digitale woche 2017

Kiel. Kiel Sailing.City.

Paranoia, Bürgerrechte und das Internet

Anonymisierungsdienste und Verschlüsselung als Werkzeuge des Selbstdatenschutzes

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Herzlich willkommen im ULD

- Wer wir sind

ULD

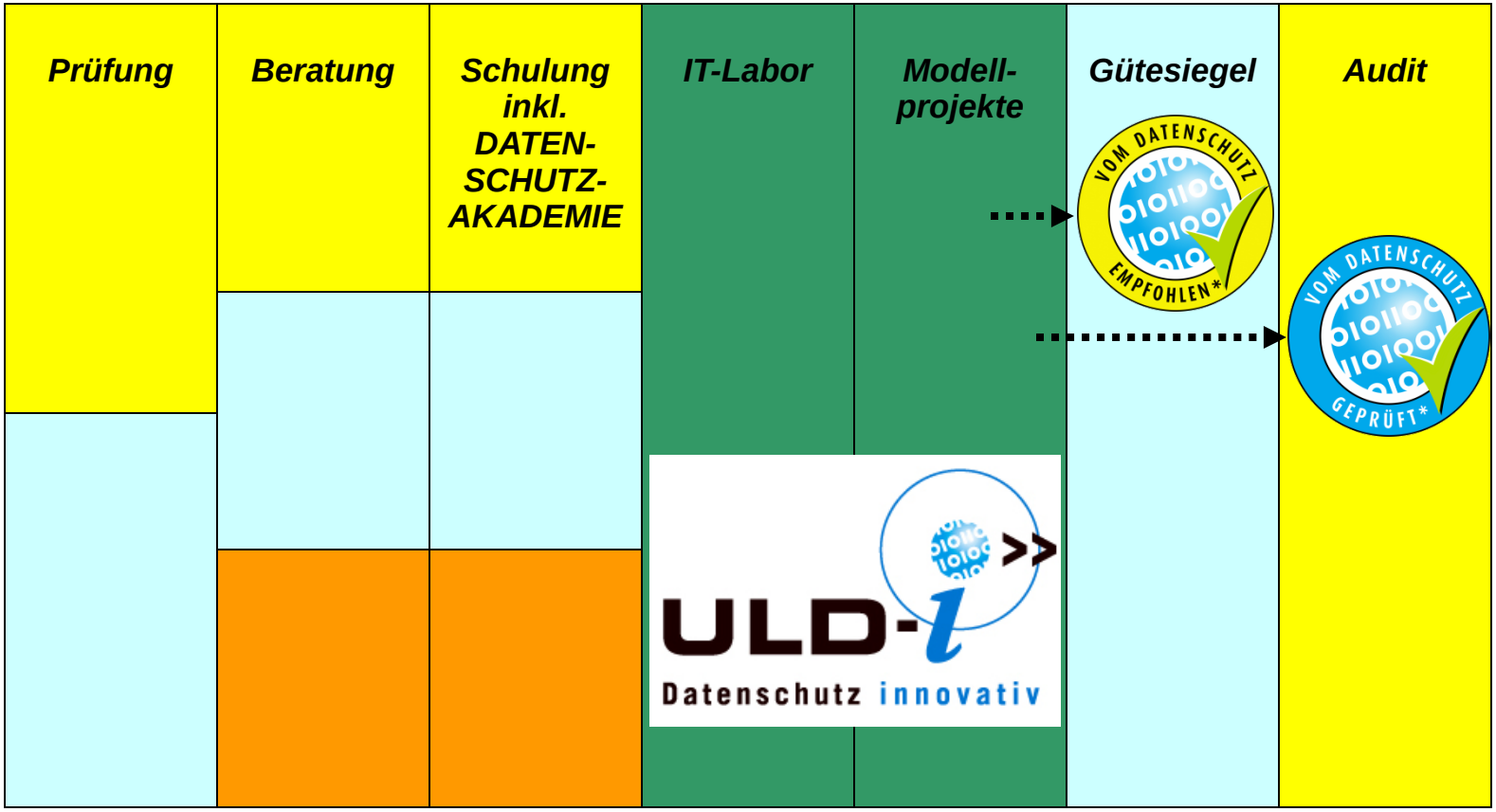
- Was wir tun

VV Vertrauenswürdige Verteilung von Verschlüsselungsschlüsseln

AN.ON NEXT GENERATION

Bundesministerium für Bildung und Forschung

Die 7 Säulen des ULD



Was Sie heute erwartet

Paranoia

- Über die Risiken

Bürgerrechte

- Welche Bürgerrechte Sie im Internet haben

Internet

- Wie Verschlüsselung funktioniert
- Anonym surfen im Netz

Paranoia, Bürgerrechte und das Internet

- „Wen interessiert es denn, was ich in einer Nachricht schreibe?! Da steht nichts Wichtiges drin.“
- „Ich habe nichts zu verbergen!“
- „Alles nur Panikmache.“

Wen interessiert es?

Freunde, Kollegen, (Ex-)Partner	Hohes Interesse
	Begrenzte techn. Möglichkeiten
Arbeitgeber/IT-Abteilung	Großes Interesse an Daten
	Umfangreiche techn. Möglichkeiten
Firmen-Konkurrenz	Großes Interesse an Daten(schatz)
	Unterschiedliche Ressourcen und techn. Möglichkeiten
IT-Dienstleister, Provider, Cloud-Betreiber	Wenig Interesse über erforderliche Daten hinaus
	Umfangreiche techn. Möglichkeiten
IT-Hersteller (Hardware/Software)	Wachsendes Interesse an Daten bei Softwareherstellern, geringes Interesse bei Hardwareherstellern
	Umfangreiche techn. Möglichkeiten
Social Web	Sehr großes Interesse an Daten
	Umfangreiche techn. Möglichkeiten
Nachrichtendienste	Hohes Interesse an Daten
	Nahezu unbegrenzte Ressourcen

Kann man etwas dagegen tun?

Freunde, Kollegen, (Ex-)Partner	Hohes Interesse Begrenzte techn. Möglichkeiten	**verschlüsseln**
Arbeitgeber/IT-Abteilung	Großes Interesse an Daten Umfangreiche techn. Möglichkeiten	**verschlüsseln**
Firmen-Konkurrenz	großes Interesse an Daten(schatz) Unterschiedliche Ressourcen und techn. Möglichkeiten	**verschlüsseln** **anonymisieren**
IT-Dienstleister, Provider, Cloud-Betreiber	Wenig Interesse über erforderliche Daten hinaus Umfangreiche techn. Möglichkeiten	**verschlüsseln** **anonymisieren**
IT-Hersteller (Hardware/Software)	Wachsendes Interesse an Daten bei Softwareherstellern, geringes Interesse bei Hardwareherstellern Umfangreiche techn. Möglichkeiten	**Voreinstellungen ändern**
Social Web	Sehr großes Interesse an Daten Umfangreiche techn. Möglichkeiten	**verschlüsseln** **Voreinstellungen ändern**
Nachrichtendienste	Hohes Interesse an Daten Kaum begrenzte Ressourcen	**verschlüsseln** **anonymisieren**

Warum sind Verschlüsselung und Anonymisierung so wenig verbreitet?

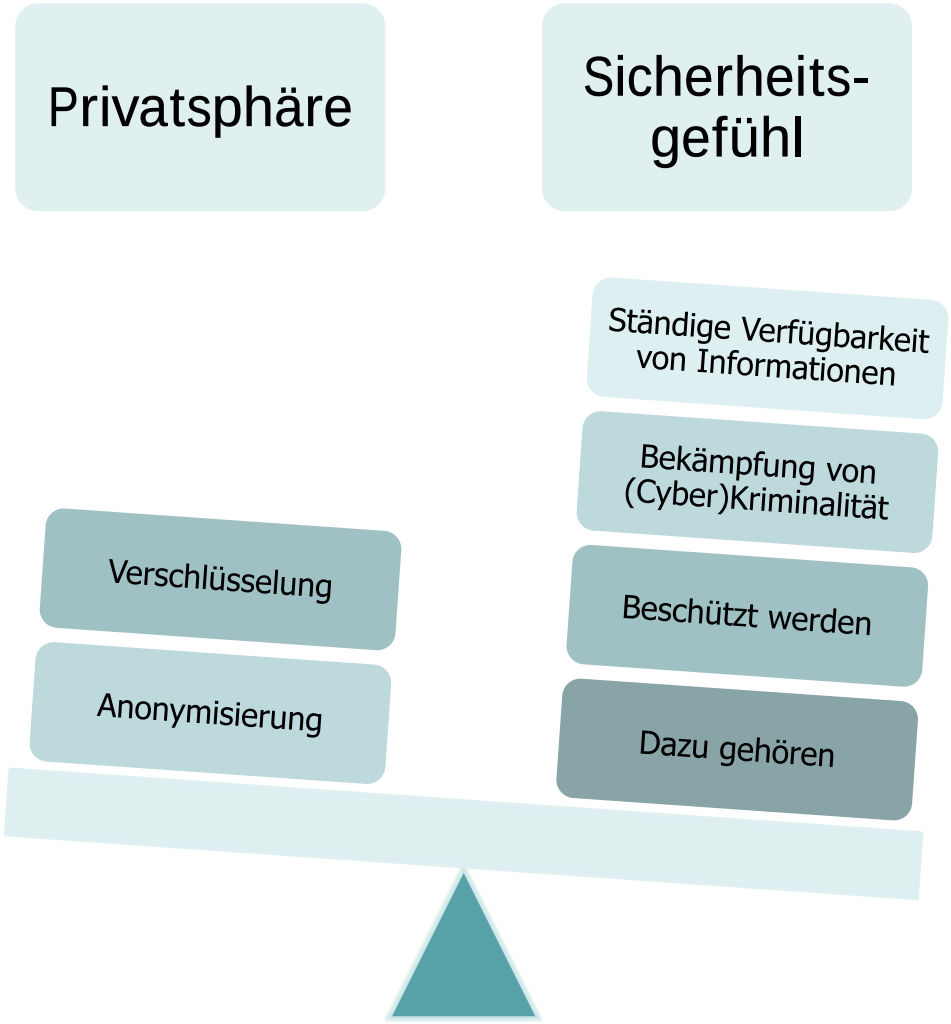
- Informationsflut überfordert: Security Fatigue
- Berichterstattung meist in negativem Zusammenhang, z.B. Terrorabwehr und Cyberkriminalität: Framing
- Angebot/Nachfrage und Sozialer Druck: Captology
- Unzureichendes Wissen durch asynchrone Entwicklung: Medienkompetenz

Framing bedeutet

- Framing = Einbettung von Fakten in gedankliche Deutungsrahmen
- Das Gehirn greift automatisch auf den vorhandenen Erfahrungsschatz zurück
- Erfahrungen mit einem Begriff färben das Verständnis eines Kontextes mit ein

Quelle: Wehling, Elisabeth: Politisches Framing, Bonn 2017.

Framing


Privatsphäre
Sicherheits-gefühl
Ständige Verfügbarkeit von Informationen
Bekämpfung von (Cyber)Kriminalität
Beschützt werden
Dazu gehören
Verschlüsselung
Anonymisierung

Aktuelle „Pannen“

- 2017 Equifax
- 2016 ARD-Recherchen zum Tracking von Browserverläufen von Millionen Bürgern
- 2015 Cyber-Angriff auf den Bundestag

Paranoia

- *Framing* bremst die Verwendung von sinnvollen Werkzeugen aus

- Vorurteile gegen Anonymisierungsdienste wie TOR-Browser
  - Darknet und TOR werden synonym verwendet
  - Verschlüsselung wird mit Verschwörungstheoretikern in Verbindung gebracht
  - Verwendung solcher Werkzeuge gelingt nur „Computer nerds“

„Paranoia“

- In vielen Bereichen gehen Privatsphäre und Sicherheit Hand in Hand
- Niemand würde die getroffenen Maßnahmen als übertrieben ansehen

Privatsphäre und Sicherheit

- Kameras erkennen keinen Sprengstoff, Spürhunde schon.
- Ihre Bank hängt ihre Kontoauszüge öffentlich aus.
- Ihr Arzt versendet Ihre Unterlagen versehentlich an die falsche E-Mail-Adresse.
- Ihre Steuerunterlagen werden an Ihre Nachbarn oder an Ihren Ex-Partner versendet.
- Details aus Ihrem Liebesleben werden in der Zeitung abgedruckt.

