Deutsche Stiftung für Recht und Informatik

EIN SCHRITT VOR, ZWEI SCHRITTE ZURÜCK?

– FOLGEN EINER VERPFLICHTENDEN ZUGRIFFSMÖGLICHKEIT AUF VERSCHLÜSSELTE DATEN

Stefan Schiffner/Sandra Schmitz-Berndt
SnT, Universität Luxemburg

The research for this article was funded by the Luxembourg National Research Fund (FNR) C18/IS/12639666/EnCaViBS/Cole, https://www.fnr.lu/projects/the-eu-nis-directive-enhancing-cybersecurity-across-vital-business-sectors-encavibs/.

Herbstakademie 2021

Rat der Europäischen Union

Brüssel, den 24. November 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

PUBLIC

VERMERK

Absender:	Vorsitz
Empfänger:	Delegationen
Nr. Vordok.:	12863/20
Betr.:	Entschließung des Rates zur Verschlüsselung – Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung

Die Delegationen erhalten in der Anlage die Entschließung des Rates zur Verschlüsselung.

Unabhängig vom derzeitigen technologischen Umfeld ist es unerlässlich, die Befugnisse der zuständigen Behörden im Bereich Sicherheit und Strafjustiz durch **rechtmäßigen Zugang** zu wahren, damit sie ihre Aufgaben wie gesetzlich vorgeschrieben und zulässig wahrnehmen können.

EUROPÄISCHE KOMMISSION

Brüssel, den 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Vorschlag für eine

RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148

(Text von Bedeutung für den EWR)

{SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

Die Nutzung der E2E-Verschlüsselung sollte mit den Befugnissen der MS, den Schutz ihrer wesentlichen Sicherheitsinteressen und der öffentlichen Sicherheit zu gewährleisten und die Ermittlung, Aufdeckung und Verfolgung von Straftaten […] zu ermöglichen, in Einklang gebracht werden. Lösungen für den **rechtmäßigen Zugang** zu Informationen in E2E-verschlüsselter Kommunikation …

EUROPEAN COMMISSION

Brussels, 9.12.2020
COM(2020) 795 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond

The Commission will work with MS to identify possible legal, operational, and technical solutions for **lawful access** and promote an approach which both maintains the effectiveness of encryption in protecting privacy and security of communications, while providing an effective response to crime and terrorism.

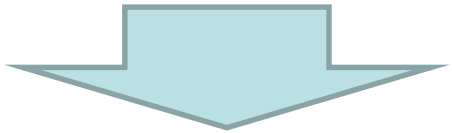
Sicherheit *durch* Verschlüsselung vs. Sicherheit *trotz* Verschlüsselung

„durch“

- Unterstützung für Entwicklung, Umsetzung und Nutzung starker Verschlüsselung als Mittel zum Schutz von Grundrechten und digitaler Sicherheit

„trotz“

- Zuständige Behörden im Bereich Sicherheit und Strafjustiz sollen ihre gesetzlichen Befugnisse zum Schutz der Gesellschaften und Bürger durch Zugriff auf verschlüsselte Daten ausüben können



Wie kann dies in Einklang gebracht werden?

Nach Terroranschlag in Wien

EU-Ministerrat will offenbar Verschlüsselung einschränken

Wenige Tage nach dem Terroranschlag in Wien planen die EU-Staaten nach Medienberichten eine Ausweitung der digitalen Überwachung. Sie fordern demnach einen "Generalschlüssel" für Messenger wie WhatsApp oder Signal.

09.11.2020, 11.46 Uhr

EU will sichere Ende-zu-Ende-Verschlüsselung für behördliche Ermittlungen lockern

NEWS 16.11.2020 Generalschlüssel für Polizei und Geheimdienste? ★★★★★ 4

Haufe Online Redaktion

NEWS Home > Security > Encryption

EU inches closer to ban on end-to-end encryption

Leaked document suggests EU wants "balance" between robust security and ease of access f

by: Dale Walker 9 Nov 2020

Verfassungsklage gegen neue Abhörmöglichkeiten der Geheimdienste durch Quellen-TKÜ

Nach der Polizei dürfen künftig auch

tagesschau Sendung verpasst?

Inland ▸ Verschlüsselte Kommunikation: Eine Hintertür für die Ermittler?

Verschlüsselte Kommunikation

Eine Hintertür für die Ermittler?

