



# Rechner- und Betriebssystemsicherheit

Physische Sicherheit

Identifikation von Menschen und IT-Systemen

Zugangs- und Zugriffskontrolle



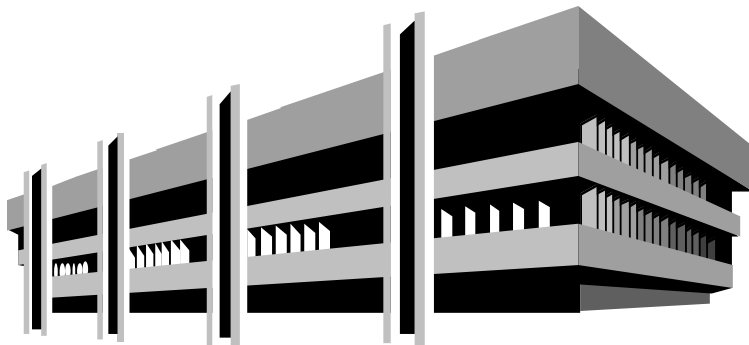
Universität Hamburg

DER FORSCHUNG | DER LEHRE | DER BILDUNG

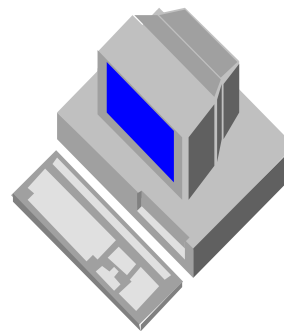
## Sicherheit im einzelnen Rechner: Physische Sicherheit

- Physische Sicherheit
  - Alle technischen Schutzmaßnahmen benötigen eine physische «Verankerung» in Form eines Systemteils, auf den der Angreifer keinen physischen Zugriff hat.
- Physische Sicherheit zu erhalten, gelingt bestenfalls auf Zeit.

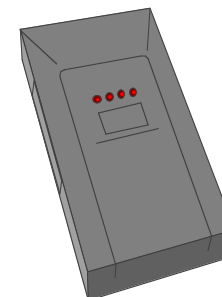
Rechenzentrum



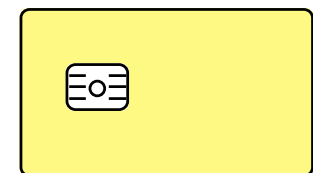
einzelner  
Rechner



Sicherheitsmodul

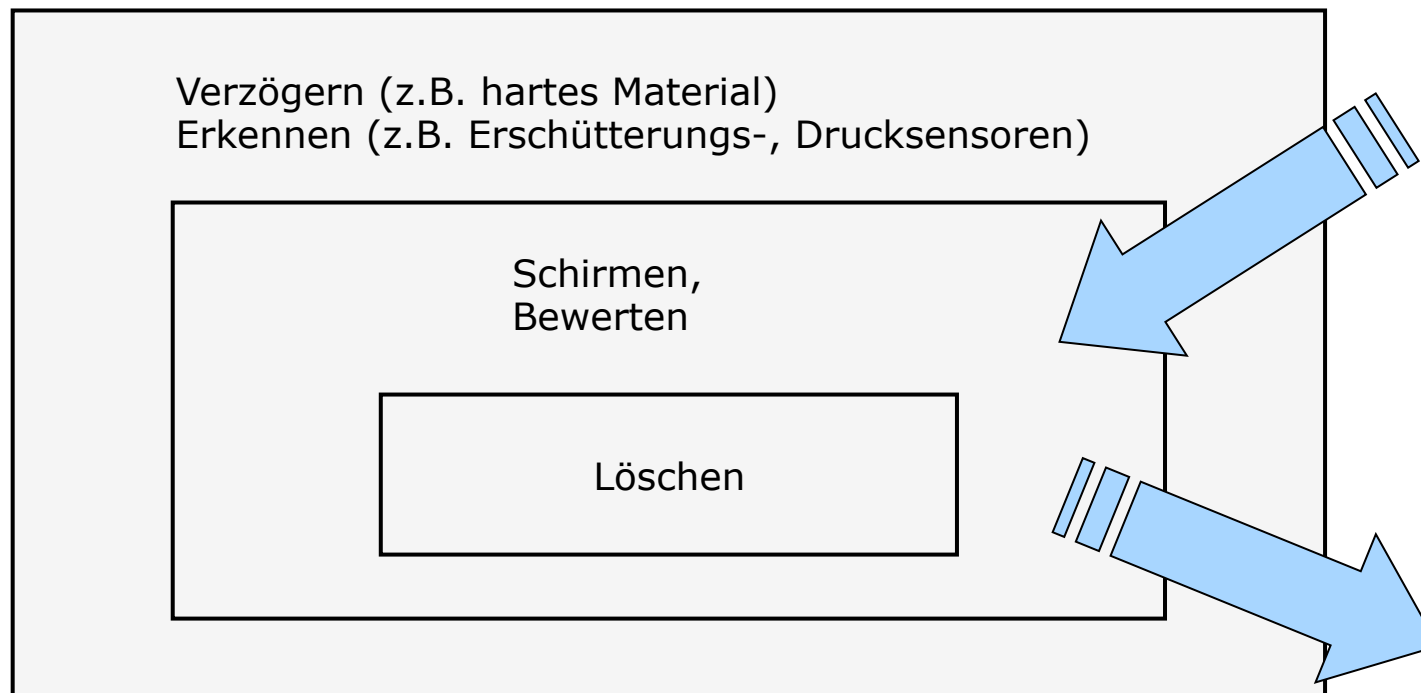


Chipkarte



## Physische Sicherheit: Grundfunktionen

- Beobachtende Angriffe:
  - **Schirmung** (elektromagnetische Abstrahlung, Energieverbrauch  
– unabhängig von den zu schützenden Geheimnissen)
- Verändernde Angriffe:
  - **Erkennen, Bewerten, Verzögern** und ggf. **Löschen** der geheimen Informationen.



