intertrust®

Is your PKI ready for factory and field provisioning?

Secure, offline identity provisioning in real-world deployments.

The challenge

Limited connectivity in manufacturing and the field makes secure device provisioning nearly impossible with traditional PKI.

The solution

A robust PKI solution must support secure certificate management even in offline factory and field environments.

5-steps to determine offline PKI readiness

1. Verify offline provisioning support

Can your PKI issue and manage certificates without continuous cloud connectivity?

2. Assess device-agnostic compatibility

Does your PKI handle diverse hardware, chipsets, and security profiles from different OEMs?

3. Evaluate secure key injection tooling

Do you support secure key generation and injection in constrained, offline factory environments?

4. Confirm zero-trust certificate issuance

Is certificate issuance policy-driven and hardware authenticated, even in disconnected environments?

5. Test factory-to-field continuity

Can you maintain certificate trust across the device lifecycle—from production to deployment?

Building at scale?

Discover how iPKI simplifies and secures provisioning across every step of your device journey.

Read more