



Cybersicherheit und Cyberdatenschutz

Prof. Dr. Hannes Federrath

Sicherheit in verteilten Systemen (SVS)

<http://svs.informatik.uni-hamburg.de>

Cybersicherheit und Cyberdatenschutz

- Wir bezahlen mit unseren Daten
 - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
 - Innere Sicherheit und Überwachung
- Die Internetwirtschaft kann es
 - aber wo bleibt die Innovation?
- Ethische Dimensionen
 - Information Governance Technologies
- Drohnenkrieg
 - Militärischer Einsatz von Informationstechnologie

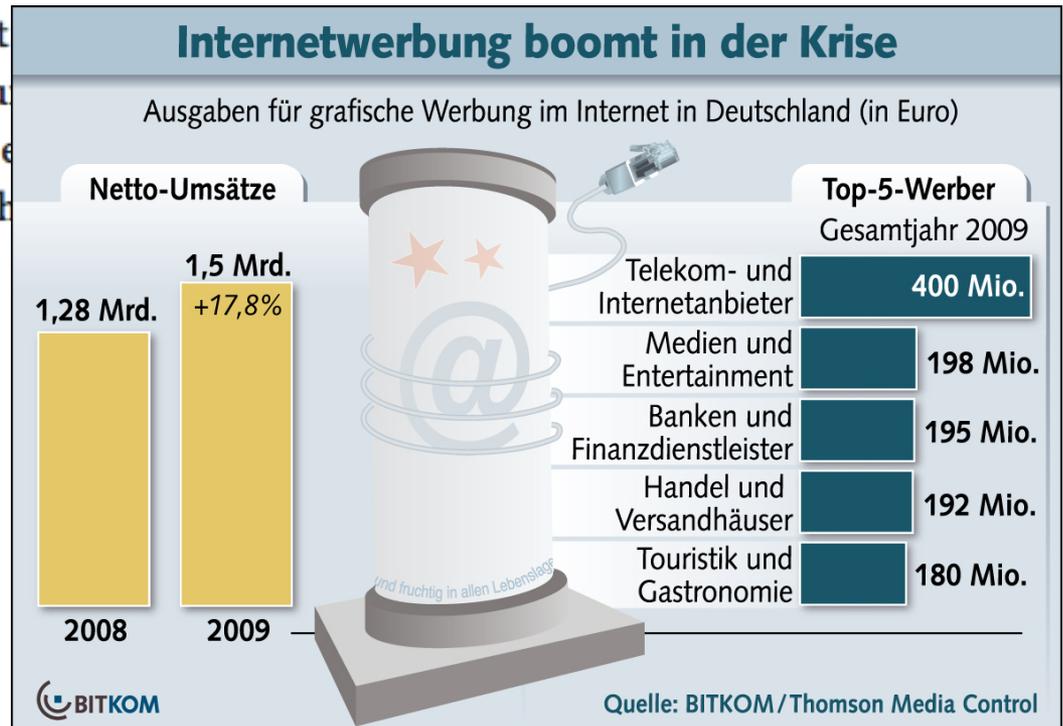
Mit Werbung wird Geld verdient! — Auch im Handel



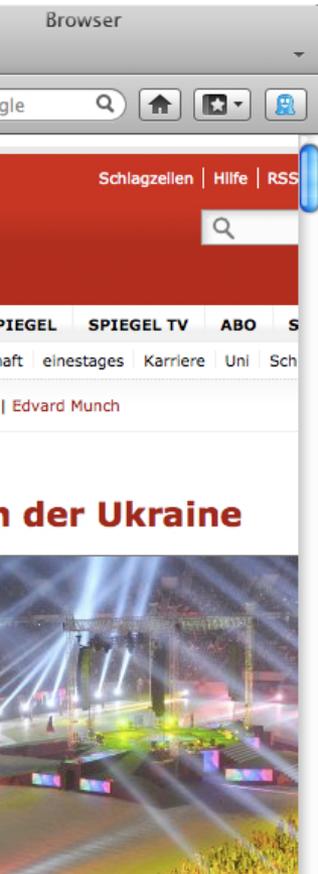
Wie Werbung wirkt

Seite 2/2 **Sieben Dollar Umsatz für einen Dollar Werbung**

Der Einzelhändler stellte ihnen sämtliche Informationen zur Verfügung, die er über seine Kunden gesammelt hat. Auf die Nutzerdaten von Yahoo und Millionen Personen konnten sie einen Account bei Yahoo als auch



Third-Party Cookies



GET <http://adnet.example.net/banner1.gif>

Cookie: guid=8867563

Referer: <http://www.bookshop.example>

GET <http://adnet.example.net/banner2.gif>

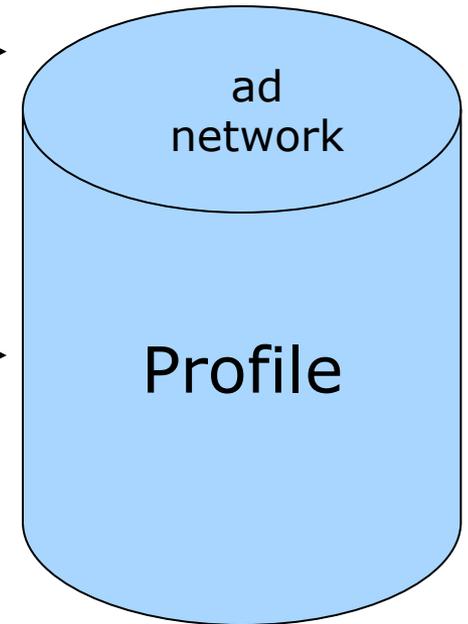
Cookie: guid=8867563

Referer: <http://www.healthinfo.example>

GET <http://adnet.example.net/banner3.gif>

Cookie: guid=8867563

Referer: <http://www.lifeinsurance.example>



Schutz: Cookies beim Schließen des Browsers löschen

Mobile logging networks



App 1: SN-Device, start, stop, ...

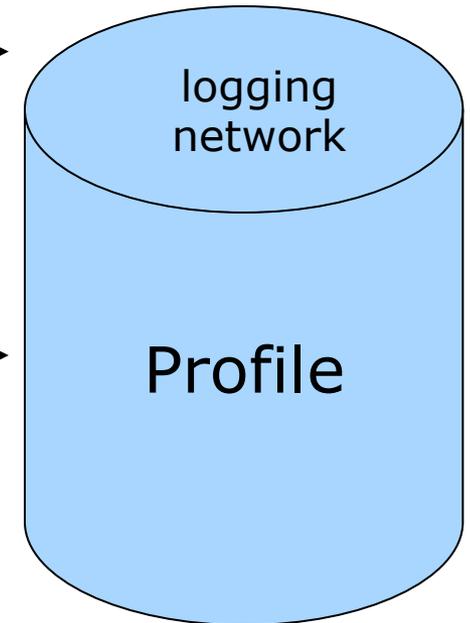
82031M6UV2F, 2012-12-19T16:39:57,
2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, ...

82031M6UV2F, 2012-12-20T12:19:11,
2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, ...

82031M6UV2F, 2012-12-20T12:21:23,
2012-12-20T12:21:55, data



Schutzmöglichkeiten?

- Verkettung anhand des «Browser Fingerprints» (ohne Cookies)
- Verwendete Verkettungsmerkmale und deren Entropie:
 - User Agent: ca. 10 Bit
 - HTTP_ACCEPT Headers: ca. 7 Bit
 - Browser Plugin Details: ca. 20 Bit
 - Time Zone: ca. 2,5 Bit
 - Screen Size and Color Depth: ca. 5 Bit
 - System Fonts: ≥ 21 Bit
 - Are Cookies Enabled? ca. 0,4 Bit
 - Limited supercookie test? ca. 1 Bit
- <https://panoptlick.eff.org>



Panopticlick

https://panopticlick.eff.org

Reader



A research project of the **Electronic Frontier Foundation**

Panopticlick

How Unique – and Trackable – Is Your Browser?

Is your browser configuration rare or unique? If so, web sites may be able to track you, *even if you limit or disable cookies.*

Panopticlick tests your browser to see how unique it is based on the **information** it will share with sites it visits. Click below and you will be given a uniqueness score, letting you see how easily identifiable you might be as you surf the web.

Only **anonymous data** will be collected by this site.

TEST ME

The screenshot shows a web browser window titled "Panopticlick" with the URL `https://panopticlick.eff.org/index.php?action=log&js=yes`. The page features a large title "Panopticlick" with a fingerprint icon in the letter 'o', and a subtitle "How Unique – and Trackable – Is Your Browser?". The main content area contains the following text:

Your browser fingerprint **appears to be unique** among the 2,650,230 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys at least **21.34 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size:

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	10.27	1231.52	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/536.26.17 (KHTML, like Gecko) Version/6.0.2 Safari/536.26.17
HTTP_ACCEPT	7.01	120.02	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Panoptick			
https://panoptick.eff.org/index.php?action=log&js=yes Reader			
User Agent	10.27	1231.52	Safari/536.26.17
HTTP_ACCEPT Headers	7.01	129.03	text/html, */* gzip, deflate de-de
Browser Plugin Details	20.34	1325115	<p>Plugin 0: Java-Applet-Plug-In; Zeigt Java-Applet-Inhalte an oder einen Platzhalter, falls Java nicht installiert ist.; JavaAppletPlugin.plugin; (Java applet; application/x-java-applet;version=1.1.3;) (Basic Java Applets; application/x-java-applet; javaapplet) (Java applet; application/x-java-applet;version=1.2.2;) (Java applet; application/x-java-applet;version=1.5;) (Java applet; application/x-java-vm;) (Java applet; application/x-java-applet;version=1.3.1;) (Java applet; application/x-java-applet;version=1.3;) (Java applet; application/x-java-applet;version=1.1.2;) (Java applet; application/x-java-applet;version=1.1;) (Java applet; application/x-java-vm-npruntime;) (Java applet; application/x-java-applet;version=1.2.1;) (Java applet; application/x-java-applet;version=1.6;) (Java applet; application/x-java-applet;version=1.4.2;) (Java applet; application/x-java-applet;plugin=1.6.0_37;) (Java applet; application/x-java-applet;version=1.4;) (Java applet; application/x-java-applet;version=1.1.1;) (Java applet; application/x-java-applet;version=1.2;). Plugin 1: QuickTime Plug-in 7.7.1; Mit dem QuickTime Plug-in können Sie eine Vielzahl von Multimedia-Inhalten auf Webseiten anzeigen. Weitere Informationen erhalten Sie auf der Web-Site fÄ¼r QuickTime; QuickTime Plugin.plugin; (Video fÄ¼r Windows (AVI); video/x-msvideo; avi,vfw) (MP3-Audio; audio/mp3; mp3,swa) (MP3-Audio; audio/mpeg3; mp3,swa) (3GPP2-Medien; video/3gpp2; 3g2,3gp2) (CAF-Audio; audio/x-caf; caf) (MPEG-Audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QuickTime Film; video/quicktime; mov,qt,mqv) (MP3-Audio; audio/x-mpeg3; mp3,swa) (MPEG-4 Medien; video/mp4; mp4) (SDP-Stream Beschreibung; application/x-sdp; sdp) (WAVE-Audio; audio/wav; wav,bwf) (Video fÄ¼r Windows (AVI); video/avi; avi,vfw) (AC3 Audio; audio/x-ac3; ac3) (MPEG-4 Medien; audio/mp4; mp4) (Video (geschÄ¼tzt); video/x-m4v; m4v) (SDP-Stream Beschreibung; application/sdp; sdp) (WAVE-Audio; audio/x-wav; wav,bwf) (AIFF-Audio; audio/x-aiff; aiff,aif,aifc,odda) (MPEG-Medien; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP-Medien; video/3gpp; 3gp,3gpp) (Video fÄ¼r Windows (AVI); video/msvideo; avi,vfw) (MPEG-Audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QUALCOMM PureVoice Audio; audio/vnd.qcelp; qcp,qcp) (MP3-Audio; audio/x-mp3; mp3,swa) (RTSP-Stream Beschreibung; application/x-rtsp; rtsp,rtts) (AMR-Audio; audio/amr; amr) (SD-Video; video/sd-video; sdv) (AIFF-Audio; audio/aiff; aiff,aif,aifc,odda) (MPEG-Medien; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP2-Medien; audio/3gpp2; 3g2,3gp2) (AAC-Audio; audio/aac; aac,adts) (AC3 Audio; audio/ac3; ac3) (AAC-HÄ¼r buch; audio/x-m4b; m4b) (AAC-Localdatei (geschÄ¼tzt); audio/x-m4p; m4p) (GSM-Audio; audio/x-gsm; gsm) (AMC-Medien; application/x-mpeg; amc) (AAC-Audio; audio/x-aac; aac,adts) (uLaw/AU-Audio; audio/basic; au,snd,u1w) (AAC-Audio; audio/x-m4a; m4a) (3GPP-Medien; audio/3gpp; 3gp,3gpp). Plugin 2: Shockwave Flash; Shockwave Flash 11.5 r502; Flash Player.plugin; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 3: WebKit-integrierte PDF; ; (PDF (Portable Document Format); application/pdf; pdf). Plugin 4: iPhotoPhotocast; iPhoto6; iPhotoPhotocast.plugin; (iPhoto 700; application/photo;).</p>

Beispiel für Anwendung von Browser Fingerprint

- Laterpay: Bezahlanbieter für Micropayments
- Zitat aus den AGBs für Nutzer von Laterpay:

«Was macht LaterPay um, Ihr Internet-fähiges Endgerät zu identifizieren?

LaterPay verwendet unterschiedliche Verfahren um sicherzustellen, dass der Bezahlanbieter dem richtigen Endgerät ermöglicht, von dem Vertrauensvorschuss zu profitieren und Inhalte zu konsumieren, bevor eine Registrierung erfolgt.

Hierfür werden wahlweise Browser Fingerprint und die IP-Adresse, Daten des Bezahlansichters, Protokolleigenschaften sowie Cookies verwendet.»

<https://www.laterpay.net/terms/>

Device Fingerprinting

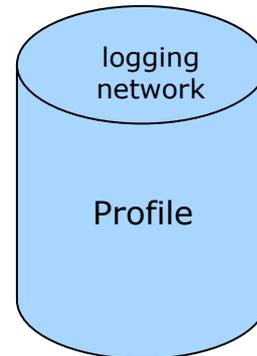
- Unique? App
 - Auskunft über mögliche Identifier
- Entwickelt an der Uni Erlangen
 - zeigt Möglichkeiten des Device Fingerprinting



App 1: SN-Device, start, stop, ...
82031M6UV2F, 2012-12-19T16:39:57,
2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, ...
82031M6UV2F, 2012-12-20T12:19:11,
2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, ...
82031M6UV2F, 2012-12-20T12:21:23,
2012-12-20T12:21:55, data



<http://www.iphone-ticker.de/oh-mein-gott-so-eindeutig-laesst-jedes-iphone-zuordnen-66244/>

Die folgende Übersicht zeigt die gesammelten Daten und hebt diejenigen Einträge farblich hervor, die zur Eindeutigkeit ihres Fingerabdrucks beigetragen haben.

FREI ZUGÄNLICH

Jailbreak installiert Nein

Gerätemodell iPhone6,2

Systemversion 7.1.1

Gerätename iPhone von Nicolas O...

identifierForVendor 9D84A766-CD...