## Physische Sicherheit

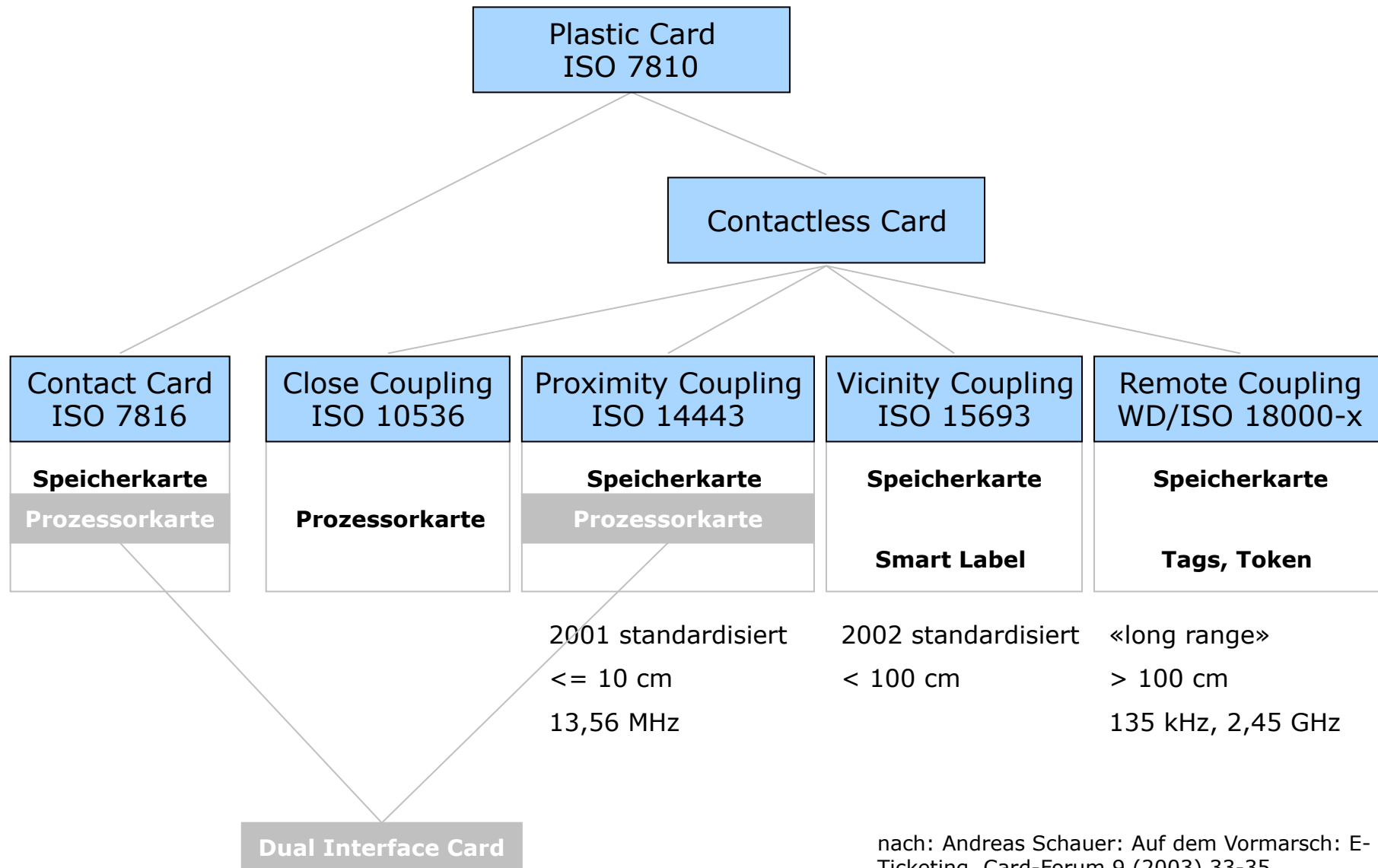
- Sicherheitsmodul



Bild: [www.lampertz.de](http://www.lampertz.de)

- Brandschutz
- Zutrittsschutz
- Klimatisierung
- Unabhängige Stromversorgung

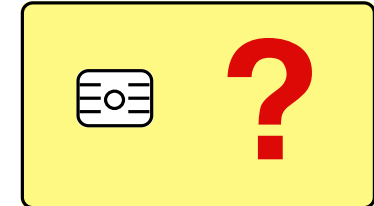
# Chipkarten



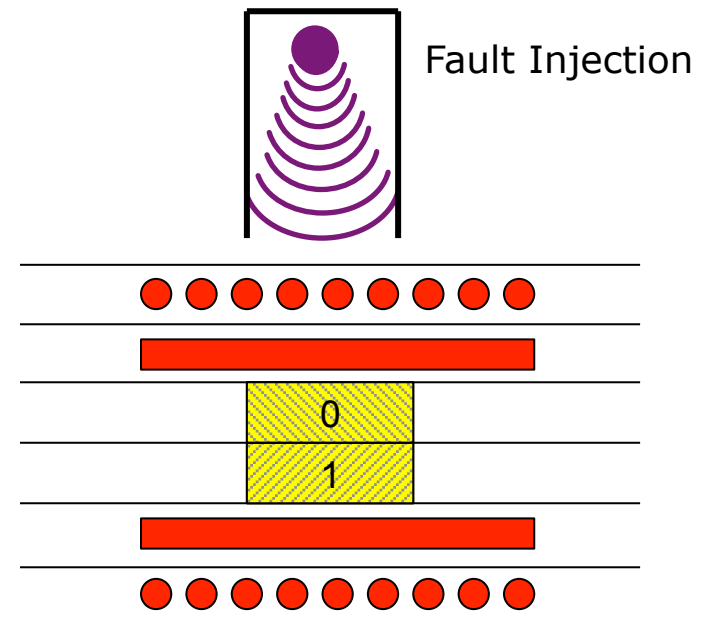
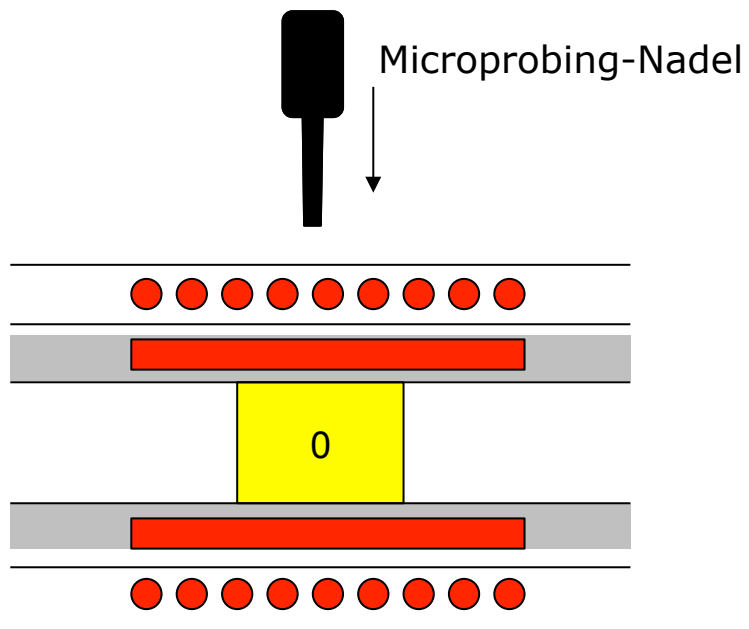
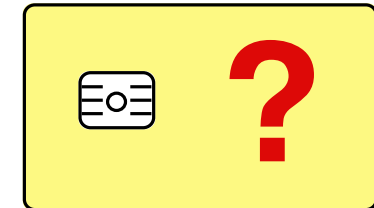
nach: Andreas Schauer: Auf dem Vormarsch: E-Ticketing. Card-Forum 9 (2003) 33-35.

## Negativbeispiel Chipkarten

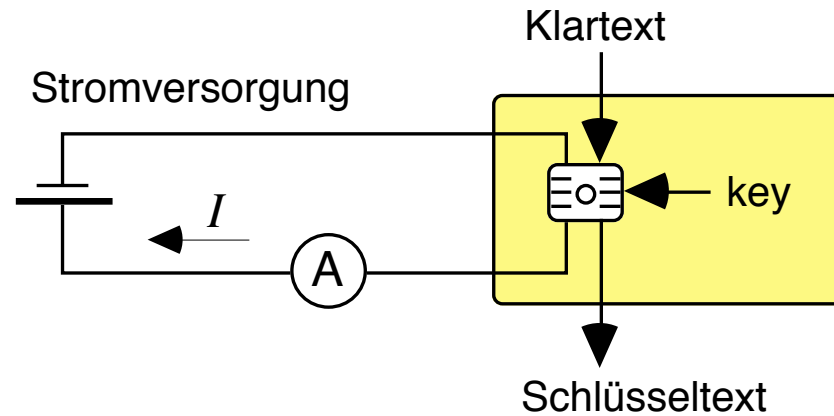
- Probleme
  - kein Erkennen (Energieversorgung auf Chip fehlt)
  - Schirmung schwierig (Karte dünn und biegsam)
  - kein Löschen vorgesehen, selbst bei Stromversorgung
- Beispiele für Angriffe:
  - Zerstörend:
    - Vorbereitung: Abschleifen und Anätzen der Schutzschichten
    - ggf. Reverse Engineering: Untersuchung der Strukturen unter Elektronenmikroskop, wenn Funktion unbekannt
    - Microprobing-Nadel
    - »Fault Injection: gezielte Manipulation von Bits durch Beschuß mit elektromagnetischer Strahlung
  - Zerstörungsfrei: meist »sidechannel attacks«
    - Messung des Energieverbrauchs (»power analysis«)
    - Messung der benötigten Rechenzeit (»timing attacks«)



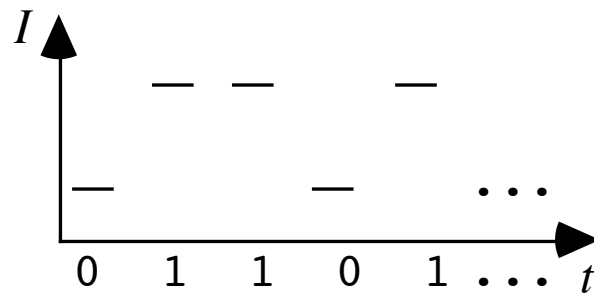
# Zerstörende Angriffe und Schutz davor



# Timing Attack / Power Analysis (Skizze)



Angriffsziel: Key ermitteln



»1« hoher Stromverbrauch  
»0« niedriger Stromverbrauch

Schlüsselbits sind direkt auslesbar.

