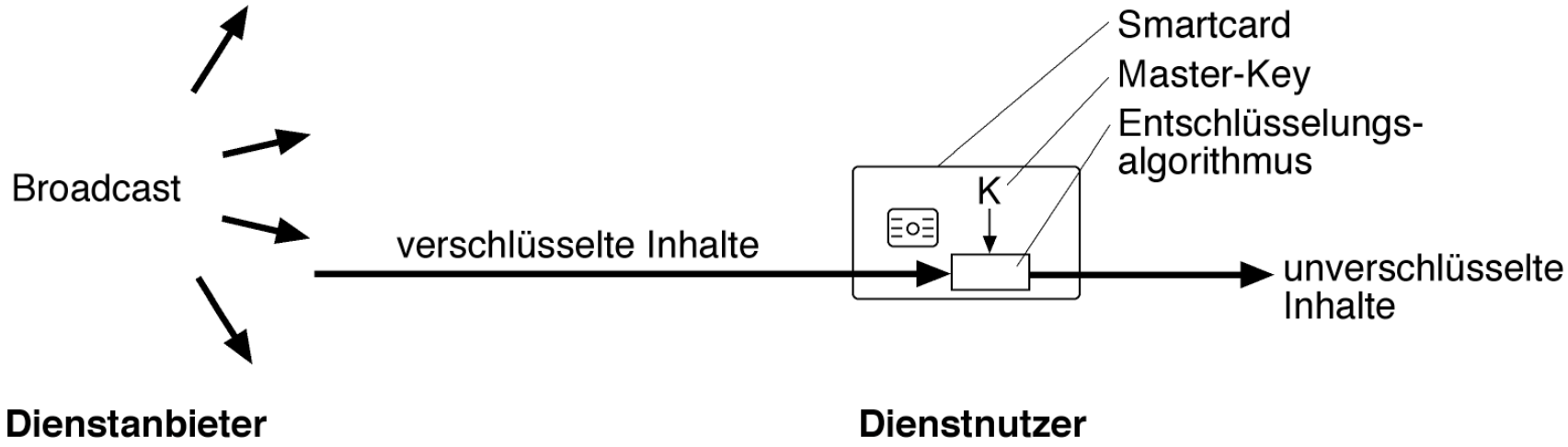
- Es wird überprüft, ob der Dienstnutzer ein Geheimnis kennt, ohne dieses Geheimnis übertragen zu müssen.



Smartcard mit Master-Key

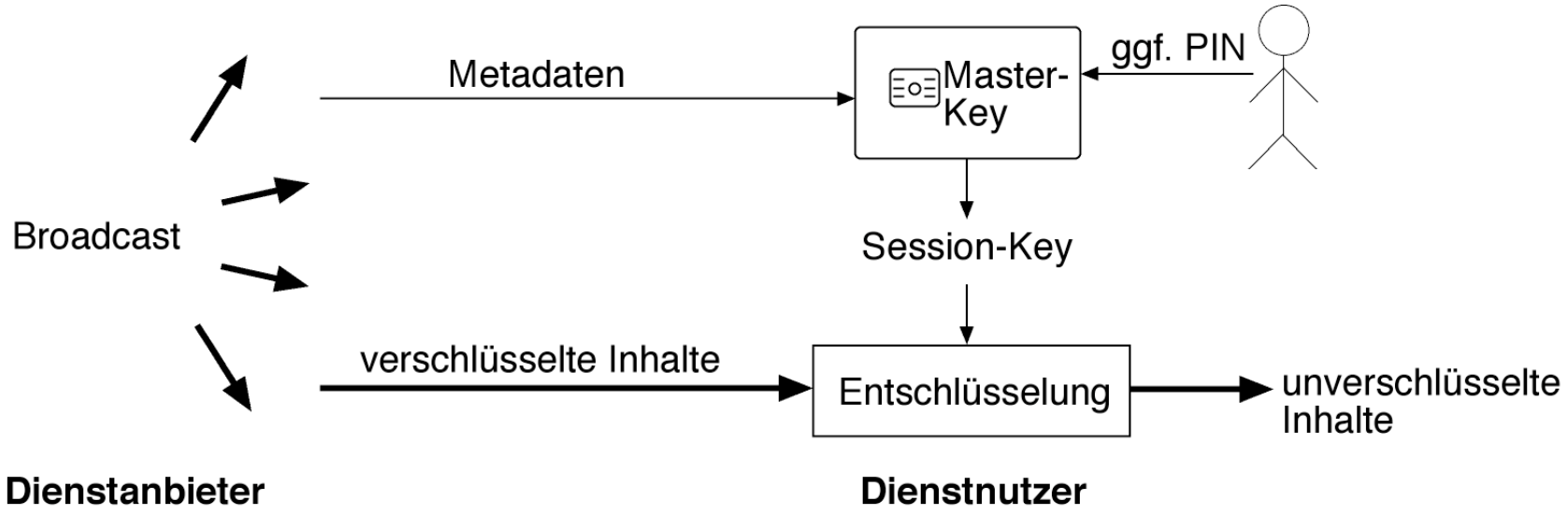
- Wenn Master-Key bekannt wird, ist das gesamte System kompromittiert.
- Physischer Schutz des Master-Key ist schwierig.

