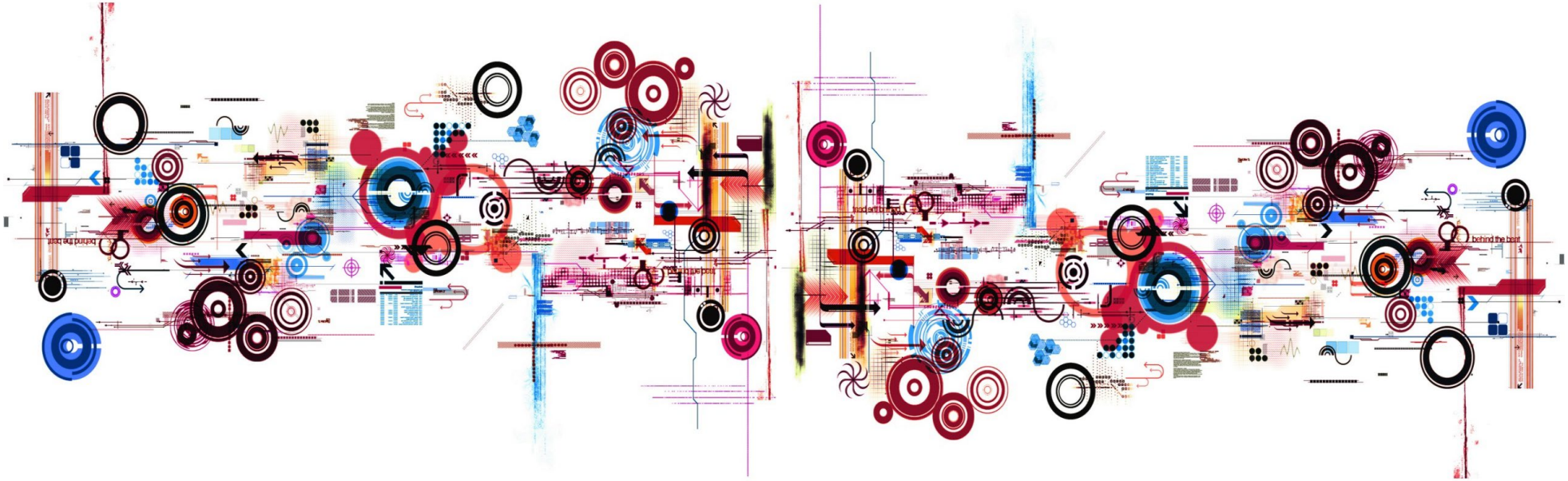
Datenschutz in Videokonferenzsystemen und vertragliche Gestaltung



Telefon- statt Videokonferenz?

- Veröffentlichte Checkliste der Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 3. Juli 2020:
  - Erster Prüfschritt nach Empfehlung der BlnBDI:
    Reicht nicht auch eine Telefonkonferenz?
  - BlnBDI: „Telefonkonferenzen können sehr viel leichter datenschutzkonform durchgeführt werden.“
- Viele Anbieter von web-/cloudbasierten Konferenzen bieten auch eine telefonische Einwahl an → das gilt hier wohl nicht als Telefonkonferenz?
- Telefonie im geschäftlichen Bereich ist inzwischen fast immer IP basiert und daher nichts anderes als Datensignal (wie Videokonferenz).
- Technisch bei Telefon via IP m.E. gleiche Probleme wie bei Video, insbesondere für Ende-zu-Ende-Verschlüsselung (E2E).

Datenarten und Betroffene

- Datenarten
  - Name, Benutzerkennung, oft E-Mail-Adresse
  - Bild- und Tondaten während der Konferenz
  - Kommunikations-Metadaten (Zeitpunkt, Dauer, IP-Adresse, ...)
  - ggf. Chat-Inhalte und ausgetauschte Dateien

- Betroffene
  - Teilnehmerinnen und Teilnehmer an der Konferenz
  - Personen, die in der Konferenz genannt werden, die in Chats oder Dokumenten genannt werden.