Dem Angreifer unbekannt:

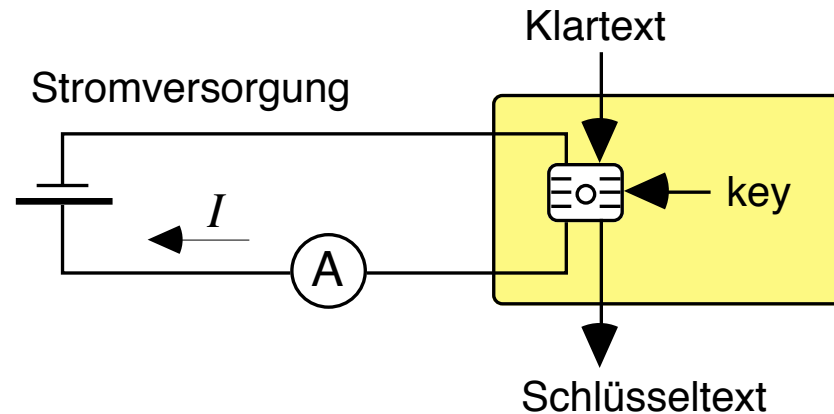
key = array of bit  
= ( 0, 1, 1, 0, 1, ... )

Dem Angreifer bekannt:

```
encrypt (Klartext, key)
{
    ...
    for i = 1 to length(key)
    {
        ...
        if (key[i] == 1)
        {
            ...
            /* Stromverbrauch,
            Δt > 0 */
        }
        else
        {
            <nothing>
            /* kein
            Stromverbrauch,
            Δt ≈ 0 */
        }
    }
    ...
}
```



## Timing Attack / Power Analysis (Skizze)



Angriffsziel: Key ermitteln

Auswege:

- interner »Energiepuffer«
- Verzweigungen vermeiden
- `<nothing>` durch Dummy-Befehle der exakt gleichen Zykluszeit wie `{ ... }` ersetzen

Dem Angreifer unbekannt:

```
key = array of bit
    = ( 0, 1, 1, 0, 1, ... )
```

Dem Angreifer bekannt:

```
encrypt (Klartext, key)
{
    ...
    for i = 1 to length(key)
    {
        ...
        if (key[i] == 1)
        { ... }
        /* Stromverbrauch,
           Δt > 0 */
        else
        <nothing>
        /* kein
           Stromverbrauch,
           Δt ≈ 0 */
    }
    ...
}
```

## Cold Boot und Hot Plug: Brechen der Festplattenverschlüsselung

- Cold Boot: <https://citp.princeton.edu/research/memory/>
  - Voraussetzung: Hauptspeicher des Rechner enthält den (flüchtigen) Key der Festplattenverschlüsselung
  - Nach Ausschalten verbleibt (nutzbare) Restladung
  - Abkühlen verlangsamt Speicherremanenz
  - Angreifer hat genügend Zeit, den Speicher auszubauen und auszulesen
- Hot Plug: <http://www1.informatik.uni-erlangen.de/sed>
  - Annahme: Festplattenverschlüsselung direkt auf der Platte; Hauptspeicher enthält nicht mehr den Key
  - Hausdurchsuchungsszenario: Rechner wird im laufenden Betrieb gefunden, nicht ausgeschaltet, die Festplatte (unter Strom) an einen externen Controller angeschlossen
  - einige Festplatten bemerken Controllerwechsel nicht

# 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**

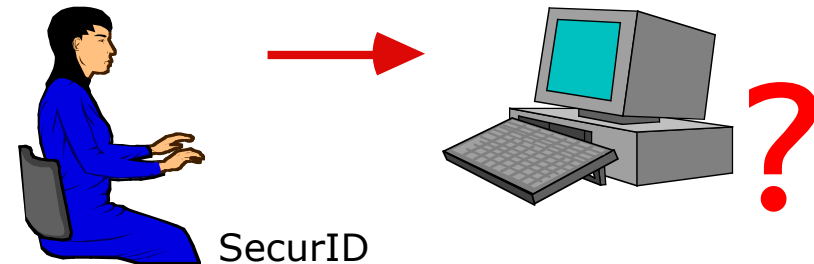


Bild:  
<http://www.rsasecurity.com>

SCHUFA-XSCard

SNr: A182C3D4E5F6

schufa

Wir schaffen Vertrauen

Ihr Zugang zu [www.meineSCHUFA.de](http://www.meineSCHUFA.de)

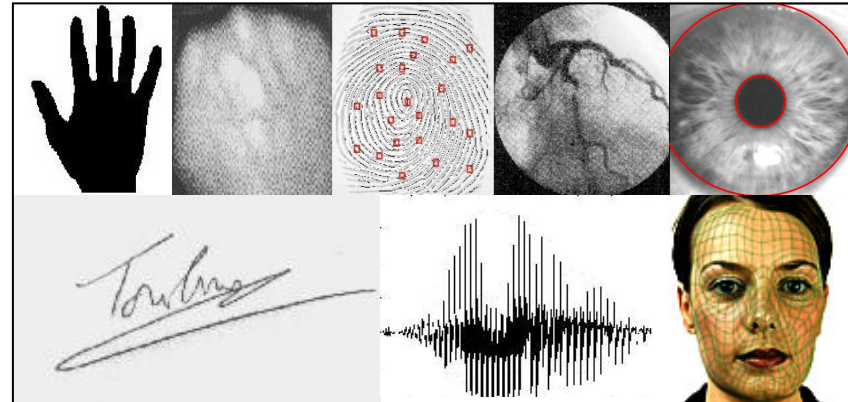
	A	B	C	D	E	F	G	H	I	J	Muster
1	QW	12	B5	A7	MW	WW	IJ	I1	8B	A7	 <div> <div>0000134</div> <div>0000134</div> </div>
2	A7	MW	II	B8	12	B5	MW	II	B8	12	
3	1L	QW	12	B5	MW	II	B8	12	CG	L7	
4	AD	J1	QW	11	B5	XK	D1	D8	D6	KH	
5	ZH	T7	P9	5X	X1	QW	12	G6	WM	KM	

SCHUFA Headline AG

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

## Passwortregeln

- Ändern Sie Ihr Passwort in regelmäßigen Abständen.
- Legen Sie niemals Passwörter in Dateien ab.
- Verwenden Sie in Ihrem Passwort nicht
  - Namen, Telefonnummern, Geburtsdaten, Autonummern,
  - Wörter aus Wörterbüchern, Eigennamen,
  - Tastaturmuster (vgl. «wertzuio»).
  - All dies rückwärts oder doppelt.
  - All dies mit Ziffern oder Sonderzeichen davor oder dahinter.
  - All dies in kombinierter Groß- und Kleinschreibweise.
- Beachten Sie, dass häufig nur die ersten acht Zeichen des Passwortes signifikant sind.
- Verwenden Sie
  - viele verschiedene Zeichen,
  - kombinierte Groß- und Kleinschreibweise,
  - Ziffern und Sonderzeichen.
- Trick: Verwenden Sie die Anfangsbuchstaben eines «verrückten» Satzes, der auch Zahlen und Sonderzeichen enthält.

