P3KI
trust yourself.

Enabling Secure Identity and Access Control in Industrial OT

Leveraging P3KI in Brownfield Environments

Version Rev2
2025-08-04

1 Context: Identity & Access Challenges in Brownfield OT

Legacy Operational Technology (OT) environments, especially in brownfield industrial installations, remain difficult to modernize. Common pain points include:

- **No integration with central Identity Providers** (IdPs) due to air-gapped or segmented Purdue-level architectures.
- **Functional (shared) account use** on standalone workstations and domain-joined assets, lacking user-level traceability.
- **Manual provisioning burden** for local IT or OT administrators.
- **Weak auditability and security** from shared credential usage.

Modern security demands, coupled with compliance frameworks (e.g., IEC 62443, NIST CSF), now require:

- **Personalized, traceable access** to OT systems.
- **Reduced operational cost** for access management.
- **Offline-capable** identity propagation.
- **No dependency on centralized or cloud-based services**.

2 P3KI's Role

P3KI introduces a **decentralized, cryptographically secure trust infrastructure** purpose-built for offline, distributed environments. Applied to industrial OT, it enables:

2.1 Solution 1: Personalized Access Without Central Connectivity

- Create **personalized user accounts in local Active Directory** (AD) domains—without requiring real-time communication with central IT.
- Transfer identity and permission **data over-the-air-gap** using **biometrically-secured** smartphones.
- Provisioning **workflows are offline-capable** and cryptographically verifiable.

2.2 Solution 2: Audit-Ready Login to Shared Functional Accounts

- Users can **log into existing functional accounts** (e.g., "Operator", "Administrator") **without knowing the password**.
- Logins are **authorized using individual, revocable, signed permissions** bound to a user's identity.
- Enables **fine-grained audit trails and accountability** in otherwise non-personalized environments.

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

3 Architecture Overview

3.1 Core Components

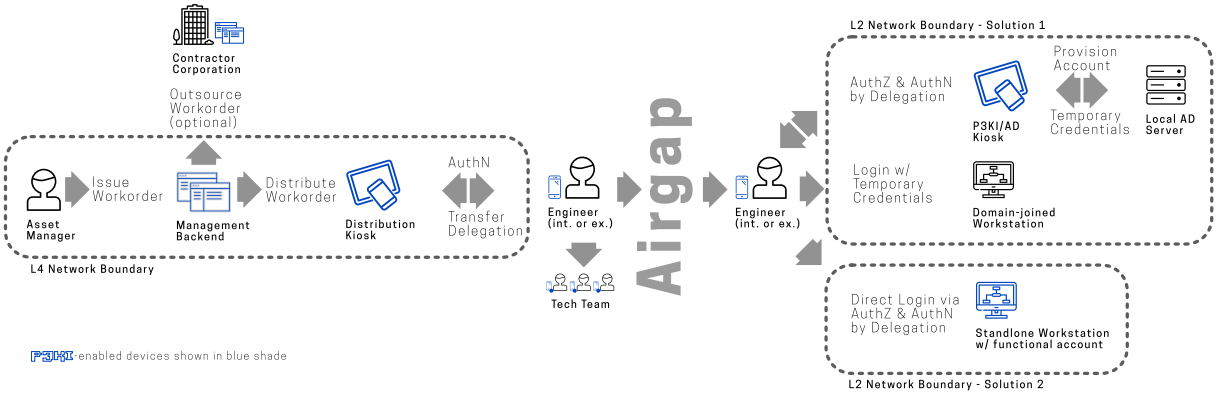
Component	Description
Local Effectors	Direct Windows login integration, or AD user bootstrap (via local P3KI service)
Management Backend	Role and permission management for users and assets. Supports centralized, local, or federated deployment.
Self-Service Kiosk	Users identity onboarding and permission distribution. Usable at plant entrance, break rooms, cafeteria.
Cross-Air-Gap Transport	Smartphone-based propagation (Android app). Smartcard and Apple support planned.

4 Key Security Mechanisms

- Secure Element-backed key storage and biometric/PIN verification on mobile devices.
- Signed, time-bound, revocable delegation artifacts.
- All delegations and logins are cryptographically auditable and tamper-proof.

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

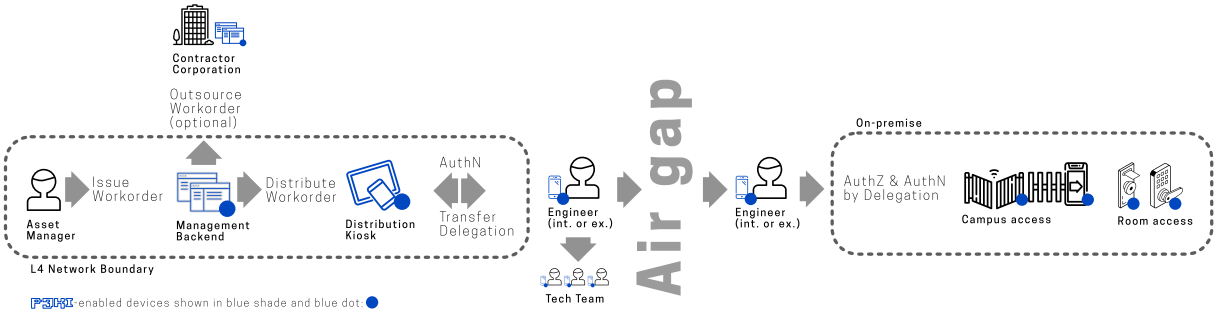
5 Example Scenario: Factory Operator Access