Brauchen wir noch Privatsphäre?

Quelle: https://commons.wikimedia.org/wiki/File:Naked_in_the_streets_-_American_censured.jpg

Brauchen wir noch Privatsphäre?

Wenn die Mehrheit **auf Privatsphäre verzichtet** – müssen dann alle darauf verzichten?

Kann durch ein **Verhalten einer Mehrheit** eine **Regel für alle** geschaffen werden?

Die **Normative Kraft des Faktischen** - Georg Jellinek


Quelle: https://de.wikipedia.org/wiki/Georg_Jellinek

Anonymität ist notwendig

Onlineberatung des WEISSEN RINGS

Sie oder eine Person aus Ihrem Umfeld sind von einer Straftat betroffen? Sie wurden Zeuge einer Straftat? Die Onlineberatung des WEISSEN RINGS unterstützt Sie gerne!

Die Onlineberatung ist anonym, kostenfrei und bundesweit erreichbar. Alle Daten werden auf einem externen Server verschlüsselt gespeichert und absolut vertraulich behandelt.

Bitte beachten Sie: In aller Regel erhalten Sie auf Ihre erste Anfrage innerhalb von 72 Stunden eine persönliche Antwort. Sollten Sie schnell und direkt Hilfe benötigen, wenden Sie sich bitte an eine unserer 420 Außenstellen oder an unser kostenfreies und bundesweit erreichbares Opfer-Telefon unter 116 006.

Weitere Informationen finden Sie in unseren häufig gestellten Fragen sowie unter Nutzungsbedingungen und Datenschutz.

Quelle: http://weisser-ring.de/hilfe/onlineberatung

Wie funktioniert die Onlineberatung?

Über uns

Nutzungsbedingungen und Datenschutz

Anonymität ist notwendig

kein täter werden.

Kostenlose Therapie unter Schweigepflicht

Aktuelles | Über uns | Hintergrund | Die Therapie | Erfahrungsberichte | Medien

Quelle: https://www.kein-taeter-werden.de

lieben sie kinder mehr, als ihnen lieb ist?

Das Präventionsnetzwerk bietet ein an allen Standorten kostenloses und durch die Schweigepflicht geschütztes Behandlungsangebot für Menschen, die sich sexuell zu Kindern hingezogen fühlen und deshalb therapeutische Hilfe suchen.

Im Rahmen der Therapie erhalten die betroffenen Personen Unterstützung, um mit ihrer pädophilen oder hebephilen Neigung leben zu lernen, diese zu akzeptieren und in ihr Selbstbild zu integrieren.

Ziel ist es, sexuelle Übergriffe durch direkten körperlichen Kontakt oder indirekt durch den Konsum oder die Herstellung von Missbrauchsabbildungen im Internet (sogenannte Kinderpornografie) zu verhindern.

Und der Durchschnittsbürger?

- „Ich habe doch nichts zu verbergen.“

- Andere dürfen alles über Sie wissen? – Glauben Sie, dass andere
  ... immer richtig liegen, wenn sie Sie beurteilen?
  ... immer gerecht sind?
  ... niemals eigene Interessen verfolgen?
  ... Informationen über Sie niemals zu Ihrem Nachteil verwenden?

- Können Sie wirklich alles, was Sie tun, so gut erklären, dass jeder das richtig findet?

  Haben Sie immer Zeit und Geduld, jedem alles zu erklären?

  Sollte man das müssen?

Informationelle Selbstbestimmung ist ein Grundrecht

Volkszählungsurteil des Bundesverfassungsgerichts (15. Dezember 1983)

- „Im Mittelpunkt der grundgesetzlichen Ordnung stehen Wert und Würde der Person, die in **freier Selbstbestimmung** als Glied einer freien Gesellschaft wirkt.“
- Aus dem Gedanken der Selbstbestimmung folgt die Befugnis des Einzelnen, **grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen** persönliche Lebenssachverhalte **offenbart** werden“.

Informationelle Selbstbestimmung ist ein Grundrecht

Volkszählungsurteil des Bundesverfassungsgerichts (15. Dezember 1983)

- „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. **Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert** und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, **wird versuchen, nicht durch solche Verhaltensweisen aufzufallen**."

- „...**kann** in seiner Freiheit wesentlich **gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden**."

Informationelle Selbstbestimmung ist nötig für die Demokratie

Informationelle Selbstbestimmung ist nötig für die Demokratie

Volkszählungsurteil des Bundesverfassungsgerichts (15. Dezember 1983)

„Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil **Selbstbestimmung** eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und **Mitwirkungsfähigkeit seiner Bürger** begründeten freiheitlichen **demokratischen Gemeinwesens** ist.“

Informationelle Selbstbestimmung ist nötig für die Demokratie

Nur wer informiert ist, kann sich eine politische Meinung bilden.

- Gibt es dafür „gute“ oder „schlechte“ Medien?
- Was denkt man über einen Leser von ...
  - der BILD
  - der taz
  - die „National-Zeitung“, anderen linken oder rechten Zeitungen

Information muss grundsätzlich aus jeder Quelle möglich sein.

- Zeitungskauf ist anonym möglich
- Auch Internetseiten sollen anonym nutzbar sein

Informationelle Selbstbestimmung ist nötig für die Demokratie

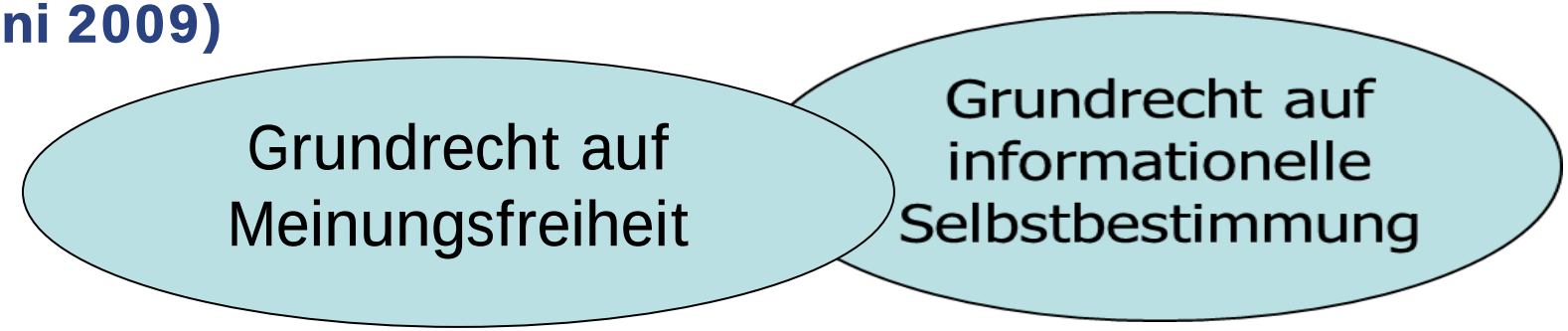
Quelle: https://www.1843magazine.com/features/the-scientists-who-make-apps-addictive

Je besser andere uns kennen, desto besser wissen sie, welche Informationen wir sehen wollen. Oder sollen.

„Microtargeting“:
Nutzer werden nach Alter, Geschlecht, Einstellungen etc. in Kategorien einsortiert.
Diese Daten werden für zielgruppengerechte Beeinflussung genutzt – und weiterverkauft.

Informationelle Selbstbestimmung ist nötig für die Demokratie

„spickmich.de“-Urteil des Bundesgerichtshofs (23. Juni 2009)



- Das Grundrecht auf **Meinungsfreiheit** umfasst auch **anonyme Äußerungen!**

- Die Meinungsfreiheit soll Selbstzensur verhindern:

  Wäre man verpflichtet, seinen Namen zu nennen, bestünde die **Gefahr**, dass Einzelne aus **Furcht vor Repressalien** ihre Meinung gar nicht äußern.

Informationelle Selbstbestimmung ist nötig für die Demokratie

- Auch Demokratien geraten in Gefahr (USA, Türkei).
- Aufdecken von Missständen durch Whistleblower.
- Politische Teilhabe und Minderheitenschutz:

  „Gesellschaftlich marginalisierte Gruppen, die im öffentlichen Diskurs höchstens als Streitgegenstand auftreten, können sich durch Verschleierung ihres wahren Ichs Diskursraum verschaffen.“

  Nik Afanasiew
- Kinder und Jugendliche: Citizenship lernen.

Das Internet vergisst nicht!

Recht auf Anonymität

Datenschutz im deutschen Recht und Europarecht

a) grundrechtliche Verankerung

Grundgesetz, Grundrechtecharta, Europäische Menschenrechtskonvention, Vertrag über die Arbeitsweise der Europäischen Union

b) europäische Normierungen

Datenschutz-Grundverordnung -> Data-Protection-by-Design

(bis Mai 2018 Datenschutzrichtlinie)

c) einfachgesetzliche Umsetzung

Bundesdatenschutzgesetz, Landesdatenschutzgesetze und Spezialgesetze (TMG, TKG, SGB)

Grundrechte – nur auf dem Papier?

- Die Snowden-Enthüllungen legen nahe, dass der Internetverkehr weltweit umfassend überwacht und gespeichert – auch der von deutschen Bürgern.
- Die Überwachung verletzt die Grundrechte deutscher Bürger.
- Pflicht des Staates, Grundrechte seiner Bürger zu schützen.

Wie funktioniert Verschlüsselung?

- 1. Schritt: Verschlüsselte Mails **empfangen** können
  - Ihr öffentlicher Schlüssel ermöglicht Ihren Kontakten, verschlüsselte E-Mails an Sie zu schicken
  - Ihr privater Schlüssel ermöglicht Ihnen, die verschlüsselte Nachricht zu lesen

- 2. Schritt: Verschlüsselte Mails **senden**
  - Wenn Sie jemandem eine (verschlüsselte) Mail senden, können Sie Ihren öffentlichen Schlüssel als Anhang beifügen

Wie funktioniert Verschlüsselung?

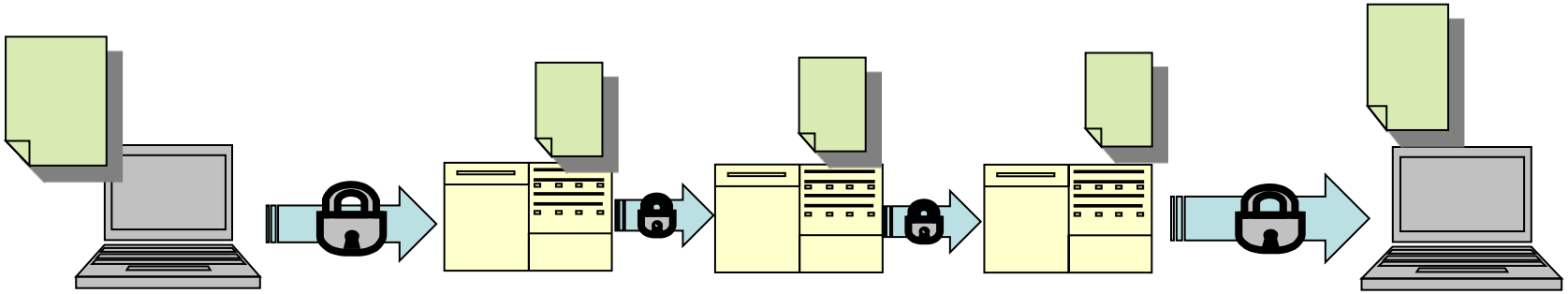
- Verschlüsseln:
  - **Verschlüsselung** (auch: **Chiffrierung**) ist die von einem Schlüssel abhängige Umwandlung von „Klartext“ genannten Daten in einen „Geheimtext“(auch: „Chiffrat“), so dass der Klartext aus dem Geheimtext nur unter Verwendung eines geheimen Schlüssels wiedergewonnen werden kann.
    Quelle: https://de.wikipedia.org/wiki/Verschl%C3%BCsselung

- Methoden sind z.B.:
  - Verstecken **K**alle **a**rbeitet **t**äglich **z**wei **E**inheiten**!**

  (immer der 1. Buchstabe) -> Katze!
  - Austauschen 3537 (3=E, 5=S, 7=L) -> ESEL

E-Mail heute

- E-Mail heute (unverschlüsselt)