Stand: 13.11.2020 04:43 Uhr

Wollen die EU-Staaten dafür sorgen, dass Ermittler einfacher bei Messenger-Diensten mitlesen können? Ein Resolutionsentwurf deutet darauf hin. Datenschützer sind alarmiert.

Net Results: Dangerous call for 'back doors' to encryption

EU set for data access exposing everyone to pernicious risk of information breaches

Thu, Nov 12, 2020, 05:00

Karlin Lillington

EU dangerously drifting towards banning end-to-end encryption

By Barclay Ballard November 11, 2020

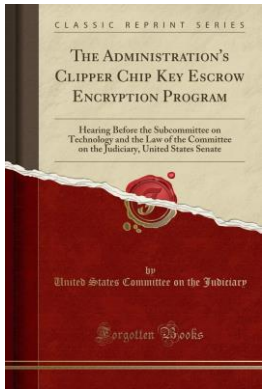
Draft EU legislation is seeking to undermine encryption tools

heise online ⟩ News ⟩ 11/2020 ⟩ Crypto Wars: Grünes Licht für umkämpfte EU-Erklärung zu…

Crypto Wars: Grünes Licht für umkämpfte EU-Erklärung zu Entschlüsselung

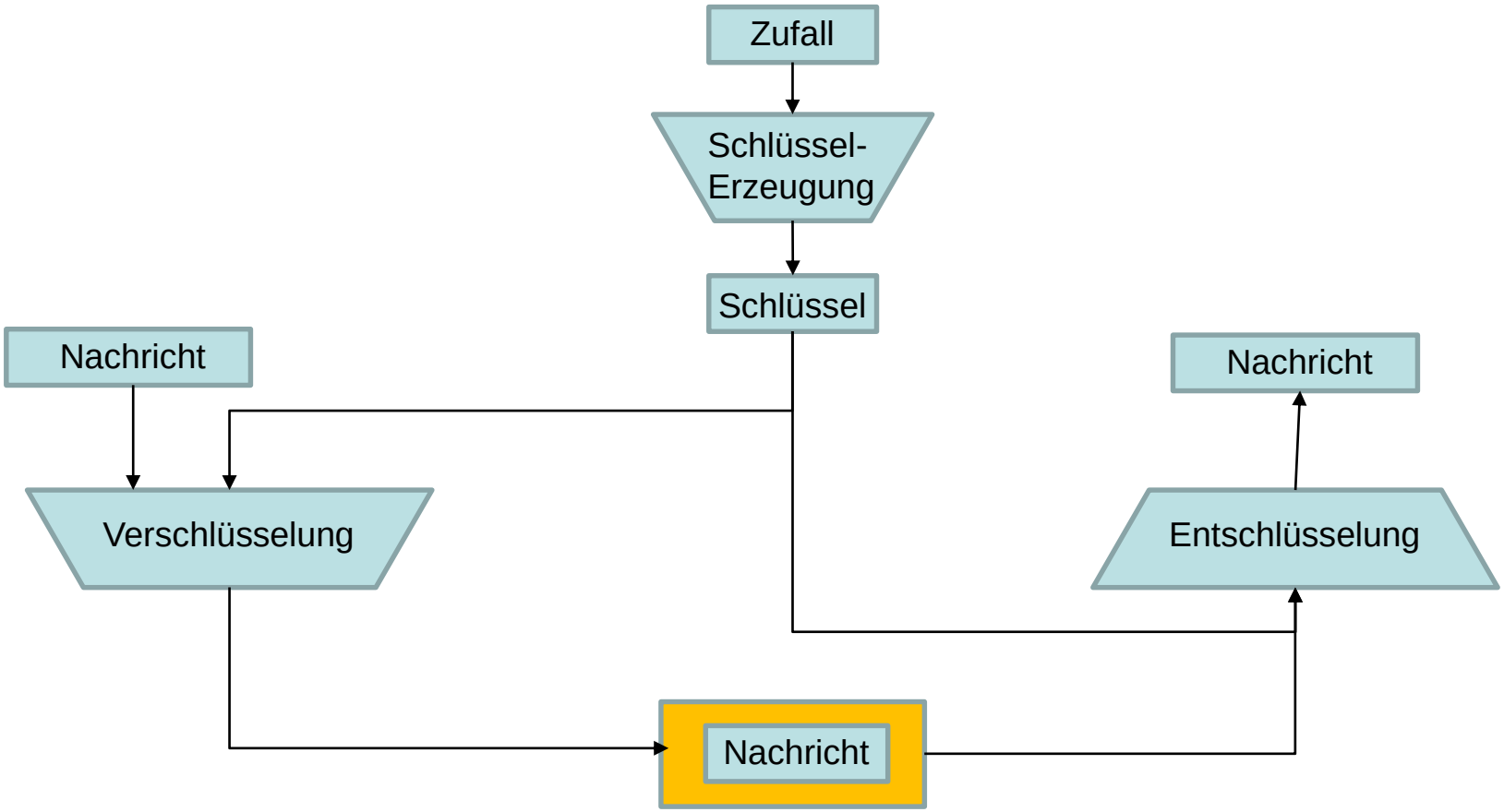
Diplomaten haben die von der Bundesregierung ausgearbeitete Entschließung des EU-Rats zur Verschlüsselung gebilligt. IT-Firmen sollen beim Entschlüsseln helfen.

