FTAPI

Browser-basierte E2E-Verschlüsselung

Sicher, skalierbar, einfach.

Kurzvorstellung Bernhard Weber

BERNHARD WEBER

- Tech Lead im FTAPI Development
- 4 Jahre bei FTAPI
- +10 Jahre Erfahrung in der agilen Softwareentwicklung
- Schwerpunkt Customer Centric Development und UX

E2EE: Das A&O beim Datentransfer

- Datenkriminalität wächst exponentiell und strukturell
- Server-seitiger Datendiebstahl ist ein großes Risiko
- Datentransfer ist weiterhin eine beliebtes Einfallstor
- Regulierungen und gesetzliche Anforderungen wie **NIS-2** und die **EU-DSGVO** fordern den Einsatz starker Verschlüsselung
- Verschlüsselung ist essenziell, um Schaden auch im Falle eines Datenverlusts zu minimieren

> **Ende-zu-Ende-Verschlüsselung** ist eine Methode, bei der Daten **zwischen Sender und Empfänger** so verschlüsselt werden, dass **nur diese beiden Parteien die Daten entschlüsseln** können, während Dritte (einschließlich der **Dienstanbieter**) keinen Zugriff auf die Klartextdaten haben.

Quelle: IBM

Warum E2EE im Browser?

kaum Wartungsaufwand

keine Updates lokaler Software erforderlich und damit für Nutzer maximal einfach

Nutzerfreundlichkeit

keine zusätzliche Installation und Konfiguration notwendig

Zugänglichkeit

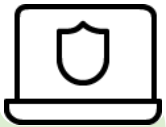
Erreichbarkeit von überall und auf jedem Gerät mit einem Webbrowser

Verbreitung

Nutzer sind an die den Einsatz Browser-basierter Lösungen gewöhnt

Erst, wenn **Verschlüsselung einfach** ist, wird sie auch genutzt - und nur dann bringt sie auch was.

Chancen und Risiken



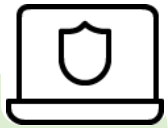
Problem

- Browser-basierte E2EE setzt häufig auf Third Party Libraries
- Sicherheitsrisiko: Libraries sind nicht standardisiert und zertifiziert

Lösung von FTAPI

- Nutzung der Browser-API
- Keine Abhängigkeiten durch Drittanbieter

Chancen und Risiken



Problem

- Browser-basierte E2EE setzt häufig auf Third Party Libraries
- Sicherheitsrisiko: Libraries sind nicht standardisiert und zertifiziert

Lösung von FTAPI

- Nutzung der Browser-API
- Keine Abhängigkeiten durch Drittanbieter

Erhöhte Sicherheit

- Standardisierte Verschlüsselung (NIST)
- Minimierung der Angriffsfläche

Verbesserte Performance

- Verschlüsselung direkt im Browser
- Schneller und sicherer als Verschlüsselung auf Anwendungsebene

Vereinfachter Export

- Dual Use für vereinfachte Software-Exportbestimmungen

FTAPI

Herausforderung bei der Entwicklung

Einbindung von OPFS (Origin Private File System)
Kompatibilitätsunterschiede von Browsern und Betriebssystemen
Hoher Konfigurationsaufwand

Kompatibilität von Verschlüsselungsalgorithmen
Rückwärtskompatibilität mit bisherigen Systemen und Algorithmen
Unterschiedliche Unterstützung in verschiedenen Browsern

Wartung / Hilfestellung bei Kunden
Erschwerter Support bei Fehlern und Problemen
Ansprechpartner mit technischem Know-How notwendig

Einsatz von Krypto-Agilität
Zukunftssicher durch austauschbare Kryptografie

Das Ergebnis

- **Browser-basierte** E2E-Verschlüsselung nach neuestem Stand der Technik
- Keine **Third Party Library** im Einsatz
- Kein **Mehraufwand** für den Nutzer
- Verschlüsselung passiert im **Hintergrund**

FTAPI

Vielen Dank für die Aufmerksamkeit!

Mehr Informationen zu FTAPI und unserem Produktportfolio gibt es an Stand 509