### Passwortflut macht Nutzer leichtsinnig

Belford (sts) – Mehr als 13 Passwörter benötigt ein Viertel der 1700 von RSA befragten Firmenanwender. Und meist sind diese regelmäßig zu ändern. Folge: Vergessene Codes, deren Reset bis zu 145 Dollar pro Fall kostet. Zudem notieren Nutzer ihre Zugangsdaten oft unsicher in PC-Dateien, PDAs oder auf Papier. Abhilfe schaffen Single-Sign-On-Verfahren. Quelle: Computerzeitung 35. Jahrgang Nr. 40, 4.10.05, S. 1

## Welche Passwörter werden tatsächlich genutzt?

- Im Dezember 2009 wurden 32 Millionen Passwörter von einem Hacker veröffentlicht: Studie von Imperva (<http://www.imperva.com>)
  - Ein blinder Log-in-Versuch mit "123456" führt in 0,9 % der Fälle zum Erfolg.
  - Rund 50 % der Passwörter können als "schwach" bezeichnet werden:
    - Wörter aus Wörterbüchern
    - Tastaturmuster

Prüfung der Passwortqualität durch Systembetreiber ist zwingend erforderlich!

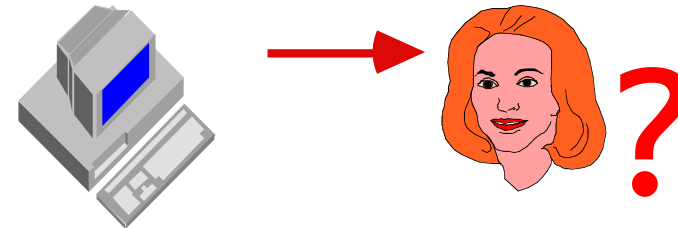
Rang	Passwort	Häufigkeit
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542
11	Nicole	17168
12	Daniel	16409

Quelle: The Imperva Application Defense Center (ADC): Consumer Password Worst Practices, 2010

## Identifikation von IT-Systemen durch Menschen

- Was es ist:

- Gehäuse
- Siegel
- Hologramm
- Verschmutzung



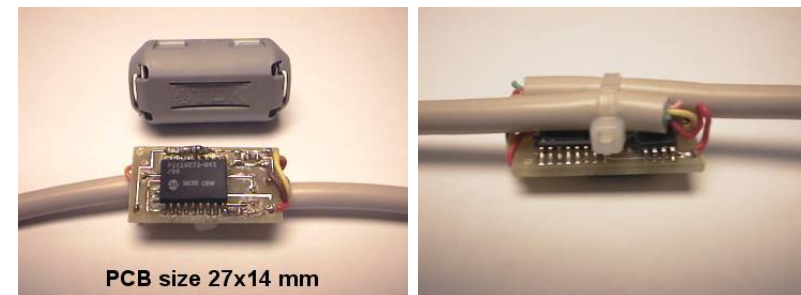
- Was es weiß:

- Passwort
- Antworten auf Fragen
- Rechenergebnisse für Zahlen

Warum ist das relevant?

- Faked Login-Screen
- Phishing
- Keylogger
- Manipulation Geldautomat

- Wo es steht.



Bilder: <http://keyspy.de.vu/>

# Manipulationen an Geldautomaten

Quelle: Bundesgrenzschutzamt Flensburg



1. Aufsatz auf Kartenschlitz liest Magnetstreifen ...



# Manipulationen an Geldautomaten

Quelle: Bundesgrenzschutzamt Flensburg



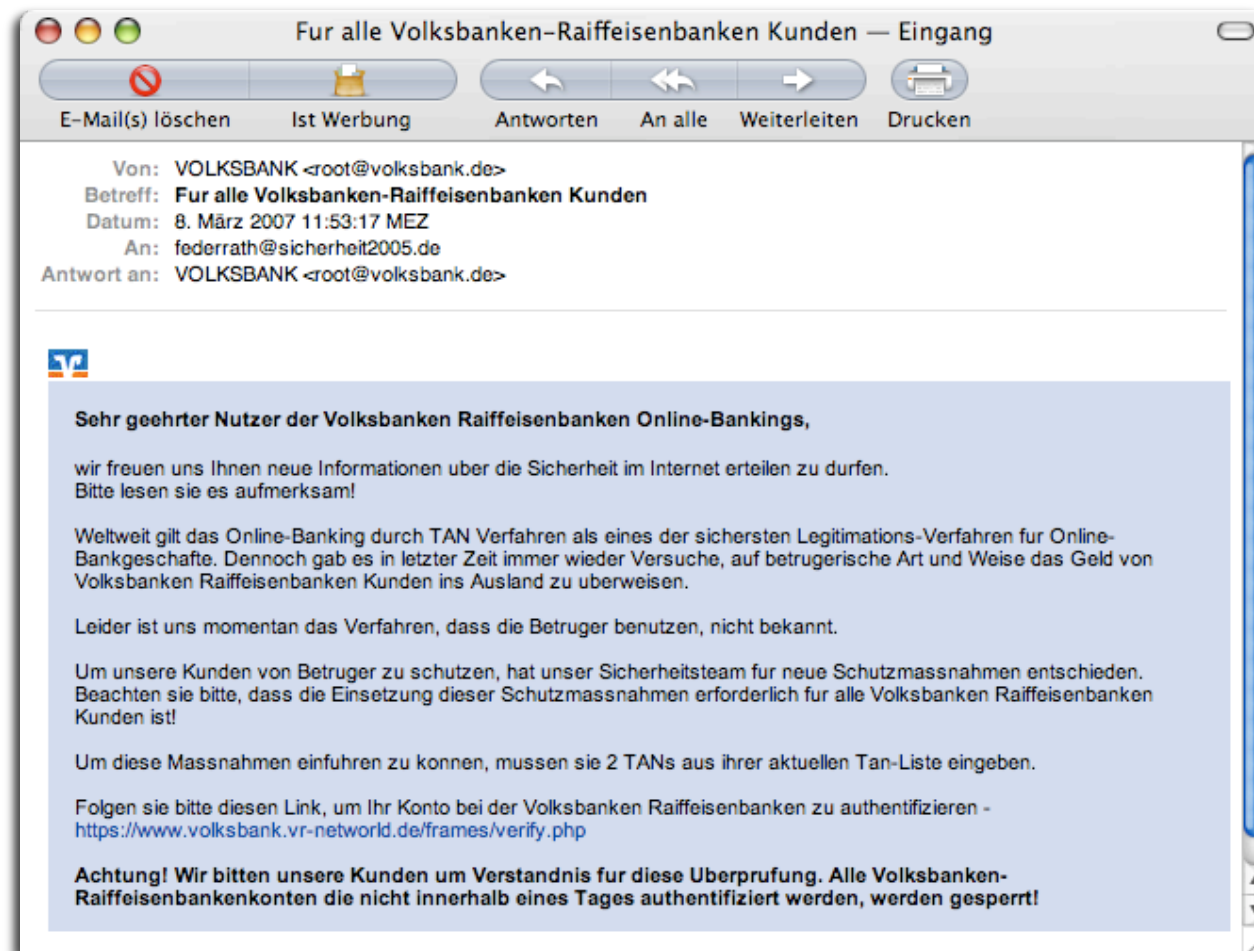
2. Kamera erfasst PIN-Eingabe und überträgt die Daten per Funk



