Wie sicher ist unsere Kommunikation?

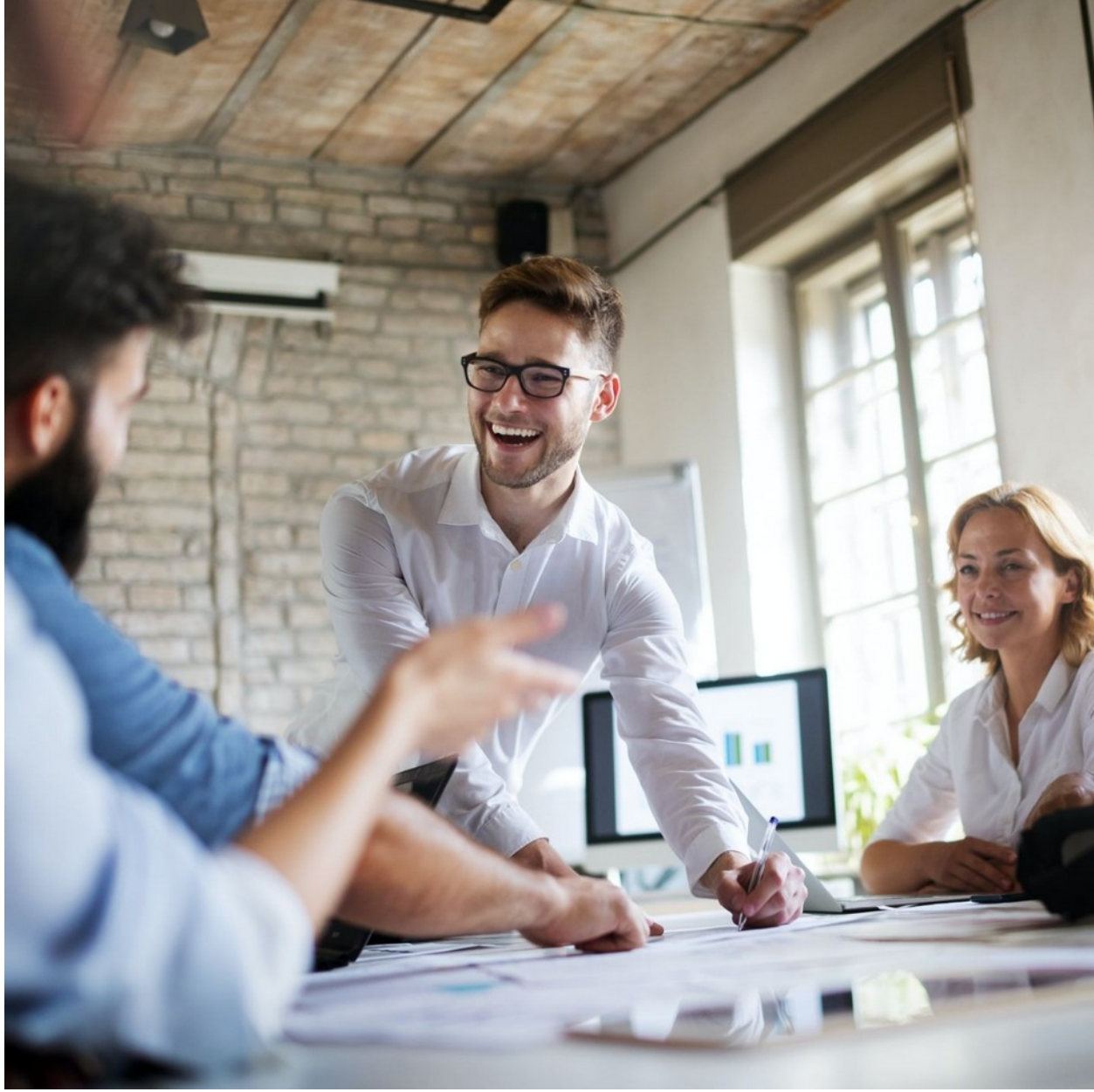
Geheim(nis)schutz und Nationale Sicherheit in Videokonferenzen

Transportverschlüsselung und Videokonferenzen

Mehr als nur Bild und Ton

- Video
- Audio
- Chat

- Dateien
- Whiteboard
- Protokolle
- Abstimmungen



Wer hat die Daten?