Rolle der Parteien

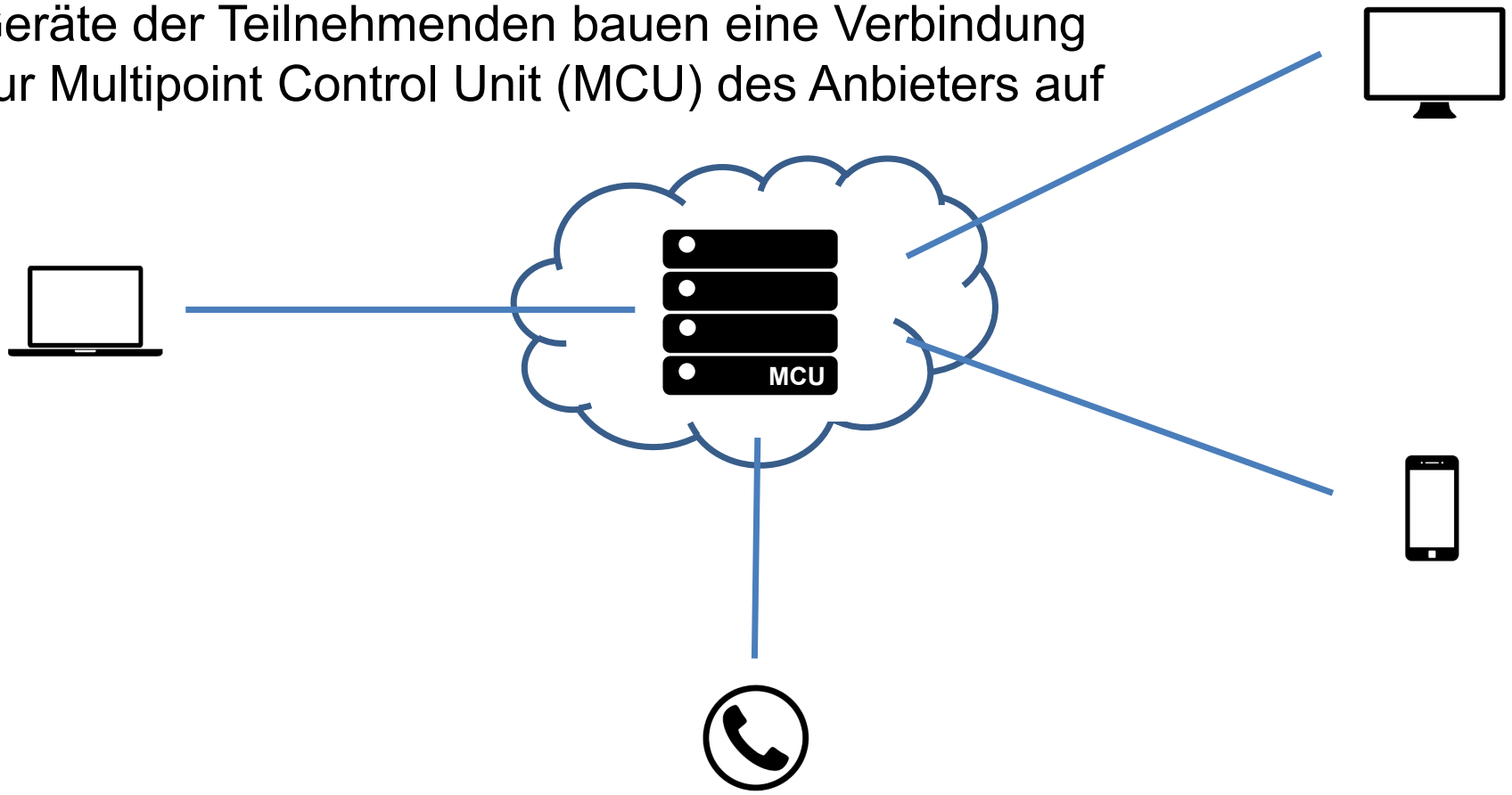
- Anbieter des Konferenzsystems werden regelmäßig als **Auftrags-verarbeiter** eingestuft. Sie verarbeiten die Kommunikationsinhalte für Zwecke des (oder der) Auftraggeber(s).
- Als **Verantwortlicher** wird allein der **Einladende** angesehen.
  - Der Einladende bestimmt jedenfalls die Mittel der Verarbeitung durch Auswahl des Konferenzsystems.
  - Er bestimmt auch die Zwecke der Verarbeitung; ob er diese wirklich allein bestimmt, oder ob er dies nicht gemeinsam mit den anderen Teilnehmenden bestimmt, muss wohl noch einmal diskutiert werden.
  - Verhältnis ändert sich aber mE, wenn der Teilnehmende ein eigenes Konto beim Anbieter hat; jedenfalls Konto- und Nutzungsdaten werden dann für den jeweiligen Kontoinhaber verarbeitet.