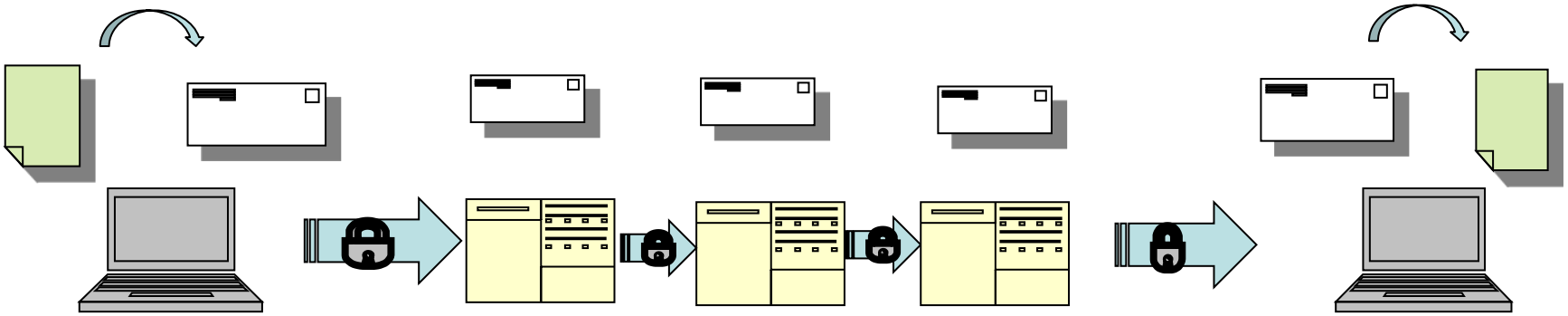


Verfasser Server Empfänger

- Unverschlüsselte Inhalte sind schlicht günstige Gelegenheiten für jeden „Angreifer“

Das Prinzip der E-Mail-Verschlüsselung

- E-Mail verschlüsselt



- E-Mail-Verschlüsselung ist ein elektronischer Briefumschlag
- E-Mail-Verschlüsselung schützt vor Kenntnisnahme Dritter

Wie funktioniert Verschlüsselung?

- Symmetrische Verschlüsselung (der Klassiker)
  - Sender und Empfänger der Botschaft müssen den geheimen Schlüssel kennen.
    - Immer der 1. Buchstabe oder (3=E, 5=S, 7=L)

- Schwachstellen der symmetrischen Verschlüsselung
  1. Um geheim zu kommunizieren, muss man vorher vertraulich kommunizieren können.
  2. Wird der Schlüssel einem Dritten bekannt, kann dieser ebenfalls die Botschaft decodieren.
  3. Mit jedem neuen Gesprächspartner muss wieder ein neuer Schlüssel getauscht werden.

Wie funktioniert Verschlüsselung?

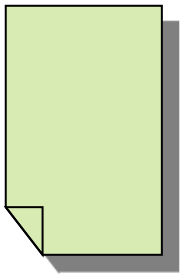
- Asymmetrische Verschlüsselung
  - Der Empfänger stellt einen öffentlichen Schlüssel für alle bereit
  - Der Empfänger besitzt einen zweiten, geheimen Schlüssel

- Die 3 genannten Schwachstellen der symmetrischen Verschlüsselung sind hier nicht mehr von Bedeutung

Wie funktioniert Verschlüsselung?

- Mit dem öffentlichen Schlüssel lässt sich nur **VER**schlüsseln

-> Jeder darf und soll den Schlüssel kennen



öffentlicher Schlüssel

Quelle Cliparts: Libre Office Writer Version: 5.1.5.2

Wie funktioniert Verschlüsselung?

- Zum **ENT**schlüsseln wird der private Schlüssel gebraucht

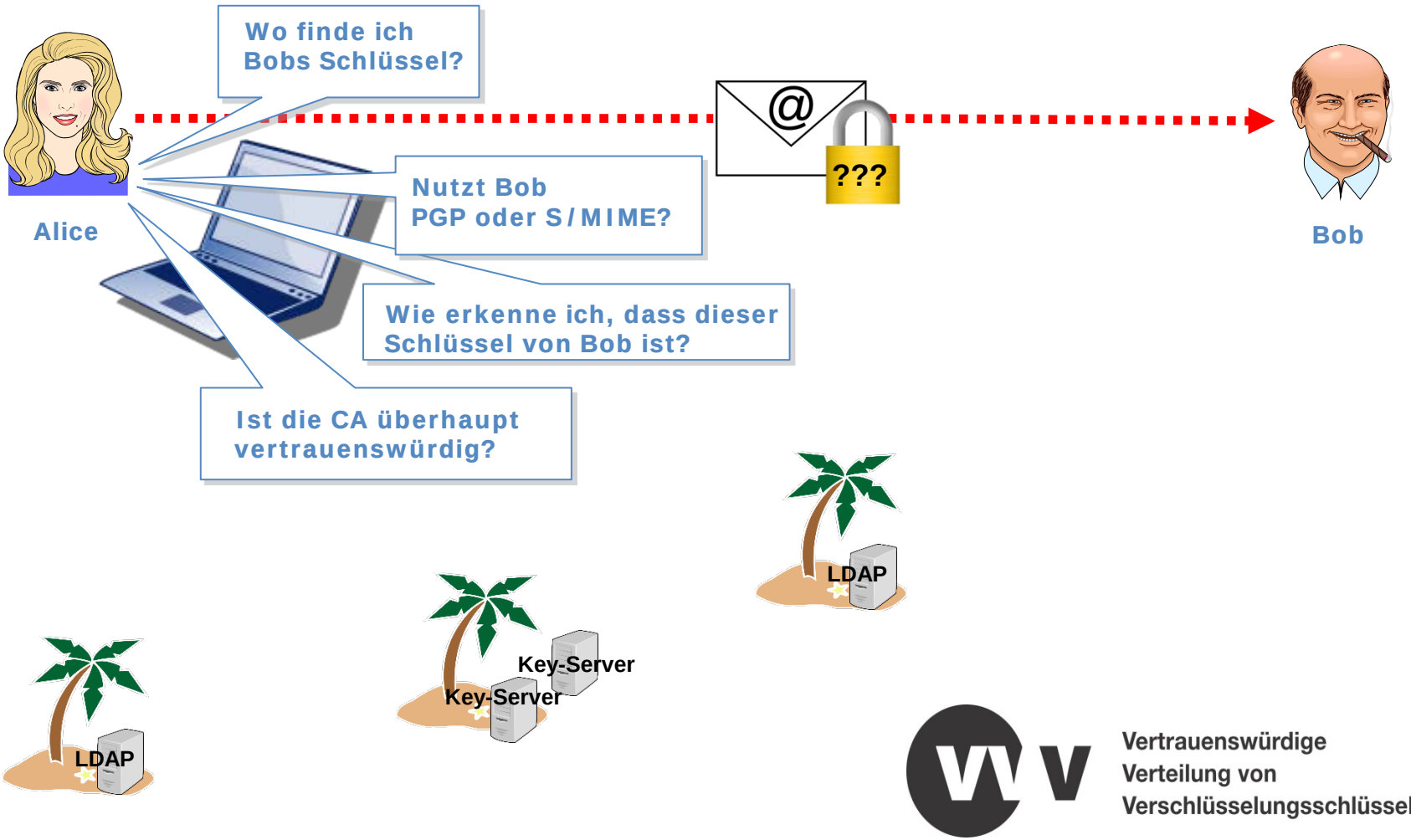
-> Nur Sie dürfen diesen Schlüssel kennen

öffentlicher Schlüssel

privater Schlüssel (geheim)

Quelle Cliparts: Libre Office Writer Version: 5.1.5.2

Ausgangslage: Alice ist ratlos ...



Warum verwenden nur wenige Ende-zu-Ende-Verschlüsselung?

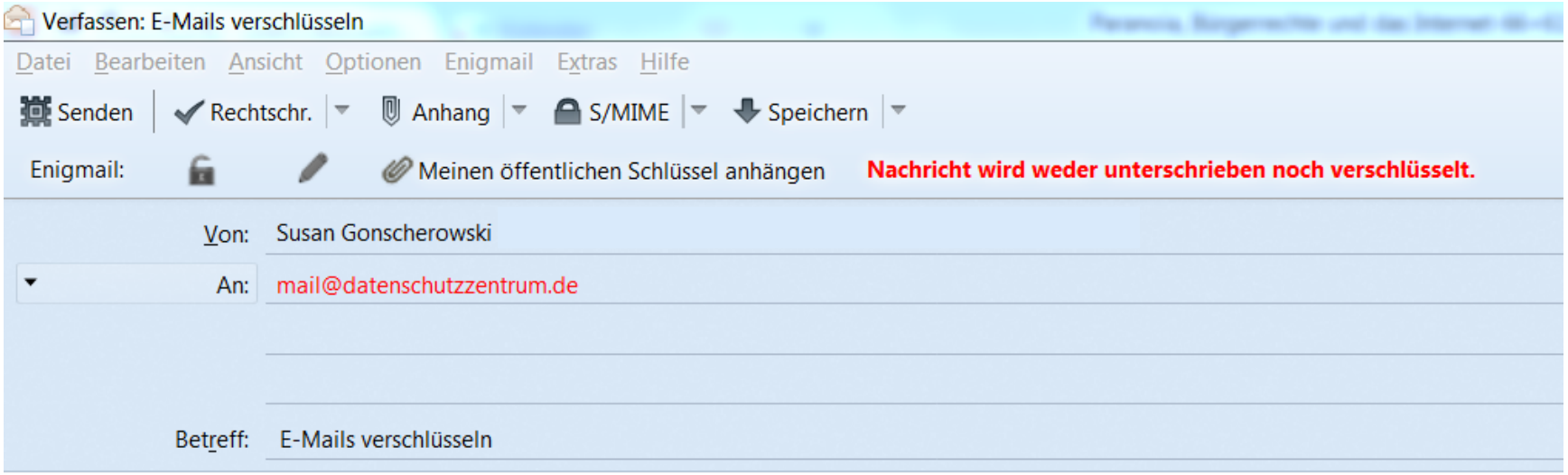
- GPG und S/MIME sind nicht interoperabel
- Es ist nicht ersichtlich, ob und wenn ja, welche Verschlüsselung vom Kommunikationspartner verwendet wird
- Dem Nutzer ist oft nicht klar, wo die öffentlichen Schlüssel zu finden sind
- Nutzer wissen oft nicht, wo sie eigene Schlüssel bekommen
- Vorhandene Tools sind schwer zu verstehen, wenn das Prinzip dahinter nicht verstanden wurde

2 Möglichkeiten, 1 Prinzip: GPG und S/MIME

- Hauptunterschied der beiden Verfahren ist das unterschiedliche Vertrauensmodell

- GPG – Web of Trust:
  - Die Nutzer bestätigen einander, dass sie dem öffentlichen Schlüssel des anderen vertrauen

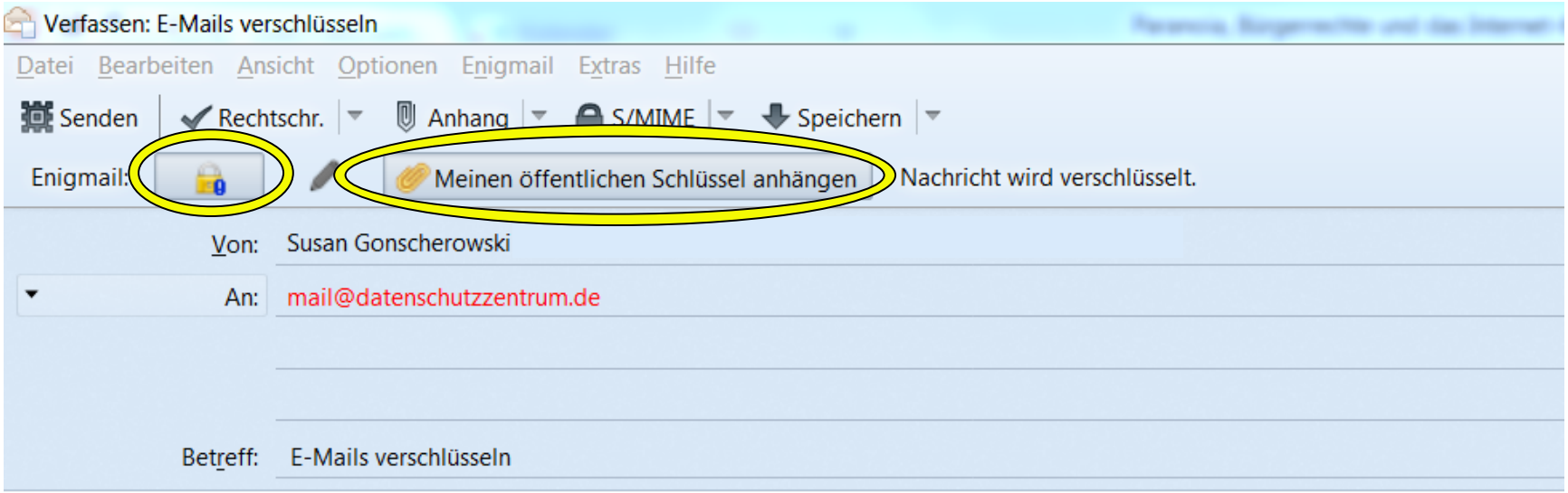
- S/MIME – Certificate Authority (Zertifizierungsstelle):
  - Eine Agentur prüft die Zugehörigkeit eines Schlüssels zu einer Mail-Adresse/Person und bestätigt dies



E-Mails verschlüsseln ist kinderleicht!