Prequel: Crypto-Wars

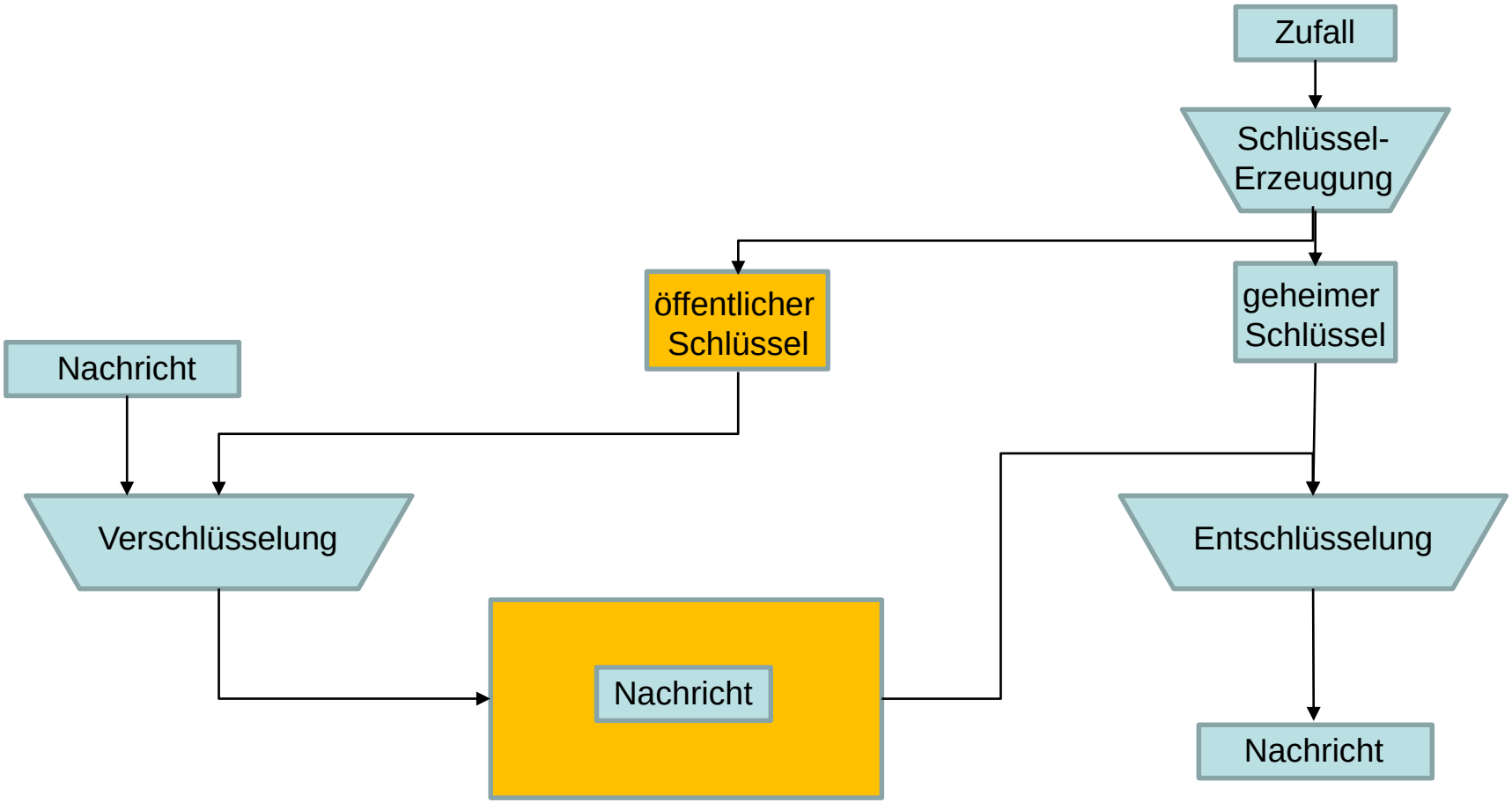


- Bis Ende der 90er: Verschlüsselungstechnologie = Produkt der Rüstungsindustrie; Anwendung: Schutz staatlicher (militärischer) Kommunikation vor Zugriff und Manipulation durch Akteure von Drittstaaten
- Dual-Use-Technologie, aber abnehmende Marktregulierung durch verstärkten Schutzbedarf der Privatwirtschaft (Kehrpunkt weitestgehende Freigabe des Marktes durch die Clinton-Regierung in den 2000ern)
- Aber Wiederkehr von Crypto-Wars im neuen Gewand: Ermöglichung polizeilicher Ermittlungen zur Aufklärung von div. Kapitalverbrechen und Bemächtigung von Geheimdiensten zur Terrorabwehr