- **Workorder Issuing**
  Asset Manager issues workorder in central or plant-local system. The workorder can be issued to internal works as well as external contractors. Workorders are ultimately represented by P3KI delegations.
- **Arrival & Authorization**
  A contracted Engineer arrives on-site for a two-week assignment. In advance, they have been granted formal delegation from their headquarters – linked to the original work order created by the Asset Manager.
- **Ad-hoc Delegation**
  If the Engineer arrives with a team of technicians, they're able to grant the team part of their authorization, even after having crossed the air gap.
- **Seamless Credential Setup**
  Equipped with a secure, company-issued mobile device, the Engineer's team is authorized to access an operator workstation based on their received delegations. Instead of receiving individual login credentials, they uses the pre-configured functional account shared by other plant operators.
- **Personalized & Traceable Access**
  - No password entry is required.
  - The Engineer's team's cryptographic identities in combination with the delegation they received are used to unlock access.
  - Although they use a shared account, all actions during their sessions are attributed to individuals of the Engineer's team, ensuring full traceability.
- **Built-in Expiry & Clean Exit** Once the assignment ends, the Engineer's and therefor also their team member's access permissions expire automatically – no manual account changes or cleanup needed.

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

6 Example Scenario: Physical Access Control



The previous **scenario can be combined** with and extension for **physical access control** systems.

There are practically **no changes to the process** from the point of view of both, the Asset Manager and the Engineer.

The Asset Manager either **explicitly grants access** to required locations or the **workflow tool automatically assigns location access** permissions as needed for the task. The Engineer and their team can use the **same mobile application to manage all identities and permissions**.

Solutions are available off-the-shelf or tailor-made:

- **Off-the-shelf**
  Industrial-grade hardware for use with electronic latch doors (12-24V AC/DC latch systems)
- **Tailor-made**
  Integration into existing access control systems possible on a case-by-case basis.
  Please get in touch with us for details.

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

7 Differentiators Compared to Traditional IAM

Feature	Traditional IAM	P3KI
Air Gap Capable	**No**	**Yes**
Shared Account Auditability	**Weak**	**Strong**
Offline Delegation	**Not supported**	**Fully supported**
System Architecture	**Centralized**	**Local/Federated/Decentralized**
Smartphone Integration	**Optional or limited**	**Secure Element + biometric authentication**
Revocation and Time-Bound Access	**Heavy, CRL/OCSP-based**	**Lightweight, built-in expiration**

8 Business Value and ROI

Feature	Benefit
Offline Operation	Works in **air-gapped environments** (Purdue L2/L3), no network dependency[1]
No Shared Passwords	**Removes** one of the biggest **audit and attack concerns** in OT
Manual Provisioning Savings	**Significant weekly time savings per site**[2] on local account management
Improved Workforce Agility	**Easier and faster onboarding** of external contractors or rotating staff[3]
Fast Deployment	**No need for centralized infrastructure** or complex setup[4]
Flexible Pilot Rollout	Plant-by-plant[5] **deployment without upfront architectural overhaul** significantly reduces installation costs
Compliance and Auditability	**Meets key controls** in IEC 62443, NIST 800-53, and ISO 27001

[1] System design is **"resilience first"**, enabling full offline operation. Optional networked capabilities may be used to speed up information propagation but are not a prerequisite.

[2] Manual management of local personalized accounts in an average manufacturing site setup with multiple plants requires a single person to invest around **two hours per week per site** according to a customer survey conducted in 2025.

[3] From the Asset Manager point-of-view, a **reduction of up to 90% in workload** is achievable, since permissions only have to be granted and all further steps are driven by the permitted party and account deactivation is an automatic process.

[4] Deployments tailored to local resources enable multi-tiered organizations to **forego time-intensive alignment with central IT services**.

[5] Individual deployments are always scoped and can be merged with other deployments later on without conflicts.

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

9 Conclusion

P3KI effectively bridges the IT/OT security gap in brownfield industrial environments by:

- Enabling **personalized, identity-based access without requiring changes** to existing infrastructure,
- **Improving security and traceability**, even when shared functional accounts are used,
- Supporting **cost-efficient, decentralized deployment** that scales alongside operational needs.

This approach offers a **practical path toward Zero Trust access in OT** environments – without relying on network connectivity or cloud services.