Beste Grüße

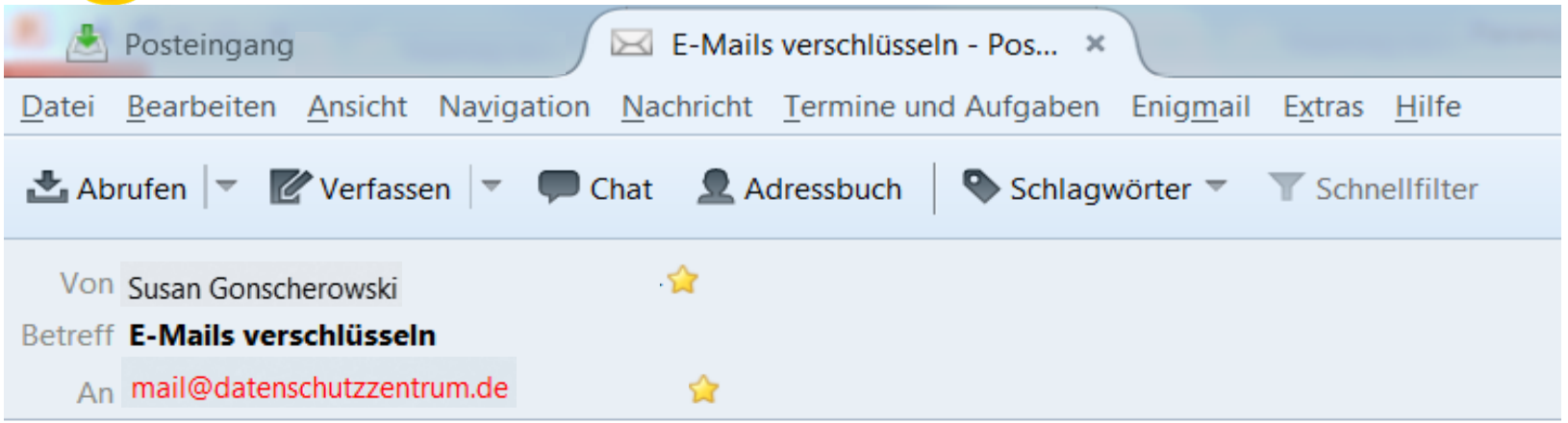
Das ULD

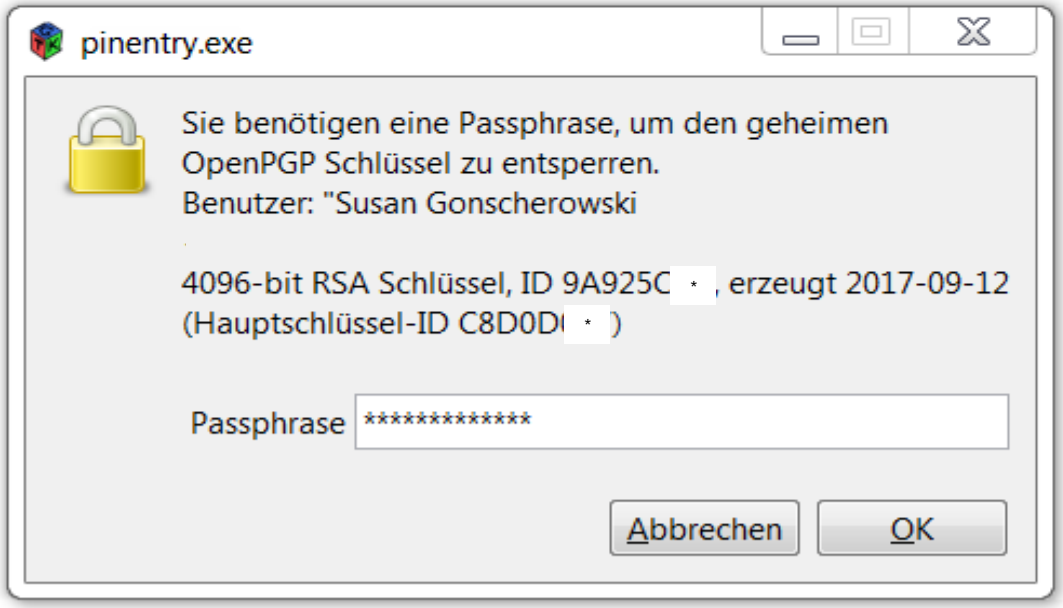


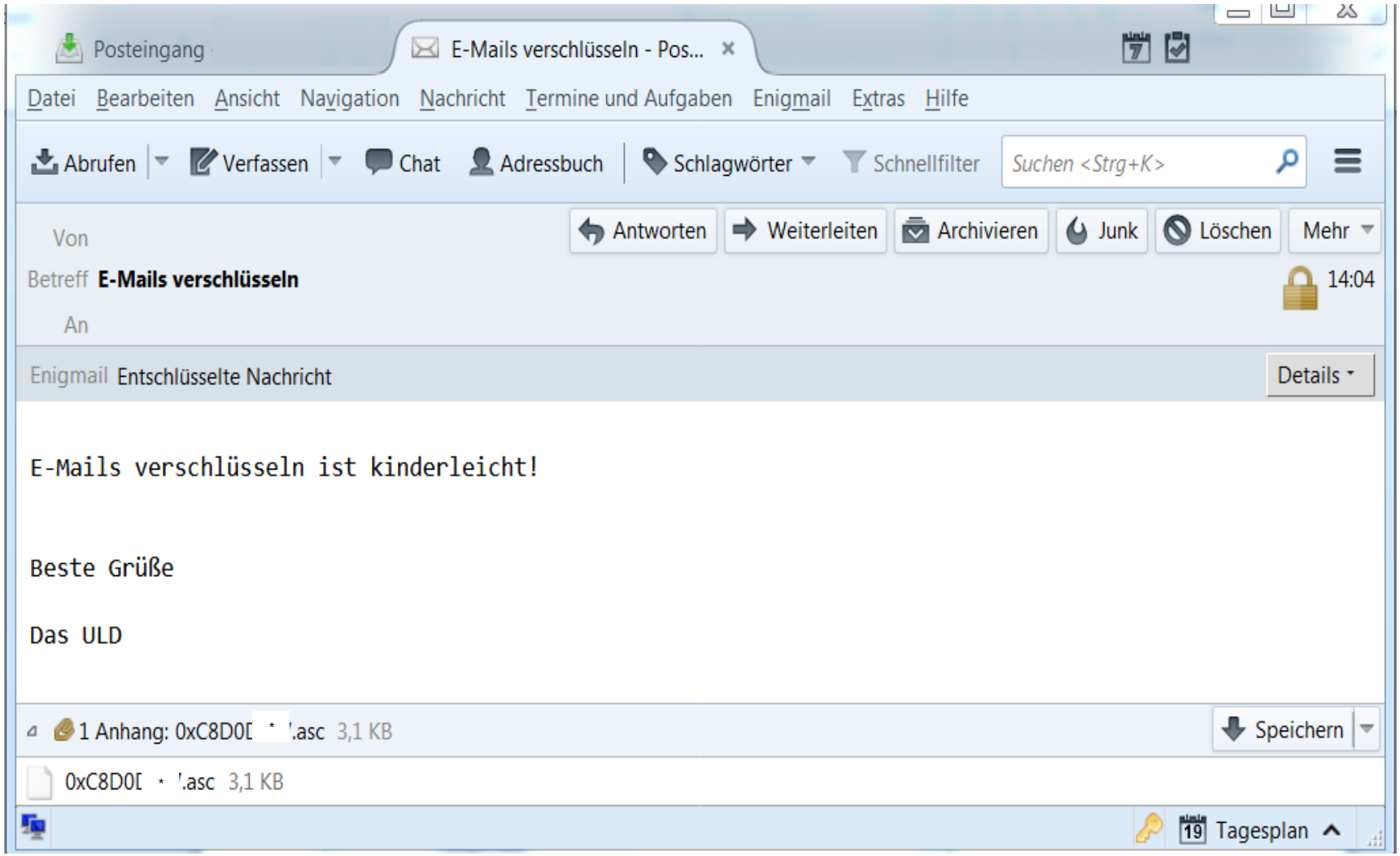
E-Mails verschlüsseln ist kinderleicht!

Beste Grüße

Das ULD


Posteingang
E-Mails verschlüsseln - Pos...
Datei Bearbeiten Ansicht Navigation Nachricht Termine und Aufgaben Enigmail Extras Hilfe
Abrufen Verfassen Chat Adressbuch Schlagwörter Schnellfilter
Von Susan Gonscherowski
Betreff E-Mails verschlüsseln
An mail@datenschutzzentrum.de


pinentry.exe
Sie benötigen eine Passphrase, um den geheimen OpenPGP Schlüssel zu entsperren.
Benutzer: "Susan Gonscherowski
4096-bit RSA Schlüssel, ID 9A925C * , erzeugt 2017-09-12
(Hauptschlüssel-ID C8D0D *)
Passphrase **********
Abbrechen
OK


Posteingang
E-Mails verschlüsseln - Pos...
Datei Bearbeiten Ansicht Navigation Nachricht Termine und Aufgaben Enigmail Extras Hilfe
Abrufen Verfassen Chat Adressbuch Schlagwörter Schnellfilter Suchen <Strg+K>
Antworten Weiterleiten Archivieren Junk Löschen Mehr
Von
Betreff E-Mails verschlüsseln
14:04
An
Enigmail Entschlüsselte Nachricht
Details
E-Mails verschlüsseln ist kinderleicht!
Beste Grüße
Das ULD
1 Anhang: 0xC8D0[* '.asc 3,1 KB
Speichern
0xC8D0[* '.asc 3,1 KB
Tagesplan

Wie funktioniert Verschlüsselung?