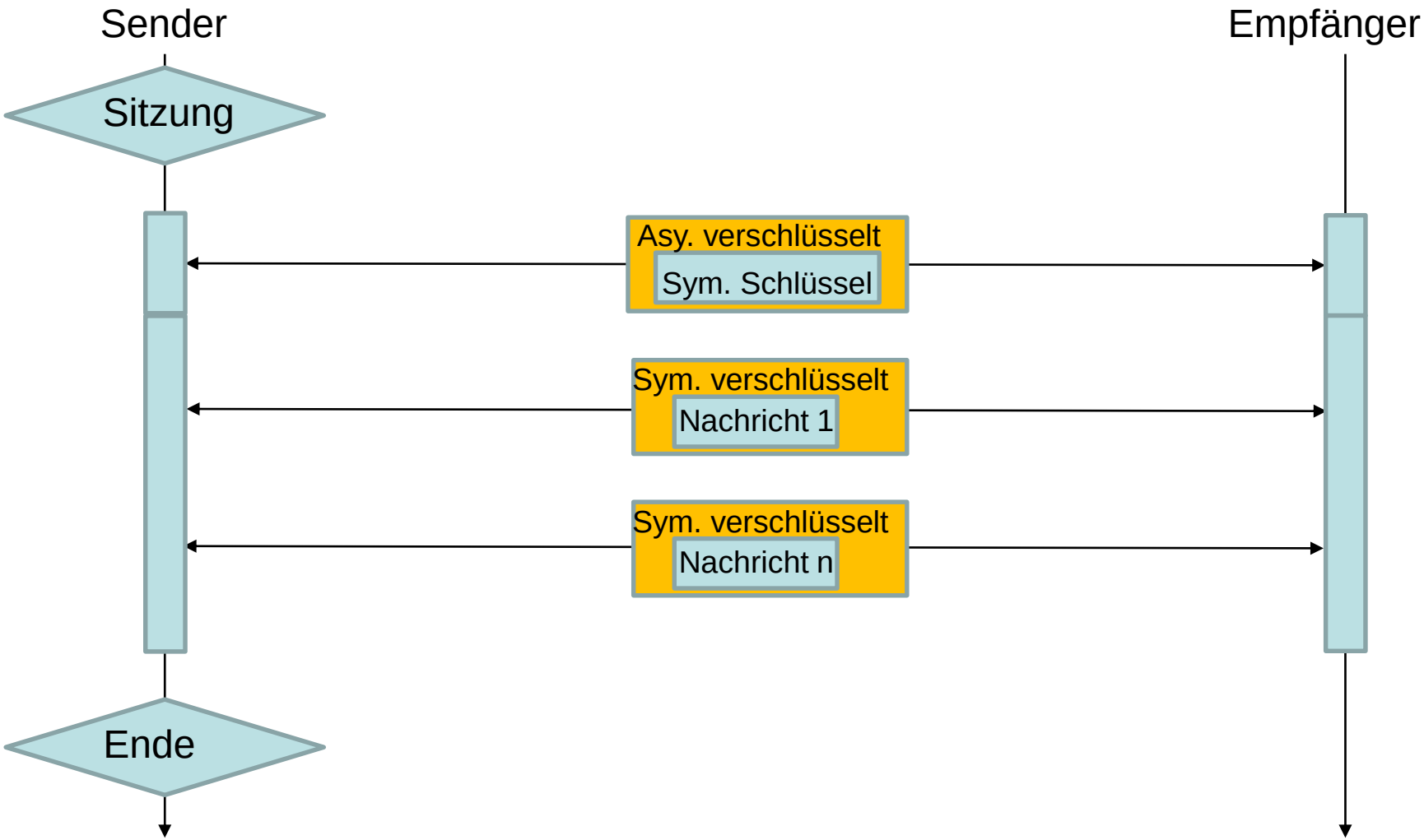
Symmetrische Verschlüsselung



Asymmetrische Verschlüsselung

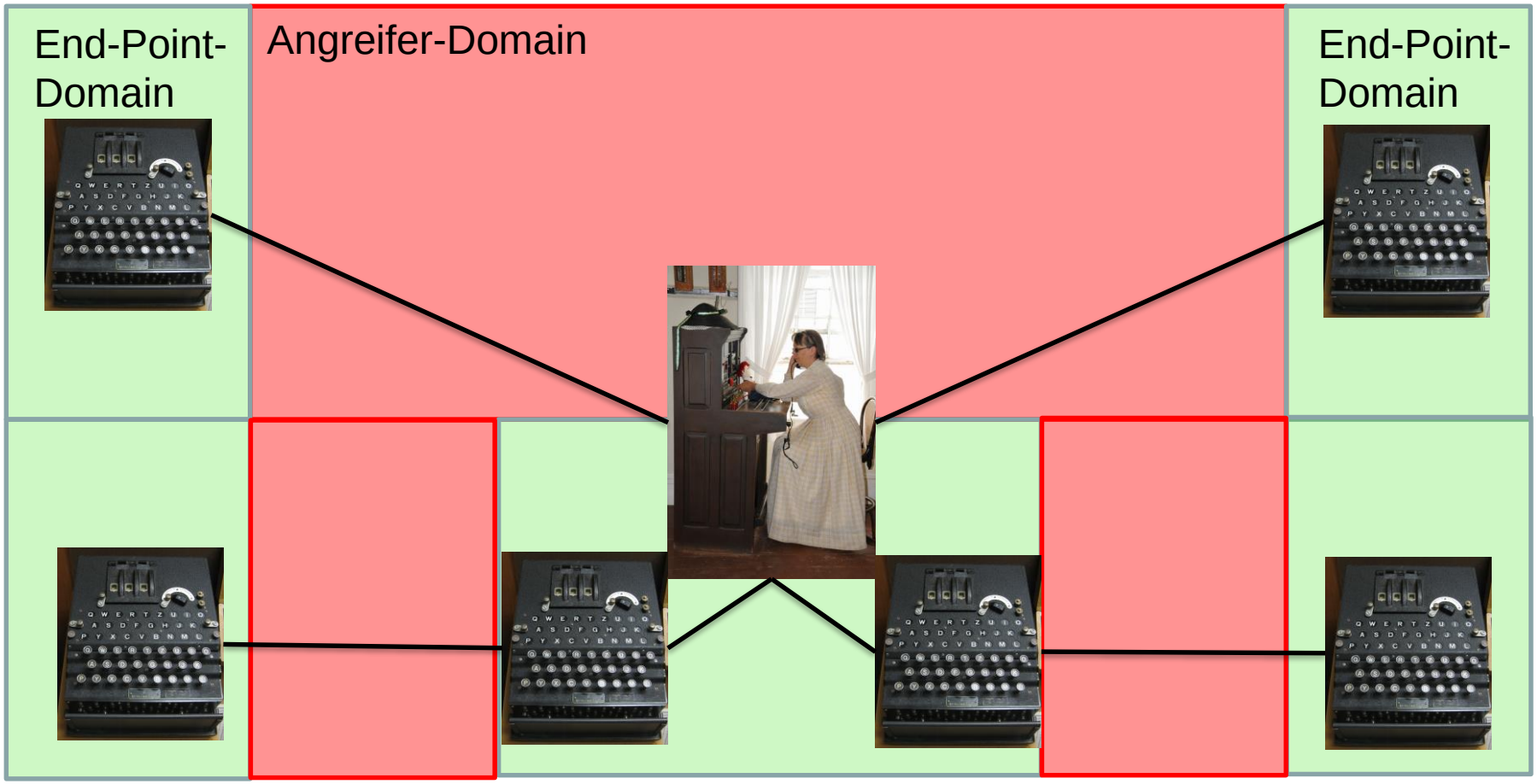