- Browser senden die Daten i.d.R. als WebRTC-Stream
  - Fat-Clients können proprietäre Protokolle.
- Diese Daten lassen sich TLS transportverschlüsseln.
- Da Peer-2-Peer nicht gut skaliert, laufen Daten i.d.R. über eine zentrale Videobridge.
- Als Endpunkt wird dort aber TLS terminiert
- Wer die Bridge hat, der hat die Daten.

Was heute möglich ist...

KI und Videodaten

- Speech2Text kann jedes Handy
- Vollständige Textprotokollierung und Zusammenfassung
- Bild-/Personen-/Gesichtserkennung
- Erkennung von Emotionen
- Übersetzung von Gebärdensprache in Text

WER redet WIE mit WEM über WAS.

Na, dann mach doch Ende-zu-Ende-Verschlüsselung!

Ende-zu-Ende-Verschlüsselung

Warum sich Videokonferenzen damit so schwer tun

- E2EE mit asymmetrischen Keys skaliert schlecht bei hohen Teilnehmerzahlen
- Schlüsselzahl ist „n*(n-1) / 2“: 100 TN = ~5000 Keys

- Ein symmetrischer Sitzungsschlüssel?
- Wie schützen wir historische aber auch zukünftige Daten der Konferenz?

- Teilnehmer kommen, Teilnehmer gehen
- Permanenter Key-Rollover
- Für eine Konferenz mit Echtzeit-Streaming

Was heute möglich ist...

E2EE bei kommerziellen Lösungen

- Einige nehmen E2EE für sich in Anspruch
- Teilweise E2EE nur in kleinem Teilnehmerkreis

- Die Umsetzungen liegen nicht als Open Source vor.
- Qualität und Hintertüren ggf. nicht überprüfbar.
- Zoom log bereits einmal https://news.ycombinator.com/item?id=22757697

- Zoom hat eine EAL2-Zertifizierung
- Aber nur für den Client, nicht für das Backend

- US-Videobridges sind stets dabei
- So oder so: Gewisse Metadaten („wer“) bleiben offen.

August 2023: Zoom ändert seine AGBs/T&C

Neue AGBs von Zoom sorgen für Wirbel:

> *10.4: You agree to grant and hereby grant Zoom a perpetual, worldwide, non-exclusive, royalty-free, sublicensable, and transferable license and all other rights required or necessary to redistribute, publish, import, access, use, store, transmit, review, disclose, preserve, extract, modify, reproduce, share, use, display, copy, distribute, translate, transcribe, create derivative works, and process Customer Content and to perform all acts with respect to the Customer Content, including AI and ML training and testing.*

Zoom COO Aparna Bawa rudert kurz darauf zurück (https://news.ycombinator.com/item?id=37034980), die AGBs werden erneut geändert.

> *We currently do not use audio, video or chat content to train AI models and we would not do so without customer consent.*

Tja...

- Welcher Content wird stattdessen genutzt?
- Currently?
- Zustimmung?

Aber was sagt uns das?

Was ist möglich?

Aber was sagt uns das?