Auftragsverarbeitung

- Aufbau und Qualität der Verträge sehr unterschiedlich. Inzwischen häufig in AGB/Nutzungsvereinbarung integriert (Klick-Verträge). Teilweise muss AVV aber weiterhin gesondert angefordert werden.
- BlnBDI hat umfassend Kritik an den AVV geübt. Dabei sehr strenger Maßstab, jede Unschärfe zu Lasten des Dienstleisters auch bei komplexen Vertragsverhältnissen. Kritik nicht immer nachvollziehbar; eigene Prüfung empfohlen. Verträge waren teilweise bei Veröffentlichung durch die Aufsicht schon veraltet.
- Häufigste Probleme nach unserer Prüfung:
  - Eigenes Nutzungsrecht an (selbst anonymisierten) Daten
  - Unklare TOM und breite Prüfberichte
  - zu viele Produkte in einer AVV, dadurch Unschärfen

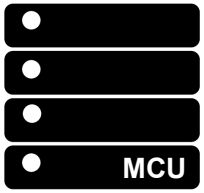
Technischer Ablauf

- Geräte der Teilnehmenden bauen eine Verbindung zur Multipoint Control Unit (MCU) des Anbieters auf



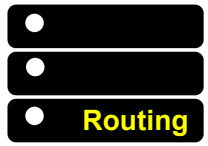
Technischer Ablauf

- Die **Multipoint Control Unit (MCU)** erledigt das Management der Datenflüsse zwischen den einzelnen Teilnehmenden:
  - Empfang der Mediendaten, Mix der Bilddaten
  - Signalisierung von Anrufen, Nachrichten, etc.
  - Anpassung der Daten an verschiedene Format



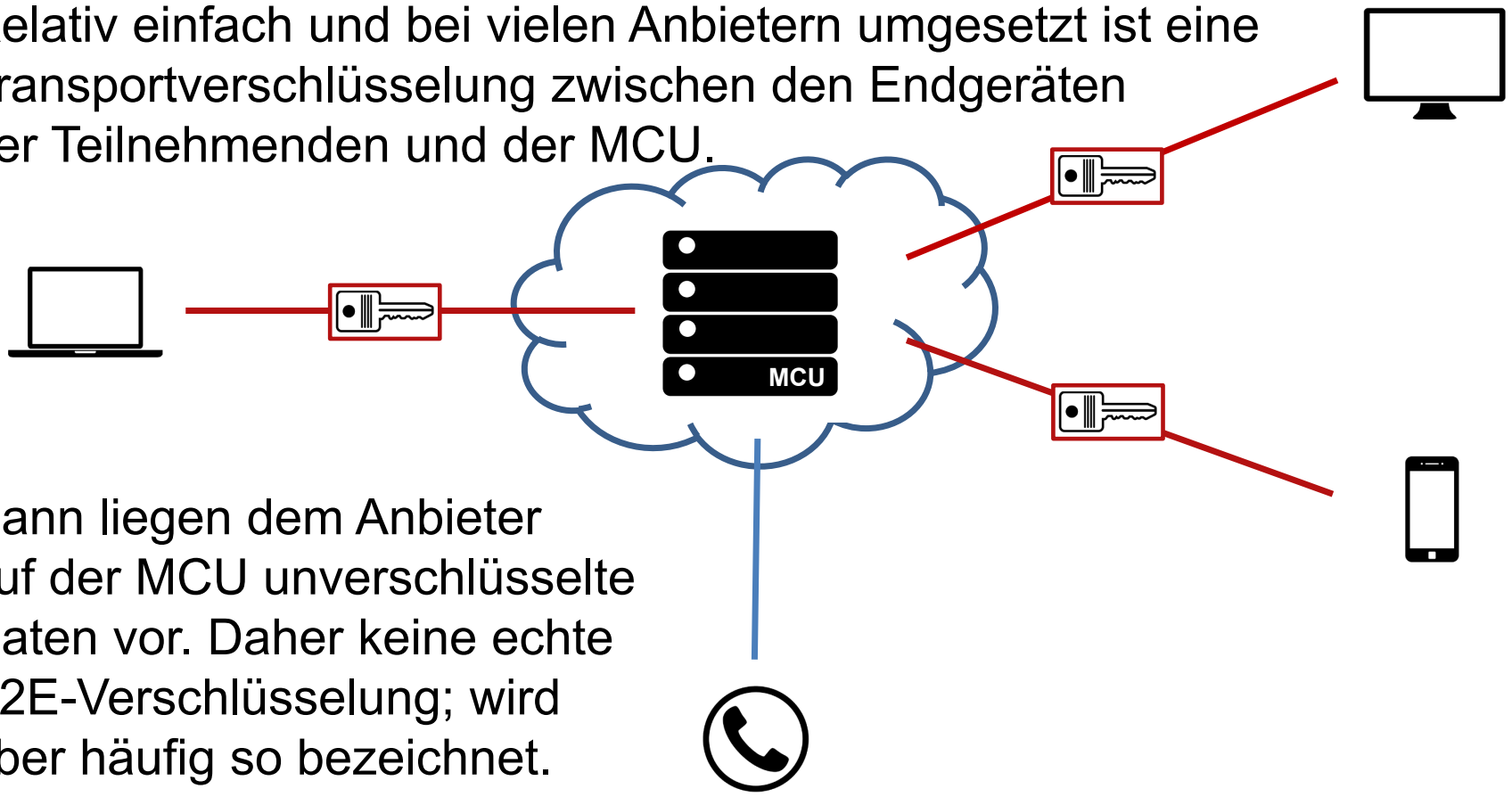
- **Registrierung** und Nutzervalidierung erfolgt in der Regel über gesonderte Registrierungseinheit