Mobilfunkanbieter Telekom.de

Anbieter erlaubt VOIP Ja

Eingestelltes Land DE

Eingestellte Sprache de

Land ≠ Sprache Nein

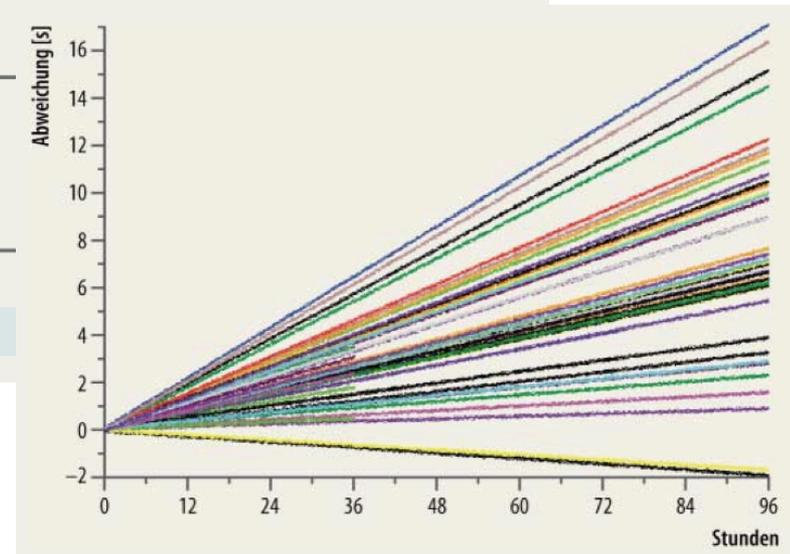
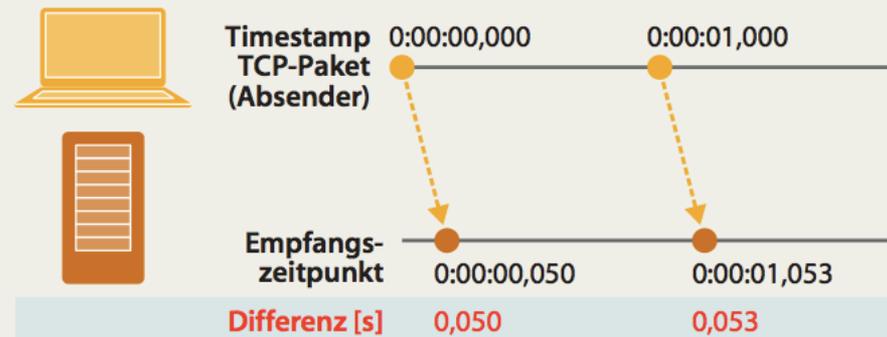
Installierte Tastaturen mehr... >

Messung von Timings zur Identifikation von (mobilen) Geräten

- Langzeitbeobachtung von deterministischen, gerätespezifischen Ungenauigkeiten der internen Uhr eines Geräts

TCP-Timestamp-Differenzen

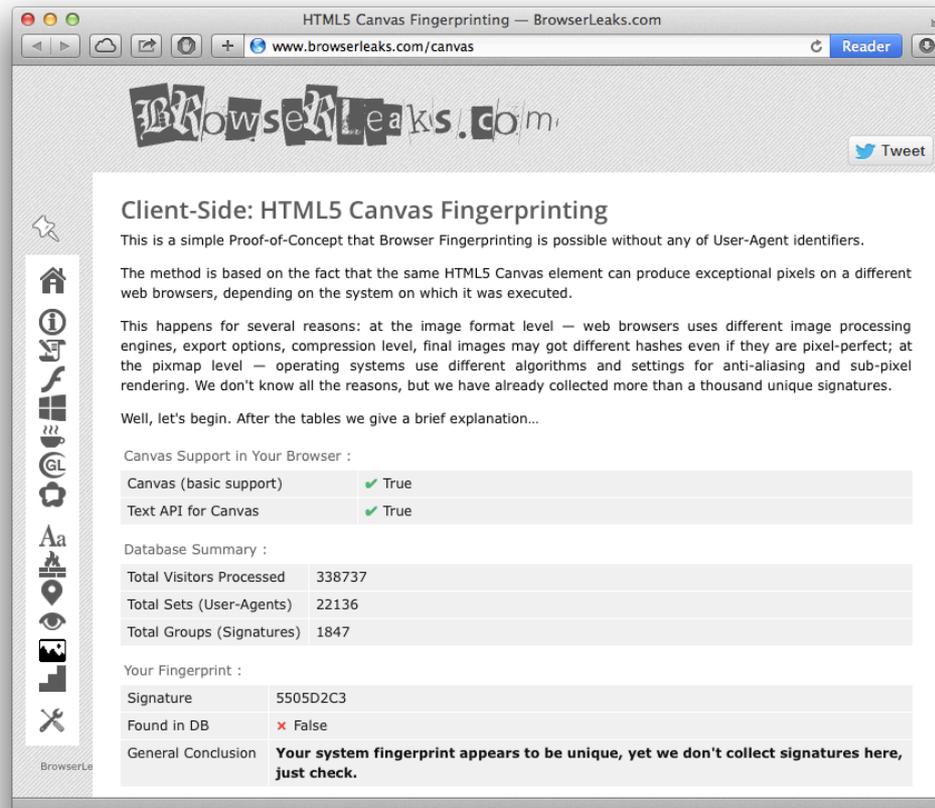
Über längere Zeit summiert sich die Differenz zwischen TCP-Timestamp und Empfangszeitpunkt auf unterscheidbare Werte.



- Schutz:
 - Modifikation des TCP-Standards
 - Hinzufügen eines künstlichen Time-Jitter

Canvas Fingerprinting

- winzige Darstellungsunterschiede innerhalb des Browsers ermöglichen individuelle Verkettung



The screenshot shows a web browser window with the address bar displaying "www.browserleaks.com/canvas". The page title is "HTML5 Canvas Fingerprinting — BrowserLeaks.com". The main content area features the "BrowserLeaks.com" logo and a "Tweet" button. The article title is "Client-Side: HTML5 Canvas Fingerprinting". The text explains that this is a simple Proof-of-Concept showing that browser fingerprinting is possible without user-agent identifiers. It details that the method is based on the fact that the same HTML5 Canvas element can produce exceptional pixels on different web browsers, depending on the system on which it was executed. The reasons for this are listed: at the image format level (web browsers use different image processing engines, export options, compression level, final images may get different hashes even if they are pixel-perfect; at the pixmap level — operating systems use different algorithms and settings for anti-aliasing and sub-pixel rendering. We don't know all the reasons, but we have already collected more than a thousand unique signatures. The text then says "Well, let's begin. After the tables we give a brief explanation...".

Canvas Support in Your Browser :

Canvas (basic support)	✓ True
Text API for Canvas	✓ True

Database Summary :

Total Visitors Processed	338737
Total Sets (User-Agents)	22136
Total Groups (Signatures)	1847

Your Fingerprint :

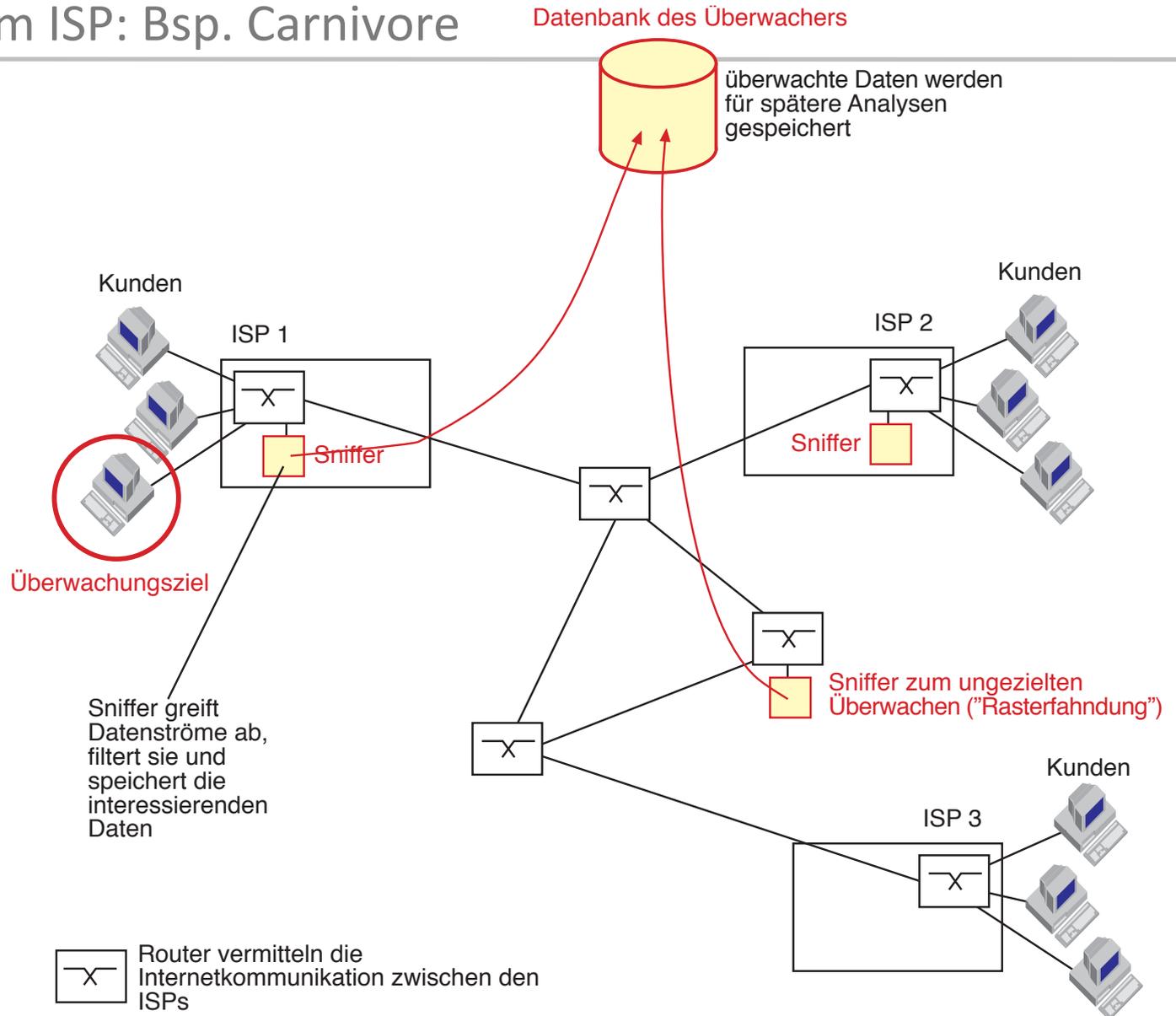
Signature	5505D2C3
Found in DB	✗ False
General Conclusion	Your system fingerprint appears to be unique, yet we don't collect signatures here, just check.

Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, Claudia Diaz. The Web never forgets: Persistent tracking mechanisms in the wild. CCS 2014

Cybersicherheit und Cyberdatenschutz

- Wir bezahlen mit unseren Daten
 - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
 - Innere Sicherheit und Überwachung
- Die Internetwirtschaft kann es
 - aber wo bleibt die Innovation?
- Ethische Dimensionen
 - Information Governance Technologies
- Drohnenkrieg
 - Militärischer Einsatz von Informationstechnologie

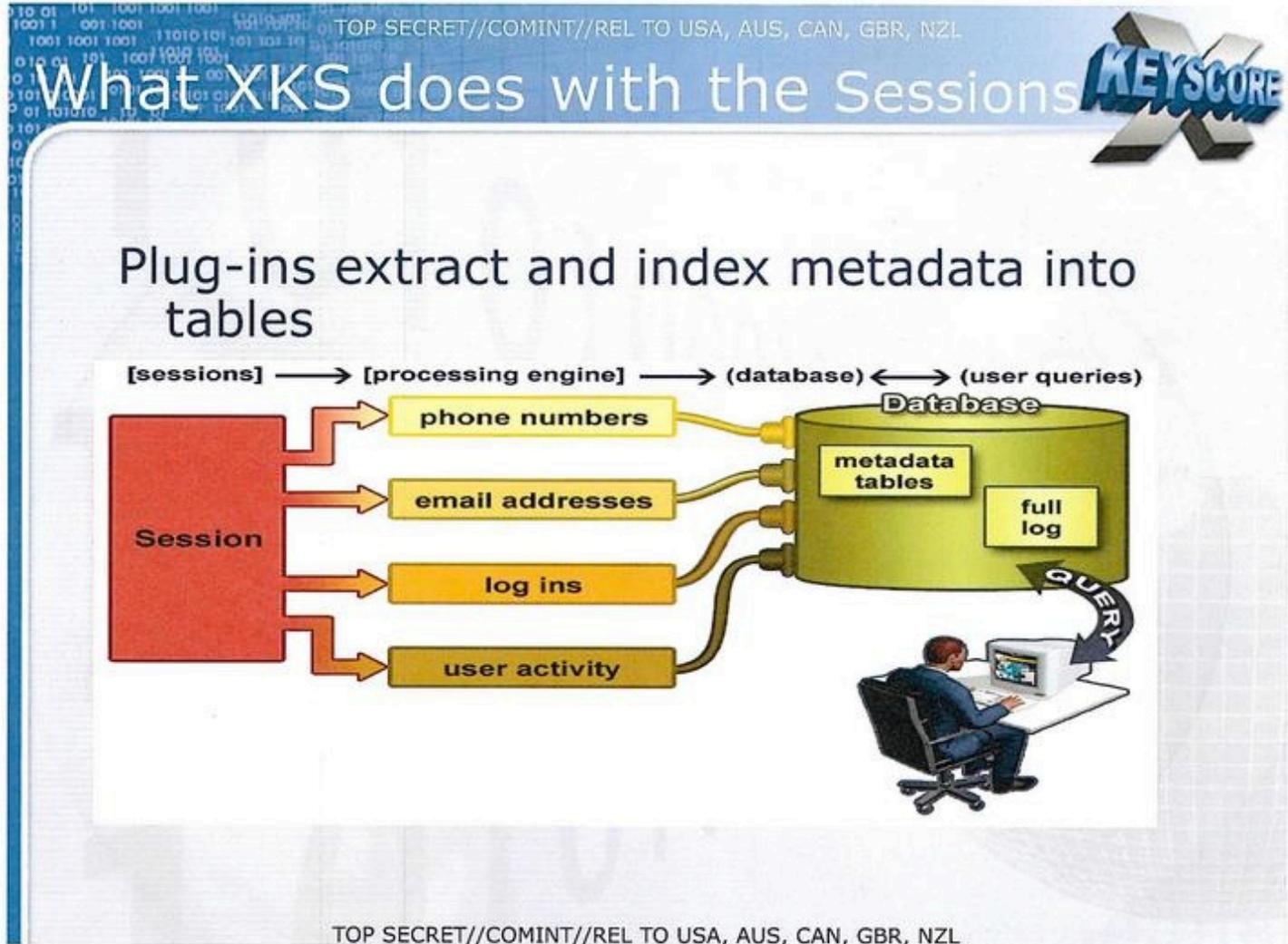
Sniffing beim ISP: Bsp. Carnivore



Sniffing beim ISP: Bsp. ~~Carnivore~~

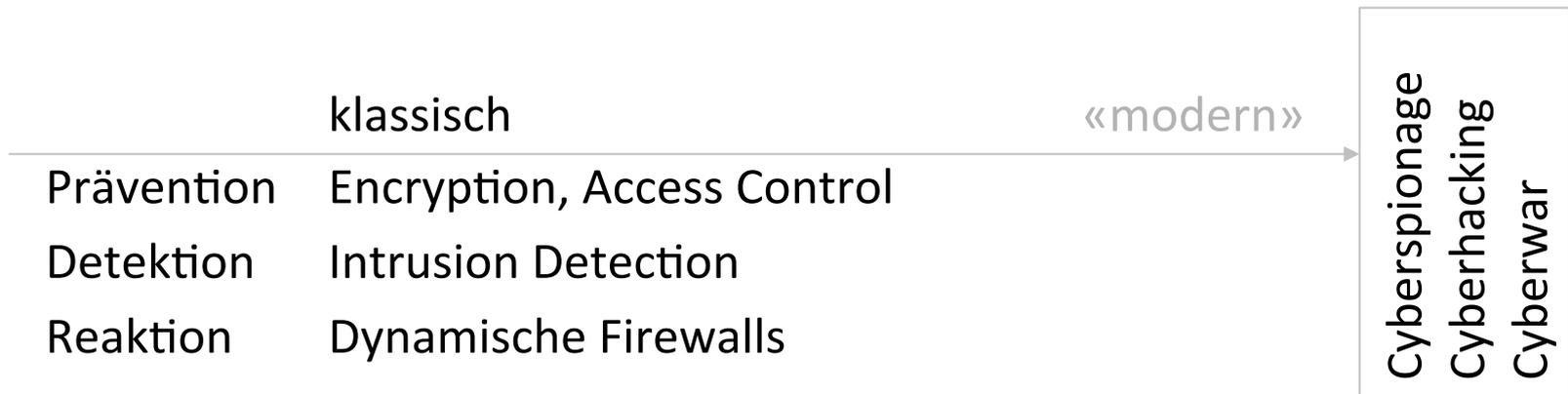
Datenbank des Überwachers

Quelle: Wikimedia



Bundestrojaner, Stuxnet

- Darf sich der Staat auch solcher Angriffsmethoden bedienen,
 - die zwar dem Schutz des Staates und seiner Bürger dienen, jedoch die Integrität und Vertrauenswürdigkeit von IT-Systemen untergraben und schlimmstenfalls auch gegen ihn selbst verwendet werden können?
- IT-Sicherheitsstrategien



Bundestrojaner, Stuxnet

- Darf sich der Staat auch solcher Angriffsmethoden bedienen,
 - die zwar dem Schutz des Staates und seiner Bürger dienen, jedoch die Integrität und Vertrauenswürdigkeit von IT-Systemen untergraben und schlimmstenfalls auch gegen ihn selbst verwendet werden können?

- Antwort: «Neues Computergrundrecht»
 - Bundesverfassungsgericht im Februar 2008:
 - Grundrecht auf «Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme»
 - Erlaubte Einschränkungen:
 - Gefährdung von Leib, Leben und Freiheit einer Person
 - Gefährdung der Grundlagen des Staates
 - Gefährdung der Grundlagen der Existenz der Menschen

Darf sich der Staat auch solcher Angriffsmethoden bedienen?