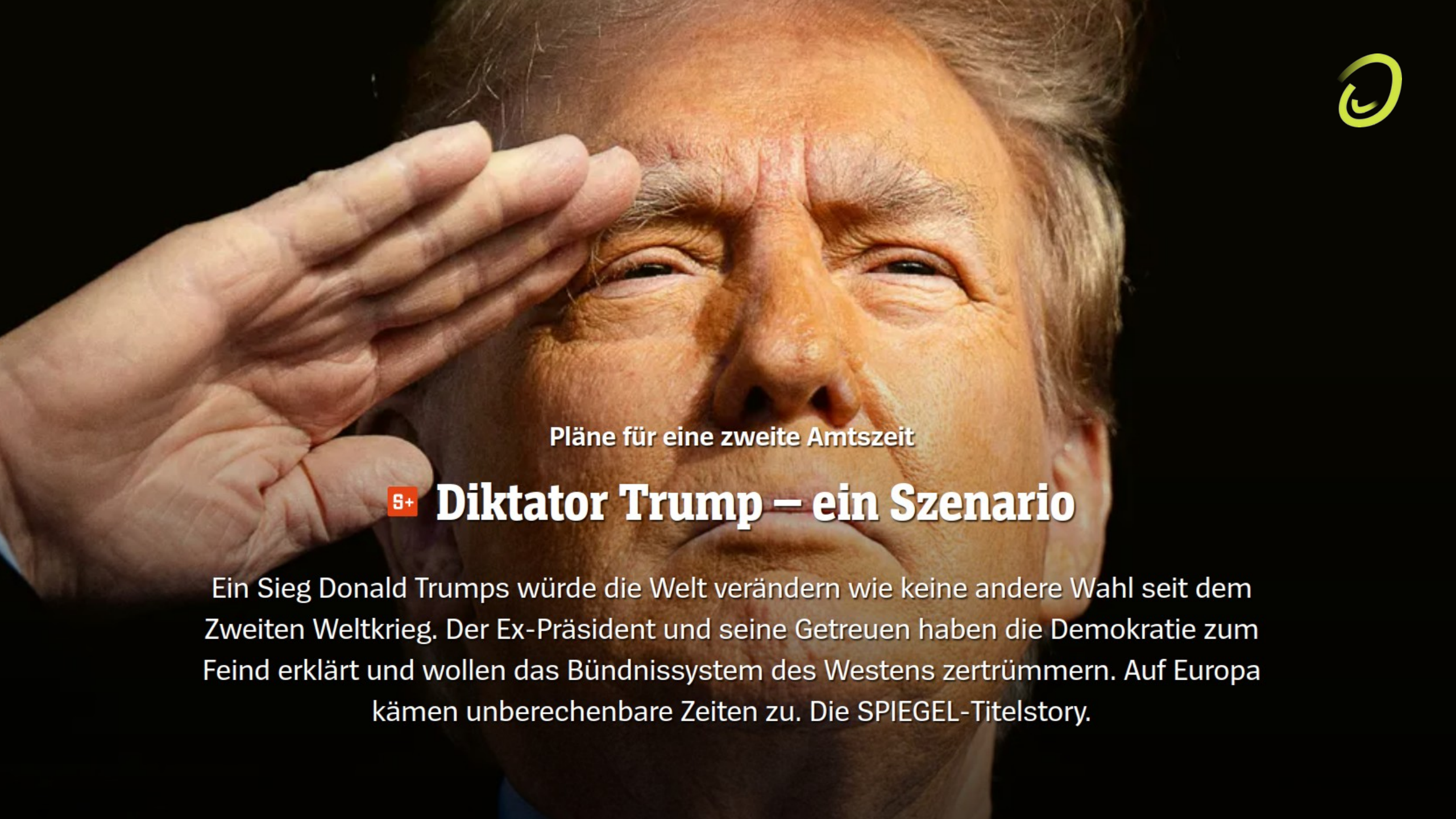
Wo liegt das Interesse?

Aber was sagt uns das?

Hätte ja klappen können.

Aber was sagt uns das?

Morgen ist ein neuer Tag.



Pläne für eine zweite Amtszeit

S+ Diktator Trump – ein Szenario

Ein Sieg Donald Trumps würde die Welt verändern wie keine andere Wahl seit dem Zweiten Weltkrieg. Der Ex-Präsident und seine Getreuen haben die Demokratie zum Feind erklärt und wollen das Bündnissystem des Westens zertrümmern. Auf Europa kämen unberechenbare Zeiten zu. Die SPIEGEL-Titelstory.

Digitale Souveränität und Nationale Sicherheit

Kommunikation muss nicht nur sicher, sondern auch verfügbar sein.

- Frei von politischer Einflussnahme ("Old Europe")
- Geographisch/Physikalisch autark verfügbar
- Kurze Wege, eigene Datacenter, eigene Kontrolle

- Kann ein Land einen Konflikt ohne Internet überstehen?
- Früher die Öl-Pipeline, heute das Datenkabel
- (Oh shit: Das geschah am 8. Oktober vor Schweden)

- Ja, Ich habe ein Problem, wenn lebenswichtige Services an US cloudbasierten Servern hängen.
- Freund oder Feind?
- Würden wir einen Konflikt "auf der falschen Seite" überstehen?

Butter bei die Fische:

Wo stehen wir also heute?

Status quo: Cloud-Videokonferenzen

Echte Performance und Stabilität nur als SaaS?

- Cloud-Dienste wie Zoom, Teams & Webex dominieren
- Stabilität und Performance stimmen
- Geräteunterstützung jenseits MS unterschiedlich

- Dienste als SaaS, teilweise inkl. Vendor-Lock-In
- Datenverarbeitung in fremden Ländern & RZs
- Code und Sicherheit nicht einsehbar

- Dienste orientieren sich an Business-Meetings
- Keine branchenspezifischen unterstützenden Features
- Nicht für Politik oder Bildung entwickelt

Status quo: OnPrem-Videokonferenzen OSS

Digitale Souveränität nur mit Open Source?