Hybride Verschlüsselung



Vergleich Ende zu Ende- und Kanal-Verschlüsselung

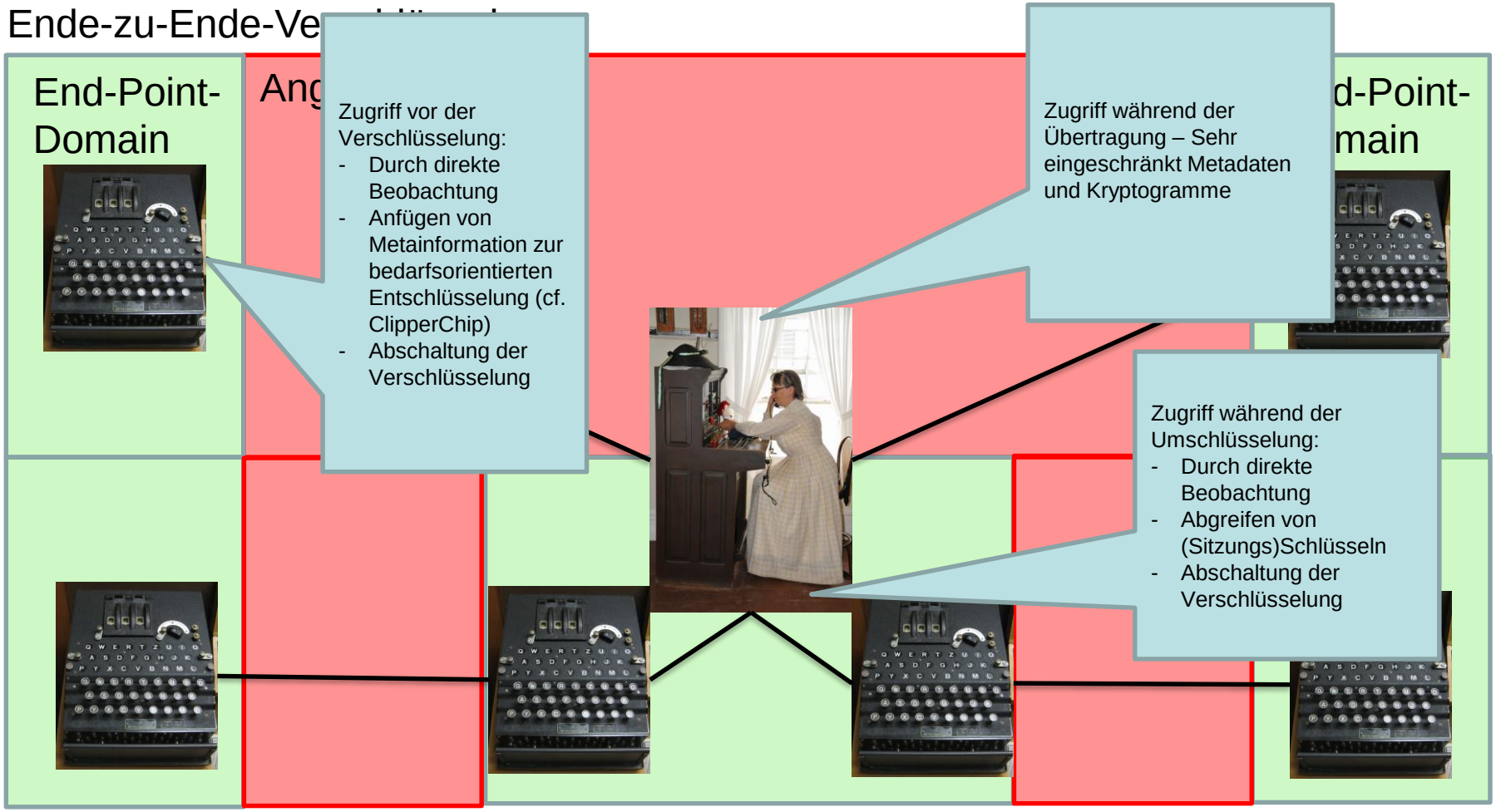
Ende-zu-Ende-Verschlüsselung



Kanalverschlüsselung

An *welcher Stelle* soll auf *was* Zugriff möglich sein?