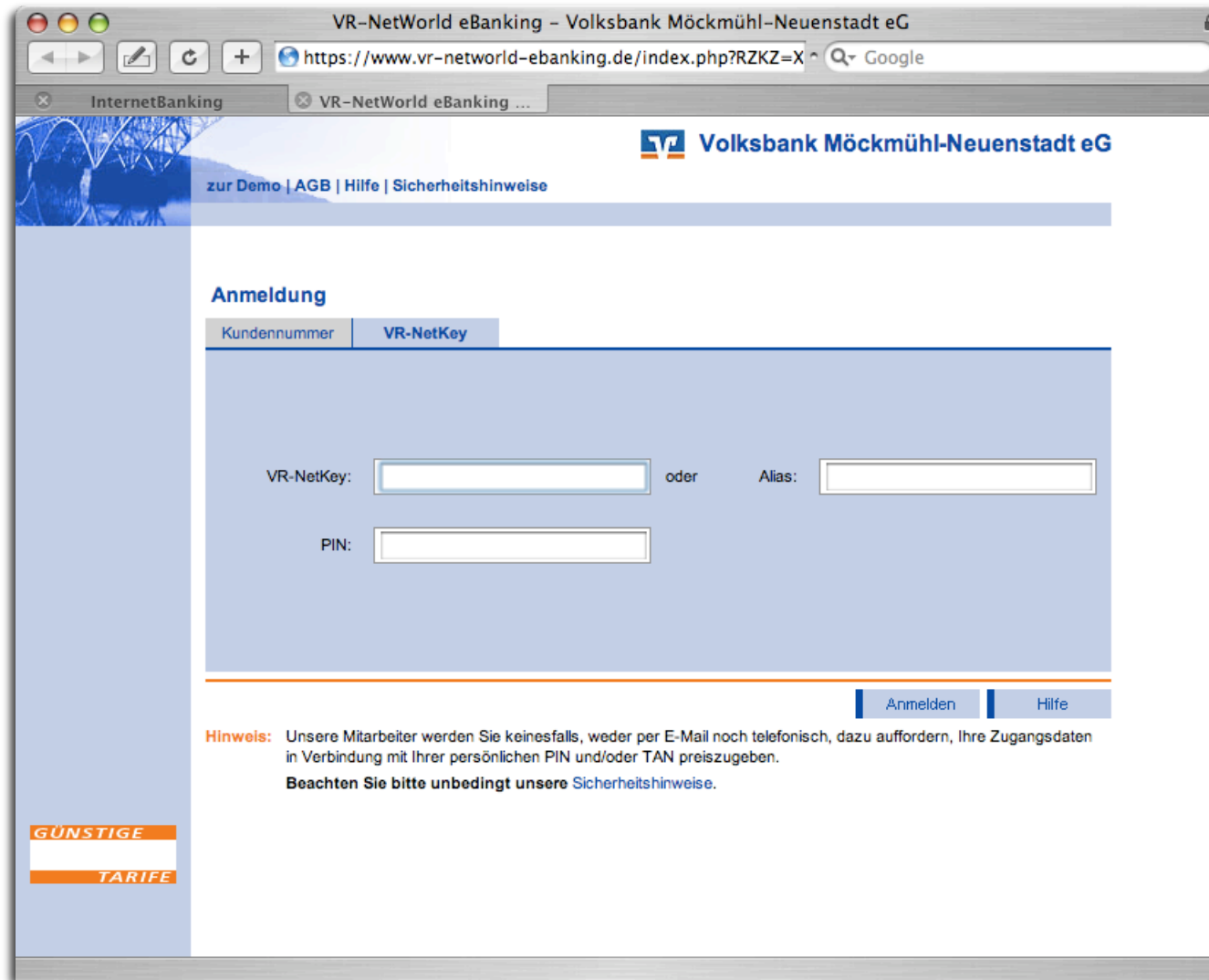
Antenne

# Phishing

- E-Mail des Angreifers (Spam-E-Mail)



# Original



VR-NetWorld eBanking – Volksbank Möckmühl-Neuenstadt eG

https://www.vr-networld-ebanking.de/index.php?RZKZ=X Google

InternetBanking VR-NetWorld eBanking ...

**Volksbank Möckmühl-Neuenstadt eG**

zur Demo | AGB | Hilfe | Sicherheitshinweise

### Anmeldung

Kundennummer VR-NetKey

VR-NetKey:  oder Alias:

PIN:

Anmelden Hilfe

**Hinweis:** Unsere Mitarbeiter werden Sie keinesfalls, weder per E-Mail noch telefonisch, dazu auffordern, Ihre Zugangsdaten in Verbindung mit Ihrer persönlichen PIN und/oder TAN preiszugeben.  
**Beachten Sie bitte unbedingt unsere Sicherheitshinweise.**

**GÜNSTIGE  
TARIFE**

# Fälschung

The screenshot shows a web browser window titled 'InternetBanking'. The address bar displays the URL 'http://www.internetbankinggad.cd/volksbank-app/'. The page has a navigation bar with links: Home, Anmelden, Demo, and Hilfe. A sidebar on the left lists various services: Impressum und Preise, Kontenwechsel, Kontoinformationen, Zahlungsverkehr, Geldanlageberatung, PIN / TAN verwalten, Service, Brokerage, and Handy aufladen. The main content area is titled 'Anmeldung' and contains the following text and form fields:

Bitte geben Sie Ihre Kontonummer sowie die zugehörige PIN ein

Bankleitzahl:

Kontonummer:

PIN:

Geben Sie bitte zwei früher nicht verwendete TAN ein.

TAN:

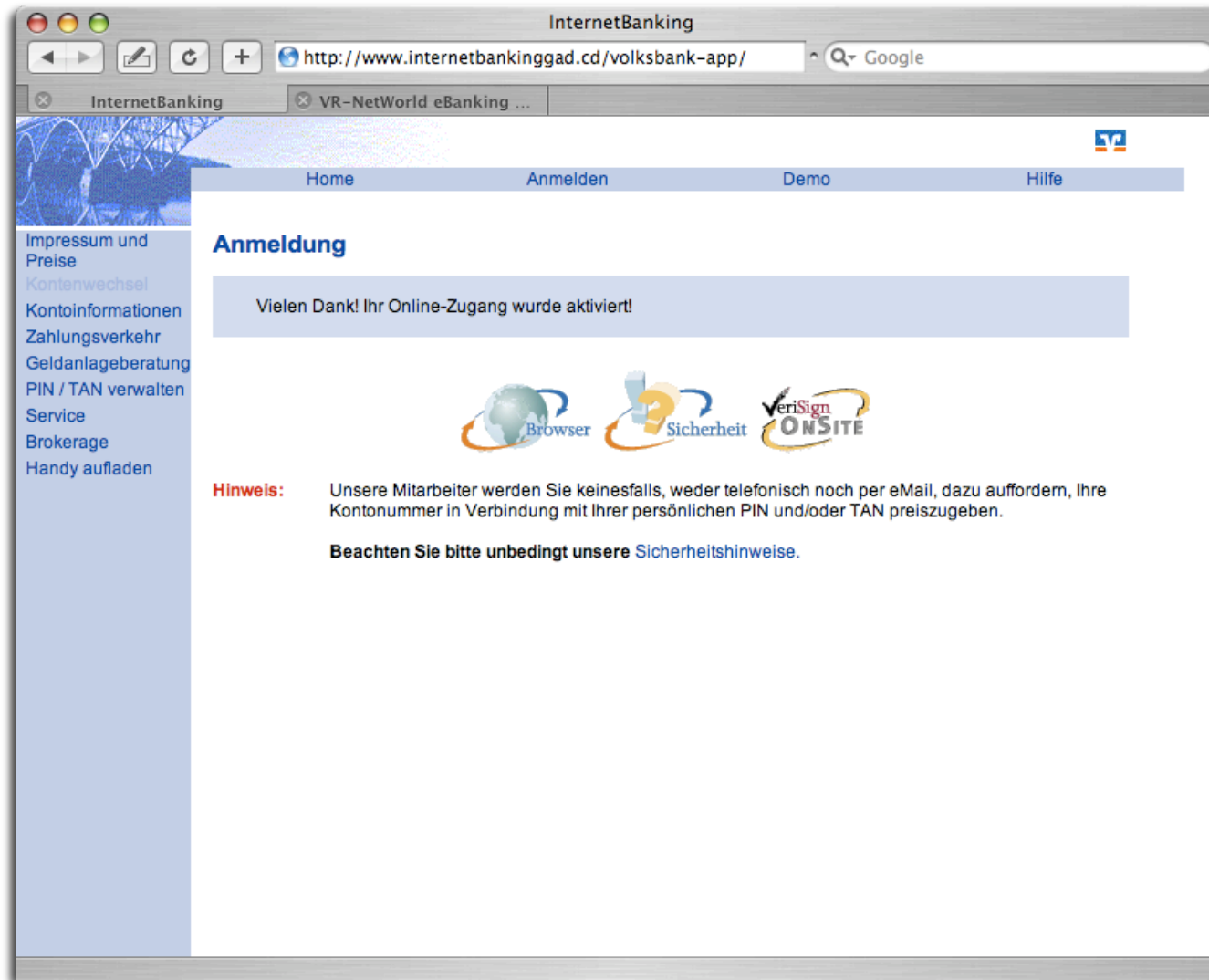
TAN:

