trust
point

PITCH DECK.

secure, compliant and streamlined digital identity management in OT environments

DECEMBER 2025

INTRO

Open-source platform for automated, secure identity management in industrial networks.

trust point

INDUSTRIAL DIGITALIZATION

Industry is shifting to **connected, intelligent, and automated** environments.

MANDATORY SECURITY

Cybersecurity and compliance (e.g., CRA, NIS2) will be mandatory.

TRUSTPOINTS APPROACH

Trustpoint enables **manufacturers and operators** to integrate digital identities easily and securely.

Let’s secure automation

PROBLEM

trust point

Security & Compliance in Industrial OT: **Still Manual, Costly, Risk-Prone**

CERTIFICATE CHAOS

Manual certificate provisioning is **error-prone** and doesn't scale.

SECURITY SKILL GAP

Engineering teams lack **time, resources, and expertise** to manage secure PKI.

VENDOR LOCK-IN

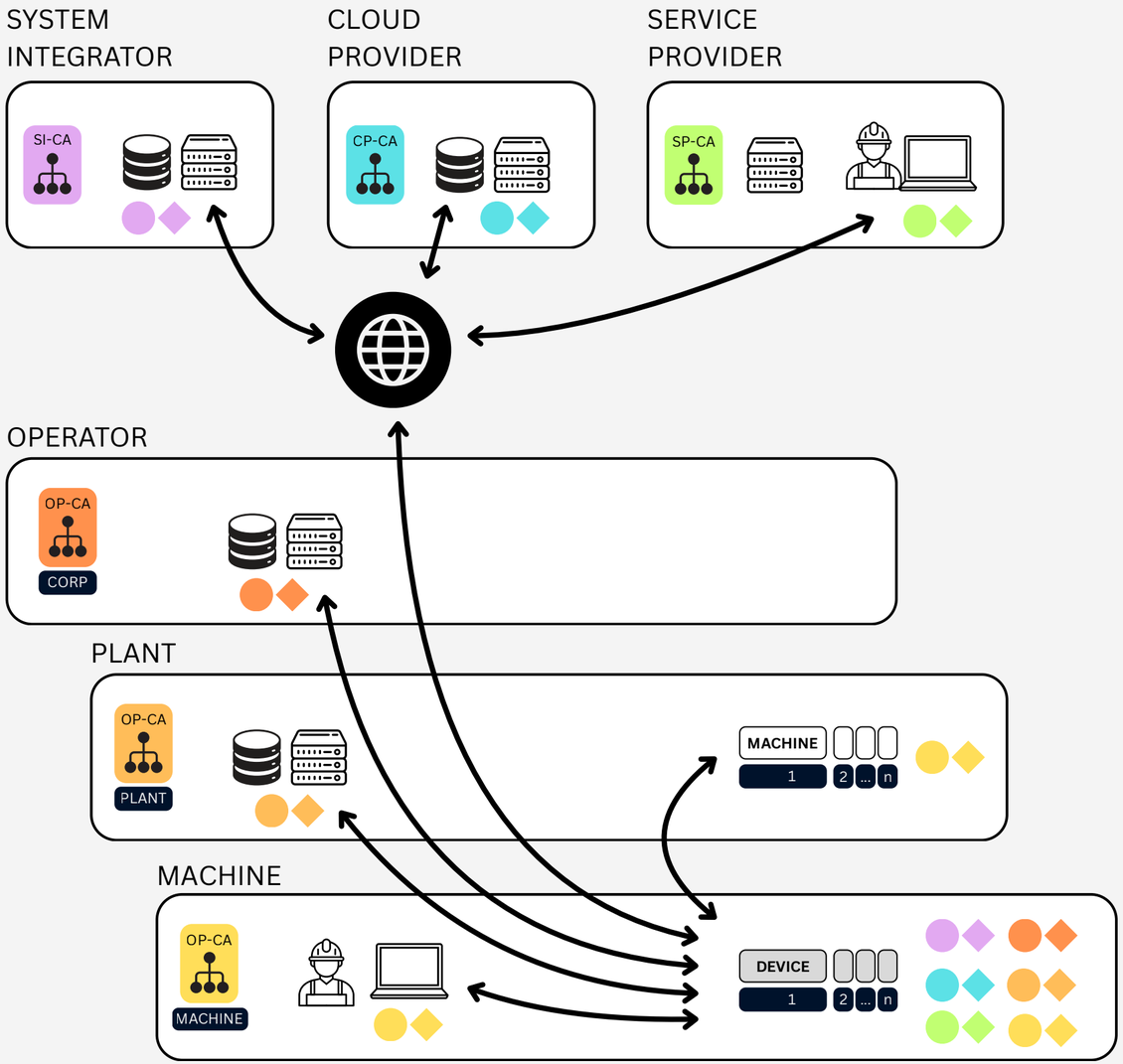
Existing solutions are often **proprietary**, **costly**, or **not designed for OT**.

