FTAPI Checkliste

Wann sich verschlüsselte Kommunikation lohnt

Sicherer Datenaustausch

Die digitale Souveränität gewinnt in einer zunehmend vernetzten Gesellschaft immer weiter an Bedeutung. Eine wichtige Rolle spielt dabei das Thema IT-Sicherheit. Obwohl das Thema immer mehr in das Bewusstsein von Behörden, Unternehmen und auch der Nutzerinnern und Nutzern rückt, besteht beim Austausch vertraulicher Daten weiterhin Nachholbedarf.

Denn die unverschlüsselte Kommunikation – sowohl im privaten, wie auch im geschäftlichen Umfeld – zählt weiterhin als häufigstes Einfallstor von Cyberkriminellen.

Dabei ist die verschlüsselte Datenübertragung längst nicht mehr umständlich, sondern mit der richtigen Lösung ganz einfach und intuitiv.

Die vier Sicherheitsstufen bei FTAPI

1 Sicherer Link

Die Zustellung liegt hinter einem sicheren Link ab. Jeder, der diesen Link kennt, kann die Zustellung öffnen und die Dateien herunterladen.

2 + Login

Nur bestimmte Empfänger können auf die Daten zugreifen. Dafür benötigen sie einen FTAPI-Account oder einen automatisch erstellten Gast-Account.

3 + Verschlüsselter Anhang

Alle Anhänge sind Ende-zu-Ende-verschlüsselt. Empfänger nutzen zur Entschlüsselung einen vorab generierten SecuPass Key.

4 + Verschlüsselte Nachricht

Auch die Nachricht ist Ende-zu-Ende-verschlüsselt und wird ebenfalls mit dem vorab festgelegten SecuPass Key entschlüsselt.

Mehr Informationen zu sicherem Datenaustauch finden Sie auf unserer Webseite.

Weiterführende Informationen

Gerne bieten wir Ihnen eine Vertiefung des Themas in einem persönlichen Gespräch mit einem unserer Experten an.

Wenn Sie bereits einen oder mehrere konkrete Anwendungsfälle haben, für die eine verschlüsselte Kommunikation notwendig sind, finden wir gemeinsam mit Ihnen eine optimale Lösung und unterstützen Sie gerne bei der Implementierung.

FTAPI Checkliste

Wann sich verschlüsselte Kommunikation lohnt

Mit unserer kompakten Checkliste erhalten Sie schnell einen Überblick darüber, wann Sie verschlüsselt kommunizieren sollten – und welche Sicherheitsstufen Ihnen dabei zur Verfügung stehen.

	Ja	Nein
Sicherheitsstufe 1 - Sicherer Link		
• Die Dateien, die Sie verschicken, enthalten personenbezogene Daten und fallen damit unter die Richtlinien der DSGVO.	☐	☐
• Die Dateien, die Sie verschicken, sind zu groß für reguläre E-Mail-Postfächer.	☐	☐
• Für den Versand der Nachricht und des Anhangs ist es wichtig, eine Empfangs- und Downloadbestätigung zu erhalten.	☐	☐
• Ihre Organisation steht für Sicherheit und Vertrauen - Transparenz und Nachvollziehbarkeit sind Ihnen wichtig.	☐	☐
Sicherheitsstufe 2 - Sicherer Link + Login		
• Die Daten, die Sie verschicken, sind so schützenswert, dass der Empfängerkreis kontrolliert werden muss.	☐	☐
Sicherheitsstufe 3 - Sicherer Link + Login + Verschlüsselte Dateien		
• Die angehängten Dateien enthalten Geschäftsgeheimnisse/Patente/geistiges Eigentum.	☐	☐
Sicherheitsstufe 4 - Sicherer Link + Login + Verschlüsselte Dateien + Verschlüsselte Nachricht		
• Die übermittelten Nachrichten sind geschäftskritisch und vertraulich.	☐	☐
• Die Inhalte der übermittelten Nachrichten können als Basis für Phishing-Angriffe genutzt werden.	☐	☐
• Ein unkontrolliertes Abfließen der Daten führt zu Vertrauensverlust, Imageschäden oder empfindlichen Bußgeldern.	☐	☐
• Compliance und vertragliche Vereinbarungen erfordern eine verschlüsselte Datenübertragung.	☐	☐

Sie haben mindestens einmal ja angekreuzt? Dann ist es Zeit für eine Lösung, mit der Sie Ihre Kommunikation einfach und sicher verschlüsseln können.

Lassen Sie uns darüber sprechen!

Beraten lassen