For integration guides or a tailored evaluation for your OT landscape, contact:

Personal contact	**Gregor Jehle**, CEO gregor@p3ki.com +49 157 86882567
Head office & mailing address	P3KI GmbH c/o Recurity Labs GmbH Wrangelstr. 4 10997 Berlin Germany

10 Appendix

10.1 About P3KI

P3KI GmbH was originally **incubated within Recurity Labs** GmbH, a Berlin-based security consultancy renowned for its deep expertise in reverse engineering, protocol design, and the secure architecture of critical systems. **Founded by Felix "FX" Lindner**, Recurity Labs has long operated in the area of defensive security, supporting **high-assurance industries and government clients globally**.

The idea for P3KI emerged from **hands-on experience** with the limitations of traditional PKI and access control in real-world, high-risk environments; especially where infrastructure could not be relied upon. Recognizing the growing need for resilient, decentralized trust systems across embedded, IoT, and tactical domains, the team began developing a new model that prioritizes autonomy, fine-grained delegation, and verifiability at the edge. What began as an internal project matured into what eventually became P3KI GmbH in 2014, with a dedicated engineering team focused on building a permission-centric, offline-capable public key infrastructure for the modern age.

Over the past decade, the company has grown into a focused R&D and engineering organization of approximately 10 security professionals. P3KI GmbH is pioneering an innovative, policy-driven public-key infrastructure, tailored for edge computing, industrial IoT, and high-risk environments. Core contributions include the "trinity" protocol suite, multi-platform runtimes (Rust, Python, Java, JavaScript), and integration bridges such as P3KIory for OpenID Connect and X.509 interoperability.

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

10.2 Technological Readiness Level (TRL) of Implementation

Element	Status	Description
Dynamic Policy language system	**Ready**	**TRL 8**. Support for multiple parallel scenarios.
Higher-order policy language system	Testing	**TRL 3-4**. Scenario specific abstraction of policy system to be more human readable (no impact on overall technical capability).
Identity and relationship management	**Ready**	**TRL 8**. Support for multiple identities per device implemented, including ephemeral identities.
Introspection and relationship visualization	**Ready**	**TRL 7**. Complex permission structures and delegation networks visualized graphically.
Multi-transport communication	**Ready**	**TRL 8**. Successfully implemented cryptographic exchanges and secured communication over NFC, BLE, WIFI, LAN, WebSockets, QR Codes. Extension to arbitrary transports possible
Hardware Security Module support	**Ready**	**TRL 5-7**. Basic PKCS#11 support validated with SoftHSM, mobile phone application uses Android(R) Secure Element for key material storage and biometric / pin user verification.
Mobile phone support	**Ready**	**TRL 7**. Mobile application for Google(R) Android(R) available from Play Store.
Embedded systems support	Testing	**TRL 4**. Successfully presented implementation of our codebase on Nordic Semi nRF5340, enabling Smartphone<>Device and Device<>Device authorization and secured communication, including full or partial ownership transfer semantics.
Integration OIDC/OAuth2	**Ready**	**TRL 5-6**. Proxy solution for interfacing with OIDC/OAuth2/OpenID Connect services.
Integration of X.509	**Ready**	**TRL 5-6**. Ability to derive P3KI identities from X.509 certificates.
Emulation and evaluation tools	**Ready**	**TRL 8**. Build dynamic scenarios and test them live using our cloud-based or on-prem deployable sandbox.
Industrial application	**Ready**	**TRL 5-7**. Self-service personal account management solution presented in collaboration with BASF, currently targeting **TRL 8-9** for 2026.

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com

10.3 Glossary

Term	Definition
AD	Microsoft Active Directory
AI	Artificial Intelligence
AuthN	Authentication
AuthZ	Authorization
BLE	Bluetooth Low Energy
CA	Certificate Authority (see: PKI, X.509)
CRL	Certificate Revocation List
CT	Certificate Transparency
HSM	Hardware security module
IdP	Identity Provider
IT	Information Technology (vs. OT)
L1, L2, L3, L4, L5	Network layers according to Purdue model
M2M	Machine-to-Machine
MANET	Mobile Ad-hoc Network
NFC	Near Field Communication
nRF5340	Bluetooth System-on-Chip (SoC) by Nordic Semiconductor
OAuth2	An authorization framework
OCSP	Online Certificate Status Protocol
OIDC	OpenID Connect
OT	Operational Technology (vs. IT)
P2P	Peer-to-peer
PKCS#11	Public-Key Cryptography Standards #11. A standard API for interfacing with cryptographic tokens (e.g., hardware security modules, smart cards).
PKI	Public Key Infrastructure (see: X.509)
QR Code	Quick Response Code
SoftHSM	A software-based implementation of a Hardware Security Module
TRL	Technology Readiness Level
WebSockets	A web protocol providing full-duplex communication channels
WIFI	A family of wireless network protocols
X.509	A standard defining the format of public key certificates
ZTA	Zero-trust Architecture

Version Rev2, 2025-08-04,
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany, +49 (0)711 22051252 (Stuttgart office), +49 (0)30 695399933 (Berlin office), contact@p3ki.com