Let's secure automation

* More information about certificates can be found in the appendix.

FRAGMENTATION

Disconnected **certificate silos** increase complexity, risk, and operational overhead in OT environments.



TRUST INFRASTRUCTURE
PKI (+CLM)

CREDENTIAL
key pair + certificate

TRUSTSTORE
Trusted CAs

Let's secure automation

SOLUTION

Trustpoint – Open, Flexible, and Automatable

trust point

LIFECYCLE AUTOMATION

Automated **certificate lifecycle management** for OT devices and systems.

FLEXIBLE ONBOARDING

Supports **manual**, **semi-automated**, and **Zero-Touch** onboarding.

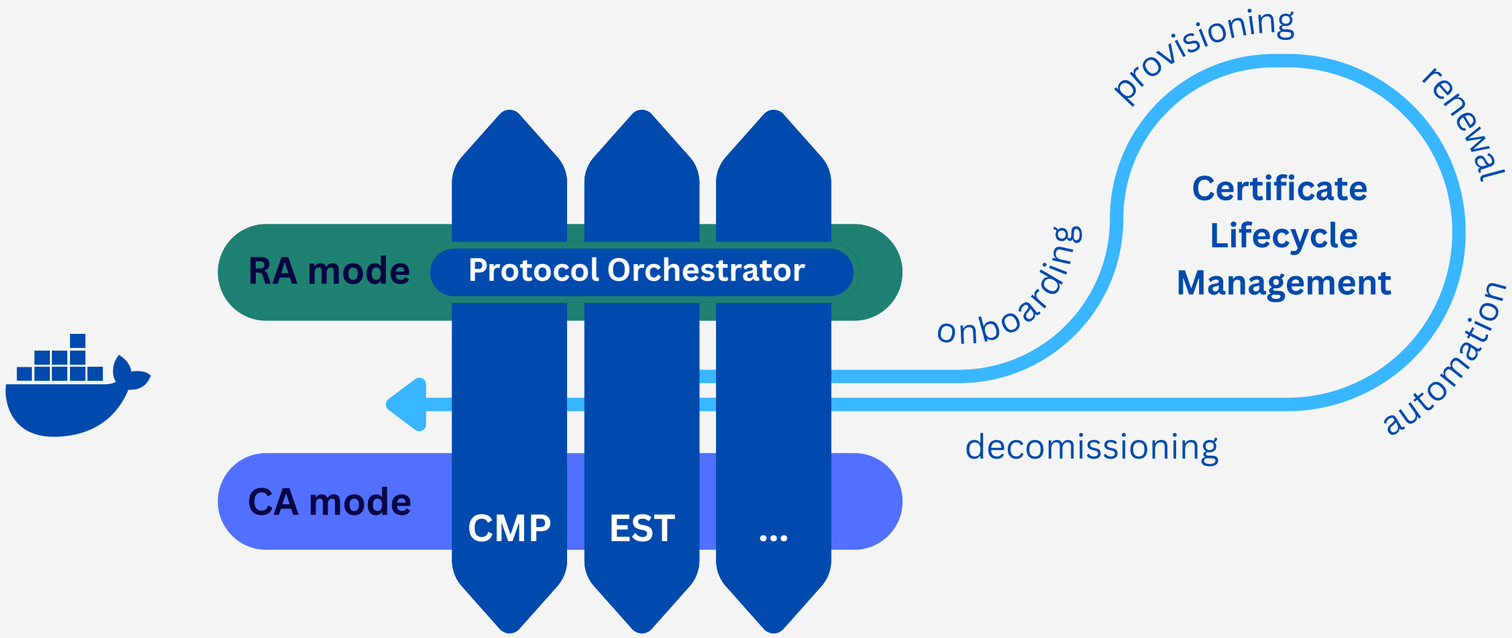
OPEN CORE

OSS foundation with optional professional services and integrations.

Let’s secure automation

ARCHITECTURE

From onboarding to decommissioning — Trustpoint automates the entire certificate lifecycle.



Features

- Containerized deployment
- Builtin industrial certificate profiles
- Secure key storage
- Workflow engine
- Open Source (MIT)

Let's secure automation

* More information about features can be found in the appendix.

