JW FROEHLICH

Test and Assembly
Solutions for Powertrain

JWF SecureClient
Integrated security architecture for your production line

The challenge

Modern production environments have to manage the generation and handling of security-critical information, including cryptographic keys, vehicle IDs, flash content and logistics registrations.

Regulatory requirements like the EU Cyber Resilience Act (CRA) that impose tighter integrity, traceability and system protection requirements have an impact on you as our customers.

A clearly defined security architecture is essential for your production IT.

The JWF SecureClient is a central security instance within production IT, which bundles security-critical functions into one controlled architecture.

Security-critical operations, including key generation, challenge-response authentication and flash encryption, take place exclusively in a protected server core.

Design principle

- → Central key generation and management
- → Secure transfer of master keys on test PCs
- → Server-side flash encryption
- → Secure logistics connection with asymmetric encrypted data exchange
- → Process interlock in case of inadequate registration

At JW Froehlich, decades of experience in test stand construction meets state-of-the-art cybersecurity architecture. With the JWF SecureClient, we translate customer requirements into a highly secure production environment, following the principle of Security by Design.

JWF SecureClient

Typical production line risk scenarios

→ Test stations with centralised operation can be vulnerable to attacks, compromising security-critical processes
→ Unencrypted or inadequately protected flash contents are prone to becoming targets of industry espionage
→ Without central control and sufficient protection, cryptographic keys can be intercepted or misused
→ Missing or inadequate logistics registrations jeopardise the integrity of the production process
→ Inadequate documentation complicates verification management for audit authorities or regulatory bodies

JWF SecureClient mitigates these risks by establishing a clearly defined trusted security zone and controlling security-critical processes on the server side.

Technical highlights

Tamper-proof key management

Secure implementation of the standardised AUTOSAR948 process for Secure Hardware Extensions (SHE)

Challenge-response authentication in the server core

Master keys remain secure within the JWF SecureClient

Asymmetrically secured logistics integration

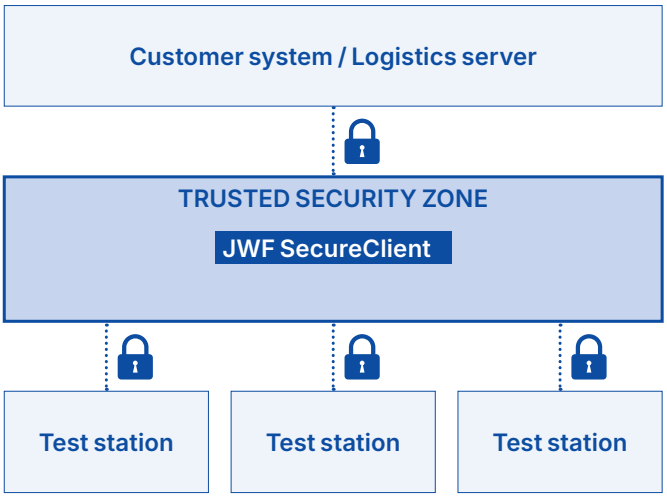
Using OpenPGP, ElGamal, SHA-512, for example

Process interlock

Test items only leave the test room once the customer system has provided validated feedback

Integration of customer-specific software

Secure handling of sensitive customer data in a protected server environment



Design overview

Your benefits

→ Protection of your intellectual property
→ Protection against production tampering
→ CRA compliance
→ Reduced vulnerability
→ Seamless integration into existing IT structures

Regulatory compliance

The JWF SecureClient creates the structural basis for:

→ Implementation of a production-orientated security architecture in accordance with the EU Cyber Resilience Act
→ Compliance with documentation and reporting requirements
→ Auditability of security-critical production steps

Do you want to protect your production line against cyber attacks and ensure compliance with future regulations?
Contact our team of experts to learn how:

JW Froehlich Maschinenfabrik GmbH
Sales Team
Tel.: +49 (0) 711 797 66-0
sales@jwf.com

Last updated 02/26 | Subject to technical modifications without notice.

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