■ Implementierungen

- politisch motivierte staatliche Angriffe mit oder auf IT-Systeme anderer Staaten (Cyberwarfare)

- Stuxnet

- Gesetzlich erlaubte Telekommunikationsüberwachung und Beweissicherung (Online Durchsuchung) direkt auf dem PC eines Verdächtigen

- Staatstrojaner / Bundestrojaner

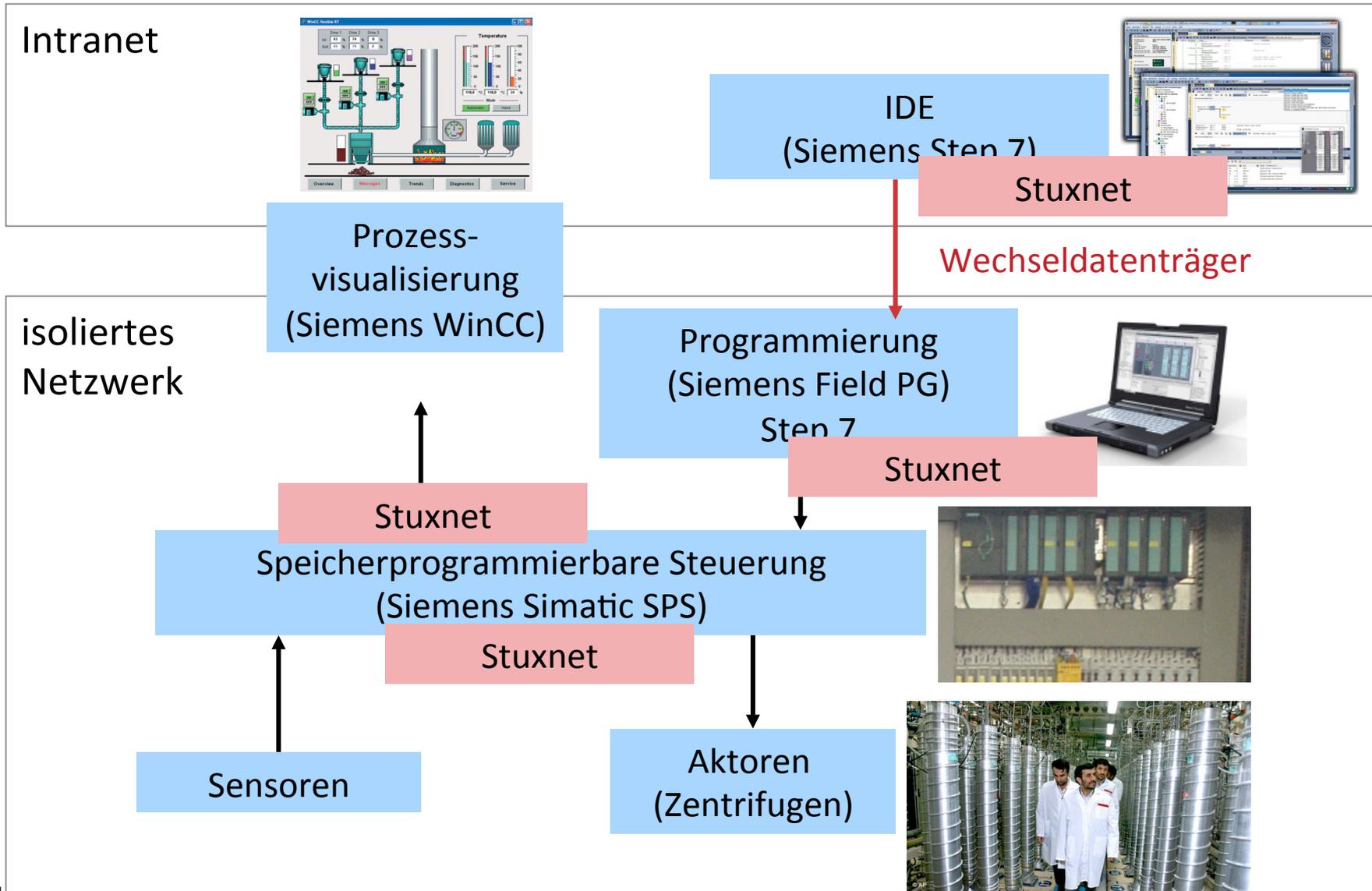
Stuxnet

- Internetwurm, der mit dem Ziel entwickelt wurde, die innerbetrieblichen Abläufe eines speziellen Typs von Industrieanlagen empfindlich zu stören.
 - Entdeckung im Juli 2010
 - Ziel: Unbemerkte Änderung von Programmteilen in speicherprogrammierbaren Steuerungen (SPS)
 - Verwendet vier Zeroday-Exploits zur Verbreitung und Rechteausweitung
 - Insiderwissen für Entwicklung erforderlich
 - Selbstzerstörung (nur Windows-Komponente) nach 35 Tagen



Bild von Natanz (Majid Saeedi/Getty Images)

Stuxnet - Szenario (Industrieanlage)



Stuxnet

■ Urheber: USA und Israel

- Anordnung von 2006 von US-Präsident Gerorge W. Bush
- in 2010 bestätigt durch Präsident Obama

Quelle: New York Times: Obama Order Sped Up Wave Of Cyberattacks Against Iran. June 1, 2012, page A1

■ Besonderheiten

- Kombination mehrerer unbekannter Zero-Day-Exploits
- befällt nur bestimmte Systeme (laut Symantec ca. 70% im Iran)
- Infektionsweg über mehrere Systemgrenzen hinweg
- P2P-Kommunikation infizierter Systeme
- Update-Mechanismus
- Verwendung gestohlener Zertifikate

Staatstrojaner

- Haupteinsatzgebiet ist die sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)
 - Oktober 2011 entdeckt
 - Mehrfach unabhängig durch Reverse Engineering analysiert und publiziert
 - Chaos Computer Club
 - Universität Mannheim

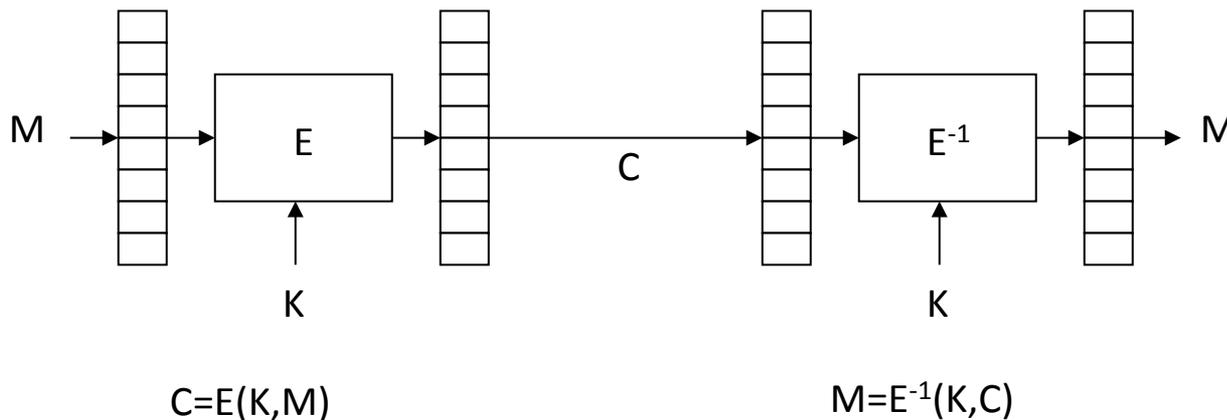
- Auftragsarbeit:
 - Auftraggeber: deutsche Sicherheitsbehörden
 - entwickelt von Digitask GmbH
 - geht vermutlich zurück auf eine Skype-Capture-Unit vom September 2007

Staatstrojaner

■ Funktionen

- Ausleiten des Skype-Datenverkehrs
- Screenshots, Mikrofon einschalten, Keylogger
- Nachladefunktion

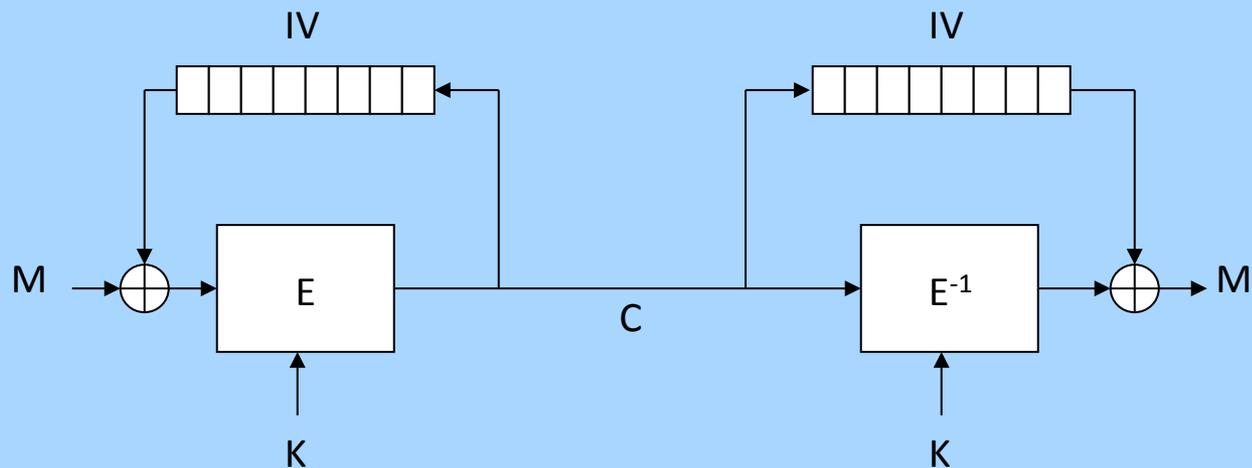
- Schwach verschlüsselte Kommunikation mit einem Command-and-Control-Server im Ausland (USA)
 - AES im ECB-Mode mit fest kodiertem Schlüssel



Staatstrojaner

- Schwach verschlüsselte Kommunikation mit einem Command-and-Control-Server im Ausland (USA)
 - AES im ECB-Mode mit fest kodiertem Schlüssel

- Richtig wäre: Cipher Block Chaining (CBC) verwenden.



$$C_0 = IV$$
$$C_i = E(K, M_i \oplus C_{i-1})$$

$$C_0 = IV$$
$$M_i = E^{-1}(K, C_i) \oplus C_{i-1}$$

Spannungsfeld von Freiheit und Sicherheit

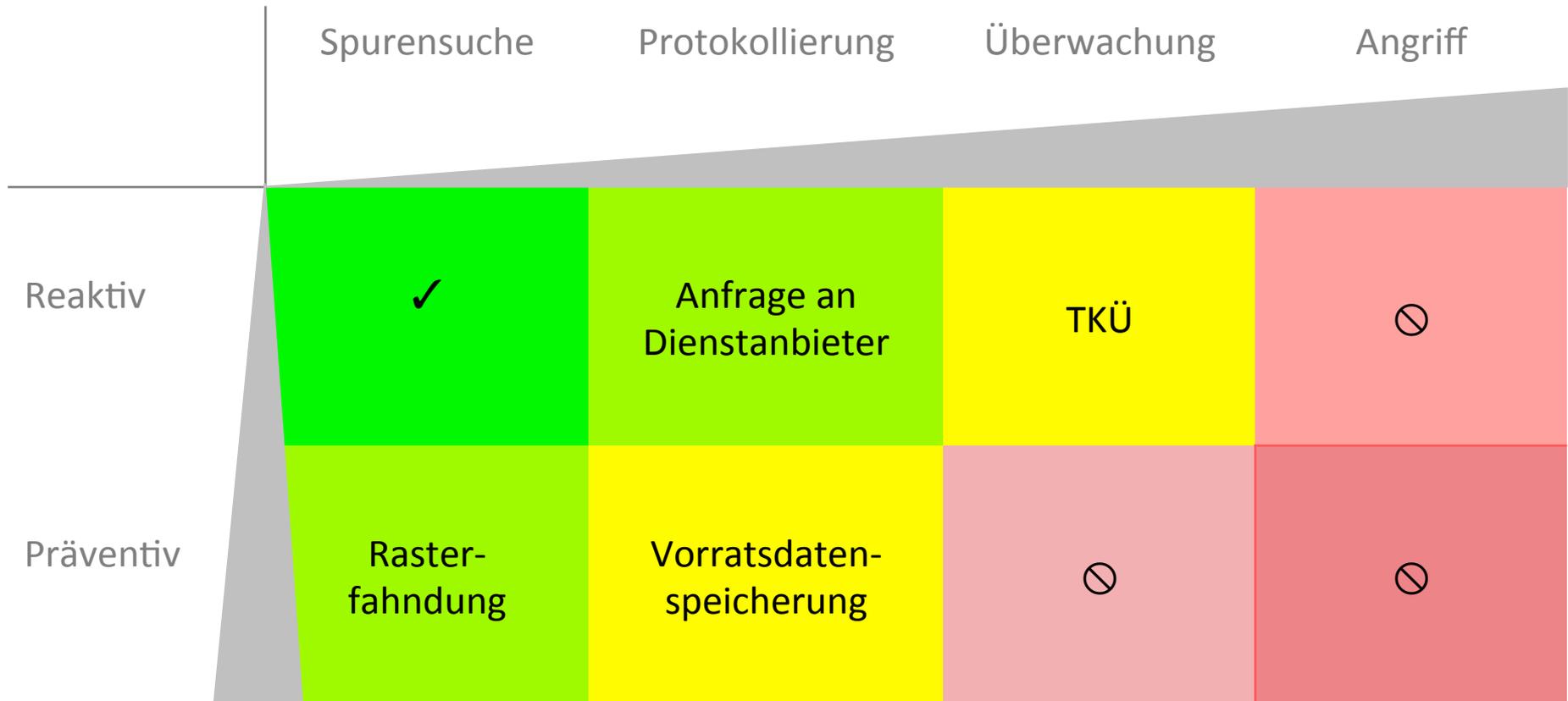
- Ziel der Informationssicherheit: möglichst wenig Vertrauen in andere setzen müssen
 - Wo keine Sicherheit erreichbar ist, bleibt nur Vertrauen [müssen]
- Freiheit: insbesondere Grundrechte
 - Recht auf informationelle Selbstbestimmung
 - Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme (Computer-Grundrecht)
- Sicherheit
 - Vorratsdatenspeicherung
 - Bundestrojaner

«Nur in schweren Fällen ...»

... aber die Bürger erleiden
Vertrauensverlust gegenüber
dem Staat

Eingriffstiefe in die Freiheit

- Darf sich der Staat solcher Angriffsmethoden bedienen?

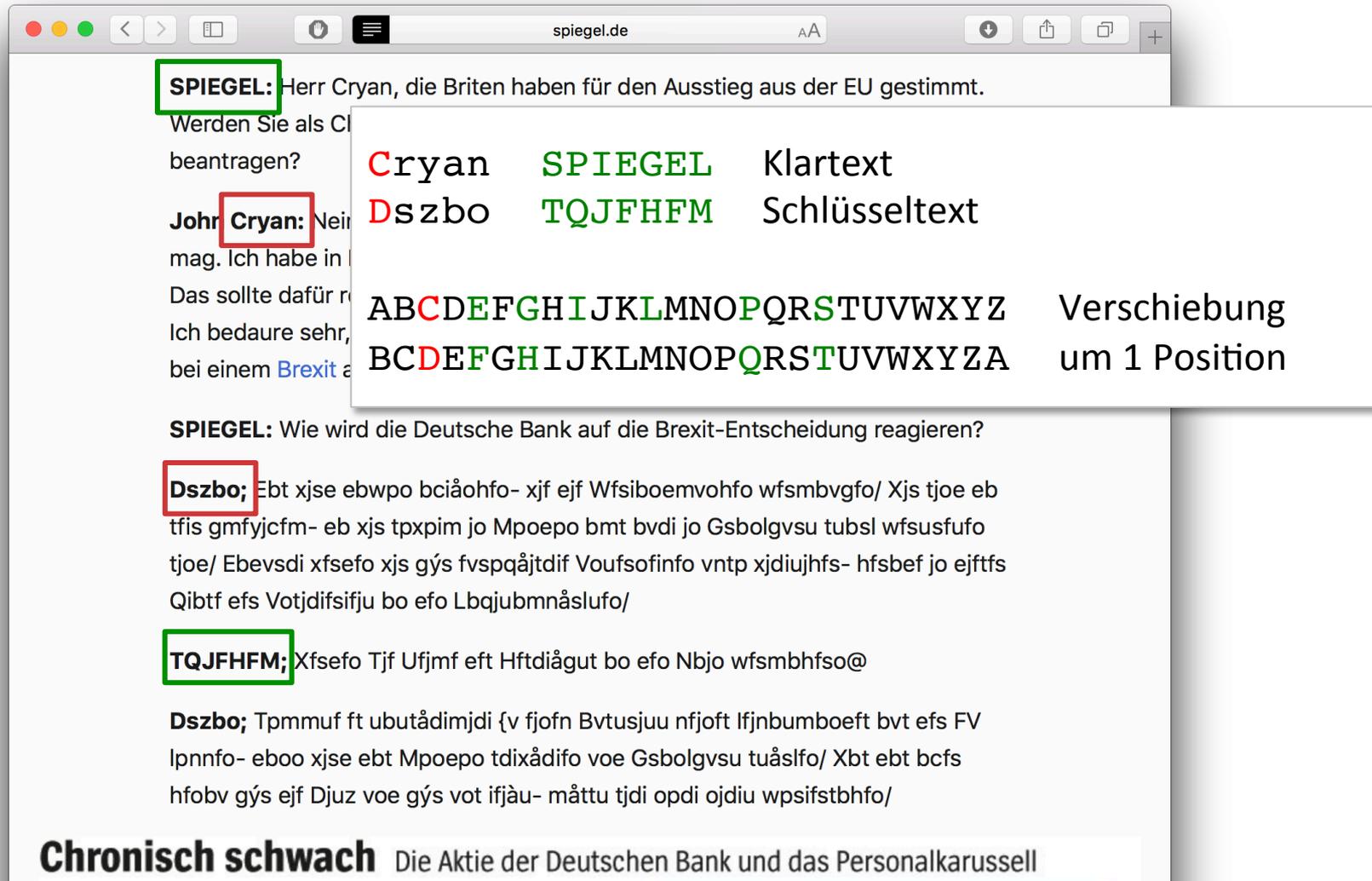


Cybersicherheit und Cyberdatenschutz

- Wir bezahlen mit unseren Daten
 - Spannungsfeld von Online-Marketing und Datenschutz
- Ich habe doch nichts zu verbergen
 - Innere Sicherheit und Überwachung
- Die Internetwirtschaft kann es
 - aber wo bleibt die Innovation?
- Ethische Dimensionen
 - Information Governance Technologies
- Drohnenkrieg
 - Militärischer Einsatz von Informationstechnologie