REFERENCE PROJECTS

Secure Device Onboarding in Real Industrial Environments

trust point

SECURE ONBOARDING

A Belden Hirschmann BOBCAT Switch is securely onboarded using its **Initial Device Identifier** (IDevID) for authentication.

Belden

OPC UA GDS

Certificates are issued to a Siemens S7-1500 via UaGDS, which handles **centralized certificate provisioning**, trust list management, and automated renewal

Unified Automation SIEMENS

Let’s secure automation

BUSINESS MODEL

Open Source Base – Sustainable Service & Support Model

trust point

REVENUE STREAMS

- **Professional services** (deployment, training, compliance consulting)
- **SLA**-based support and incident response
- **Custom integrations & feature** development

GO-TO-MARKET STRATEGY

- **Community-first** (GitHub, DockerHub, events)
- Partner & integrator channels
- OEM-ready modules
- Industrial marketplace visibility

Let's secure automation

* As of today, Trustpoint is not yet an operating company (due to funding guidelines; expected 09/26). Nevertheless, we look forward to discussing use cases and PoCs with you.

Funded by:

Bundesministerium für Forschung, Technologie und Raumfahrt

RESSOURCES & ACCESS

trust point

Everything You Need to Explore, Deploy, and Contribute

Github

hub

Docs & Demos

Let’s secure automation

THANK YOU.

trust point

CONTACT US:

Florian Handke

Director Industrial Security

Campus Schwarzwald

+49 151 55360339

florian.handke@campus-schwarzwald.de

www.industrial-security.io

Let’s secure automation

trust point

APPENDIX

DIGITAL CERTIFICATES

trust point

Digital Certificates – The Trust Layer for Machines

*“Digital certificates are essential for **securing communication, proving device identity, and ensuring compliance** in connected industrial environments”*

WHAT IS IT?

A **digital certificate is a digital ID** for machines, proving their **identity** and enabling **secure communication**.

WHY IT MATTERS?

- **Verifies** machines and components
- Enables **encrypted, trusted connections**
- Replaces insecure passwords and manual configs
- Supports **CRA**, **NIS2**, IEC 62443 compliance

Let’s secure automation

LOGISTICS

Trustpoint different ways to manage certificates on end devices. From zero-touch to manual ways.