- **Routing** kann Funktion der MCU sein, häufig aber ausgelagert in eigenen Routing-Server, der dann auch Metadaten zur Konferenz und zu den Teilnehmenden verarbeitet.



Verschlüsselung

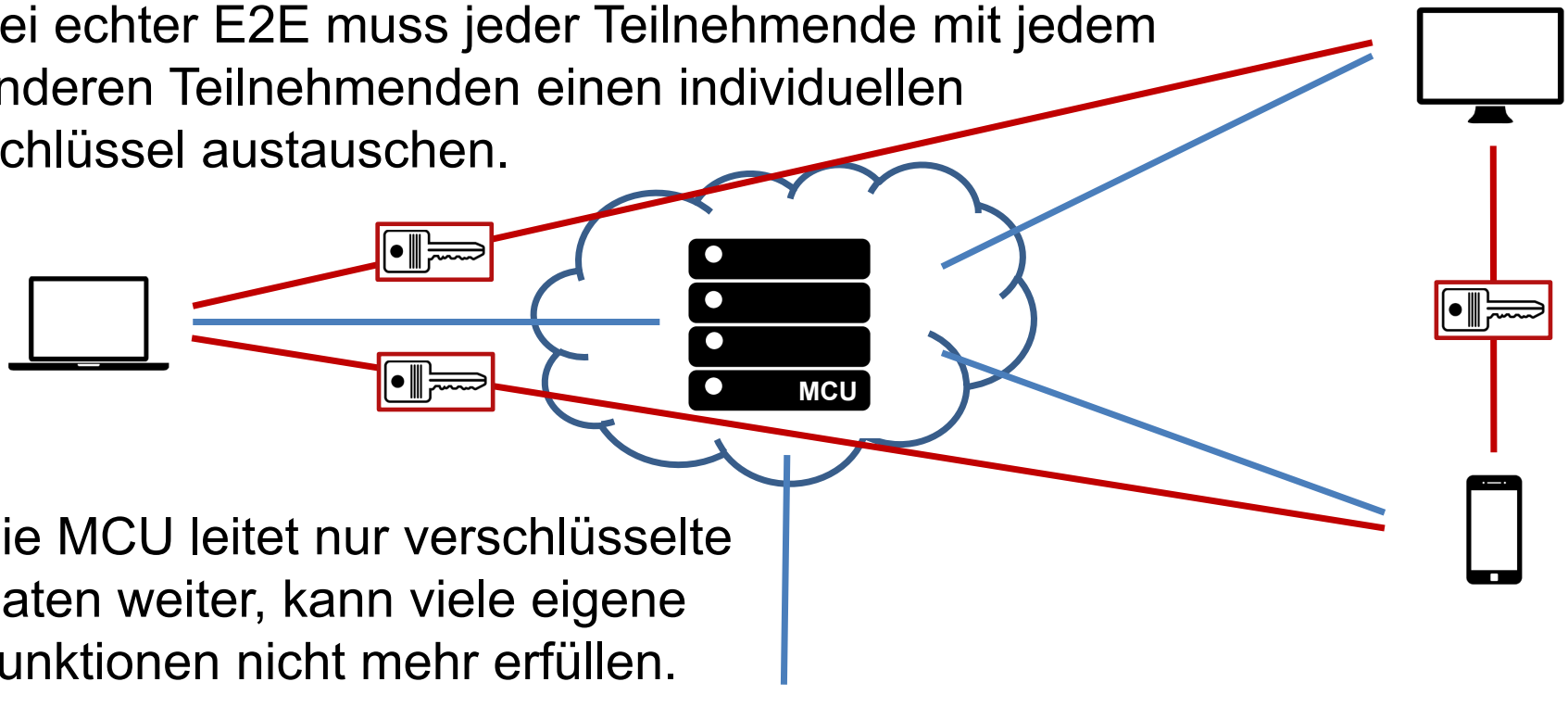
- Relativ einfach und bei vielen Anbietern umgesetzt ist eine Transportverschlüsselung zwischen den Endgeräten der Teilnehmenden und der MCU.