Beispiel für Verschiebechiffre – Spiegel Plus

Quelle: <http://andreas-zeller.blogspot.de/2016/06/spiegel-online-nutzt-unsichere-casar.html>



The screenshot shows a browser window with the URL `spiegel.de`. The page content includes several paragraphs of text. A white box with a black border is overlaid on the page, containing a key for a Caesar cipher. The key shows the original alphabet (A-Z) and the shifted alphabet (B-Z, A), indicating a shift of 1 position. The text in the browser is partially obscured by this box. The text visible in the browser includes: "SPIEGEL: Herr Cryan, die Briten haben für den Ausstieg aus der EU gestimmt. Werden Sie als Cl beantragen? Jahr Cryan: Nein mag. Ich habe in Das sollte dafür r Ich bedaure sehr, bei einem Brexit a SPIEGEL: Wie wird die Deutsche Bank auf die Brexit-Entscheidung reagieren? Dszbo; Ebt xjse ebwpo bciãohfo- xjf ejf Wfsiboemvohfo wfsmbvgfo/ Xjs tjoe eb tfis gmfyjcfm- eb xjs tpxpim jo Mpoepo bmt bvdi jo Gsbolgvsu tubsl wfsusufuo tjoe/ Ebevsvdi xfsefo xjs gýs fvspqãjtdif Voufsofinfo vn timer xjdjuhfs- hfsbef jo ejftfs Qibtfer Votjdifsifju bo efo Lbqjubmnãslufo/ TQJFHFM; Xfsefo Tjf Ufjmf eft Hftdiãgut bo efo Nbjowfsmbhfso@ Dszbo; Tpmmf ft ubutãdimjdi {v fjofn Bvtusjuu nfjoft Ifjnbumboeft bvt efs FV lppnfo- eboo xjse ebt Mpoepo tdixãdifo voe Gsbolgvsu tuãslfo/ Xbt ebt bcfs hfobv gýs ejf Djuz voe gýs vot ifjàu- mãttu tjdi opdi ojdiu wpsifstbhfo/ Chronisch schwach Die Aktie der Deutschen Bank und das Personalkarussell

Beispiel für Verschiebechiffre

Cäsar Verschiebechiffre bzw. Cäsar Verschlüsselung

Original

Cryan; Das wird davon abhängen- wie die Verhandlungen verlaufen/ Wir sind da sehr flexibel- da wir sowohl in London als auch in Frankfurt stark vertreten sind/ Dadurch werden wir für europäische Unternehmen umso wichtiger- gerade in dieser Phase der Unsicherheit an den Kapitalmärkten/

SPIEGEL; Werden Sie Teile des Geschäfts an den Main verlagern@

Cryan; Sollte es tatsächlich {u einem Austritt meines Heimatlandes aus der EU kommen- dann wird das London

Verschiebung

1

Kodiert

Dszbo; Ebt xjse ebwpo bciâohfo- xjf ejf Wfsiboemvohfo wfsmbvgfo/ Xjs tjoe eb tfis gmfyjcfm- eb xjs tpxpim jo Mpoepo bmt bvdi jo Gsbolgvsu tubsl wfsusfufo tjoe/ Ebevsvdi xfsefo xjs gÿs fvspqâjtdif Voufsofinfo vntp xjdiujhfs- hfsbef jo ejftfs Qibtfe efs Votjdifsifju bo efo Lbqjubmnâslufo/

TQJFFHM; Xfsefo Tjf Ufjmf eft Hftdiâgut bo efo Nbjo wfsmbhfso@

Dszbo; Tpmnuf ft ubutâdimjdi {v fjofn Bvtusjuu nfjoft Ifjnbumboeft bvt efs FV lpnnfo- eboo xjse ebt Mpoepo

Methode:

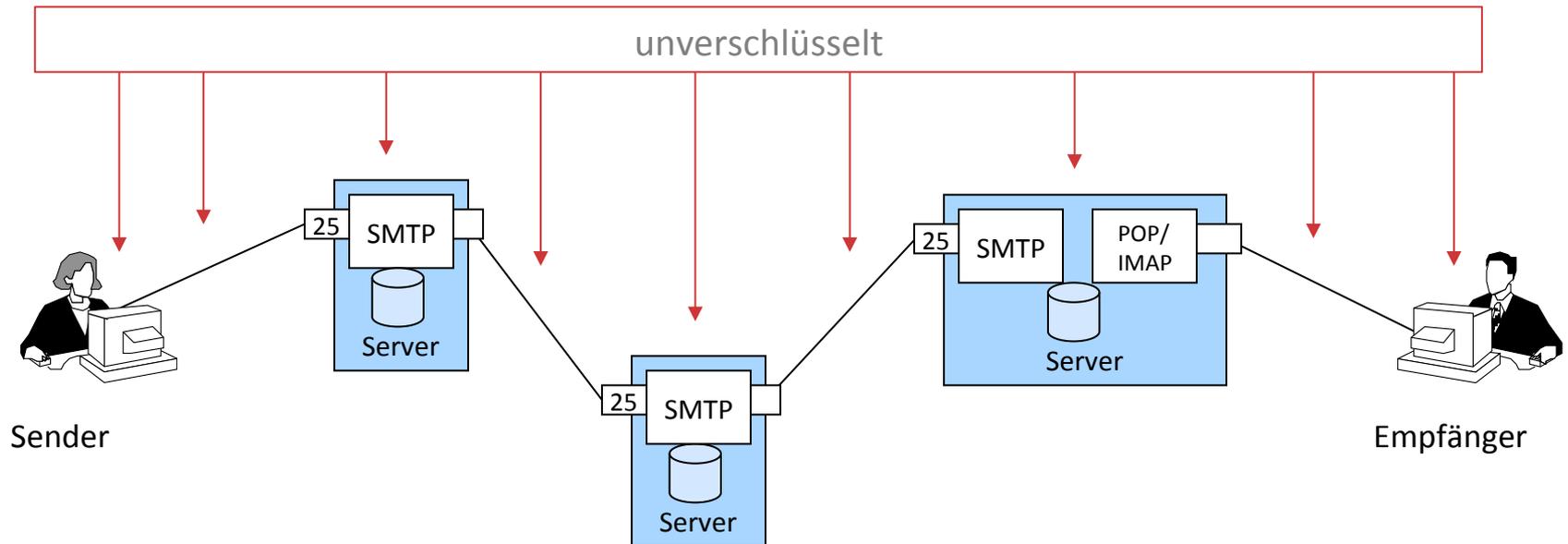
Cäsar Verschiebechiffre

Hilfe: A-Z,a-z werden um die gewünschte Anzahl von Positionen im Alphabet zyklisch nach rechts oder links verschoben, alle anderen Zeichen bleiben unverändert. ROT13 ist eine Sonderform der Cäsar Verschiebechiffre mit einer Verschiebung um 13 Positionen. Die Umwandlung funktioniert in beide Richtungen. Bei einem Verschiebewert von '0' werden alle Verschiebemöglichkeiten von 1-25 ausgegeben.

Encode ▼ Decode ▲ ▼▲

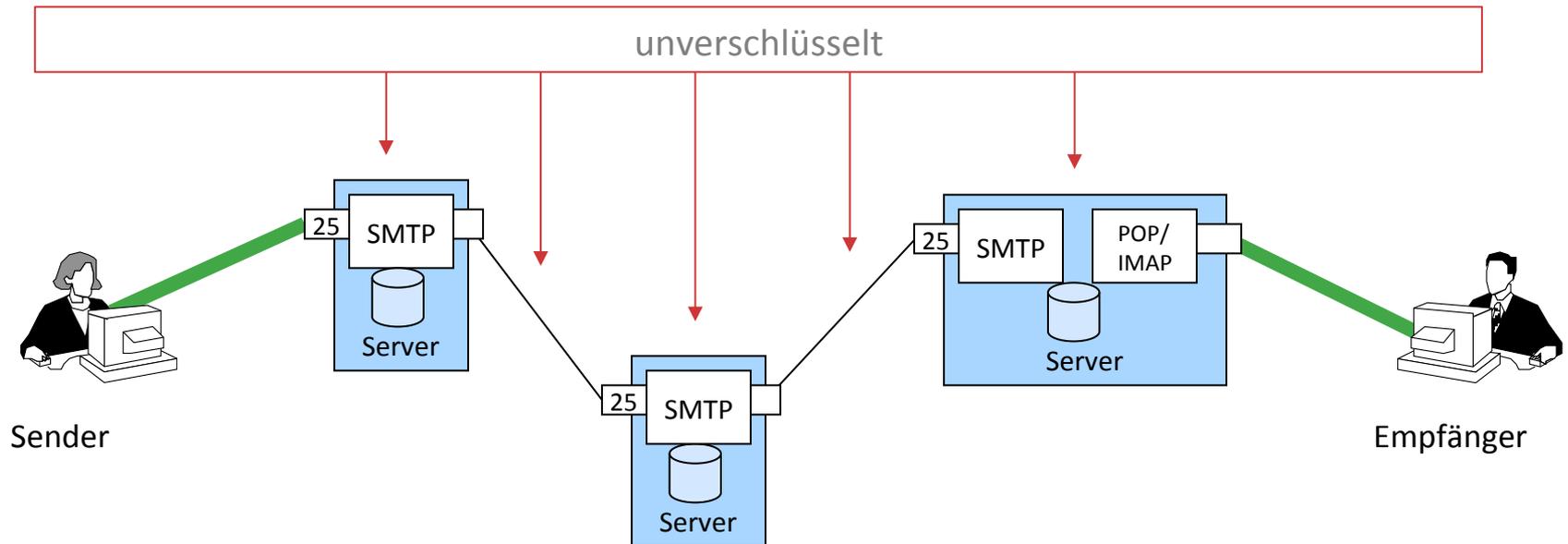
Grundlagen der E-Mail-Kommunikation

- Store & Forward-Prinzip:
 - E-Mail wird nicht direkt an Empfänger, sondern über MTA (Mail Transfer Agents) geschickt
- Senden via SMTP: Textbasiertes Protokoll auf TCP-Port 25
- Empfangen: POP, IMAP



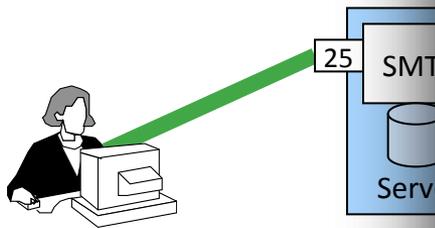
Verbindungsverschlüsselung

- SMTP/POP/IMAP over SSL
 - Verschlüsselte Teilstrecke zwischen
 - Sender und MTA
 - MTA und Empfänger
 - alle MTAs können mitlesen



Verbindungsversc

- SMTP/POP/IMAP
 - Verschlüsselte
 - Sender und
 - MTA und E
 - alle MTAs könn



Sender

Accounts

Allgemein Accounts Werbung Schrift & Farbe Darstellung Verfassen Signaturen Regeln GPGMail

Besc...	Servername	Verwendet von Account
mail...	mailhost.informatik.uni-hamburg.de	federrath@informatik.uni-h...
mail...	mailhost.uni-hamburg.de	hannes.federrath@uni-ham...

+ -

Accountinformationen **Erweitert**

Accounteinstellungen automatisch erkennen und übernehmen

Port: SSL verwenden

Authentifizierung:

Unsichere Authentifizierung erlauben

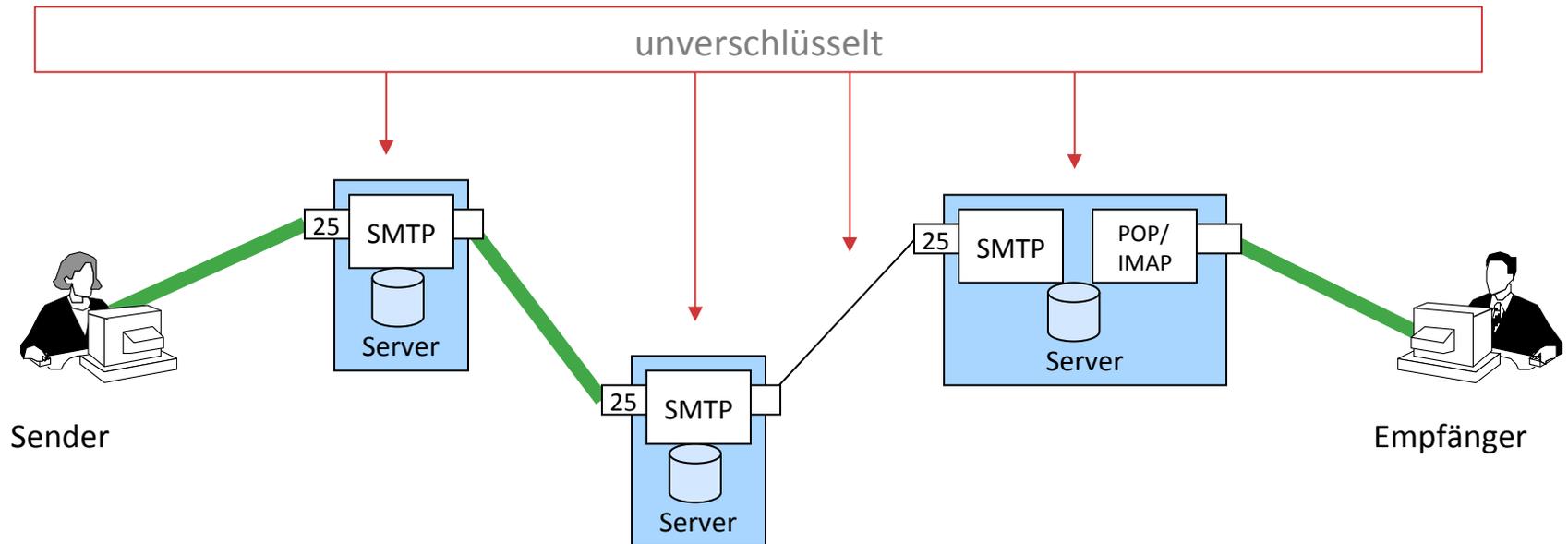
Benutzername:

Passwort:

Abbrechen **OK**

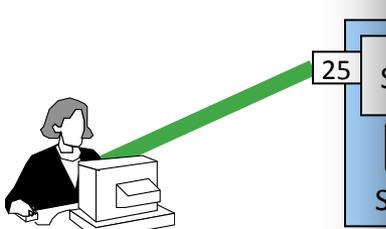
Verbindungsverschlüsselung

- SMTP/POP/IMAP over SSL
- Verschlüsselung zwischen MTAs
 - Verschlüsselte Teilstrecke zwischen MTAs
 - nicht alle Teilstrecken müssen verschlüsselt sein
 - alle MTAs können mitlesen



Verbindungsver

- SMTP/POP/IMAP
- Verschlüsselung
 - Verschlüssel
 - nicht alle Te
 - alle MTAs kö



Sender

heise online

"E-Mail Made in Germany": SSL-Verschlüsselung für (fast) alle UPDATE

09.08.2013 12:40 Uhr - Detlef Borchers

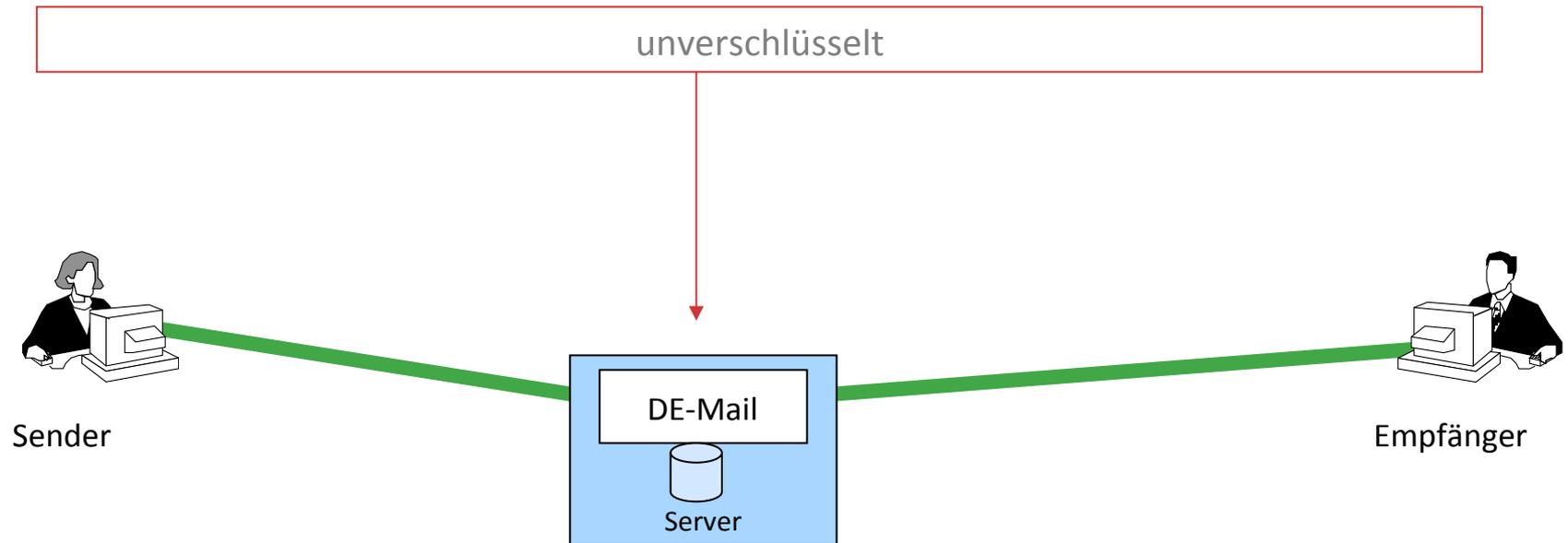
Die Deutsche Telekom und United Internet haben das Projekt "E-Mail made in Germany" [1] in Berlin vorgestellt. Dabei handelt es sich um eine SSL/TSL-Verschlüsselung zwischen den Mail-Servern und Rechenzentren der beteiligten Firmen, die ab sofort genutzt werden kann. Ab 2014 sollen nur noch SSL-verschlüsselte Mails transportiert werden. Rund 20 Millionen Kunden der Telekom und 30 Millionen von GMX und Web.de sollen die "deutsche E-Mail" nutzen können. Sie ist bereits in den Webmailern der beteiligten Firmen freigeschaltet und kommt automatisch zum Einsatz: Bei Eingabe von Empfängeradressen aus dem Mail-Verbund wird eine Information angezeigt, dass die Mails verschlüsselt übertragen werden. Bislang gibt es allerdings noch keine entsprechende Anzeige bei empfangenen Mails.