- Öffentlicher Schlüssel des ULD:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQSuBFXe+LkRDACqYurI1BcXZiYeP96K/fLomhYu4Ry4ihZf/8I+v89b9NIr5g/k
CXWmjTjTRr45pHhBUPD4X8CNqI+oEzv4FeVLWPbFsaYzF3nDI3O9xJl8wT9ewZ9g
4TqEKxxAkXr3V9NXGPFedSrLydqIcMbe0ydP7S7lvndHnfw3zczEo07YEnB3N4IN
pnUl8n0m1JEqmWyaB4EBkpJiX4rxTE2bCdTfeaJsozUWH/kyOHKw89eJyJ91teLO
D5/9X4LsSGdwOwNrjDSzt1EaeFIjpswcYjeUdNnAbQ/VmwOSc60pN+8UVl6A2Nfx
jtj8frR4Dkd9FEUrkEue7HKjU7ZB8lLavVNrbr1481l3VipxPuu5cuNrzLXfi2lR
tGcclGnSeVOPq2oFezCM/egvJAYf0RZ5u3gc61uvH/qAPamCLGqWZ6uYXM8EA5Qv
fWuW0oGM/OJdEBtC1bZJ1Qfe9DRhfnXZIINHjaVbLC4c6PfLuiYwnWsBWteYSQdl
LhGui0HuAUdQZYsBAJkvBl3qxOUcgve0pUoUh4OVmzBbS38GgqnDpxTrByw5DACY
W6Lhfyk9VPmf+VKbIoQRob3V5MrOWIi+zOWi85laLKHn2StxSHQJBa1+S6EZ16Ov
m4wE+LKvJ7/beqq0VBNHi/vuhjzLozeHe+BeXM9cLXzSU0TQXQxqa8A4J1bwikvb
OLFTgI/2LKn5zylyeljJUNRmgQMsITqaQbHlw8jw7LT/3mVplHT+wWxRQ+RZcOQZ
qbI+SF3TlgLj4kf0ZA8muYbfUAc2PlythbVsdk8KTXJK3u5v/0bvvPjtPxkzCsmW
l7XsaF+MKkczhin9fw9IofwNnkGsYR4YYJSuBtXJs+6jyhAUH4vqKusNC/Tt6PjR
3QX+e6A0o+c6XVKoaJzG3kTDghsbYJxDOqPKDj6SzlZUURQQ65MUSxBKN0De8Qmm
Pgy7N1sPD9MCet338/rMWFYH6lq74gK8J7SO/tzA/OyWEWTaig5tdwkV7PU+Rx2m
0l5LX0cDXVPSNxwZ7NjQohvu6bmJ4QD6yw1j0n3DlJbcaYvZOkbb+UXjbLuJsMIL
/AmyLFz1FIUV8TESy/9AZmtihzxaP0Z1JuCIxOBqFOziPmrYRpkiifg1knptxIxa
GCvvY+czFpcHsLn1F5Y4hQzyTFZFdgV8UnlIZpWhMO6/NmEer13G15zO1QLSTPHx
aoRKGzwCtRTEJQ+nxwPIP73E+rGha0sOPwvT6zNi7d248RuVrpT8EsfScDn4W7So
4Odiwf6+Nv63BtMjEDlxURVpf6jTqVxrqWqGzR4boI06jqa4tZk6NLQEP91JgpRN
kchLpGsDzbw5Zu2ZyMtaBMq9HcwDlOxw8lTbL9t43TRUnE/y88eikXJ44bnzE39d
lvu/YmtIcwNYgs/tF5t+DuxLTmNqQbJp3487cRpy86EuubmXJT4fWnlE4W3dR2zS
vkG7eMNkOe4ru9YbL4NasNhUVGSeoryL9/xu3WVqTX7bLsFSljws2jDZXAe7JhBD
7sceS7auieC/HgPWFYDH8PGJ8dEmvn2PJfh/99MCdZz1h7o+bXqF13r6jevqmpBX
MbRcVW5hYmjDpG5naWdlcyBMYW5kZXN6ZW50cnVtIGbDvHIgRGF0ZW5zY2h1dHog
U2NobGVzd2lnLUhvbHN0ZWluIDxtYWlsQGRhdGVuc2NodXR6emVudHJ1bS5kZT6I
gwQTEQgAKwIbAwUJCWYBgAIeAQIXgAUCVd77RwkLCQgHAwQKAQIFFQoJCAIFFgID
AQAACgkQZtXAVZkcUGCFnAD+M9di8gCJGFBjcUTUnqdUO0ioC/KBk0egdiTFTnO9
MdYBAIN2i1SloEnHGRGg2pvahzCxq8EligdY75YckmMhM9xyiF4EExEIAAYFAlXe
/U0ACgkQDXUZnhE1cyT5OgD+JdVpiTRWywrPcpZXAKRK3P0KMBwtxS+9YHGaLgu1
eq8A/1In4txqzBPc0QlUdmY7Coit5t0k3vtlyGyKnsDJMwnsuQMNBFXe+LkQDADH
bYLO257CKI29UbfjP2Jw7uoSzMe5iO3ZcPRB1145iVdZkHNPXd0BfuWEEWlWOvl8
OitlgSS9ovzWQBizKJD4w2mXfcHlFtoE95Ei1MkdAYISuQ4mFi0CA7Ic7YHSBYGU
G+/95PC1+9A2ZX3VF2KDJ3WZ9ZZh8eygZvRqStE+OuFdqvtYYpqr9lN8tszAORAe
xeUp2tJbQyEnMg4KDdleSyVi8L1CvCCAkg5WAsxlEzrNNmC/ox66R+Q3ktMMfmJs
zGLh75DPFiko+ebNgkSDDr5kg4J/GUfcBHzXMcxalAOJxFb3O4VPhzOvvwCzoRFK
DRb/R8Ad+UTZ+HHVjgVEIpuRDUZncp9eSG+6AR07vMixXhLbdz7IuwsbiHDBN+dq
rL8RFVoxAXnWVWLvs74DVvY0pKcRc24Aj+eqpTPhfeQyccI0rvity5ll9kd6fwRL
U1qSDiTINkPxv212hm0JhSlvrT/VKE919ApzQpTDc+lo9RS6sRiBj/D3M8zIH8cA
AwUMAMYmYypKSeMlb7dc40r/OQ+tspXWRx2oGLtUhMp/J9C2/ZLULfT1C/4e/INr
XLWpq8DjOUo0v1xcEcII5SGq7yOLzQLgMJlFEMw3NRpRJ5YZoMJ9KFbG6vNoVxF9
CkFK0D9hJ91enI+nJePt3e0zl3J81JdnINQ363cN2q2uOospkXFHpjeFY2pmfRJO
vOKBtZF8dtUqNNSyj4pewizcDocrhtaR1MrERgZNNiQWBFScmkBKfgbktqLGaONR
9ltH2F+ElkJ4e2CILI/GcLALcuEeLZeBGSwWnKwPCYDumN+dikieY9nA725nTD7r
CmSqEI66a5WZPnG+d5lLPzAnTve7qNOQYLfVO5LLFgijOdyguIwsit/FcWZYIS2L
ZQndVUJneScUJ5C0WFT/rk+OKKz9r/swe1wl5s28tTkMX1Z8ALLo2fb5xHigO9U2
U5TGxoig5qisJToXvQ+HdQZQtmR1IMIICH7QEBf10YaFL4DzQIAbfAg0GHaRuG9O
mWfNAYhnBBgRCAAPBQJV3vi5AhsMBQkJZgGAAAoJEGbVwFWZHFBgtg0A/2GjtyAX
cHhSA28ZGSkhd4IrvGQnFNZD0ZF8I3O2UwZbAP9Wcq1wMEqL23g37ZF/ISTY1jPa
VgqKx0g1G8QYueDznw==
=1tKG
-----END PGP PUBLIC KEY BLOCK-----

Warum Ende-zu-Ende-Verschlüsselung?

- Unberechtigte Empfänger
- Provider: Der „Briefträger“ kann mitlesen
- Ermittlungsbehörden und Geheimdienste (auch von Drittstaaten) haben z.Z. fast unbegrenzten Zugang zu Daten
- Hacker haben es leichter

Darum Verschlüsselung!

- Mündige Bürger statt bevormundete Bürger – Sie sollen entscheiden, wann eine Nachricht persönlich und schützenswert ist

- Schützen und Nutzen Sie Ihre Grundrechte – Sie haben ein Recht auf „Geheimnisse“ (Brief, Telefon, Arzt, Anwalt, Geschäft/Unternehmen, Privatsphäre)

Datenschutzkonflikte im Internet

- Vieles findet online statt:
  - Mailen, Chatten, Videotelefonate
  - Suche nach Nachrichten, Produkten, Krankheitssymptomen
  - Musikstreaming, Internet-TV
- Diese Informationen sagen viel über uns aus:
  - Alter, Geschlecht, Wohnort, Zahlungsfähigkeit
  - Gewohnheiten, Vorlieben, Einstellungen
  - Kontakte, Persönlichkeit – Sorgen und Ängste
- ➢ Diese Informationen können andere nutzen:
  - Einstellungen und Verhalten beeinflussen (Konsum, Wahlen)
  - Zugang zu Angeboten (Versicherungen, Mietwohnungen, Kredite, Arbeitsplätze, Preisgestaltung bei Produkten) einschränken
- ➢ Sind wir noch autonom und selbstbestimmt?

Nutzer verfolgen und Daten verkaufen

- **Gezielte Auslieferung von Werbung (Targeting)**
  - Targeting ist profitabel und Kerngeschäft von Facebook, Google und diversen spezialisierten Tracking-Firmen als Zulieferer (z.B. Acxiom)
  - Konzernumsatz von Facebook im dritten Quartal 2016: 7 Mrd. $ (+56%) fast ausschließlich mit Vermarktung von Werbeplätzen = 2,4 Mrd. $ Reingewinn
- **Nutzerbeobachtung (Tracking)**

Targeting

Erreiche jeden Tag und überall die richtigen Nutzer, um mehr Besuche auf deiner Webseite zu generieren und die Online-Umsätze zu steigern.

Auf Facebook bezahlst du nur dafür, deine Werbeanzeigen genau auf die Nutzer auszurichten, mit denen du gerne eine Verbindung aufbauen möchtest. Die Auswahl der Zielgruppe für deine Werbeanzeigen hilft dir bei den folgenden Aktivitäten:

- Ansprechen der richtigen Kunden auf den verschiedenen Geräten, inklusive Computer, Handys und Tablets.
- Bereitstellen von relevanten Botschaften für bestimmte Nutzer.
- Optimale Wertausschöpfung deiner Ausgaben für Werbeanzeigen, indem du nur die Personen erreichst, die für dich wichtig sind.