- Dann liegen dem Anbieter auf der MCU unverschlüsselte Daten vor. Daher keine echte E2E-Verschlüsselung; wird aber häufig so bezeichnet.

Technischer Ablauf

- Bei echter E2E muss jeder Teilnehmende mit jedem anderen Teilnehmenden einen individuellen Schlüssel austauschen.

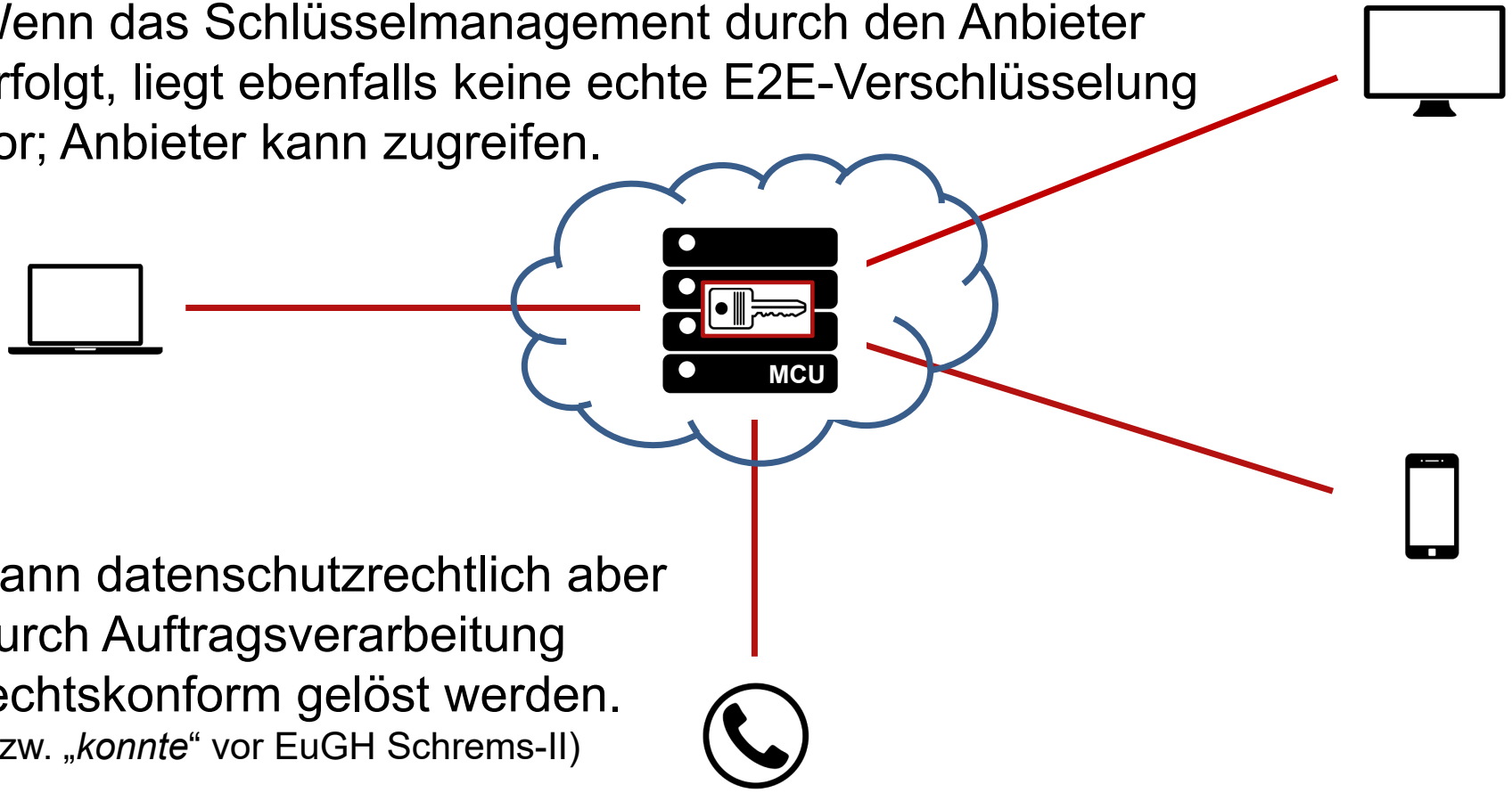