Wie Telekom-Chef René Obermann erklärte, hofft man, dass sich andere Wettbewerber wie Freenet oder Arcor der deutschen Initiative anschließen werden. Geprüft werde derzeit, wie die Tochterfirmen Strato (Telekom) und 1&1 (United Internet) in das System eingebunden werden können, damit auch Kleingewerbetreibende mit Domains wie z.B. Obermann.de die sichere deutsche "Mail made in Germany" nutzen können. Zudem hofft Obermann darauf, dass aus der deutschen Initiative eine europäische wird. Ralph Dommermuth von United Internet erklärte, dass 90 Prozent der Mail innerhalb von Deutschland ausgetauscht werde und somit die "E-Mail made in Germany" zum Standard werde.

Meldung: <https://heise.de/-1932962>

Verbindungsverschlüsselung

- Sicherheit von DE-Mail etc.
 - gleiche Sicherheit wie «E-Mail Made in Germany»
 - keine Ende-zu-Ende-Verschlüsselung
 - Server kann mitlesen



Verbindungsverschlüsselung

- Sicherheit von DE-Mail etc.
 - gleiche Sicherheit wie «E-Mail Made in Germany»
 - keine Ende-zu-Ende-Verschlüsselung
 - Server kann mitlesen



The screenshot shows a web browser window displaying the German Wikipedia article for 'De-Mail'. The browser's address bar shows the URL 'de.wikipedia.org/wiki/De-Mail'. The page header includes the Wikipedia logo, the text 'WIKIPEDIA Die freie Enzyklopädie', and navigation links such as 'Hauptseite', 'Themenportale', and 'Zufälliger Artikel'. The article title 'De-Mail' is prominently displayed. The main text explains that De-Mail is a communication method based on E-Mail technology, designed for secure and confidential communication. It mentions that De-Mail is typically used by private companies and providers. A search bar and navigation tabs are visible at the top of the article content.

de.wikipedia.org/wiki/De-Mail

Nicht angemeldet [Diskussionsseite](#) [Beiträge](#) [Benutzerkonto erstellen](#) [Anmelden](#)

Artikel [Diskussion](#) Lesen [Bearbeiten](#) [Quelltext bearbeiten](#) Mehr ▾

De-Mail

De-Mail [deːˈleːmeːl] ist der Name eines auf **E-Mail**-Technik beruhenden, hiervon aber technisch getrennten Kommunikationsmittels zur „sicheren, vertraulichen und meist nachweisbaren“ Kommunikation im Internet (§ 1 [Abs. 1 De-Mail-Gesetz](#)). Realisiert und betrieben wird De-Mail in der Regel von privatwirtschaftlichen Unternehmen, den De-Mail-Anbietern (oder auch: De-Mail-Provider).^[1]

Inhaltsverzeichnis [\[Verbergen\]](#)

1 Hintergrund



Quelle: Wikipedia

Systeme von Absender und Empfänger die Identität der jeweils anderen Seite sicherstellen können. Eine Möglichkeit hierfür ist der Einsatz [digitaler Zertifikate](#).

- Eine abschnittsweise [Verschlüsselung](#) der Übertragungswege soll Sicherheit gegen den Zugriff durch Unbefugte bieten.

Bei besonders hohen Anforderungen an die Vertraulichkeit der Nachrichten haben De-Mail-Nutzer wie bei herkömmlichen E-Mails die Möglichkeit, die mit De-Mail übermittelten Inhalte noch zusätzlich selbst zu verschlüsseln („[Ende-zu-Ende-Verschlüsselung](#)“). In diesem Fall erfolgt die Verschlüsselung auf dem Rechner des Absenders und die Entschlüsselung der Inhalte erst auf dem Rechner des Empfängers. Hierfür ist jedoch die Installation zusätzlicher Software erforderlich, die die Ver- und Entschlüsselung durchführt. Der Verzeichnisdienst, der bei De-Mail obligatorisch durch den Diensteanbieter angeboten werden muss, unterstützt den Anwender, indem dieser seinen öffentlichen Schlüssel anderen Anwendern zur Verfügung stellen kann. Es soll also ermöglicht werden, an einer zentralen Stelle nach öffentlichen Schlüsseln von Personen suchen zu können, um mit diesen vertraulich zu kommunizieren. Dies ist bisher nur schwer möglich und stellt den wesentlichen „Hemmschuh“ für die Verbreitung von Verfahren zur Ende-zu-Ende-Verschlüsselung („Wo finde ich den gültigen Verschlüsselungsschlüssel meines Kommunikationspartners?“). Mit De-Mail soll auf diese Weise der Einsatz der Ende-zu-Ende-Verschlüsselung unterstützt und gefördert werden.

[S/MIME](#) oder [OpenPGP](#) können zusätzlich durch den Nutzer für die Abbildung der Ende-zu-Ende-Sicherheit eingesetzt werden. Die Liste der hauptsächlichen Sicherheitsfunktionen wurden in einem Dokument des BMI zusammengefasst.

Technische Konzeption [[Bearbeiten](#) | [Quelltext bearbeiten](#)]

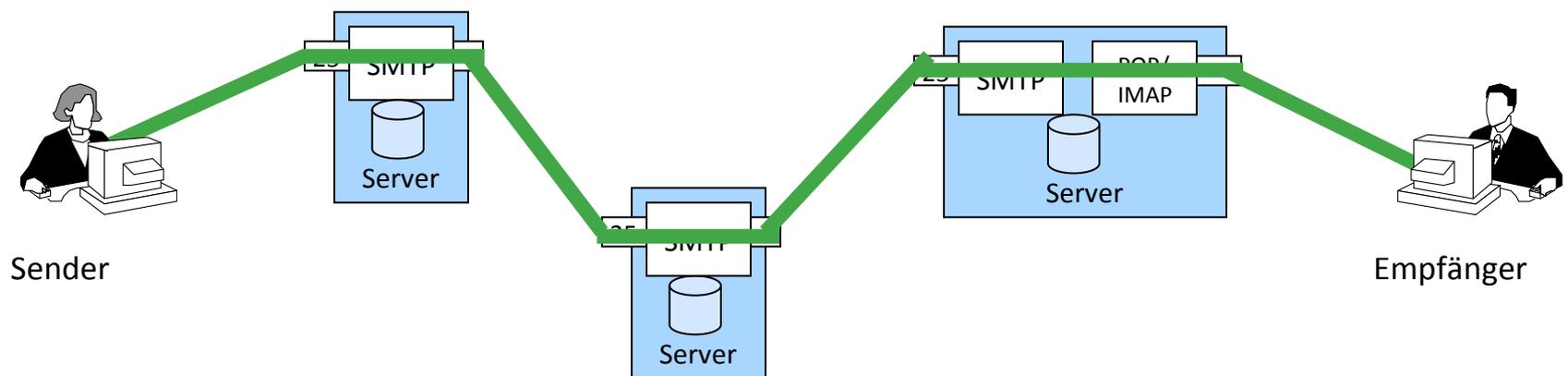
Das technische Konzept ist innerhalb von technischen Richtlinien beschrieben, die auf der Webseite des BSI^[19] veröffentlicht sind.

Standardmäßige Transportsicherheit [[Bearbeiten](#) | [Quelltext bearbeiten](#)]

Sowohl die Kommunikation der De-Mail-Nutzer mit ihren De-Mail-Provider als auch die Kommunikation von De-Mail-Anbietern untereinander verläuft grundsätzlich über TLS-gesicherte Kommunikationskanäle.^[5] Reicht einem Nutzer das dadurch realisierte Sicherheitsniveau nicht

Ende-zu-Ende-Verschlüsselung schützt die Vertraulichkeit

- Ende-zu-Ende-Verschlüsselung
 - Inhalte sind durchgehend verschlüsselt
 - MTAs (Server) können nicht mitlesen
 - Adressierungsinformation kann nicht mit verschlüsselt werden
- Konkrete Ende-zu-Ende-Verschlüsselungslösungen
 - S/MIME
 - PGP



Ende-zu-Ende-Verschlüsselung schützt die Vertraulichkeit

- Verschlüsselte E-Mail (schematisch):

Von: alice@example.de

An: bob@mail.com

Betreff: Abendessen

-----BEGIN ENCRYPTED MESSAGE-----

```
AkRFMRcwFQYDVQQDEw5Sb2xmIFdlbmRvbHNreTEUMBI
GA1UECBMLRGV1dHNjaGxhbmxEzARBgNVBAcTClJlZ2V
uc2J1cmcxZzANBgNVBAoTBnBaXZhdDEkMCIGCSqGSIB
3DQEJARYVcm9sZi53ZW5kxza3lAZ214LmRlMIGfMA0G
CSqGSIB3DQEBAAQUAA4GNABDCBiQKBgQDUVvgaQK9OQP
XvgZm2bU/QqDnsbenv83gDiSuCq07S/cSMiGFjEZas6
5MZ47W951LlNLvFTjwS2fUfsZ5oAxfU+RDWb3GgijZp
5cAxTfFKQ/amaWAtmCkt1FMntRXZ393gOkSSU1WQ7Cr
6GWAYF+deC5CuWptRPpSLYRqSwIDAQABMA0GCSqGSIB
3DQEBBAUAA4GBAIGVTNbu0eOTfGuuL0MWHLfVD
```

-----END ENCRYPTED MESSAGE-----

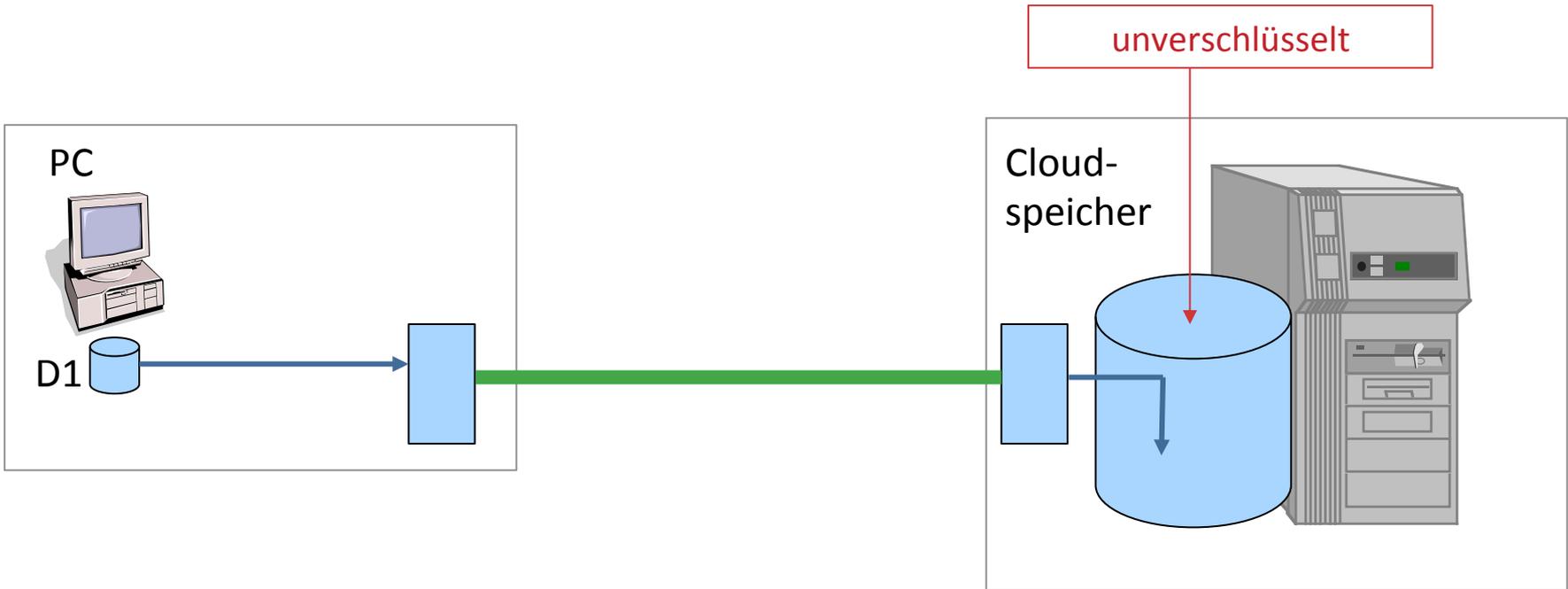
Konkrete Ende-zu-Ende-Verschlüsselungslösungen

- S/MIME (Secure Multipurpose Internet Mail Extensions)
 - ursprünglich von RSA Data Security Inc.
 - S/MIME v3 im Juli 1999 als IETF-Standard verabschiedet
 - in die meisten E-Mail-Clients integriert
 - One-pass processing: Die Mail ist in einem Schritt verarbeitbar, da alle benötigten Daten in die Mail selbst integriert sind

- PGP (Pretty Good Privacy)
 - 1991 von Philip Zimmermann entwickelt
 - heute: Open PGP, GnuPG (Gnu Privacy Guard)
 - Zahlreiche grafische Frontends erhältlich, z.B. GPA, WinPT
 - Plugins für verschiedene Mailclients, z.B. Outlook, Thunderbird, Pegasus, KMail