- In der Praxis viel zu gefährlich

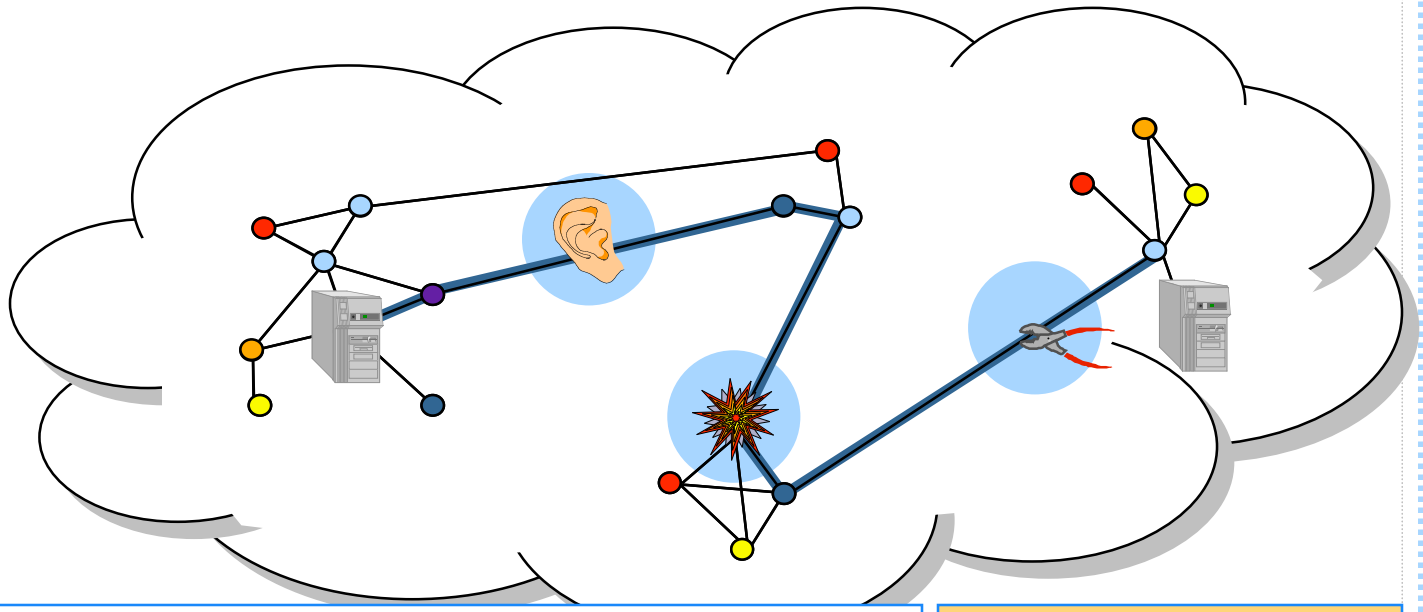


Smartcard mit Master und Session-Key

- Schlüssel-Hierarchie soll Kompromittierung des Gesamtsystems verhindern
- Es existieren mehrere Master-Keys, mit den der momentane Session-Key verschlüsselt ist.
- Bei Kompromittierung eines oder weniger Master-Keys werden diese von der verteilung der verschlüsselten Session-Keys ausgeschlossen.



Technischer Schutz von Bezahlinhalten



Anforderung

Inhalte sollen vom Berechtigten nur in der vereinbarten Weise genutzt werden

Mechanismus

Digital Rights Management Systeme

Digital Rights Management Systeme

- Schutzziel:
  - Es muss sichergestellt werden, dass der Inhalt nur in der vorgesehenen Weise genutzt wird.

