



Zero Touch. Zero Trust. Full control.

Automated Zero Touch Onboarding and Identity Management for your (I)IoT devices – secure, scalable, and flexible.

The Key Challenge

Manual onboarding and identity management of a large number of connected devices in industrial infrastructures is time-consuming, error-prone, and entails significant IT security risks. 92% of all industrial devices are insecurely configured. At the same time, regulatory requirements for identification, authentication, and encrypted communication are increasing due to the Cyber Resilience Act (CRA), the NIS-2 Directive, and IEC 62443.

The Solution: KEYNOA

With our software KEYNOA, the onboarding of devices and the integration with external systems such as cloud and data platforms are fully automated through our innovative zero-touch process. This reduces onboarding costs by up to 90%. Our solution protects digital identities throughout the entire device lifecycle and simplifies future authentications and updates.

Your Benefits with KEYNOA

-  **Reduced Costs:** Save time and money through automated device onboarding and identity management.
-  **Maximum Flexibility:** Devices can be individually configured right up until installation.
-  **Open Ecosystem:** KEYNOA is built on a modular, API-first architecture based on open standards.
-  **Future-Proof Cryptography:** Compliant with NIS-2, CRA, IEC 62443, and modern PKI standards.

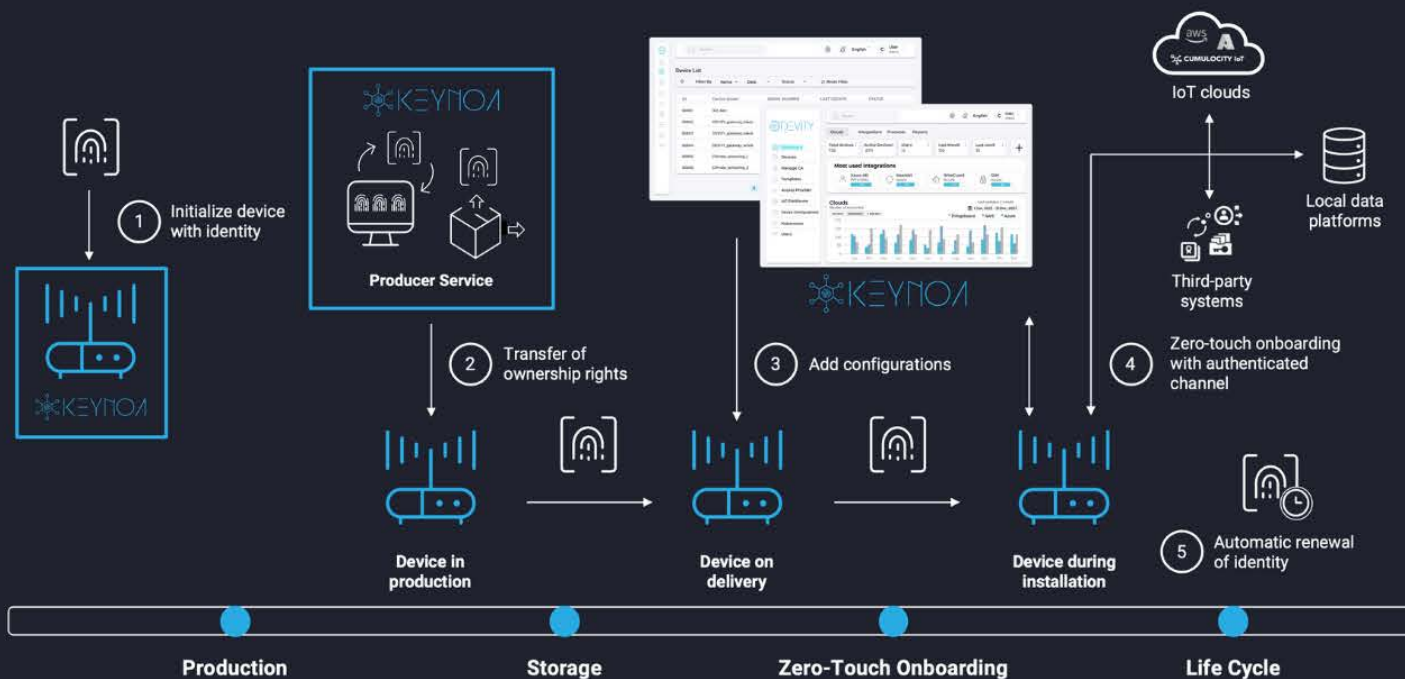
KEYNOA Features

-  **Zero Touch Onboarding**
As soon as a new device is turned on, KEYNOA detects it and assigns the right deployment configuration automatically.
-  **Zero Trust Identity Management**
Automatically and securely managing digital identities throughout every stage of the device lifecycle
-  **Untrusted installer**
Installers can onboard devices into the network without needing access to sensitive infrastructure.
-  **Centralized Management**
Secure, centralized, and standardized – configuration no longer happens in the field but within a protected management platform.



**Get your KEYNOA
demo now!**

Build a Secure and Trusted Value Chain



The Components of KEYNOA

KEYNOA consists of device software, the KEYNOA Engine, and orchestration software including a robust backend, comprehensive APIs, and a user-friendly UI for efficiently managing digital identities and configurations.

Secure Production

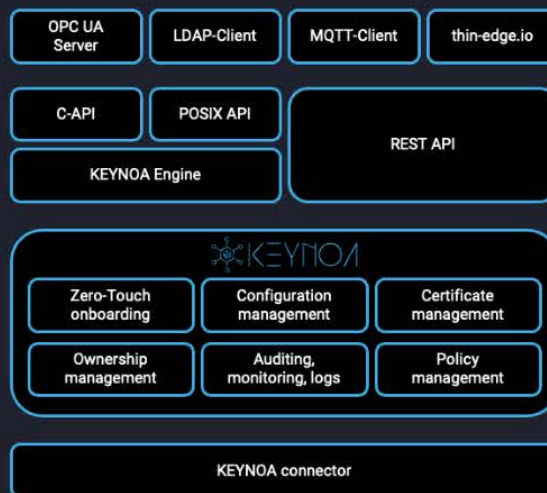
- Issuance of unique device identities.
- Secure IoT identity protocols and open, standardized onboarding.
- Lightweight client.
- TPM support.
- Secure installation of updates.

Trusted Supply Chain

- Secure transfer of device identities.
- Assignment of devices to customers.
- Seamless integration with commissioning systems.
- Ensured device integrity.

Secure Device Onboarding

- Mutual authentication between device and external systems.
- Configuration with templates.
- Device-specific configuration right up until installation.
- Service technicians do not require access to sensitive infrastructure.



Integration

- Seamless integration into existing landscapes & third-party solutions.
- External and internal PKIs.
- IoT clouds & data platforms.
- User management.
- Asset management.

Secure Lifecycle

- Structured PKI hierarchy.
- Automated certificate management.
- Trust anchor management.
- Roles and responsibilities.
- Certificate profiles & recommendations.
- Revocation and end-of-life procedures.
- Reliable backup and recovery.
- Patch management.
- Compliance and customer activity auditing.
- High system availability.
- HSM support.
- Intuitive interface.
- Batch actions.



**Try
KEYNOA
now**

- 30-Day free trial
- Test Tenant in KEYNOA Cloud (SaaS)
- KEYNOA Engine as container or with test device (Janz Tec AG)