- Die MCU leitet nur verschlüsselte Daten weiter, kann viele eigene Funktionen nicht mehr erfüllen.
- Die Datenmenge erhöht sich (hier) auf 2-Streams pro Gerät

- Ein Call-In via Telefon ist nicht möglich

Verschlüsselung

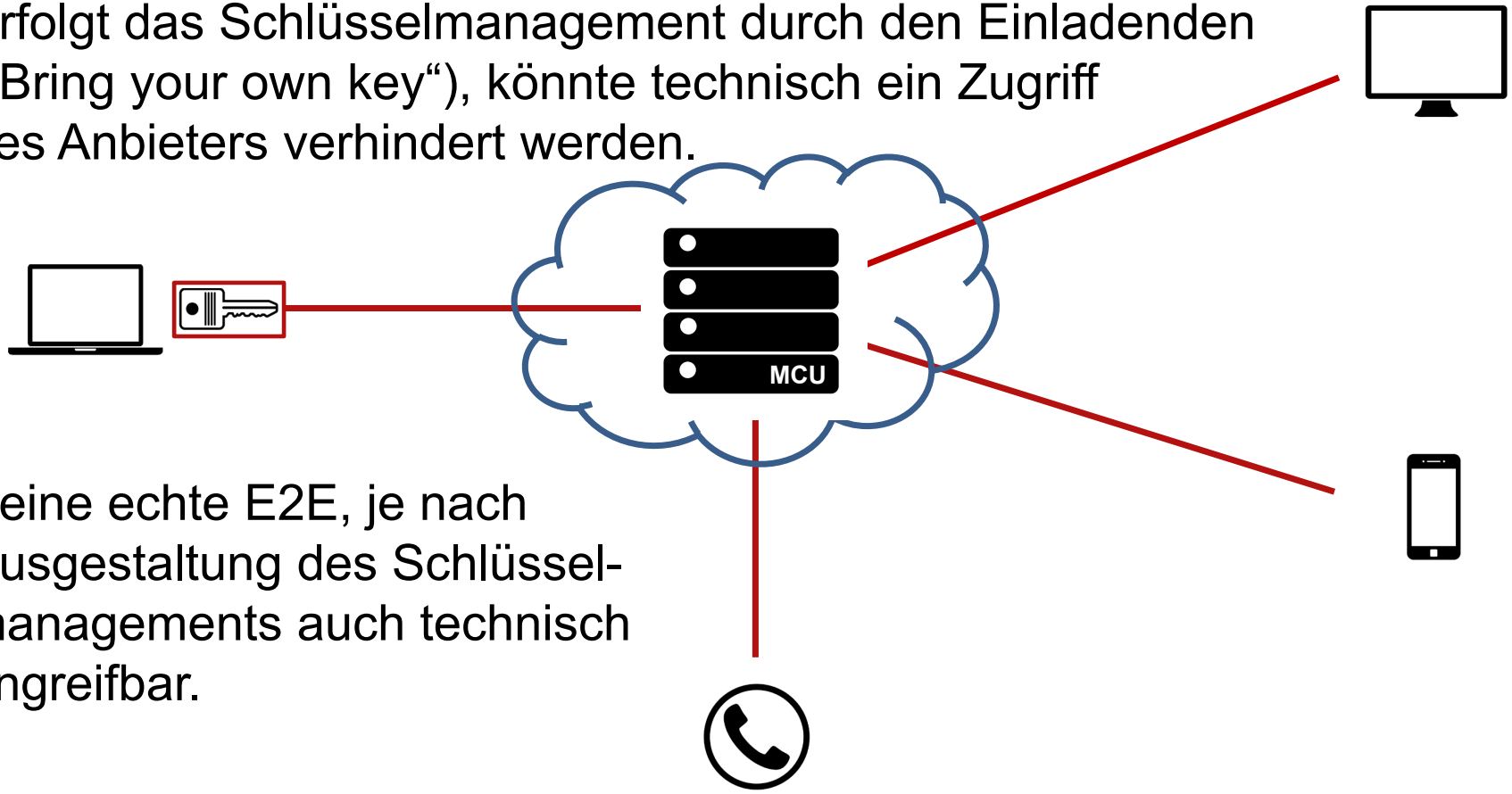
- Wenn das Schlüsselmanagement durch den Anbieter erfolgt, liegt ebenfalls keine echte E2E-Verschlüsselung vor; Anbieter kann zugreifen.