https://de-de.facebook.com/business/a/online-sales/ad-targeting-details

Targeting

- ✓ Ort
- ✓ Alter
- ✓ Generation
- ✓ Geschlecht
- ✓ Sprache
- ✓ Bildungsniveau
- ✓ Ausbildungsbereich
- ✓ Schule
- ✓ ethnische Zugehörigkeit
- ✓ Einkommen und Eigenkapital
- ✓ Hausbesitz und -typ
- ✓ Hauswert
- ✓ Grundstücksgröße
- ✓ Hausgröße in Quadratmeter
- ✓ Jahr, in dem das Haus gebaut wurde
- ✓ Haushaltszusammensetzung
- ✓ Nutzer, die innerhalb von 30 Tagen ein Jubiläum haben
- ✓ Nutzer, die von der Familie oder Heimatstadt entfernt sind
- ✓ Nutzer die mit jemandem befreundet sind, der einen Jahrestag hat, frisch verheiratet oder verlobt ist, gerade umgezogen ist oder bald Geburtstag hat
- ✓ Nutzer in Fernbeziehungen
- ✓ Nutzer in neuen Beziehungen
- ✓ Nutzer mit neuen Jobs
- ✓ Nutzer, die frisch verlobt sind
- ✓ Nutzer, die frisch verheiratet sind
- ✓ Nutzer, die vor Kurzem umgezogen sind
- ✓ Nutzer, die bald Geburtstag haben
- ✓ Eltern
- ✓ Werdende Eltern
- ✓ Mütter in Typen unterteilt („Fußball, trendy" etc.)
- ✓ Nutzer, die sich wahrscheinlich politisch betätigen
- ✓ Konservative und Liberale
- ✓ Beziehungsstatus
- ✓ Arbeitgeber
- ✓ Branche
- ✓ Berufsbezeichnung
- ✓ Art des Büros
- ✓ Interessen
- ✓ Nutzer, die ein Motorrad besitzen
- ✓ Nutzer, die planen, ein Auto zu kaufen (welche Art/Marke, und wann)
- ✓ Nutzer, die kürzlich Autoteile oder Zubehör gekauft haben
- ✓ Nutzer die wahrscheinlich Autoteile oder Service benötigen
- ✓ Art und Marke des Autos, dass man fährt
- ✓ Jahr, in dem das Auto gekauft wurde
- ✓ Alter des Autos
- ✓ Wieviel Geld der Nutzer vermutlich für sein nächstes Auto ausgeben wird
- ✓ Wo der Nutzer vermutlich sein nächstes Auto kaufen wird
- ✓ Wieviele Mitarbeiter die eigene Firma hat
- ✓ Nutzer, die kleine Unternehmen haben
- ✓ Nutzer, die Manager oder Führungskräfte sind
- ✓ Nutzer, die für wohltätige Zwecke gespendet haben (unterteilt nach Art)
- ✓ Betriebssystem
- ✓ Nutzer, die Browserspiele spielen
- ✓ Nutzer, die eine Spielekonsole besitzen
- ✓ Nutzer, die eine Facebook-Veranstaltung erstellt haben
- ✓ Nutzer, die Facebook-Payments benutzt haben
- ✓ Nutzer, die mehr als üblich per Facebook-Payments ausgegeben haben
- ✓ Nutzer, die Administrator einer Facebookseite sind
- ✓ Nutzer, die vor Kurzem ein Foto auf Facebook hochgeladen haben
- ✓ Internetbrowser
- ✓ Emailanbieter
- ✓ „Early Adopters" und „late Adopters" von Technologien
- ✓ Auswanderer (sortiert nach dem Ursprungsland)
- ✓ Nutzer, die einer Genossenschaftsbank, einer nationalen oder regionalen Bank angehören
- ✓ Nutzer, die Investoren sind (sortiert nach Typ der Investition)
- ✓ Anzahl der Kredite
- ✓ Nutzer, die aktiv eine Kreditkarte benutzen
- ✓ Typ der Kreditkarte
- ✓ Nutzer, die eine Lastschriftkarte haben
- ✓ Nutzer, die Guthaben auf der Kreditkarte haben
- ✓ Nutzer, die Radio hören
- ✓ Bevorzugte TV-Shows
- ✓ Nutzer, die ein mobiles Gerät benutzen (nach Marke aufgeteilt)
- ✓ Art der Internetverbindung
- ✓ Nutzer, die kürzlich ein Tablet oder Smartphone gekauft haben
- ✓ Nutzer, die das Internet mit einem Smartphone oder einem Tablet benutzen
- ✓ Nutzer, die Coupons benutzen
- ✓ Arten von Kleidung, die der Haushalt des Nutzers kauft
- ✓ Die Zeit im Jahr, in der der Haushalt des Nutzers am meisten einkauft
- ✓ Nutzer, die „sehr viel" Bier, Wein oder Spirituosen kaufen
- ✓ Nutzer, die Lebensmittel einkaufen (und welche Art)
- ✓ Nutzer, die Kosmetikprodukte kaufen
- ✓ Nutzer, die Medikamente gegen Allergien und Schnupfen/Grippe, Schmerzmittel und andere nicht-verschreibungspflichtige Arzneimittel einkaufen
- ✓ Nutzer, die Geld für Haushaltsgegenstände ausgeben
- ✓ Nutzer, die Geld für Produkte für Kinder oder Haustiere ausgeben (und welche Art von Haustier)
- ✓ Nutzer, deren Haushalt mehr als üblich einkauft
- ✓ Nutzer, die dazu neigen online (oder offline) einzukaufen
- ✓ Arten von Restaurants, in denen der Nutzer isst
- ✓ Arten von Läden, in denen der Nutzer einkauft
- ✓ Nutzer, die „empfänglich" für Angebote von Firmen sind, die Online-Autoversicherungen, Hochschulbildung oder Hypotheken, Prepaid-Debitkarten und Satellitenfernsehen anbieten
- ✓ Wie lange der Nutzer sein Haus bereits bewohnt
- ✓ Nutzer, die wahrscheinlich bald umziehen
- ✓ Nutzer, die sich für Olympische Spiele, Cricket oder Ramadan interessieren
- ✓ Nutzer, die häufig verreisen (geschäftlich oder privat)
- ✓ Nutzer, die zur Arbeit pendeln
- ✓ Welche Art von Urlaub der Nutzer bucht
- ✓ Nutzer, die kürzlich von einem Ausflug zurückkommen
- ✓ Nutzer, die kürzlich eine Reise-App benutzt haben
- ✓ Nutzer, die ein Ferienwohnrecht haben

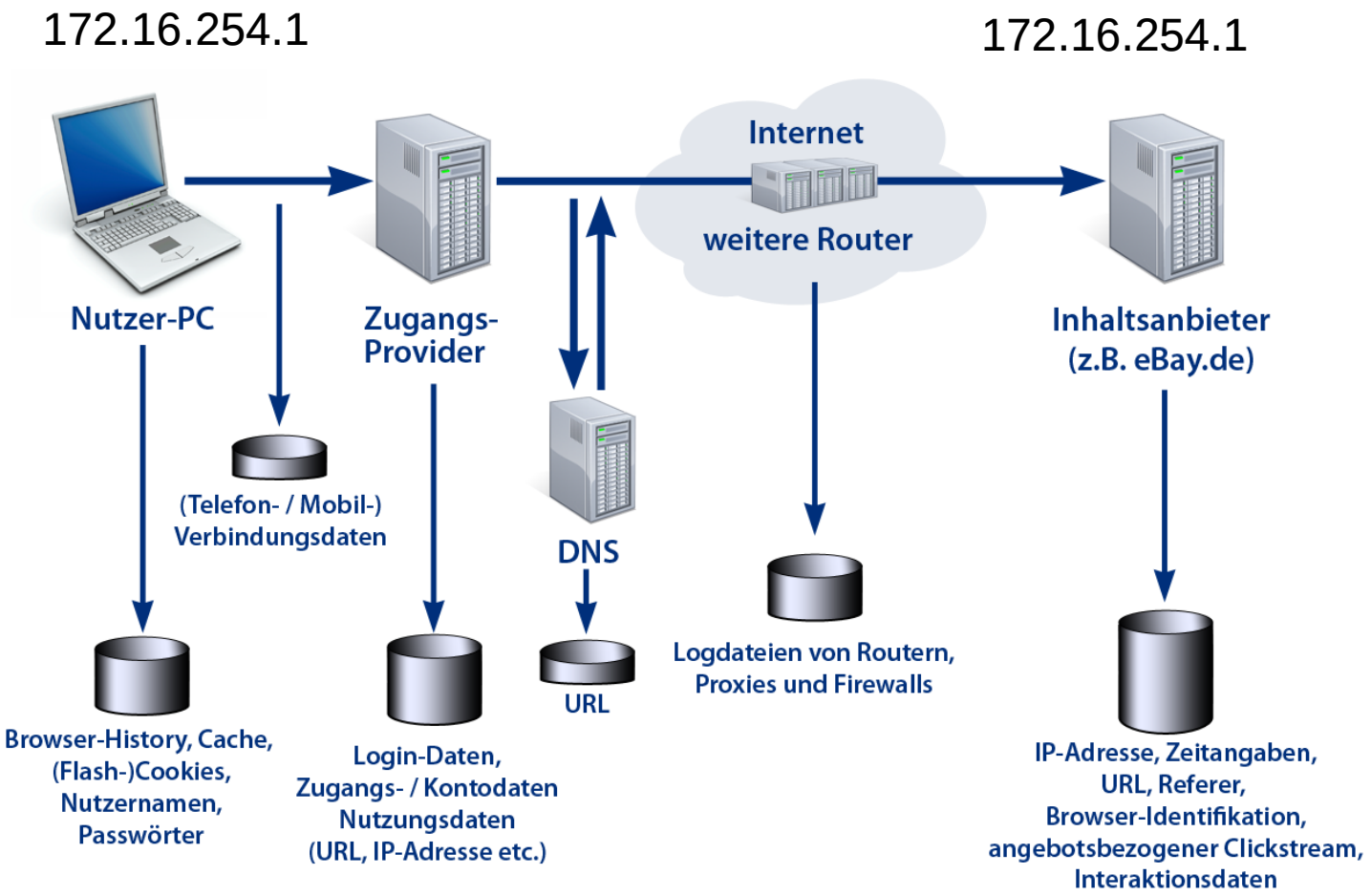
Quelle: https://comidio.de/wp-content/uploads/2016/10/Comidio-TrutzBox-Kompendium_v4-70-1.pdf, mit Verweis auf: https://netzpolitik.org/2016/98-daten-die-facebook-ueber-dich-weiss-und-nutzt-um-werbung-auf-dich-zuzuschneiden/, Originalauswertung: https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/

Targeting

- Personengenaue Profile (egal an welchem Endgerät) Einteilung in Kategorien für Werbetreibende wie z.B.
  - Soccer and SUVs
  - Apple Pie Families
  - Shooting Star
  - Tots and Toys
  - **“Waste”**
- Diskriminierung möglich (rassische u.a.)

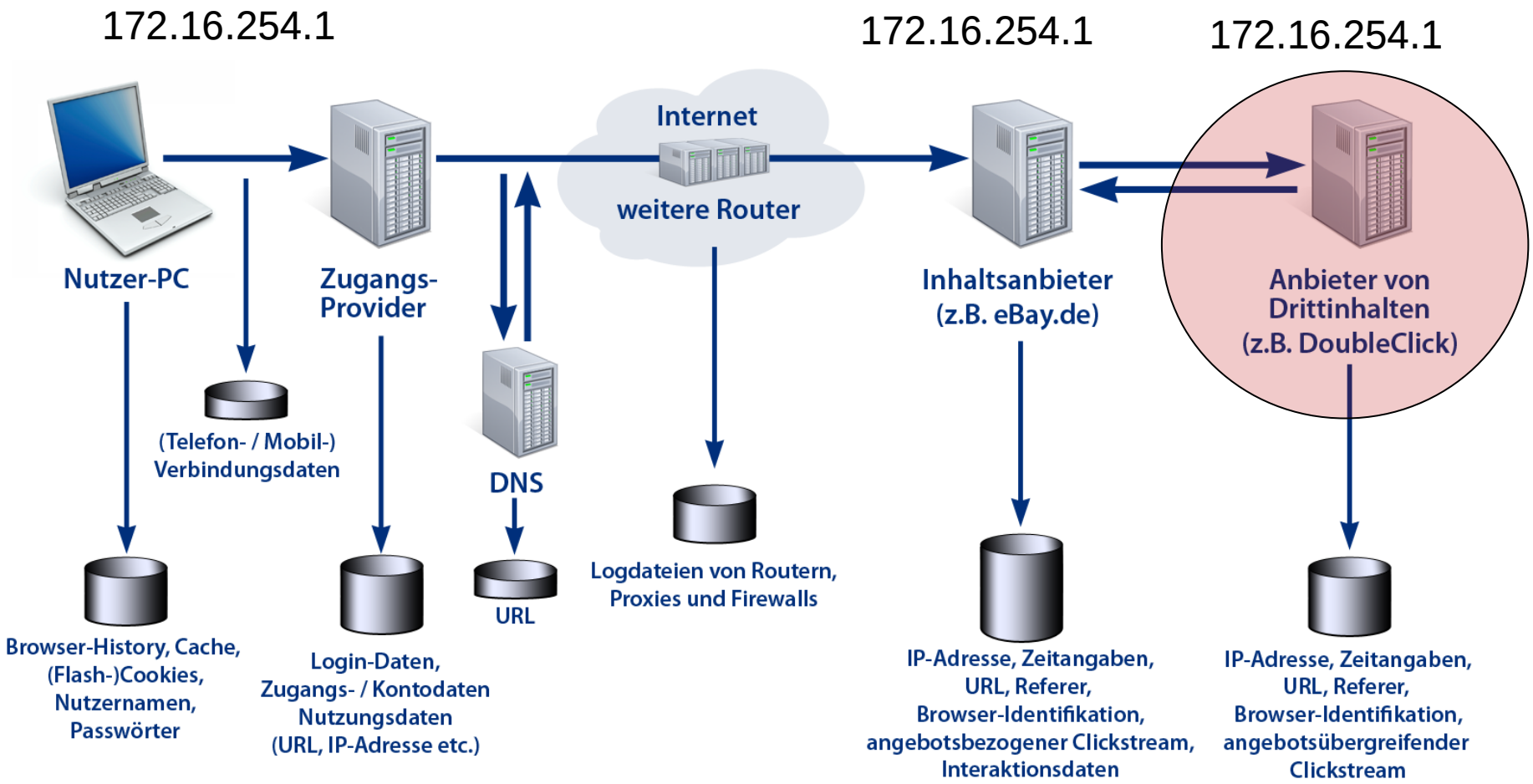
https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

Tracking – technisch



Marit Hansen: "Spuren im Netz - der Schutz der Privatsphäre". In: Dieter Korczak (Hrsg.): Spurensuche. Kulturwissenschaftliche Interpretationen und gesellschaftliche Rezeption. Kröning: Asanger (2010), S. 105-128