- Nutzungsarten: Beispiele:
  - X-mal nutzen (anschauen, anhören, ...) mit X>=1
  - Y-mal kopieren (z.B. auf CD) mit Y>=0
  - nur in Territorium Z nutzbar
  - nur bis zum Zeitpunkt T nutzbar

- Stärke der existierenden Verfahren
  - erschweren das Kopieren,
  - können es aber nicht verhindern
  - Es ist kein System in Sicht, das Kopieren wirklich verhindert.

DRM-Systeme heute

- Realisierungsansatz:
  - Inhalt wird um Meta-Daten ergänzt
  - Meta-Daten tragen Informationen über die erlaubten Nutzungsarten
  - "Offizielle" Abspielsoftware liest Meta-Daten und gibt Inhalte für erlaubte Nutzungsarten frei

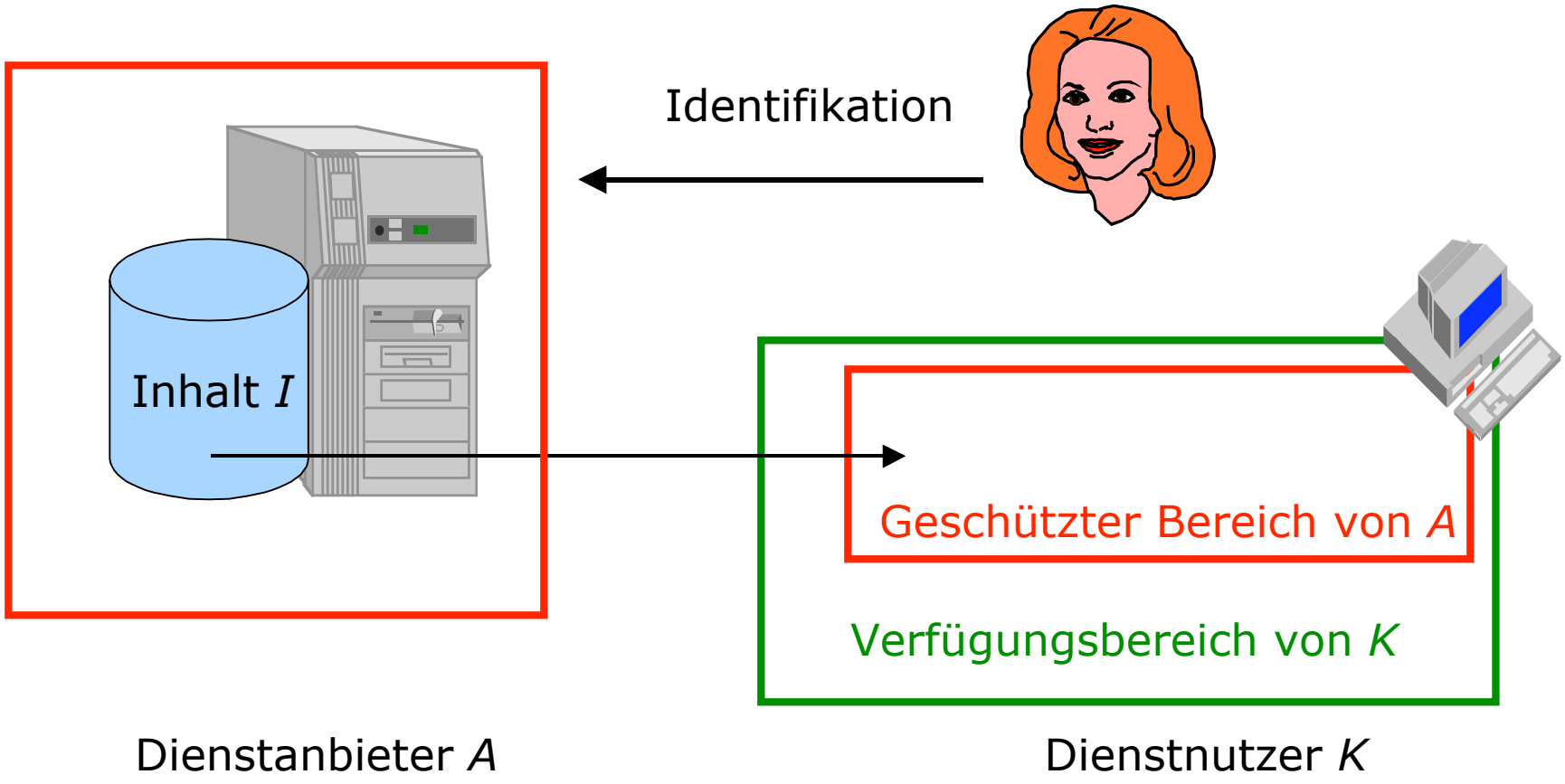
- Problem:
  - Geräte, auf denen Inhalte heute typischerweise genutzt werden:
    - frei programmierbarer Universal-PC
    - umprogrammierbare Set-Top-Box