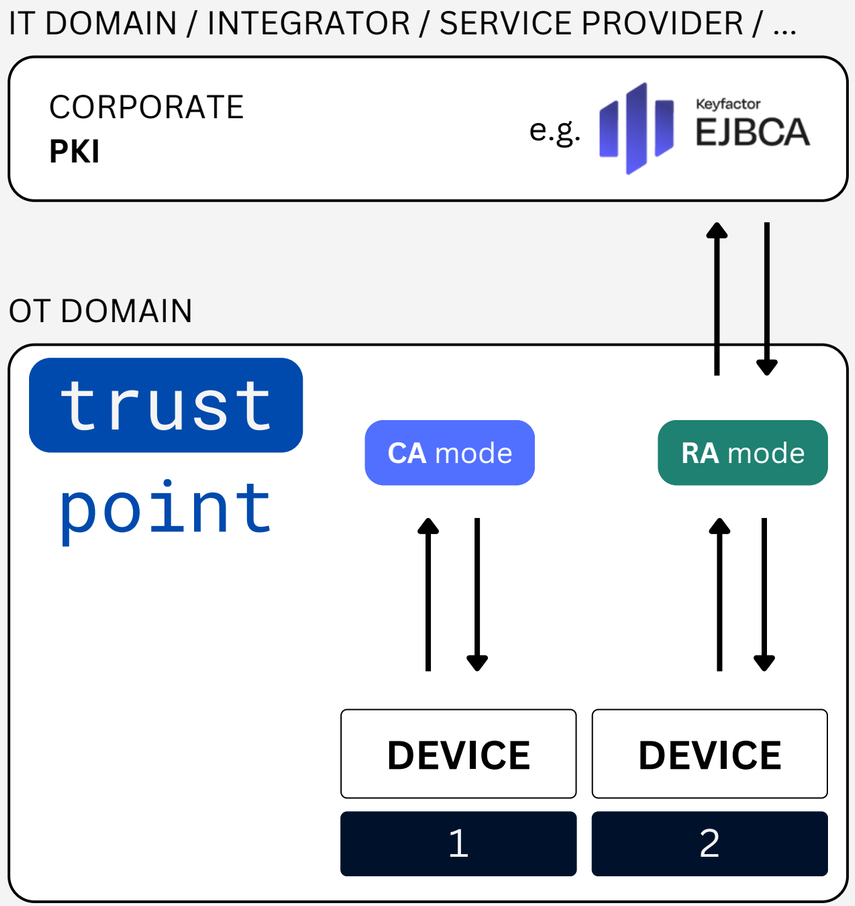
trust point

Method	Auth Methods	Key Capabilities
AOKI (Zero-Touch)	IDevID	Zero-touch onboarding; automatic LDevID issuance
EST (RFC 7030)	Username+Password, IDevID, mTLS	LDevID onboarding; app cert enrollment; renewal & re-enrollment
CMP (RFC 9483)	Shared Secret, IDevID, mTLS	LDevID onboarding; app cert enrollment; automated renewal & rekey
Manual Download	—	Server-generated credentials; PKCS#12/PEM download
Remote Credential Download	OTP	Browser-based retrieval of issued credentials

Let’s secure automation

OPERATION

Trustpoint supports **local (air-gapped)** certificate management and acts as a local **registration authority**, issuing certificates via a remote PKI.



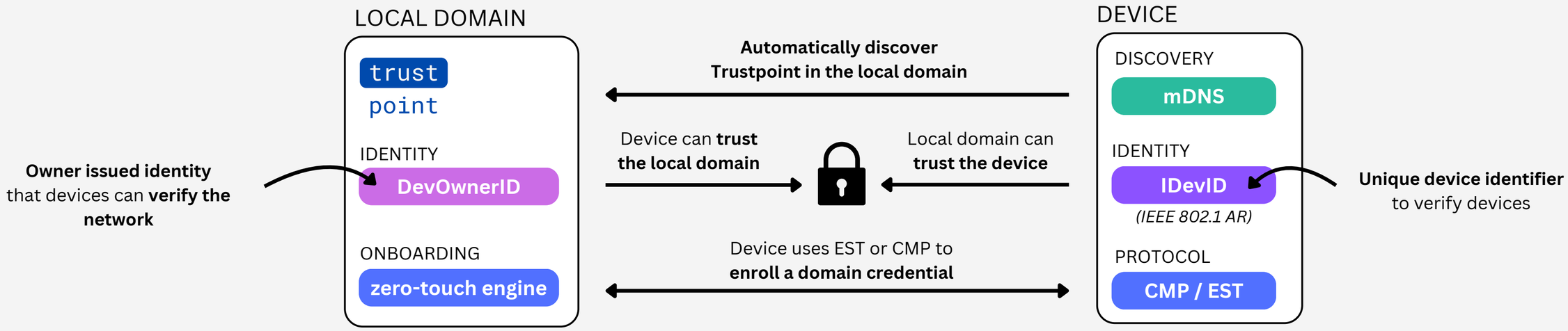
Let's secure automation

AOKI

BETA

trust point

Devices can automatically onboard into Trustpoint using the Automated Onboarding Key Infrastructure (AOKI) for **zero-touch onboarding**, leveraging their manufacturer device identity and multicast DNS for Owner Service discovery.



Let's secure automation

AOKI OPTIONS

BETA

trust point

Devices can **automatically onboard** into Trustpoint using their manufacturer device identity utilizing multicast DNS.

PER-DOMAIN AOKI

- DevOwnerIDs are **issued per owner domain**, not per device.
- Device establishes trust by **pinning the DevOwnerID issuer chain** used during onboarding.

No direct device–owner cryptographic binding, but more scalable for large and distributed environments.

PER-DEVICE AOKI

- Each device is associated with a **device-specific DevOwnerID** (by referencing the IDevID in the SAN)
- Ownership is **cryptographically tied to the individual device** from the beginning.

Maximum security through device-intrinsic ownership binding, at the cost of higher operational effort