At the bottom of the form area, there are buttons for 'Hilfe' and 'Weiter'. Below the form, there are logos for 'Browser', 'Sicherheit', and 'VeriSign ONSITE'. A red 'Hinweis' (Note) section contains the following text:

**Hinweis:** Unsere Mitarbeiter werden Sie keinesfalls, weder telefonisch noch per eMail, dazu auffordern, Ihre Kontonummer in Verbindung mit Ihrer persönlichen PIN und/oder TAN preiszugeben.

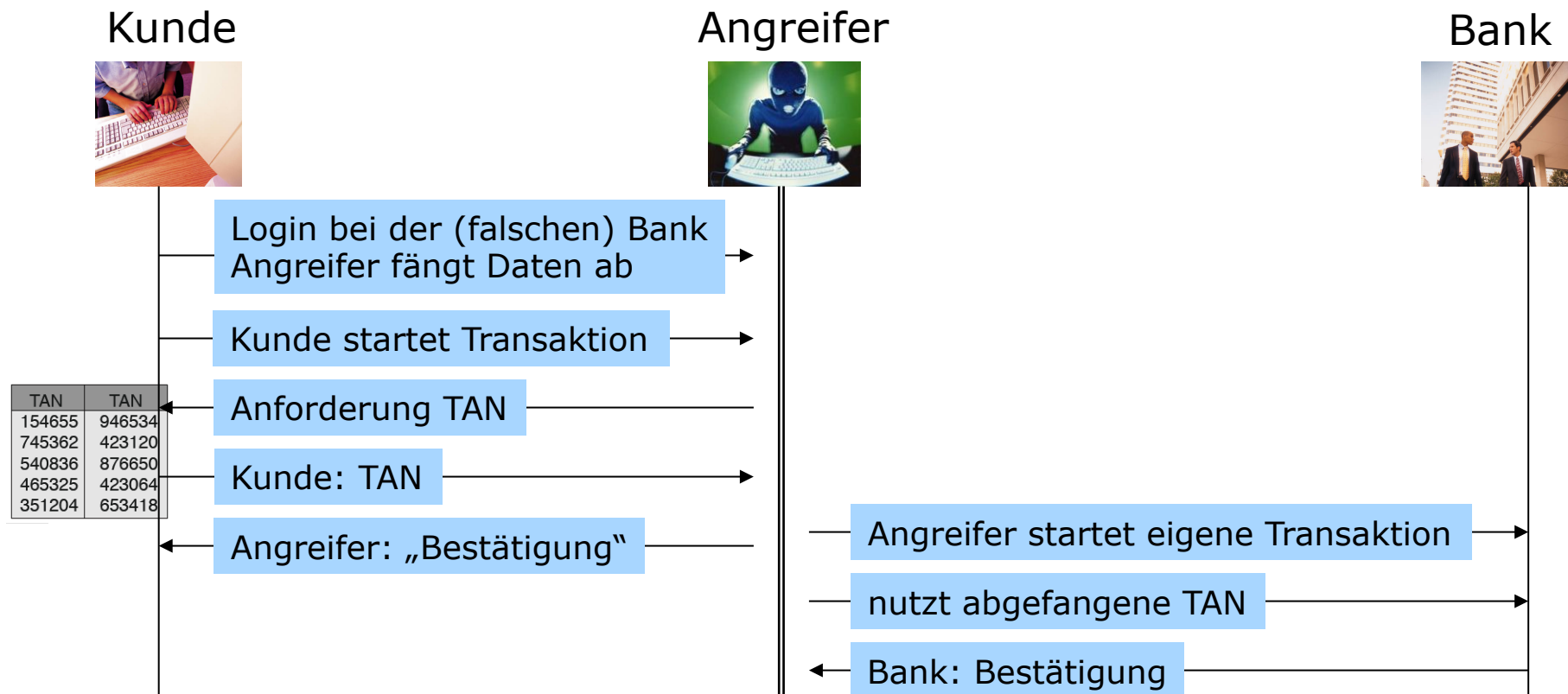
**Beachten Sie bitte unbedingt unsere Sicherheitshinweise.**

# Fälschung



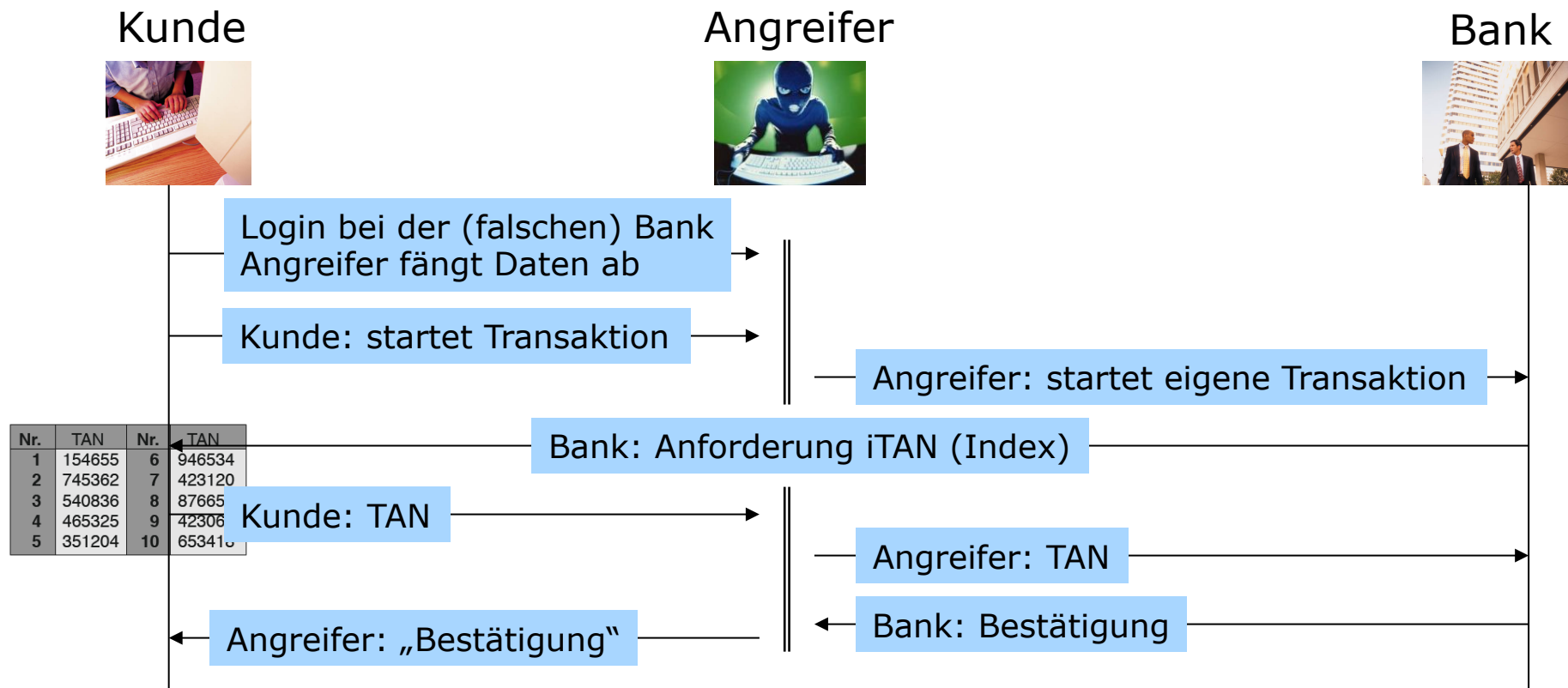
## Man-in-the-middle-attack auf TAN-Verfahren (Skizze)