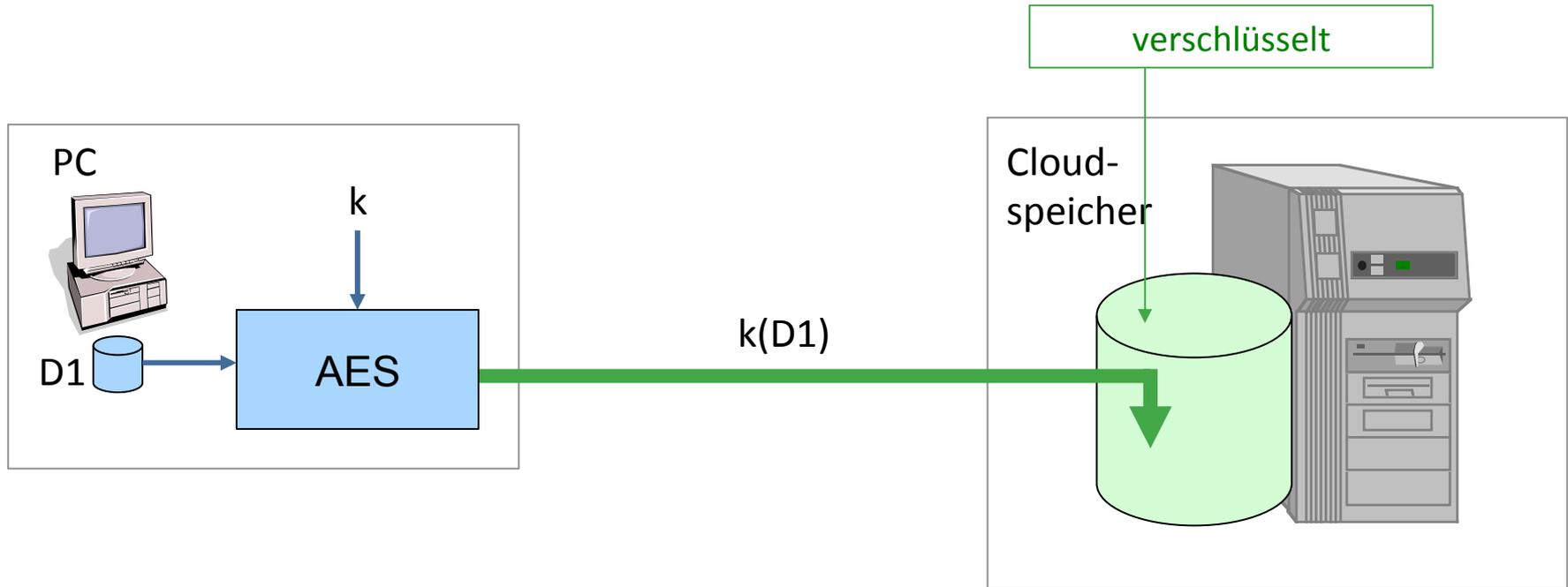
Verschlüsselte Cloud-Speicher

- Verbindungsverschlüsselung ist heute Standard



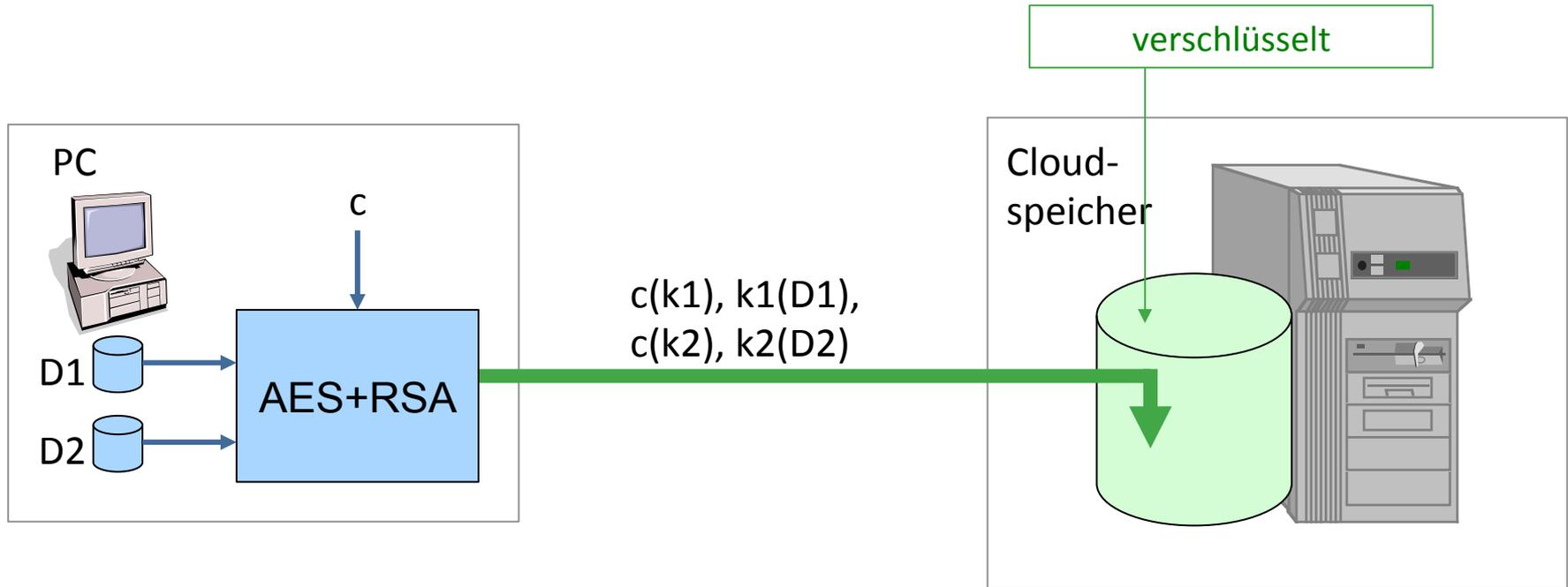
Verschlüsselte Cloud-Speicher

- Ende-zu-Ende-Verschlüsselung wäre kein Problem



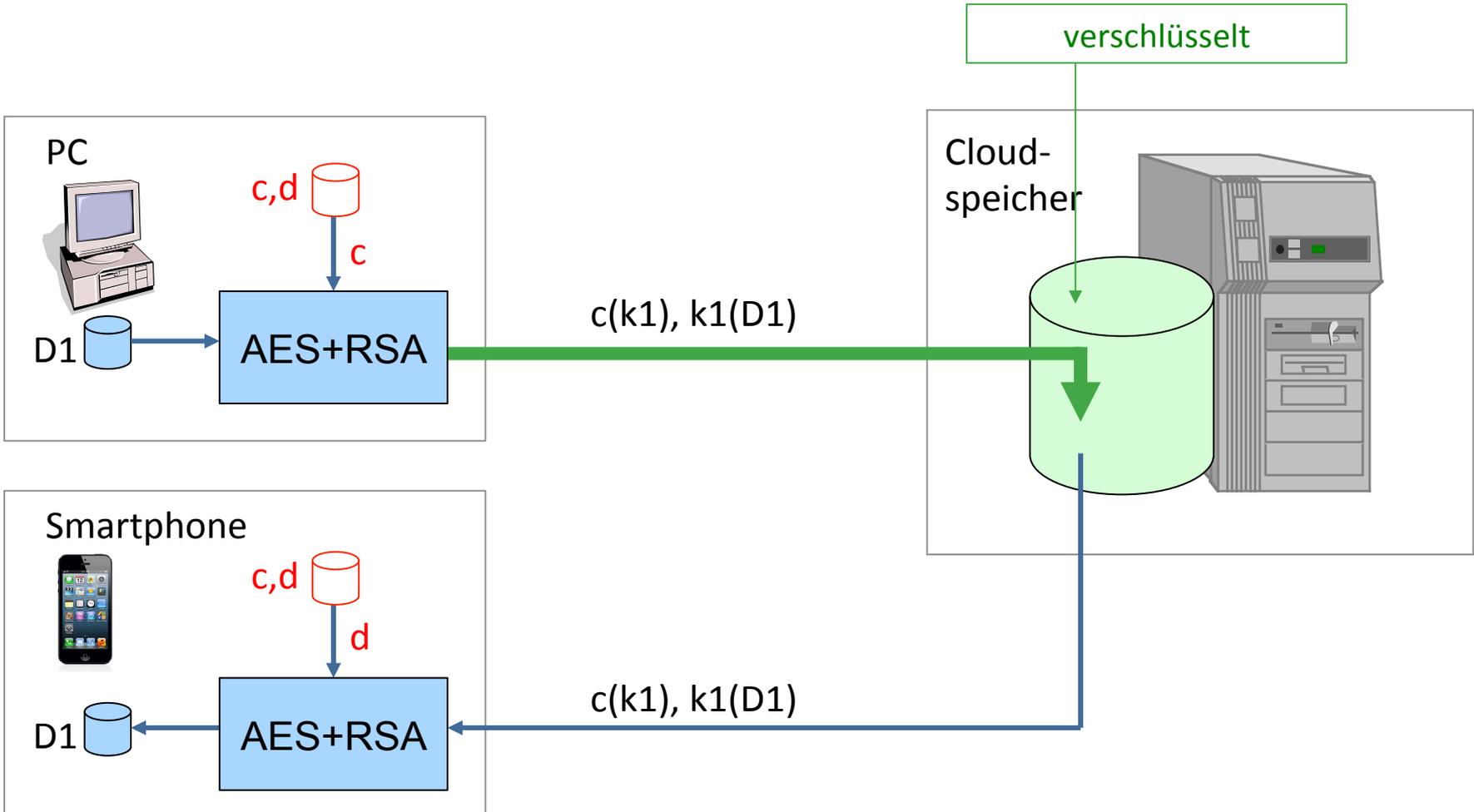
Verschlüsselte Cloud-Speicher

- Ende-zu-Ende-Verschlüsselung besser hybrid ...



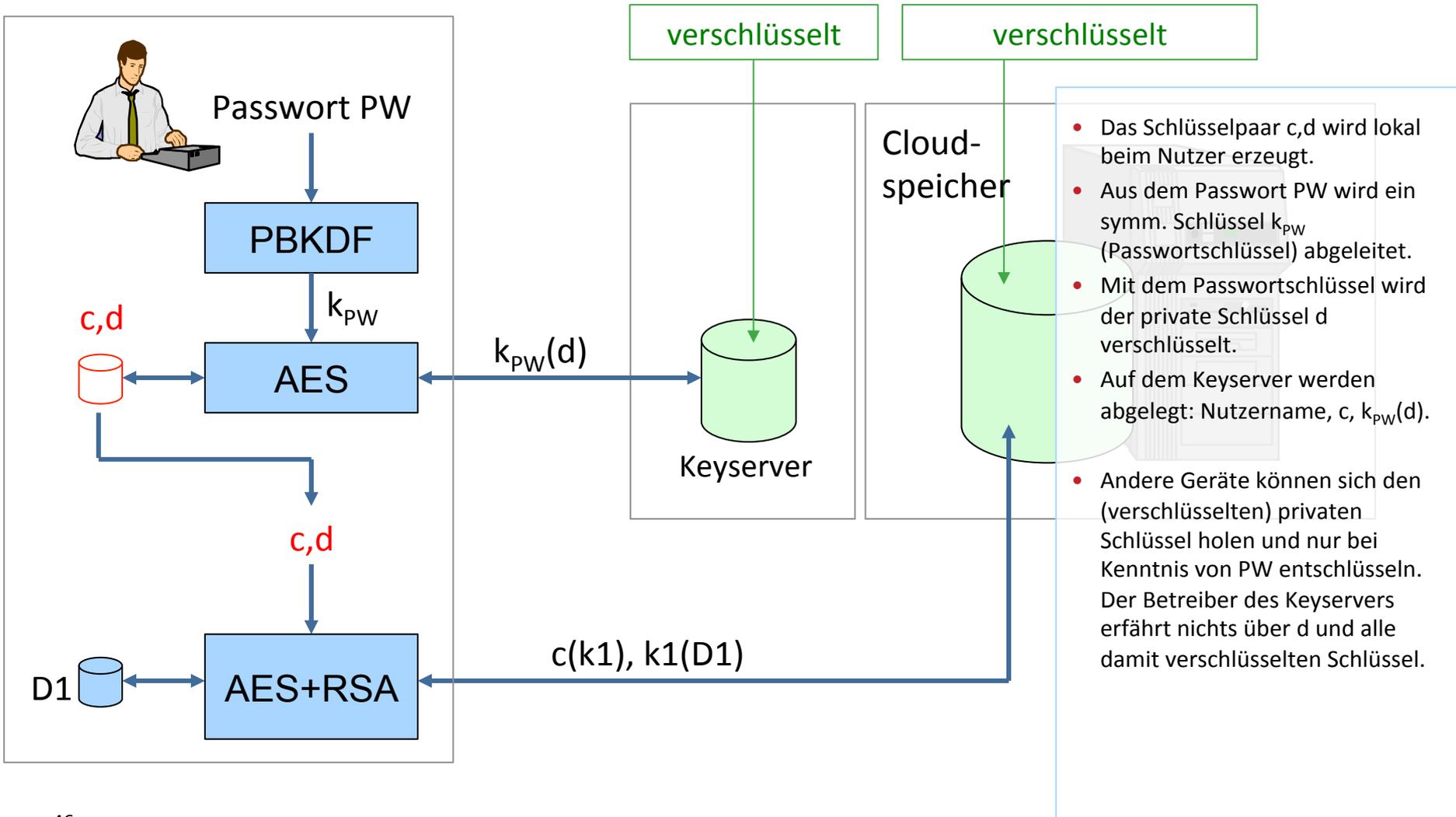
Verschlüsselte Cloud-Speicher – Usability-Aspekte

- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?



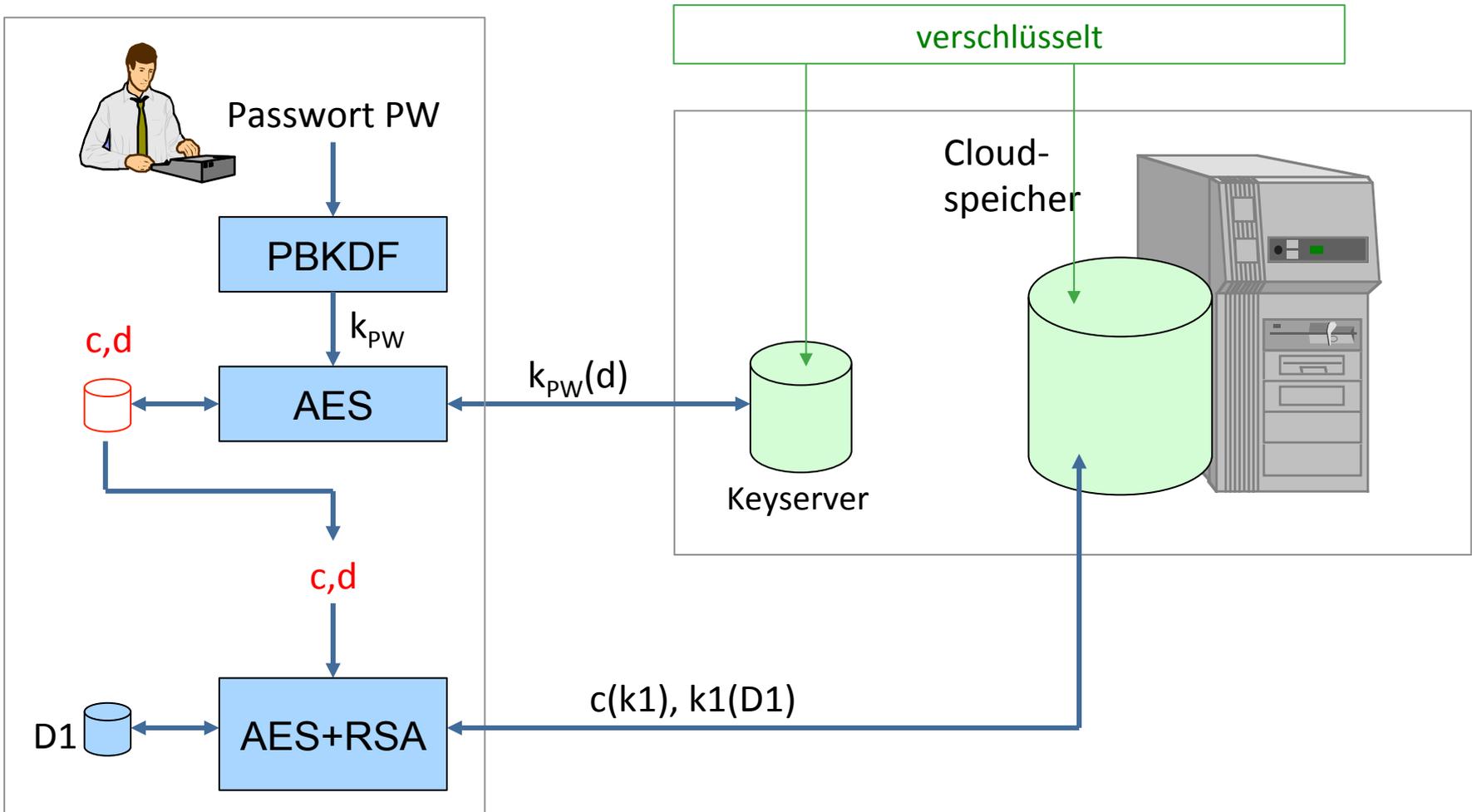
Verschlüsselte Cloud-Speicher – Usability-Aspekte

■ Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?



Verschlüsselte Cloud-Speicher – Usability-Aspekte

- Wie bekommt der Nutzer auf alle seine Geräte seine(n) Schlüssel?



Ethische Dimensionen

- Dreiteilung nach Simon, 2016:

- Ethik des Berufs
- Ethik des Designs
- Ethik der Nutzung



Association for
Computing Machinery



Ethische Leitlinien der Gesellschaft
für Informatik

ACM Code of Ethics and Professional
Conduct

IEEE Code of Ethics

www.ieee.org/about/corporate/governance/p7-8.html

IEEE - IEEE Code of Ethics ACM Code of Ethics and Professional Conduct Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.

IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites Cart (0) | Create Account | Sign in



The world's largest technical professional organization dedicated to advancing technology for the benefit of humanity

[About IEEE](#) |
 [Membership & Services](#) |
 [Societies & Communities](#) |
 [Publications & Standards](#) |
 [Conferences & Events](#) |
 [Education & Careers](#) |
 [Contact & Support](#)

Search IEEE [Search](#)

Home > About IEEE > Corporate > Governance

IEEE Code of Ethics

- ◆ **Governance**
- ◆ [IEEE Governing Documents](#)
- ◆ [IEEE Governance Committee](#)
- ◆ [Governance Committee Charter](#)
- ◆ [Committee Member Log In](#)

The following is from the IEEE Policies, Section 7 - Professional Activities (Part A - IEEE Policies).

◆ 7.8 IEEE Code of Ethics

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology; its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to

Governance Procedures

- ◆ [Board 30-Day Review/Approval Process](#)
- ◆ [Revisions to IEEE Governing Documents](#)
- ◆ [Glossary of Terms \(PDF, 62 KB\)](#)
- ◆ [IEEE Email Terms and Conditions](#)

www.acm.org/about-acm/acm-code-of-ethics-and-...
IEEE - IEEE Code of Ethics ACM Code of Ethics and Professional Conduct Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.

acm Association for Computing Machinery

Home > About ACM > ACM Code Of Ethics And Professional Conduct

ACM Code of Ethics and Professional Conduct

Adopted by ACM Council 10/16/92.

