JW FROEHLICH
Test and Assembly
Solutions for Powertrain

JWF-SecureClient
Zentrale Sicherheitsarchitektur für Ihre Produktionslinie

Die Herausforderung in der Praxis

In modernen Produktionsumgebungen werden sicherheitskritische Informationen erzeugt und verarbeitet – darunter kryptografische Schlüssel, Fahrzeug-IDs, Flash-Inhalte und Logistikregistrierungen.

Regulatorische Vorgaben wie der EU Cyber Resilience Act (CRA) erhöhen die Anforderungen an Integrität, Rückverfolgbarkeit und Schutz der Systeme auch für unsere Kunden deutlich.

Die Sicherheitsarchitektur Ihrer Produktions-IT muss klar definiert sein.

Der JWF-SecureClient fungiert als zentrale Sicherheitsinstanz innerhalb der Produktions-IT und bündelt sicherheitskritische Funktionen in einer kontrollierten Architektur.

Sicherheitskritische Operationen – darunter Schlüsselgenerierung, Challenge-Response-Berechnung und Flashdaten-Verschlüsselung – werden ausschließlich im geschützten Serverkern ausgeführt.

Architekturprinzip

→ Zentrale Schlüsselgenerierung und -verwaltung
→ Geschützte Übertragung von Master-Keys auf Prüf-PCs
→ Serverseitige Flashdaten-Verschlüsselung
→ Sichere Logistik-Anbindung mit asymmetrisch verschlüsseltem Datenaustausch
→ Prozessverriegelung bei fehlender Registrierung

Bei JW Froehlich trifft jahrzehntelange Erfahrung im Prüfstandsbau auf modernste Cybersecurity-Architektur. Mit dem JWF-SecureClient übersetzen wir Kundenanforderungen in hochsichere Produktionsumgebungen – konsequent nach dem Prinzip „Security by Design“.

Der JWF-SecureClient

Typische Risikoszenarien in Produktionslinien

→ Dezentral betriebene Prüfstationen können zum Angriffspunkt werden und sicherheitskritische Prozesse kompromittieren.
→ Unverschlüsselte oder unzureichend geschützte Flash-Inhalte bergen das Risiko gezielter Industriespionage.
→ Kryptografische Schlüssel können bei fehlender zentraler Kontrolle oder unzureichendem Schutz abgegriffen oder missbräuchlich verwendet werden.
→ Fehlende oder fehlerhafte Logistik-Registrierungen gefährden die Integrität des Produktionsablaufs.
→ Unzureichende Dokumentation erschwert die Nachweisführung gegenüber Audit- und Aufsichtsstellen.

Der JWF-SecureClient reduziert diese Risiken durch eine klar definierte Trusted Security Zone und serverseitige Kontrolle sicherheitskritischer Prozesse.

Technische Highlights

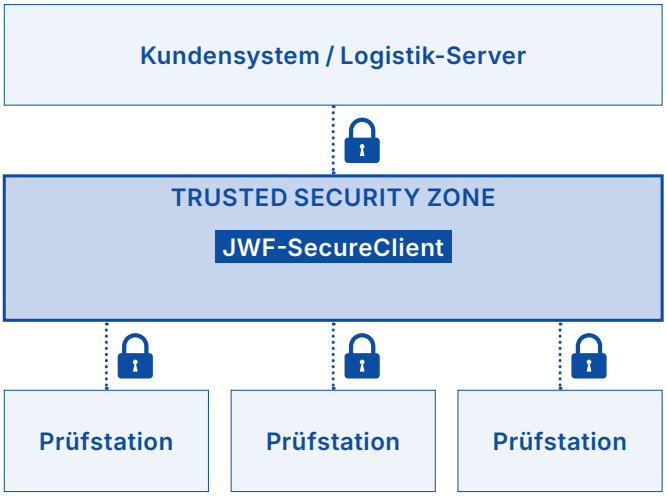
Manipulationsgeschützte Schlüsselverwaltung
Sichere Durchführung des standardisierten AUTOSAR 948-Prozesses für Secure Hardware Extensions (SHE)

Challenge-Response-Berechnung im Serverkern
Master-Schlüssel verbleiben geschützt im JWF SecureClient.

Asymmetrisch gesicherte Logistik-Integration
beispielsweise über openPGP, ElGamal, SHA-512

Prozessverriegelung
Ein Prüfling verlässt das Prüffeld erst nach validierter Rückmeldung des Kundensystems.

Integration kundeneigener Software
Sicheres Handling sensibler Kundendaten in geschützter Serverumgebung



Architektur im Überblick

Ihr Mehrwert

→ Schutz Ihres geistigen Eigentums
→ Absicherung gegen Produktionsmanipulation
→ Konformität mit CRA-Anforderungen
→ Minimierte Angriffsfläche
→ Passgenaue Integration in bestehende IT-Strukturen

Regulatorische Absicherung

Mit dem JWF-SecureClient schaffen Sie die strukturelle Grundlage für:

→ Umsetzung einer produktionsorientierten Sicherheitsarchitektur gemäß EU Cyber Resilience Act
→ Dokumentations- und Nachweispflichten
→ Auditierbarkeit sicherheitskritischer Produktionsschritte

Möchten Sie Ihre Produktionslinie resilient gegenüber Cyberangriffen aufstellen und regulatorisch zukunftssicher gestalten?
Unsere ExpertInnen beraten Sie gerne:

JW Froehlich Maschinenfabrik GmbH
Vertrieb
Telefon +49 711 797 66-0
sales@jwf.com

Stand 02/26 | Technische Änderungen vorbehalten.

JW FROEHLICH
Test and Assembly Solutions for Powertrain
Germany | UK | USA | China
www.jwf.com