- Jitsi und BBB sind die bekanntesten Vertreter
- Open Source-Lösung zum Eigenbetrieb
- Beschränktes Featureset und Usability

- Langjährige verdiente Veteranen
- Softwarestack + Architektur teilweise > 10 Jahre alt
- Keine IT-Designziele von heute (Sicherheit/Skalierung)

- Nicht explizit für Videokonferenzen entwickelt (XMPP)
- Echte (Cloud-) Skalierbarkeit nicht gegeben
- Wenig/Keine API für Integration und Management

Wir brauchen eine state-of-the-art

Videokonferenzlösung für das Jahr 2022.

Was wäre denn „state of the art“?

- Open Source
- Sichere Programmierung (Rust!)
- Containerbasiert
- Skalierbar (Kubernetes)
- Zero-Trust-Konzept
- Anwenderfreundlich für Groß und Klein
- Funktionen auch für Bildung und öffentliche Hand
- Und auch ZITiS & BSI sollen einverstanden sein:
  Freigabe für VS-NfD und zertifizierbar nach EAL4

Also haben wir genau das entwickelt.

- ✔ Alles „from scratch“
- ✔ Saubere Konzepte, saubere Architektur
- ✔ Als Open Source unter EUPL auf OpenCoDE veröffentlicht
- ✔ 3 Jahre Entwicklungszeit, 20 Entwickler

Videokonferenzen „state of the art“

Videokonferenzen neu und zu Ende gedacht.

- Holt Nutzer ab, kümmert sich um Wohlfühlfaktor
- Ist zielgruppen- und kindgerecht (Grundschule!)
- Optimiert Workflows für nicht-technikaffine Nutzer

- Definiert Funktion einer Videokonferenz neu
- Unterstützt Moderatoren, Vortragende und Lehrer
- Kann auch Plenar- und Podiumsdebatten

- Mächtige Features mit Alleinstellungsmerkmalen
- „Videokonferenzen sind mehr als ein Sales-Meeting“
- Nutzung per Browser, eigenen Apps & Telefoneinwahl

- Ziel: „state-of-the-art Videokonferenzen“ neu definiert

Technik „state of the art“

On Premise.
Skalierbar.
Open Source.

- Installierbar im eigenen RZ (on-prem) oder SaaS in DE
- Videokonferenzsystem auch für >500.000 Nutzer
- Performant, skalierbar, sicher & stabil

- Open Source IT-Architektur und Sicherheit von heute
- Qualität und Scale-Out cloudbasierter Lösungen
- Optimaler Nachfolger von Jitsi, BBB, Nextcloud-Talk

- Integrierbar in (Lern-) Plattformen, Landesdatennetze, Telefonanlagen, bestehende Provider-Produkte uvam.

- Zero-Trust-Konzepte und Videobridges in wählbaren IT-Sicherheitszonen für Konferenzen

Einsatzszenarien:
OpenTalk ist optimal für...

OpenTalk ist optimal für...

Schulen & Universitäten

- Übersichtliche Klassenansicht bei >30 Teilnehmern
- Sortierbare Speaker-Listen zeigen inaktive Schüler
- API-Integration in Lernplattformen wie Moodle & Co.

- Moderationstools für modernen Unterricht
- Gamification für Abwechslung und Aufmerksamkeit
- Wheel-of-Names, Wollknäuel, Breakouts

- Einfacher Modus für nicht-technikaffine Lehrkräfte
- Modus für Prüfungen und Stillarbeit ("Subraumaudio")
- Umfragen, Gruppenarbeit uvam. vorab speicherbar

OpenTalk ist optimal für...

Politik & Behörden

- Skalierbar – geeignet für ganze Bundesländer
- Auch Ende-zu-Ende-Verschlüsselung möglich
- Unterstützt IT-Sicherheitszonen in Datennetzen

- Rechts- und revisionssichere Abstimmungen
- Telefoneinwahl, Aufzeichnung, Dolmetscher-Modus
- Konferenzen-in-Konferenzen ("Subraumaudio")

- Usermanagement nach Fraktionen/Gruppen
- Moderations-Teams, Podiums-Teilnehmer und VIPs
- Gremienarbeit, Plenardebatten, Zuschauer-Streaming

OpenTalk ist optimal für...