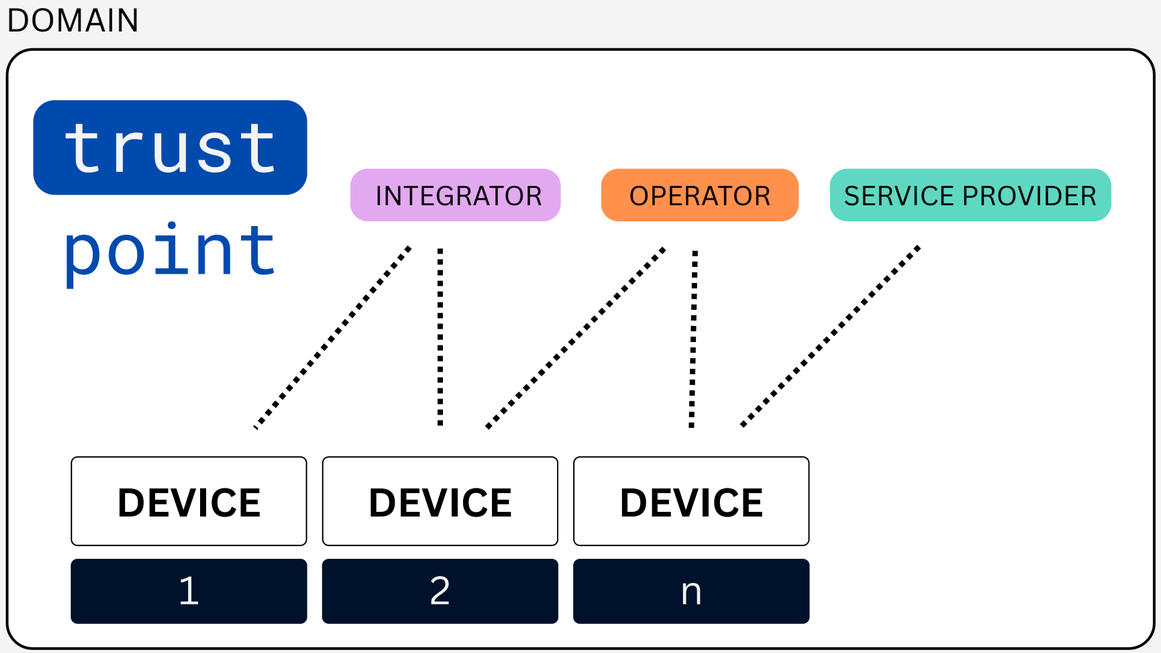
Let’s secure automation

MULTI-TENANCY

UPCOMING FEATURE

trust point

Since multiple actors need to manage certificates on the device, Trustpoint offers **multi-tenancy for different actors**, such as integrators, operators, and service providers.



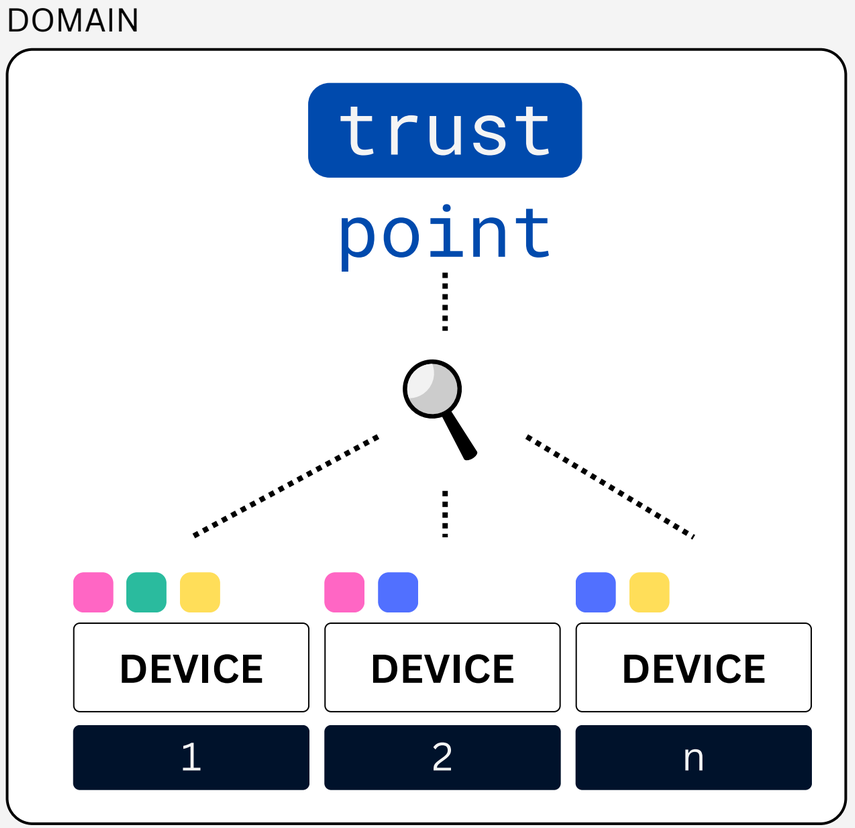
Let’s secure automation

CRYPTO DETECTION

UPCOMING FEATURE

trust point

Trustpoint **detects devices** and their capabilities on certificates. Our device library offers an individualized workflow for certificate management.



HTTPS WEBSERVER
OPC UA SERVER
IPsec
BACnet

Let’s secure automation