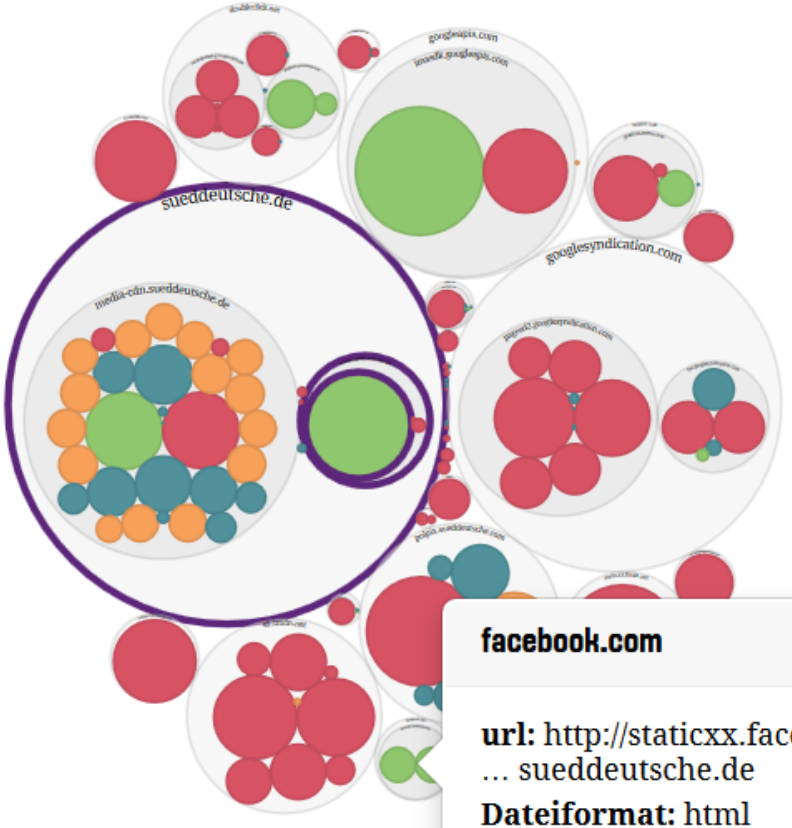
Tracking – technisch



Marit Hansen: "Spuren im Netz - der Schutz der Privatsphäre". In: Dieter Korczak (Hrsg.): Spurensuche. Kulturwissenschaftliche Interpretationen und gesellschaftliche Rezeption. Kröning: Asanger (2010), S. 105-128

Tracking – technisch

Problem:
automatisches Laden von Drittanbietern am Beispiel:
www.sueddeutsche.de



https://developers.facebook.com/docs/plugins/like-button#configurator

Quelle: http://datenblumen.wired.de/

Tracking – technisch

Über IP-Adresse hinaus u.a.:

- Betriebssystem
- Browserversion
- Zeitzone
- bevorzugte Sprachen
- Bildschirmauflösung
- installierte Schriften
- AdBlocker installiert?
- Cookies erlaubt/verboten
- Tracking erlaubt?
- von welcher Seite kommend

Identifizierung möglich

„Browser-Fingerprint“

Selbsttest z.B. über:
https://panopticlick.eff.org

Tracking – technisch

Cookies

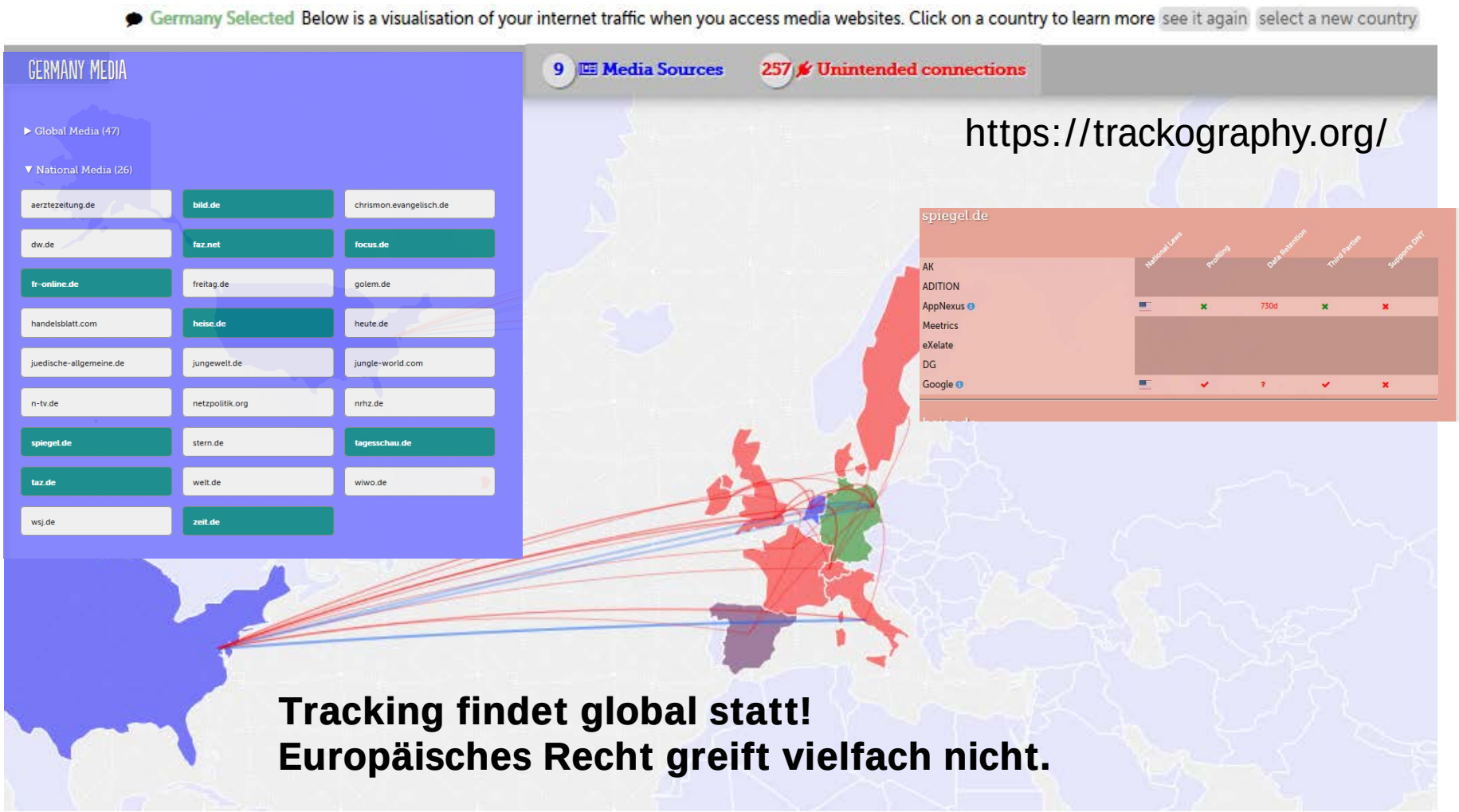
Textdateien auf dem Endgerät des Nutzers, die von aufgerufenen Seiten (Drittseiten!!!) gesetzt und gelesen werden können

Nützliche Funktionen:

- geladene Inhalte nicht erneut laden
- Nutzereinstellungen
- Warenkorbinhalt bleibt (Online-Shop)
- bestehende Logins bleiben (Facebook!!!)

Möglichkeit der **Identifizierung des Nutzers** durch Setzen und Lesen einer Unique-ID bei jedem Besuch der Website, die Cookie gesetzt hat (Drittanbieter!!!)

Tracking – rechtlich

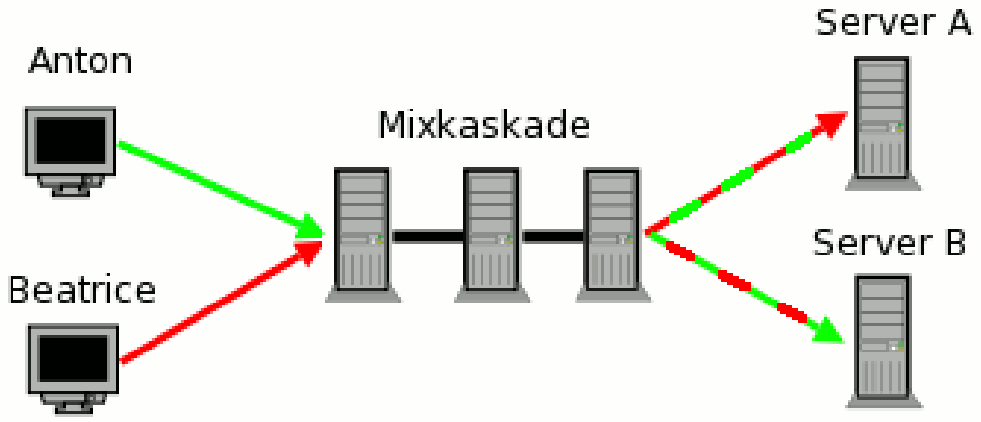


Tracking findet global statt!
Europäisches Recht greift vielfach nicht.

Selbstdatenschutz

a) IP-Adresse verschleiern

JonDonym feste Proxy-Kette, Mix

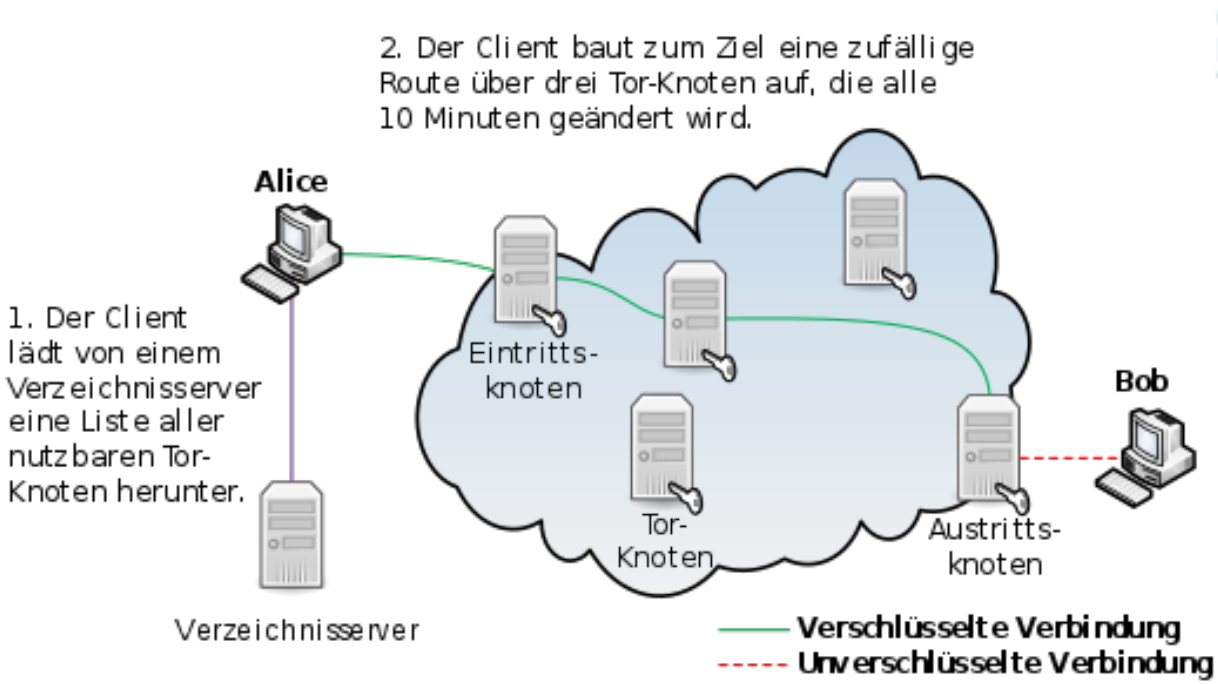


Quelle: https://www.privacy-handbuch.de/handbuch_23.htm

Selbstdatenschutz

a) IP-Adresse verschleiern

TOR Vielzahl Proxys



Quelle: https://de.wikipedia.org/wiki/Tor_(Netzwerk)

Selbstdatenschutz

b) Laden von Drittanbieterseiten & Scripten (Java-Script) verhindern, z.B. durch:

- NoScript
- Disconnect
- uBlock Origin
- Privacy Badger
- und andere ...