Preamble

[Contents & Guidelines](#)

Preamble

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

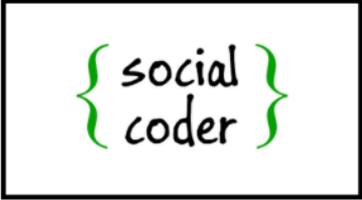
This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. [Section 1](#) outlines fundamental ethical considerations, while [Section 2](#) addresses additional, more specific considerations of professional conduct. Statements in [Section 3](#) pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in [Section 4](#).

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondly, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of [Section 1](#), the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful



Volunteer with SocialCoder

You can use your technical skills for social good and offer volunteer support on software development projects to organizations who could not otherwise afford it. SocialCoder connects volunteer programmers/software developers with registered charities and helps match them to suitable projects based on their skills, experience, and the causes they care about. Learn more about ACM's new partnership with SocialCoder, and how you can get involved.



CAREER RESOURCE

www.gi.de/wir-ueber-uns/unsere-grundsaeetze/ethische-leitlinien

IEEE - IEEE Code of Ethics ACM Code of Ethics and Professional Conduct Ethische Leitlinien - GI - Gesellschaft für Informatik e.V.



Gesellschaft für Informatik



Zum Mitgliederbereich >

Startseite Aktuelles Themen Gliederungen Service Presse Wir über uns **Mitgliedschaft** English 

Sie befinden sich hier: Startseite/Wir über uns/Unsere Grundsätze/Ethische Leitlinien

Ziele und Aufgaben

Unsere Grundsätze >

- > Satzung
- > Ethische Leitlinien**
- > Steckbrief der GI
- > Perspektiven, Positionen und Empfehlungen

Unsere Mitglieder

Unsere Jahrestagungen

Testimonials

GI-Mitglieder einmal anders

Leitung

Personen

Wettbewerbe

Unsere Partner

Unsere Botschafter

Assoziierte Gesellschaften

Ansprechpartner/innen

Geschäftsstelle

Die Leitlinien der Gesellschaft für Informatik e.V. (GI) wurden am 13.01.1994 vom Präsidium der GI verabschiedet und am 16.12.1994 von den Mitgliedern bestätigt. Am 29. Januar 2004 hat das GI-Präsidium die Ethischen Leitlinien in einer komplett überarbeiteten Version angenommen.

Inhalt

- Präambel
- I Das Mitglied
- II Das Mitglied in einer Führungsposition
- III Das Mitglied in Lehre und Forschung
- IV Die Gesellschaft für Informatik
- Erläuterungen der Begriffe
- Kontakt

Die ethischen Leitlinien zum Ansehen und Herunterladen:
Ethischen Leitlinien (PDF-Format, Größe 149 KB)

Präambel

Das Handeln von Informatikerinnen und Informatikern steht in Wechselwirkung mit unterschiedlichen Lebensweisen, deren besondere Art und Vielfalt sie berücksichtigen sollen. Mehr noch sehen sie sich dazu verpflichtet, allgemeine moralische Prinzipien, wie sie in der Allgemeinen Deklaration der Menschenrechte formuliert sind, zu wahren. Diese Leitlinien sind Ausdruck des gemeinsamen Willens, diese Wechselwirkungen als wesentlichen Teil des eigenen individuellen und institutionellen beruflichen Handelns zu betrachten. Der offene Charakter der nachfolgenden Artikel wird mit dem Begriff Leitlinien unterstrichen.

Die Gesellschaft für Informatik e.V. (GI) will mit diesen Leitlinien bewirken, dass berufsethische Konflikte Gegenstand gemeinsamen Nachdenkens und Handelns werden. Ihr Interesse ist es, ihre Mitglieder, die sich mit verantwortungsvollem Handeln exponiert haben, zu unterstützen. Vor allem will sie den Diskurs über ethische Fragen in der Informatik mit der Öffentlichkeit aufnehmen und Aufklärung leisten.

Mitgliedschaft

Mitglied werden

Informatik-Lexikon

Fachbegriffe zu Informatik und deren Anwendung

>

Unsere Struktur

- > Fachbereiche
- > Regionalgruppen
- > Präsidiumsarbeitskreise
- > Beiräte
- > Hochschulgruppen

Wir sind Informatik



Jörg Sievers
"Zusammen kann man immer mehr erreichen!" und darum bin ich Mitglied geworden.

Geistiges Eigentum

Aus- und Weiterbildung

Grand Challenges

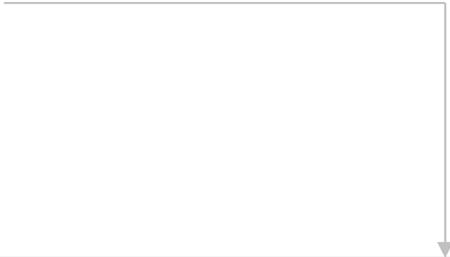
Informatikpersönlichkeiten Fachbereich

Datenschutz **Downloads** Beiräte

Ethische Dimensionen

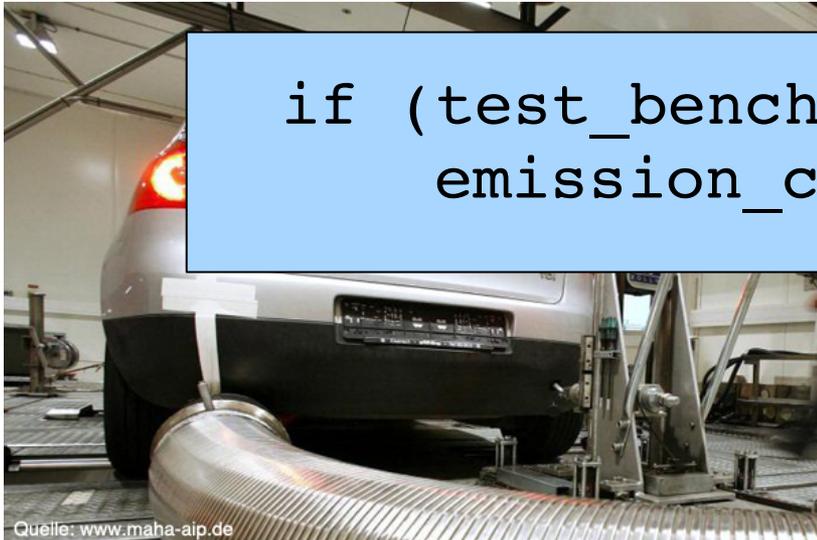
- Dreiteilung nach Simon, 2016:

- Ethik des Berufs
- Ethik des Designs
- Ethik der Nutzung



```
if (test_bench_detected())  
    emission_clean(FULL)  
else  
    <ignore_laws>
```

Abgasmessungen auf dem Prüfstand und mobil



```
if (test_bench_detected())  
    emission_clean(FULL)
```

(Pseudocodedarstellung)



- Adaptive Motorsteuerung erkennt anhand von Lenkradbewegungen, Umgebungsluftdruck, Raddrehzahlen und Motorlaufzeit die Messbedingungen

	Abgasreinigung	Kraftstoffverbrauch
Prüfstand	verbessert	hoch
Straße	reduziert	verringert

Verkehrszeichenerkennung mittels maschineller Lernverfahren



ERKENNUNG

Gefahr

»normal«

REALITÄT

Gefahr

richtig positiv	falsch negativ
falsch positiv	richtig negativ

»normal«

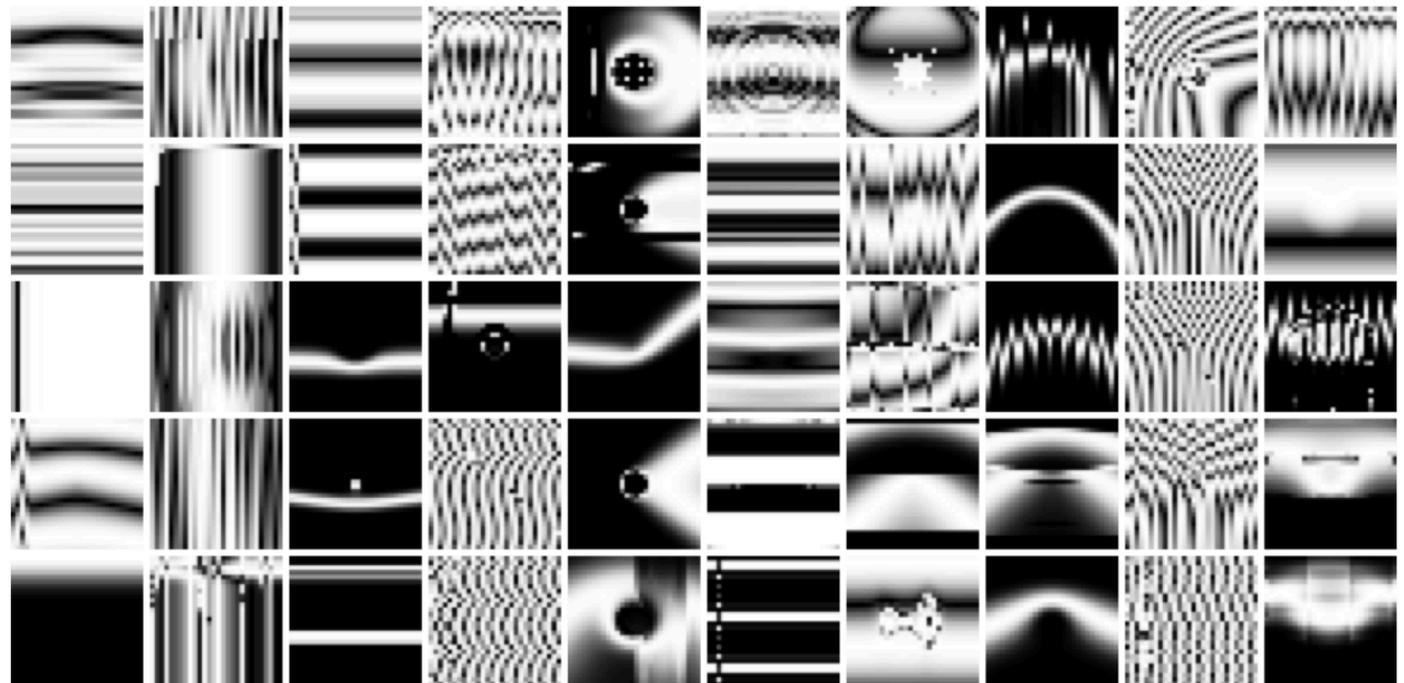
J. Stallkamp, M. Schlipfing, J. Salmen, C. Igel, Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition, Neural Networks, Volume 32, August 2012, Pages 323-332, ISSN 0893-6080

Verkehrszeichenerkennung mittels maschineller Lernverfahren

...klappt leider nicht immer

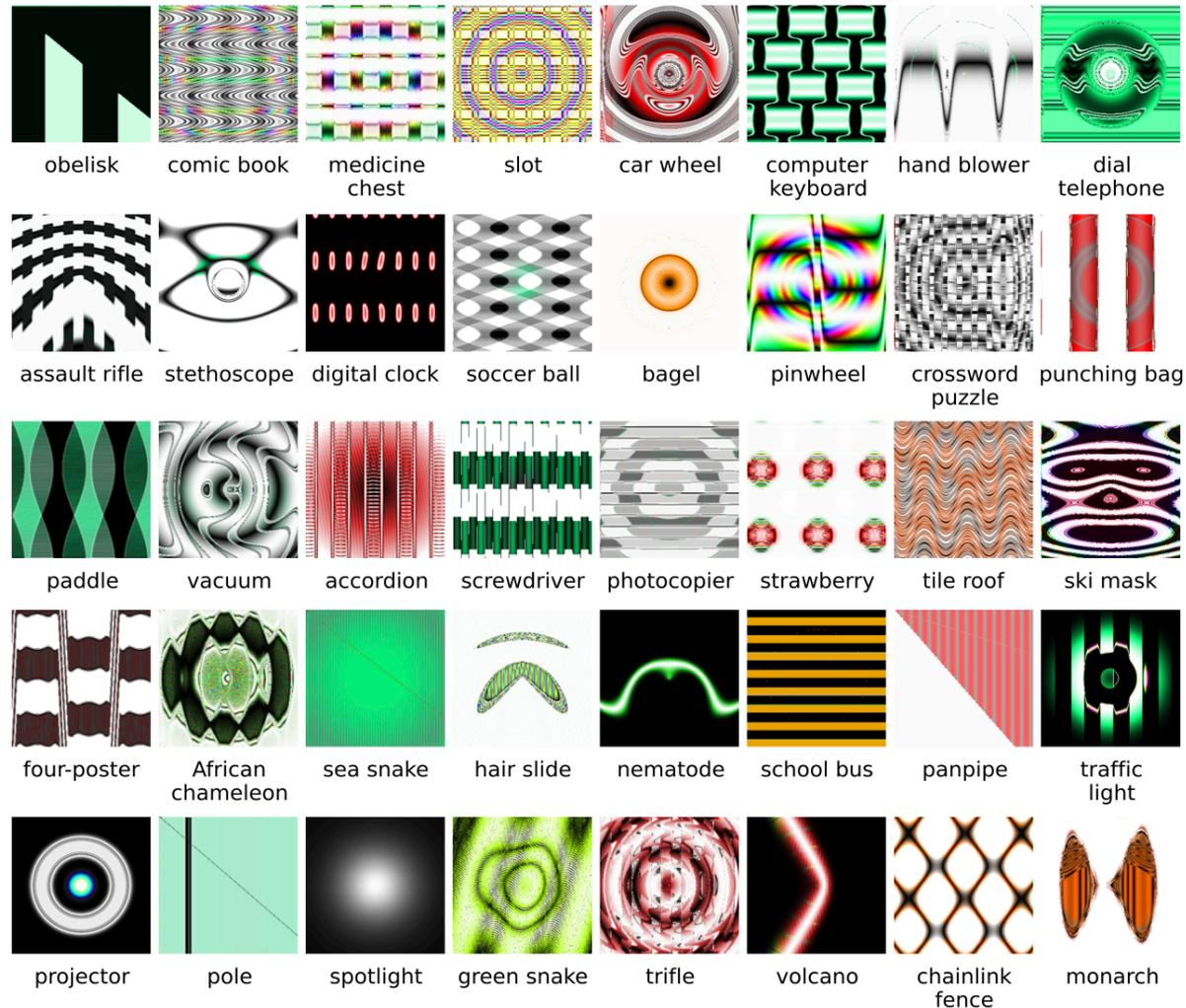
Erkannte Ziffer

0 1 2 3 4 5 6 7 8 9



Eingabedaten, die
fälschlicherweise
als Ziffer erkannt
werden

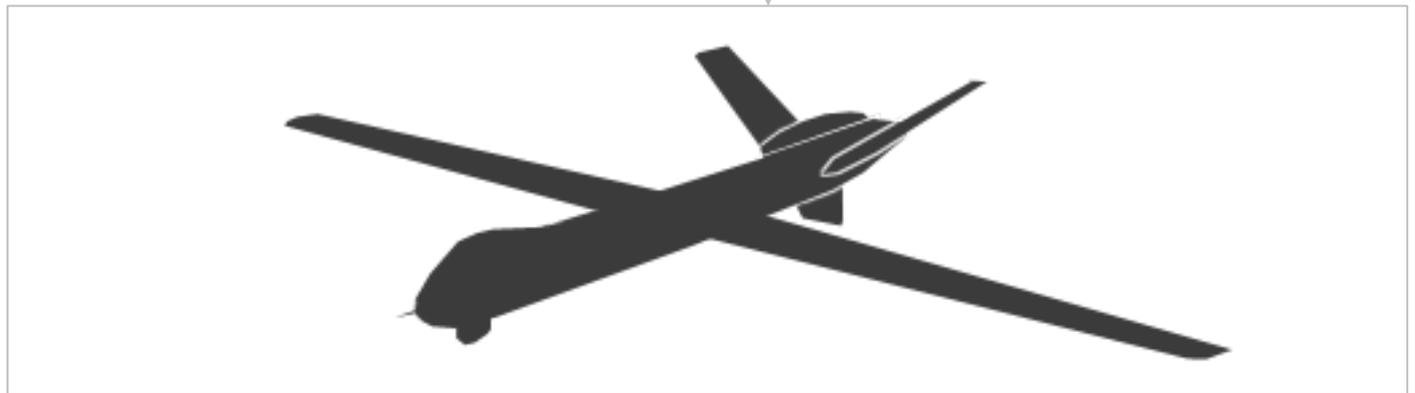
Gezielte Manipulationen eines autonomen Fahrzeugs möglich



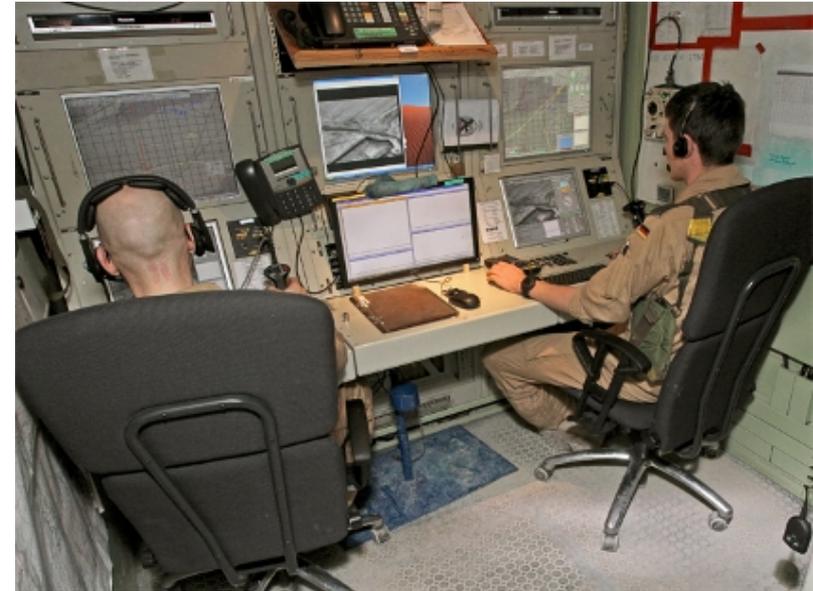
Nguyen A, Yosinski J, Clune J. Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images. In CVPR '15, IEEE, 2015.