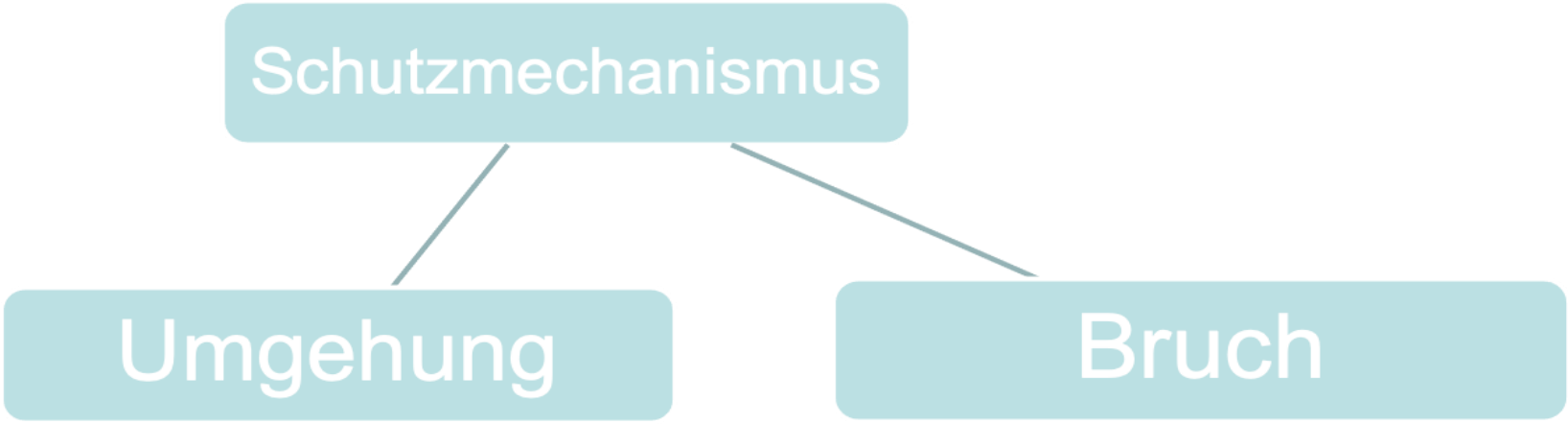
Vergleich Ende zu Ende- und Kanal-Verschlüsselung



Notwendigkeit der Sicherheit durch Verschlüsselung

- Schutz von Grundrechten, u.a. Kommunikationsgrundrechte, Art. 10 GG, IT-Grundrecht
- Datenschutz:
  - DSGVO: Prioritäre Sicherheitsmaßnahme zum Schutz persönlicher Daten (vgl. Art. 32 Abs. 1, ErwG 83)
  - DSGVO: ein Mittel zur Zulässigkeit von Übermittlung personenbezogener Daten in Drittstaaten
- IT-Sicherheit:
  - NIS-RL 2.0: Art. 18 NIS-RL 2.0 Vorschlag: angemessene und verhältnismäßige technische und organisatorische Maßnahmen zur Risikobewältigung unter Berücksichtigung des Stands der Technik sollen ein dem Risiko angemessenes Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, z.B. durch Verschlüsselung

Sicherheit trotz Verschlüsselung: Zugriffsmöglichkeiten



- **Ansatz außerhalb Übertragungsvorgang, z.B. durch**
  - **Manipulation Endgerät**
  - **Keyescrow (z.B. Clipper Chip)**
- **Quellen-TKÜ**

- **Kanalverschlüsselung: Speichern von Session-Keys durch Diensteanbieter**
- **Überwachung Echtzeit-Kommunikation vs. Generelle Speicherpflicht**
- **Speicherung von Schlüsseln = Speicherung von Inhalten?; → Vorratsdatenspeicherungs problematik**

- **Öffnen von Kryptogrammen z.B. durch Brute-Force-Angriff**
- **Hacking**
- **Gesetzl. Einschränkung von Kryptografie**

Zugriff auf Daten bei E2E-Verschlüsselung

Schwächung zugrundeliegender Kryptografie

Gesetzl. Einschränkung der Verschlüsselungsverfahren oder Verpflichtung zur Implementierung von Keyescrow-Mechanismen

FOLGEN:

Netzwerke werden generell unsicher