- **Voraussetzung:** Angreifer
  - betreibt täuschend echte Webseite der Bank
  - bewegt den Kunden zum Besuch dieser Seite



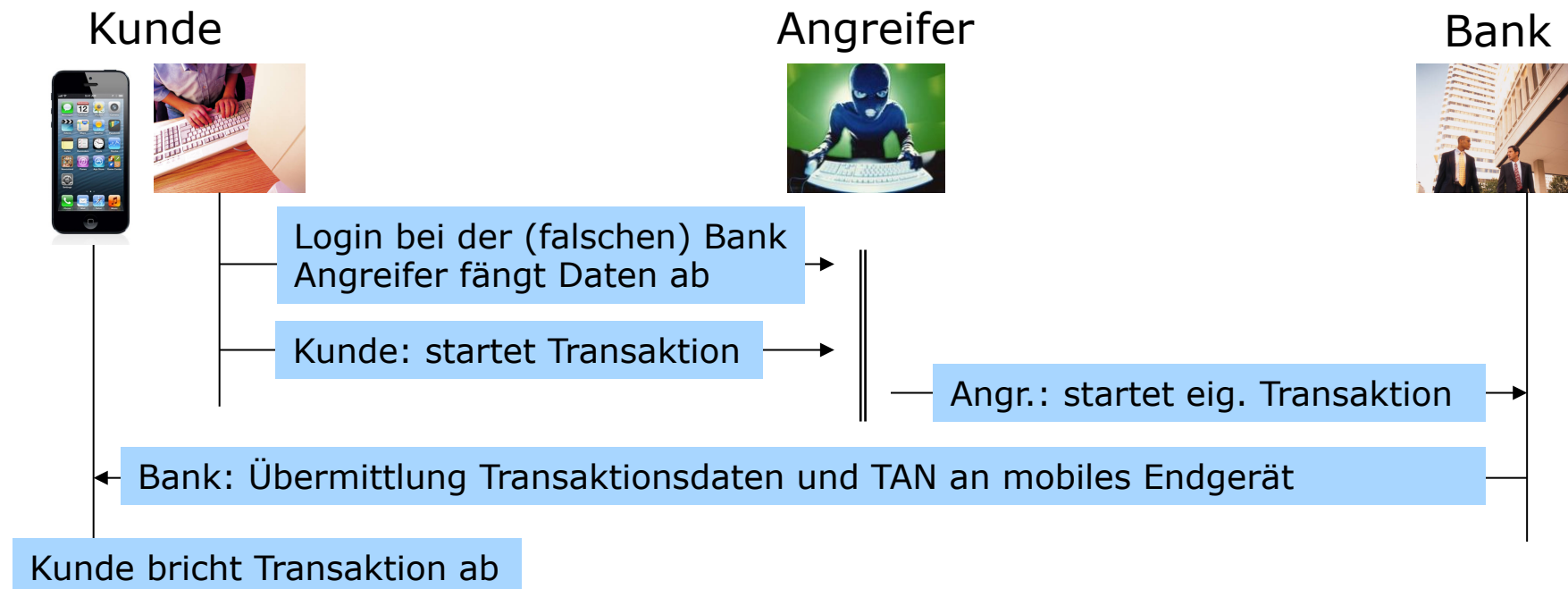
## Man-in-the-middle-attack auf iTAN-Verfahren (Skizze)

- Verbesserungen gegenüber normalem TAN-Verfahren:
  - Angreifer benötigt «Online-Hilfe durch Kunden», d.h. er kann nur Transaktionen erfolgreich durchführen, wenn Kunde dies selbst gerade tun will



## mTAN-Verfahren (Skizze)

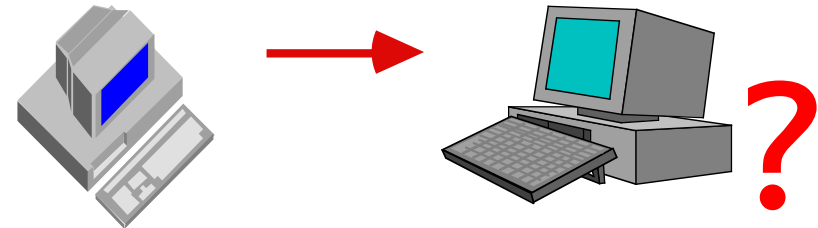
- Voraussetzung für Sicherheit:
  - mobiles Gerät wird nicht gleichzeitig für die Transaktion verwendet (Medienbruch beim Kunden)



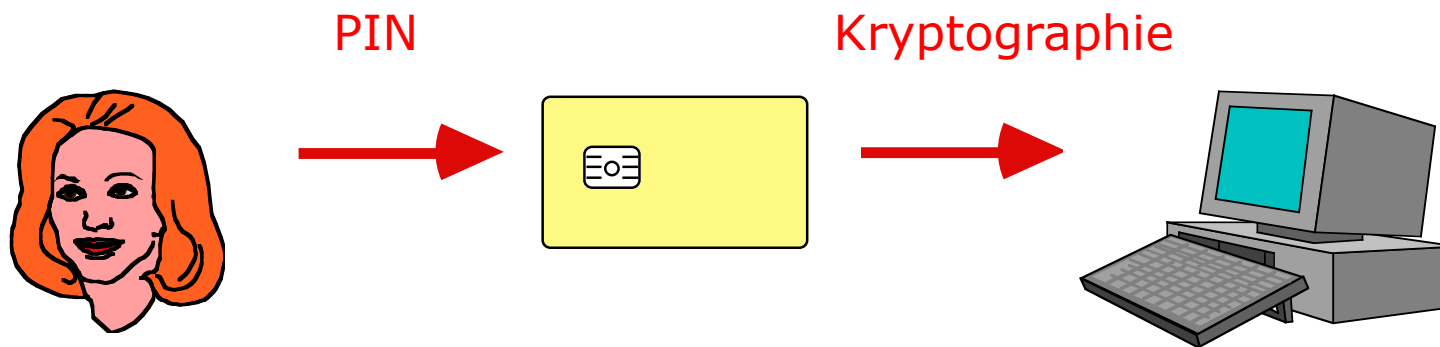


## Identifikation von IT-Systemen durch IT-Systeme

- Was es weiß:
  - Passwort
  - Antworten auf Fragen
  - Rechenergebnisse für Zahlen
  - **Kryptographie**
- Leitung woher.