Frei programmierbarer Universal-PC

- Angriff:
  - Anstelle der "offiziellen" Nutzungssoftware wird fremde Software genutzt, die die Nutzungsmöglichkeiten nicht einschränkt.
  - Das ist nicht verhinderbar!
- Vorgehen aus Angreifersicht:
  - Reverse Engineering des offiziellen Programms.
- Beispiele:
  - RealPlayer-Modifikation mit Abspeicherfunktion
  - DRM von Microsoft
  - E-Book-Software von Adobe

Das DRM-Problem

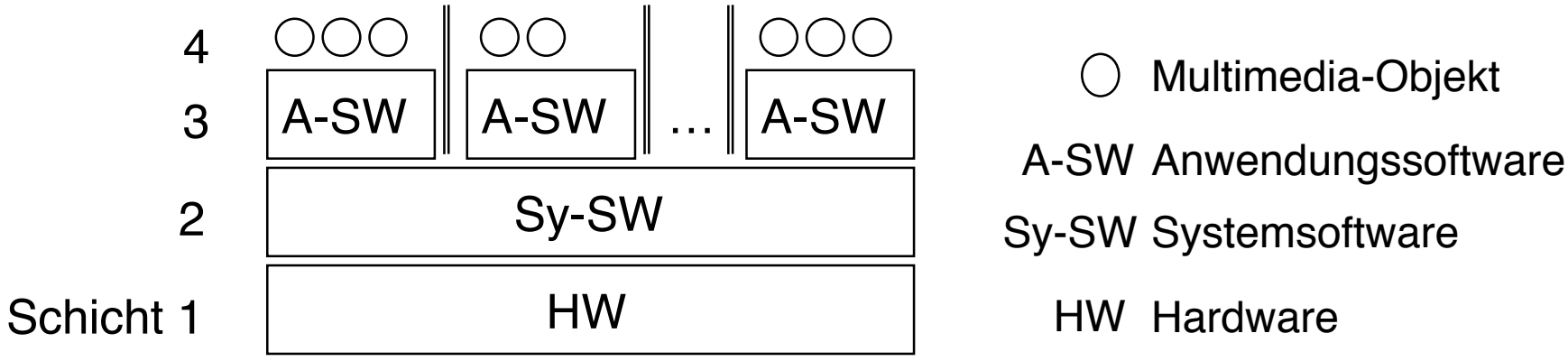
- Einem Kunden *K* einen Inhalt *I* in einer bestimmten Weise zugänglich machen, ihm aber daran hindern, *alles* damit tun zu können.



Frei programmierbarer Universal-PC

- Ausführungs-Schichtenstruktur
  - Objekte können vor den darunter liegenden Schichten nicht effizient geschützt werden.

- Folge:
  - Auf frei programmieren PCs werden Multimedia-Objekte nie wirklich schützbar sein.



[Nicht] Frei programmierbarer Universal-PC

- Abwehr:
  - spezielle Hardware (Tamper Proof Module, TPM), die im PC eingebaut ist
  - schützt vor Ausführung nicht autorisierter Programme
- Folge:
  - Es können nur noch offizielle Programme mit einem geschützten Inhalt verwendet werden.
- Beachte:
  - Autorisierung muss bis auf Hardware-Treiber-Ebene erfolgen!

- Grundproblem:
  - Selbst Hardwaremodul bietet nicht ewig Sicherheit.
- Hoffnung:
  - Zeitraum, über den das Geheimnis geschützt bleibt, ist länger als Schutzbedarf des Inhalts

Nicht frei programmierbarer Universal-PC

- Zu beachten:
  1. Entweder: Inhalte werden in Hardwaremodul entschlüsselt
  2. Oder: Server darf unverschlüsselte Inhalte erst nach Autorisierung durch das Hardwaremodul ausgeben.

  - Bei 2. muss Content-Server die Authentizität des Hardwaremoduls überprüfen
  - Weder 1. noch 2. momentan in der Spezifikation des Hardwaremoduls der TCG (Trusted Computing Group, früher TCPA, Trusted Computing Platform Alliance) vorgesehen.

- Datenschutzsicht
  - Funktionen zur Identitätsprüfung durch Content-Server sind wegen der Erstellungsmöglichkeit von Nutzungsprofilen nicht zu empfehlen.
  - siehe z.B. Diskussionen bzgl. Prozessor-IDs auf Intel-Chips