Ethische Dimensionen

- Dreiteilung nach Simon, 2016:
 - Ethik des Berufs
 - Ethik des Designs
 - Ethik der Nutzung



Militärischer Einsatz von Informationstechnologie



Aufklärungsdrohne Heron 1 und deren Steuerung

Bilder: www.bundeswehr.de

■ Spannungsfeld:

- Fern-Aufklärung mittels Informationstechnik ✓
- Fern-Tötung mittels Informationstechnik ?

Aus dem Beweisbeschluss SV-14 vom 7. Juli 2016 des 1. Untersuchungsausschusses der 18. Wahlperiode des Deutschen Bundestages:

«... Ist unter Berücksichtigung der festgestellten Bedingungen eine Telefonnummer – beziehungsweise eine IMEI- oder IMSI-Identifizierung – als einziges technisches Datum mittelbar oder unmittelbar ausreichend, um eine Fernlenkwaffe mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können? ...»

Geleakte Fassung unter <https://tinyurl.com/gtv552j>



IMSI-Catcher in Drohne
simuliert
Mobilfunkzelle

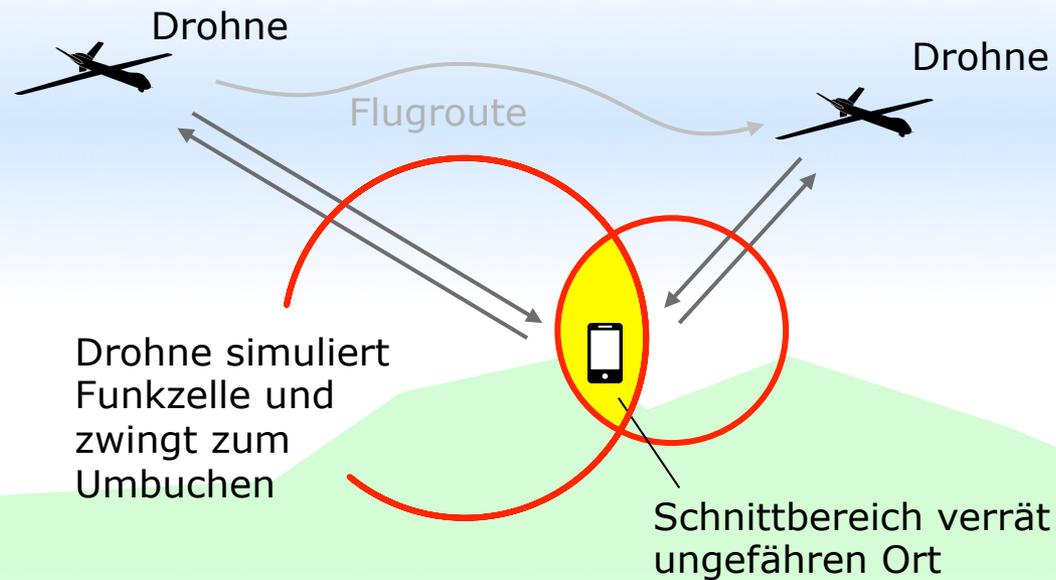
MFG wählt sich in die
Funkzelle ein und es
werden IMSI/TMSI und
IMEI übertragen

Drohne bestimmt
Empfangsrichtung der
Funkwellen

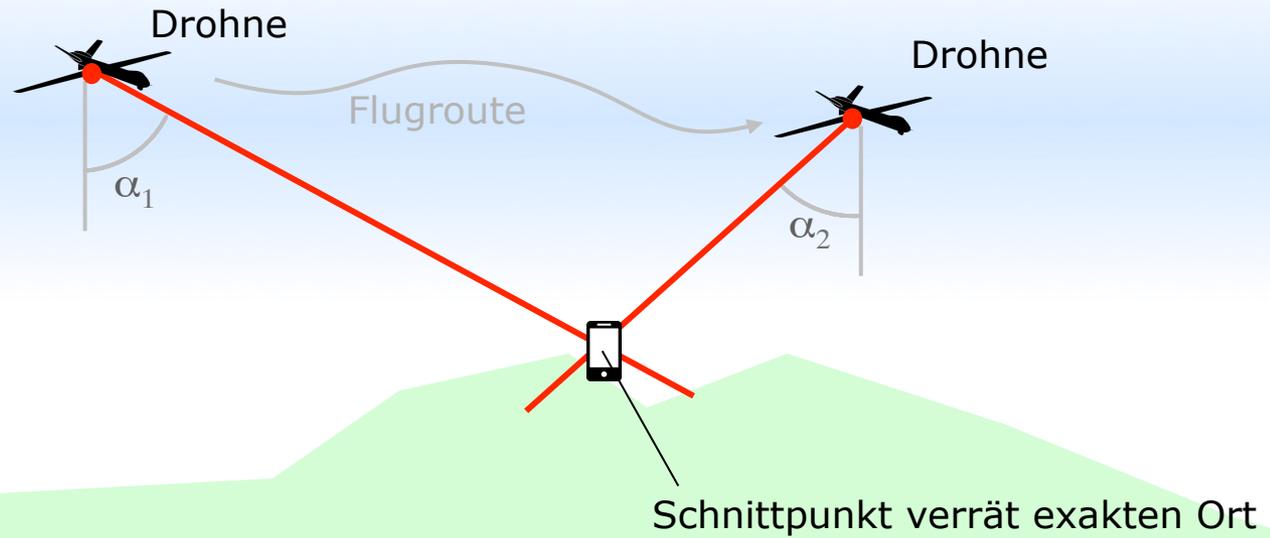
Positionsermittlung als
Schnittpunkt der
Erdoberfläche mit der
Empfangsrichtung



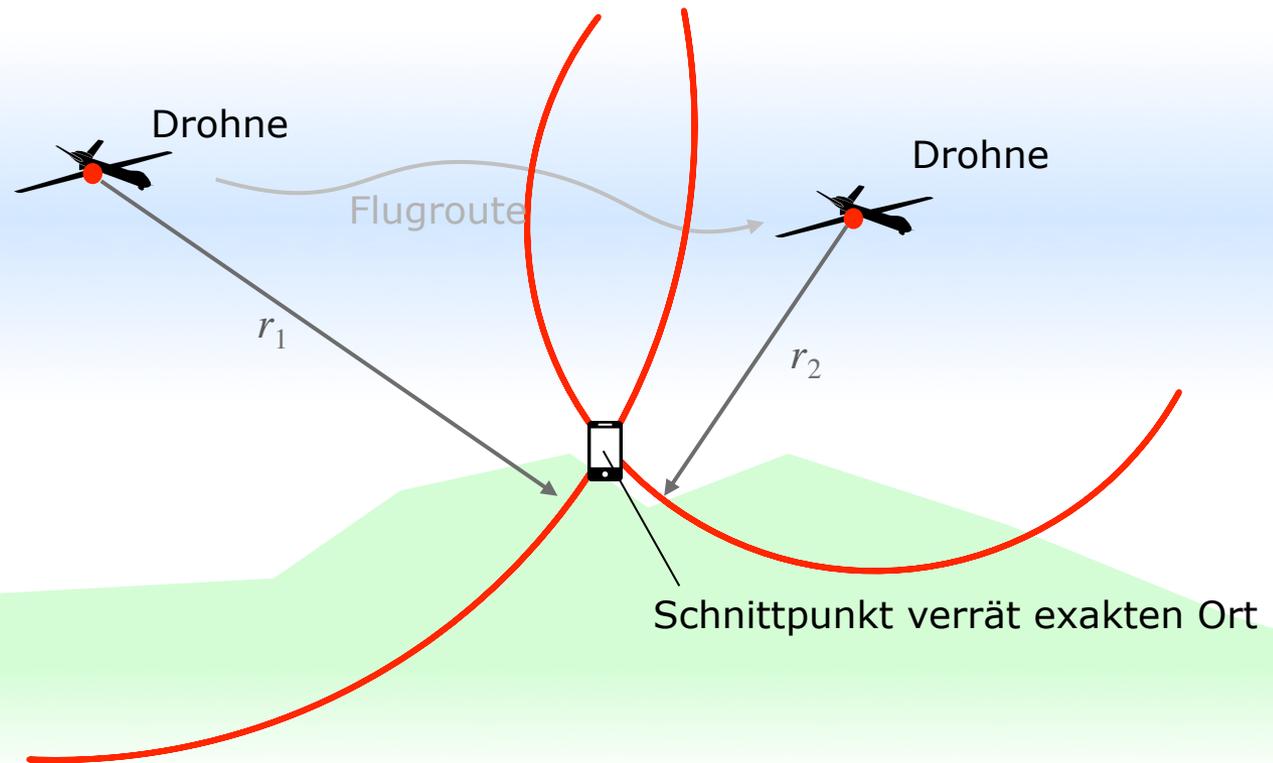
IMSI-Catcher in Drohne simuliert Mobilfunkzelle



Drohne bestimmt Empfangsrichtung der Funkwellen



Drohne bestimmt Empfangsrichtung der Funkwellen

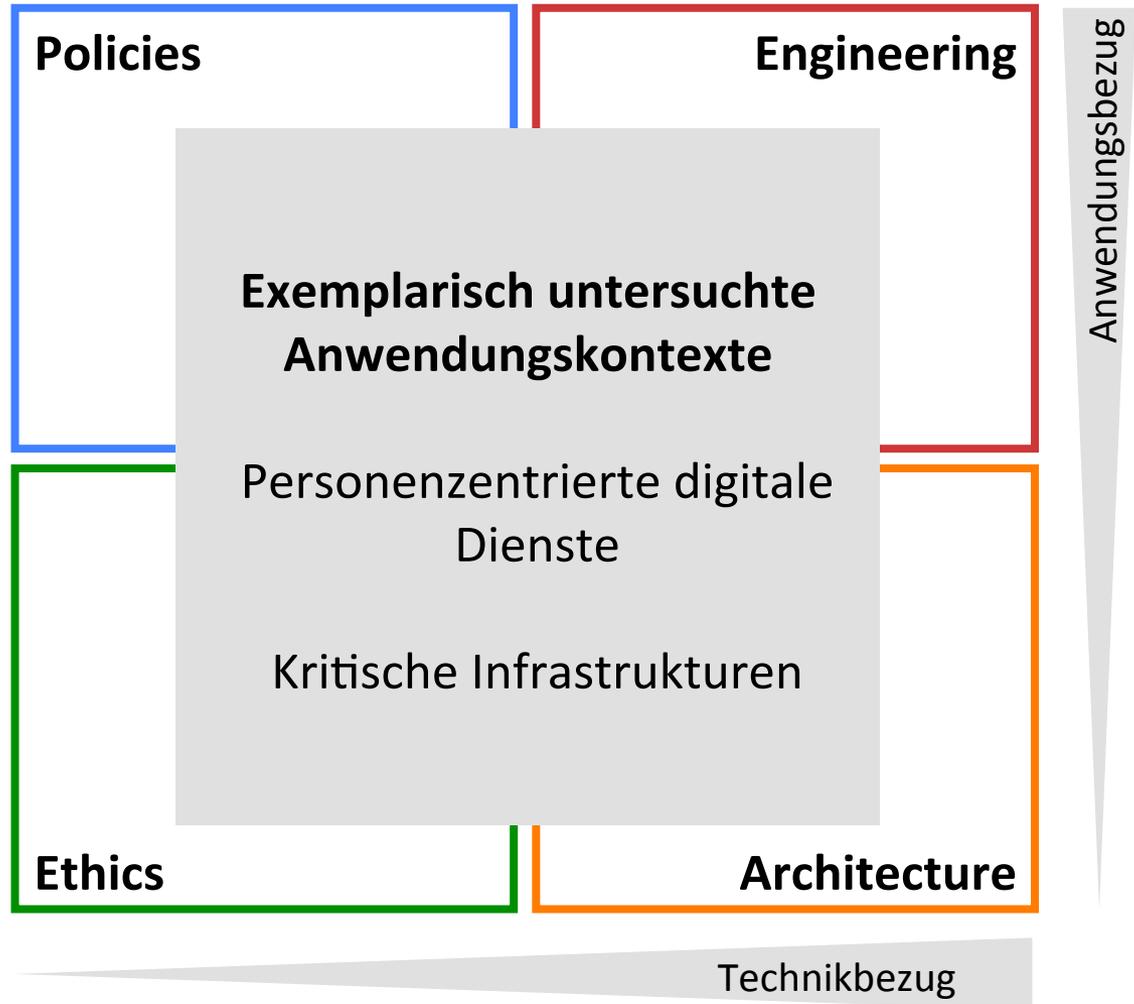


Information Governance Technologies

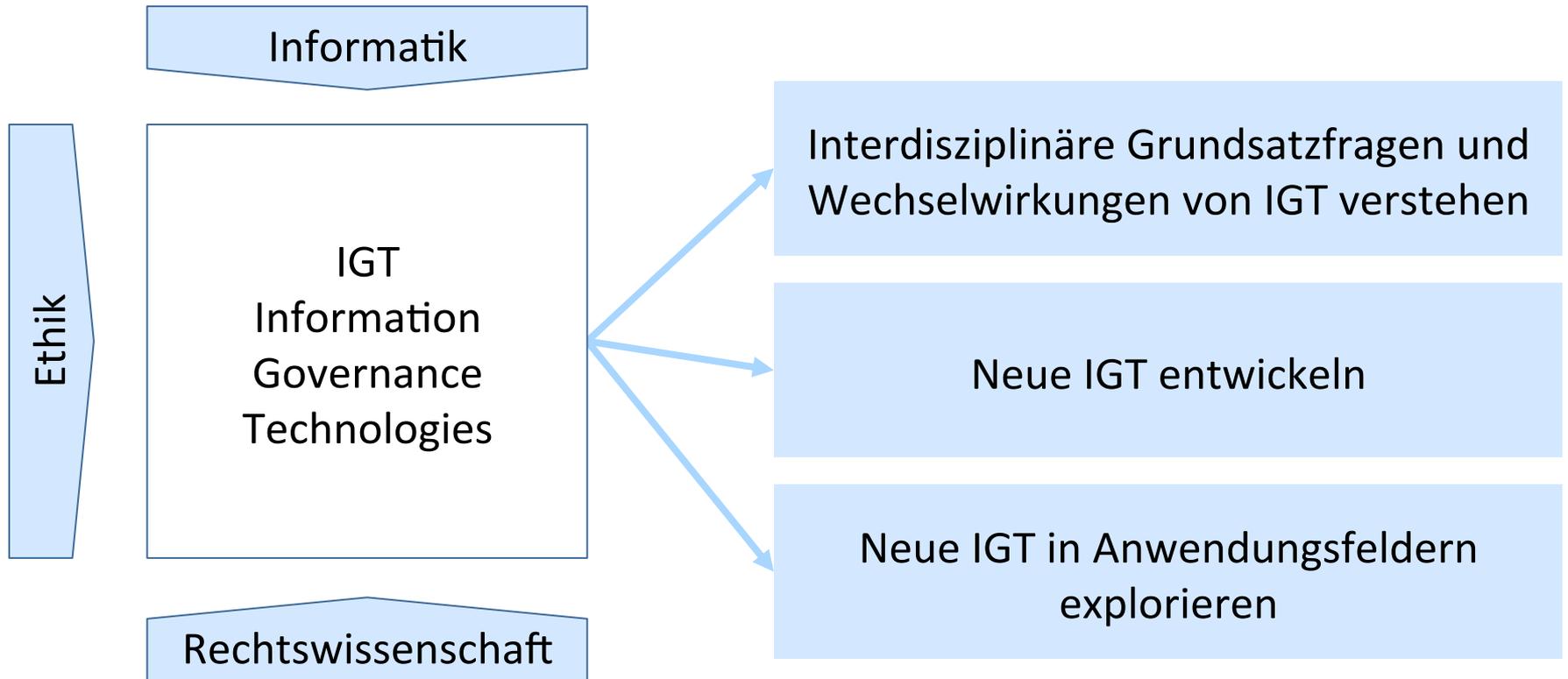
Verbundprojekt mit Uni Hamburg, TU Hamburg, Hans-Bredow-Institut

Projektbeginn vorauss. 1. Juni 2017, für 3 Jahre gefördert

Projektziel: Die menschenzentrierten technischen Möglichkeiten für den verantwortlichen Umgang mit Daten in der digitalen Gesellschaft erforschen



Information Governance Technologies





Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

<https://svs.informatik.uni-hamburg.de>