Unternehmen & NGOs

- Digital souveräner Betrieb OnPrem oder als SaaS
- Auch Ende-zu-Ende-Verschlüsselung möglich
- IT-Sicherheitszonen in Datennetzen und Geo-Location

- Branding und Theming individuell je Konferenz
- Vorgabe CI-konformer Bluescreen-Hintergründe
- Zeitüberwachung von Konferenz, Breakouts und Pausen

- Agenda und Einladungsmanagement
- Authentifizierung über zentrales ID-Management
- 24/7 Enterprise-Support möglich

OpenTalk ist optimal für...

Provider & Plattformen

- Scale-Out für Millionen Nutzer und Konferenzräume
- Performante sichere Programmierung in Rust
- Backend Scale-Out "ohne Limit" mit Kubernetes

- Räume, Nutzer & Konfigurationen per API steuerbar
- Whitelabel in ISP-Portale integrierbar
- Accounting-, Abrechnungs- und Monitoring-Schnittstellen

- Limitierung zeitgleicher Konferenzen/Teilnehmer möglich
- Theming individuell je Kunde/Konferenz/Nutzer möglich
- Von Heinlein als Provider für Provider gemacht ;-)

Wo ist OpenTalk heute?

- Landeslösung in Thüringen
- Im scale out Providerbetrieb @mailbox.org
- Bestandteil der Telekom Magenta Cloud

- Derzeit im PoC für Umweltbundesamt, Land Schleswig-Holstein/Dataport und anderen
- Partnerschaften mit Telekom, Plusserver, mgm, Cancom uvam.

- Als SaaS sofort frei buchbar
- Als OSS in Containern sofort selbst installierbar

Roadmap 2024:
Woran wir arbeiten

Besondere Features

#1 H.323

- Implementierung einer H.323/SIP-Bridge
- Ermöglicht die Weiternutzung vorhandener Raumkommunikationssysteme (CISCO, Poly)
- Wichtig für den Bestands-/Investitionsschutz

#2 Integration Matrix

- Tiefe technische Kooperation mit Element/Matrix
- Gegenseitige Integration von Chat und Video
- Wir nehmen den Matrix-Chat, Element nimmt OpenTalk

Besondere Features

#3 Echtes E2EE

- Echte E2EE mit Schlüsselrotation bei TN-Wechsel
- Implementierung eines eigenen Protokolls oder Nutzung des Matrix-Protokolls durch Integration
- Problem: Browser-Support

#4 Lokale KI

- KI bietet für Konferenzen spannende Features – Protokollierung, Zusammenfassung, Checklisten, Übersetzungen
- Wir arbeiten an der Integration einer lokal mitlaufenden KI im Container und/oder Integration einer Cloud-KI eines deutschen KI-Anbieters
- Spannend auch für Barrierefreiheit

Besondere Features

#5 Digitale Teilhabe

- OpenTalk ist bereist sehr weitgehend barrierefrei
- Zusammen mit der Uni Bremen arbeiten wir an einer über die Standards hinausgehenden Barrierefreiheit
- Lokale KI kann insb. im Bereich Gehörlosigkeit wichtige Text-Unterstützung bieten
- Implementierung eines speziellen Gebördendolmetschermodus für Konferenzen

#6 CC-EAL4

- Zertifizierung von OpenTalk nach CC-EAL4 beim BSI
- Antrag eingereicht, akzeptiert, Kickoff durchgeführt
- Dauer: Ca. 9 Monate
- CC-EAL4 hat sonst keine OSS-Videokonferenz (und bei den kommerziellen Lösungen uWn nur Webex in Teilen)
- Nebeneffekt: CC-EAL4 für Keycloak
- Extrem spannend: Aufkommende NIS2-Richtline erfordert ggf. Einsatz von CC-EAL4-Software

Vielen Dank bis hierhin.

OpenTalk live testen?

https://opentalk.eu/de/demo

Bock auf'n PoC? ;-)

Sprechen wir darüber

Peer Heinlein

Tel: +49 30 40 50 51-42
p.heinlein@opentalk.eu

OpenTalk GmbH
Schwedter Straße 9a | 10119 Berlin
https://opentalk.eu
https://demo.opentalk.eu