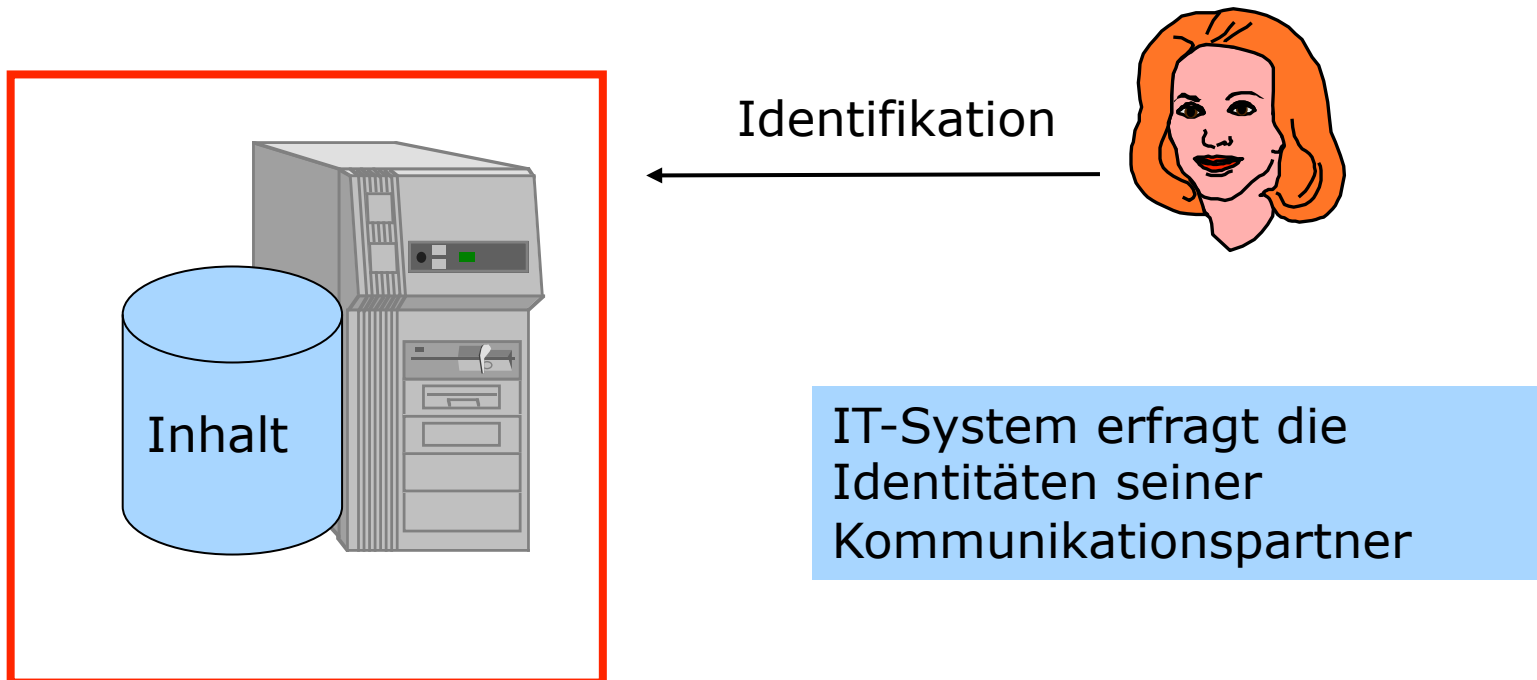


### Zusammenspiel:



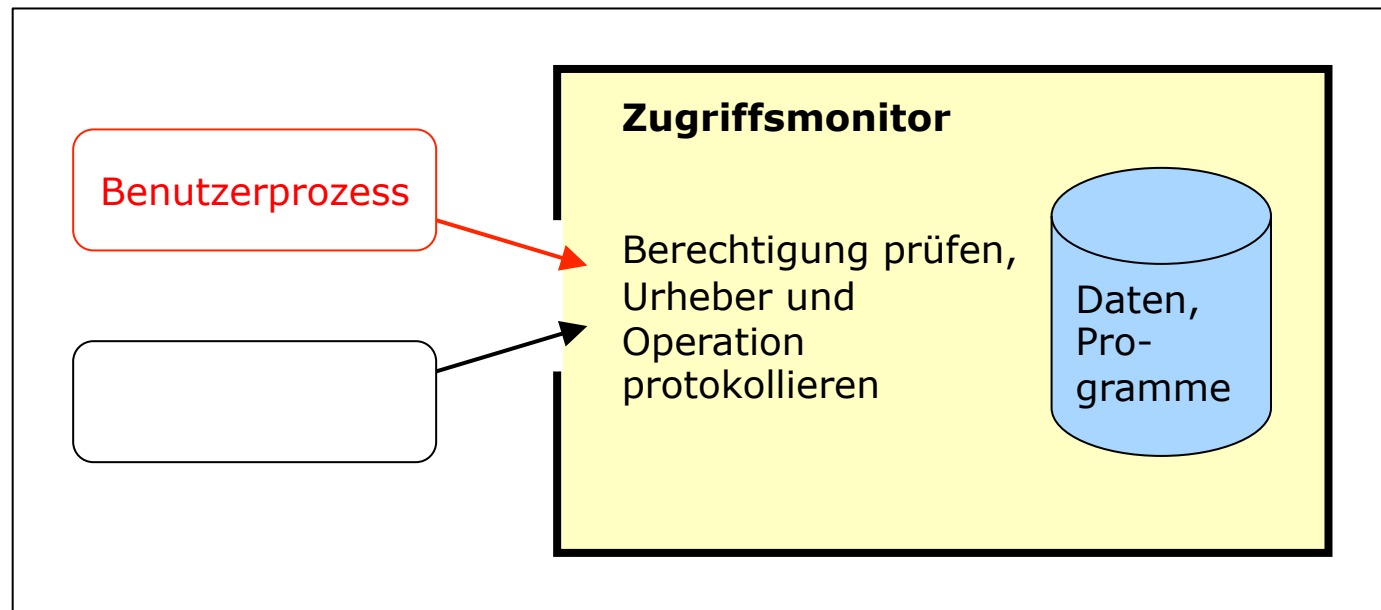
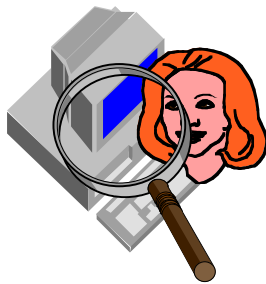
## Zugangskontrolle (admission control)

- Zweck
  - Nur mit berechtigten Partnern weiter kommunizieren
  - Verhindert unbefugte Inanspruchnahme von Betriebsmitteln



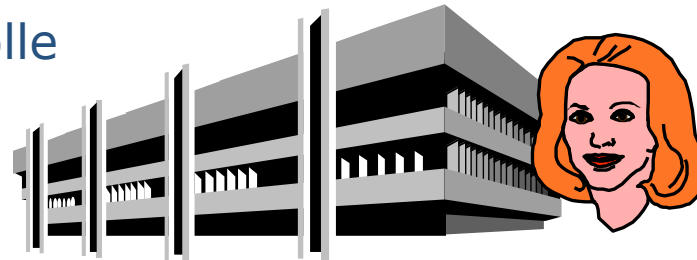
## Zugriffskontrolle (access control)

- **Subjekt** kann Operation auf **Objekt** nur ausführen, wenn es das **Recht** dazu hat.
  - setzt Zugangskontrolle voraus
  - realisiert durch Zugriffsmonitor

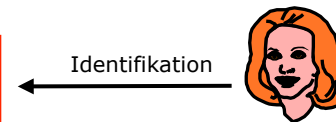
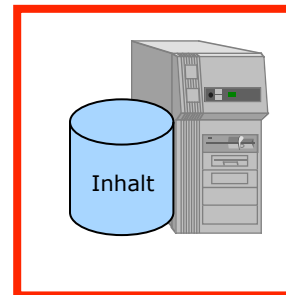


# Abgrenzung: Zutritts-, Zugangs-, Zugriffskontrolle

## Zutrittskontrolle



## Zugangskontrolle



IT-System erfragt die Identitäten seiner Kommunikationspartner

## Zugriffskontrolle