- Kann datenschutzrechtlich aber durch Auftragsverarbeitung rechtskonform gelöst werden.
  (bzw. „*konnte*“ vor EuGH Schrems-II)

Verschlüsselung

- Erfolgt das Schlüsselmanagement durch den Einladenden („Bring your own key“), könnte technisch ein Zugriff des Anbieters verhindert werden.



- Keine echte E2E, je nach Ausgestaltung des Schlüssel-managements auch technisch angreifbar.

Reaktionen auf EuGH Schrems-II

- Unter Geltung des EU-US Privacy Shields, bzw. vor der Klarstellung des EuGH zum Anwendungsbereich der EU Standardvertragsklauseln (SCC) waren Anbieter mit AVV und Selbstzertifizierung nach Privacy Shield oder eingebundener SCC auch ohne E2E-Verschlüsselung datenschutz-konform nutzbar.
- Viele Anbieter haben nach der EuGH-Entscheidung Aktualisierungen ihrer Verträge durchgeführt. Bisher scheinen weit überwiegend die Hinweise auf das EU-US Privacy Shield entfernt worden zu sein. Statt dessen werden SCC ohne weitere Ergänzungen eingebunden.
- Allein der Wechsel auf SCC dürfte nicht ausreichen, faktisch werden mE nur technische Maßnahmen Lösungen bringen (E2E oder jedenfalls MCU in der EU ohne Zugriffsmöglichkeit aus Drittländern).

Zentrale Kriterien für die Anbieterauswahl

- ***Nie Einladender sein, dann hat man kein Problem*** **;)**

- Funktionalität und Kompatibilität mit der bestehen IT-Landschaft
- Akzeptanz bei Beschäftigten und (ggf.) Betriebsrat

- Sauberer Vertrag zur Auftragsverarbeitung
- Bei Anbietern mit Verarbeitung im Drittland:
  - technische Absicherungsmöglichkeiten sowohl in der Anwendung als auch durch extern Zusatzdienste
  - falls möglich Zusatzvereinbarung zu den Standardvertragsklauseln verhandeln („SCC Plus“)

Vielen Dank für die Aufmerksamkeit.

Nikolaus Bertermann
Rechtanwalt, Fachanwalt IT-Recht
zert. Datenschutzauditor (TÜV)

SKW Schwarz Rechtsanwälte
Kurfürstendamm 21, 10719 Berlin
n.bertermann@skwschwarz.de

Weiterführende Informationen und Links

- BSI - Kompendium Videokonferenzsysteme
  https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Videokonferenzsysteme/videokonferenzsysteme.html
- GDD-Praxishilfe - Videokonferenzen und Datenschutz
  https://www.gdd.de/downloads/praxishilfen/gdd-praxishilfe_xvi-videokonferenzen-und-datenschutz
- BlnBDI - Checkliste Videokonferenzen
  https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Checkliste_Videokonferenzen.pdf
- BlnBDI - Empfehlungen
  https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Empfehlungen_Videokonferenzsysteme.pdf
- Datenschutz Nord - Ende-zu-Ende Verschlüsselung von Videokonferenzen
  https://www.datenschutz-notizen.de/ende-zu-ende-verschluesselung-von-videokonferenzen-1825597/
- Wikipedia - Comparison of web conferencing software
  https://en.wikipedia.org/wiki/Comparison_of_web_conferencing_software