Problem:

- Funktionalität der Webseite häufig eingeschränkt
- Vertrauen kann enttäuscht werden (Ghostery, AdblockPlus, WOT)

S. dazu: https://www.ndr.de/nachrichten/netzwelt/Nackt-im-Netz-Millionen-Nutzer-ausgespaeht,nacktimnetz100.html

Selbstdatenschutz

c) Cookies

- „normale“ Cookies sind über den Browser zu verwalten
  - alle Cookies verbieten
    - häufig Probleme mit Website-Funktionalität!
  - Drittanbieter-Cookies verbieten
  - Löschen bestehender Cookies
    - werden aber neu gesetzt, wenn nicht zugleich verboten

- Flash-Cookies/Supercookies (z.B. HTML5)
  - werden an Orten abgelegt, auf die Nutzer nicht ohne weiteres Zugriff haben
    - Add-On gegen Supercookies (z.B. Better Privacy)

https://addons.mozilla.org/de/firefox/addon/betterprivacy/

Selbstdatenschutz

Problem:

Gängige Selbstdatenschutztools sind bekannt, daher wenden Tracker stets neue Techniken an

- Anti-Werbeblocker
- Audio-Fingerprinting
- Battery-Fingerprinting
- Canvas-Fingerprinting
- Font-Fingerprinting
- verhaltensbasiertes Tracking

s. dazu ausführlich: https://svs.informatik.uni-hamburg.de/publications/2016/2016-06-13-Herrmann-Unzureichend-informiert-ungefragt-ueberwacht.pdf

Selbstdatenschutz

Fazit:

- Datenminimierung ist der beste Datenschutz
  - bedeutet konsequenterweise Kompromisse
- Manche Selbstdatenschutztools sind gut, manche nicht
  - Vertrauen kann enttäuscht werden
- Selbstdatenschutztools einzusetzen ist Arbeit
  - aber keine Raketenwissenschaft
- Selbstdatenschutztools bringen nur teilweise(!) Schutz
  - nicht mehr aber auch nicht weniger!

Betreute Projekte

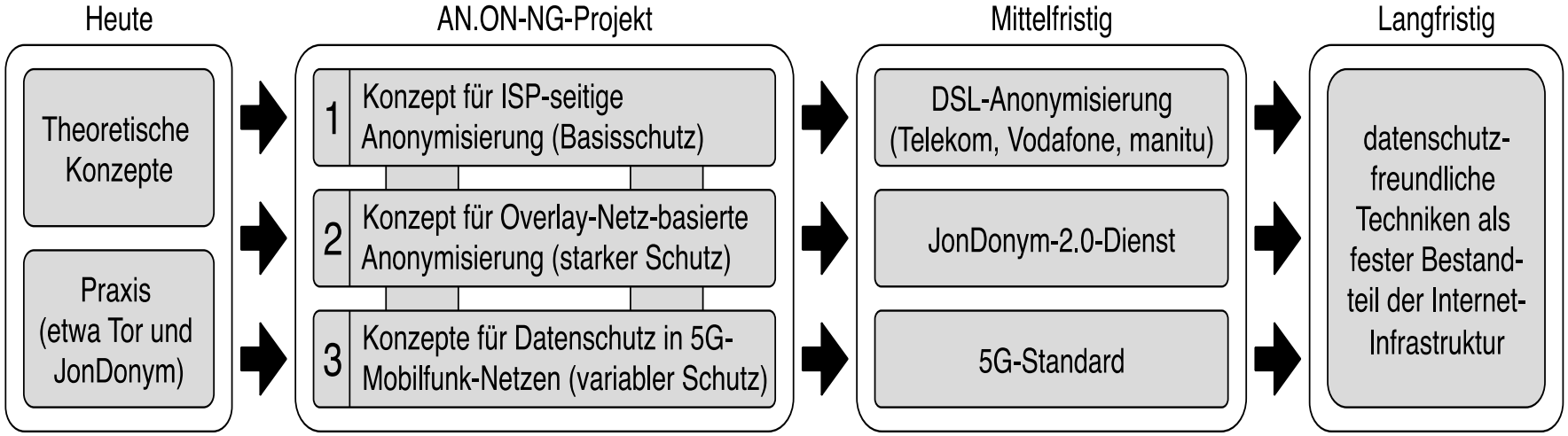
a) **AN.ON Next Generation**
Anonymität Online

b) **AppPETS**
Datenschutzfreundliche Smartphone-Anwendungen ohne Kompromisse

- Beide Projekte gefördert vom BMBF
- Beteiligung verschiedener Universitäten und Partner auch aus der Wirtschaft (u.a. ein Internet Service Provider und Anonymisierungsdiensteanbieter)

Projekt AN.ON NEXT GENERATION

- Effizientere datenschutzfreundliche Lösungen mit kaum spürbar eingeschränkter Dienstqualität
- „Zero Effort Privacy“: Verlagerung der Anonymisierung so weit wie möglich in die Internet-Infrastruktur, kein Aufwand mehr für den Endanwender



Projekt AN.ON NEXT GENERATION

- **Beispiel: ISP-seitiger „Basisschutz“**
  - IP-Adresse wird dynamisch durch ISP (z.B. Telekom) verteilt
  - wechselt meist täglich (wenn Router getrennt wird)
  - es reichen Minuten, um IP-Adresse einem Nutzer eindeutig zuzuordnen
  - derzeitiger Standard IPv4 (2^{32} IP-Adressen ≈ 4 Mrd.)

    172.16.254.1

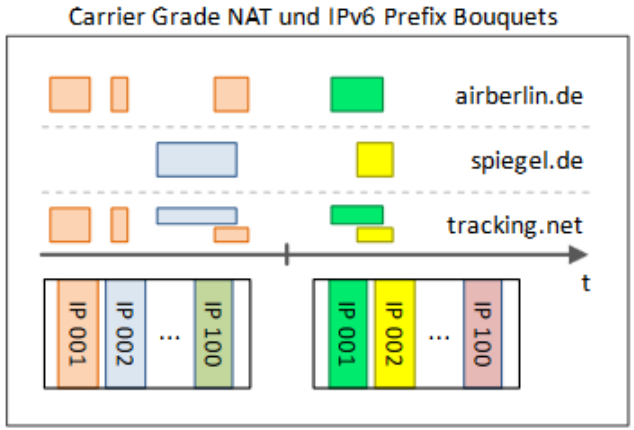
  - zukünftig IPv6 (2^{128} IP-Adressen ≈ 340 Sextillionen)

    6420:0db6:65a3:07c3:1417:7b2d:0370:7344

Projekt AN.ON NEXT GENERATION

- **Anonymisierung durch Internet Service Provider**
- **Vergabe einer Vielzahl unterschiedlicher IPv6-Adressen pro Nutzer**
- **IPv6 Prefix-Wechsel**

Schutz vor Tracking:
IP-Adresse möglichst häufig ändern



<u>Ziel</u>: Dritten (Serverbetreibern und Werbenetzen) Verkettung von Aktionen einzelner Nutzer (zur Profilbildung) zu erschweren

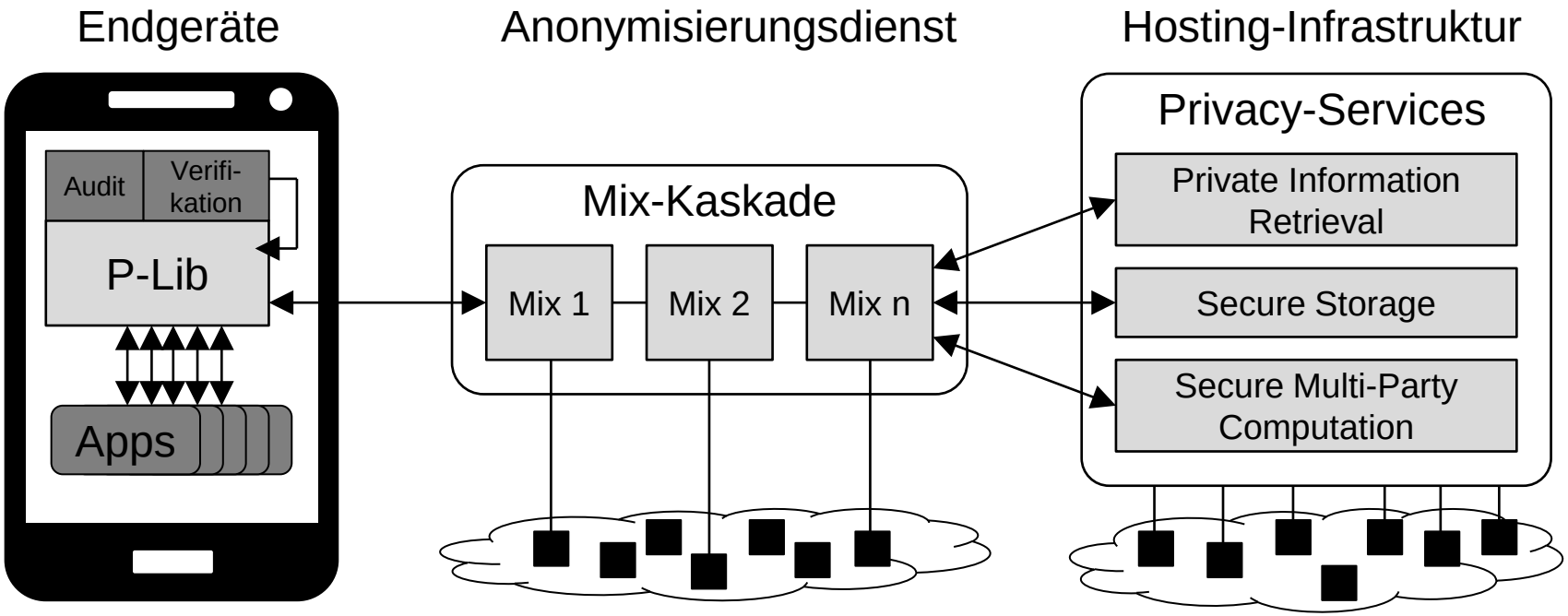
Quelle: Dominik Herrmann, https://svs.informatik.uni-hamburg.de/publications/2016/2016-06-13-Herrmann-Unzureichend-informiert-ungefragt-ueberwacht.pdf

Projekt AppPETs Datenschutzfreundliche Smartphone Anwendungen ohne Kompromisse

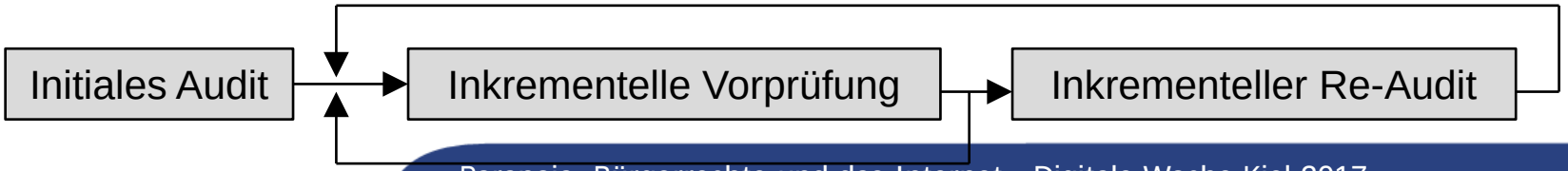
Ziel: Datenschutzfreundliche Smartphone-Anwendungen

- Entwicklern die Integration von datenschutz-freundlichen Technologien in ihren Smartphone-Apps erleichtern: Bereitstellen von Programmbausteinen („P-Lib“)
- Schaffen einer Infrastruktur, in der persönliche Daten abgelegt werden können und geschützt auf sie zugegriffen werden kann (secure storage)

Projekt AppPETs
Datenschutzfreundliche Smartphone Anwendungen ohne Kompromisse



Auditierungsverfahren



Fazit


Zuerst das Suchwort 'Misstrauen'
Terroristen Suchmaschine
80 Millionen Treffer
Alf

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Susan Gonscherowski

Eva Schedel

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

https://www.datenschutzzentrum.de

mail@datenschutzzentrum.de

0431 988-1200