Keyfactor
Tech Days
2023

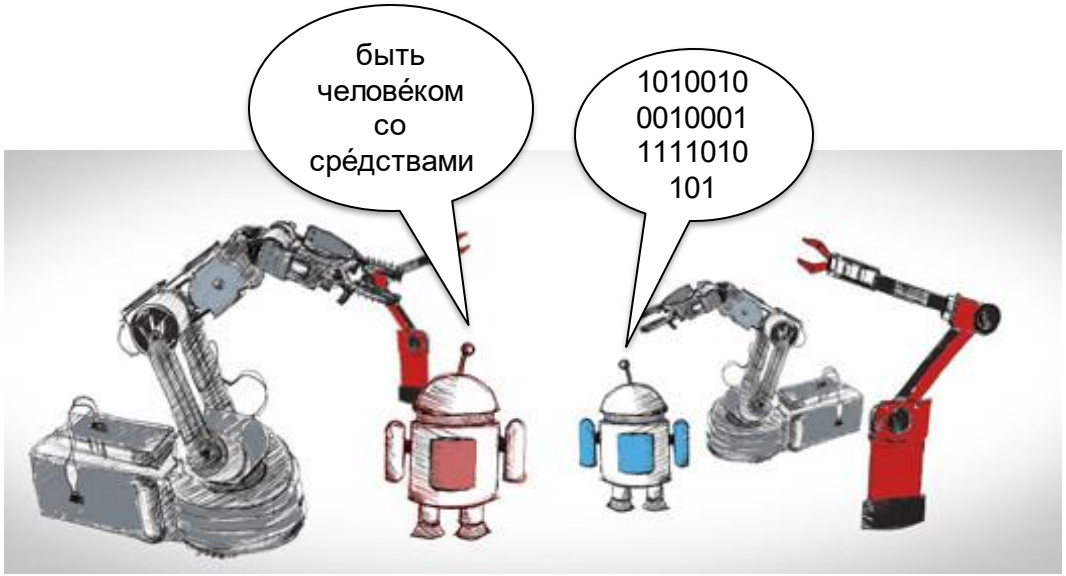
Industrial Automation and Certificate Management

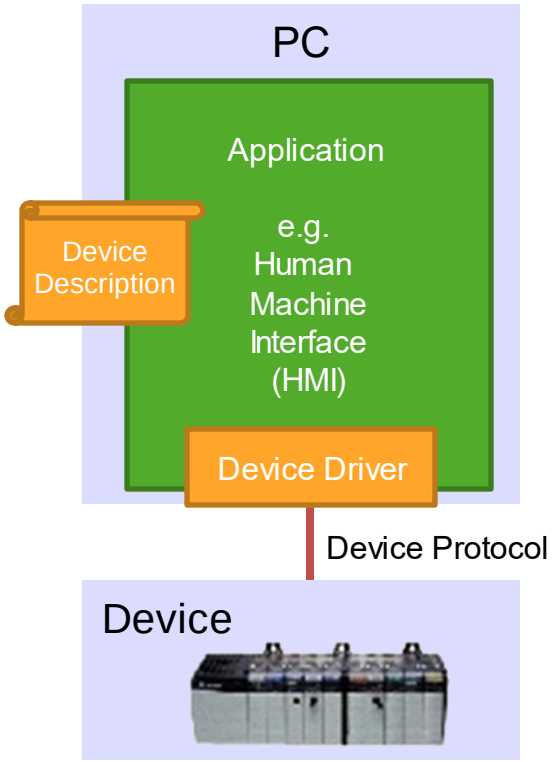
Matthias Damm

Executive Director

Unified Automation

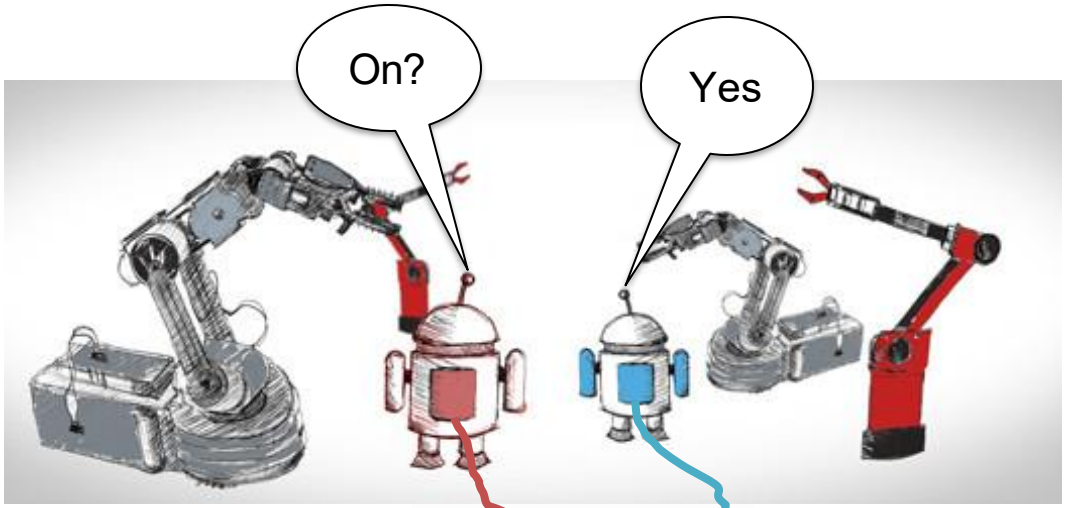
Before OPC (The Industrial Interoperability Standard – Open Platform Communication)





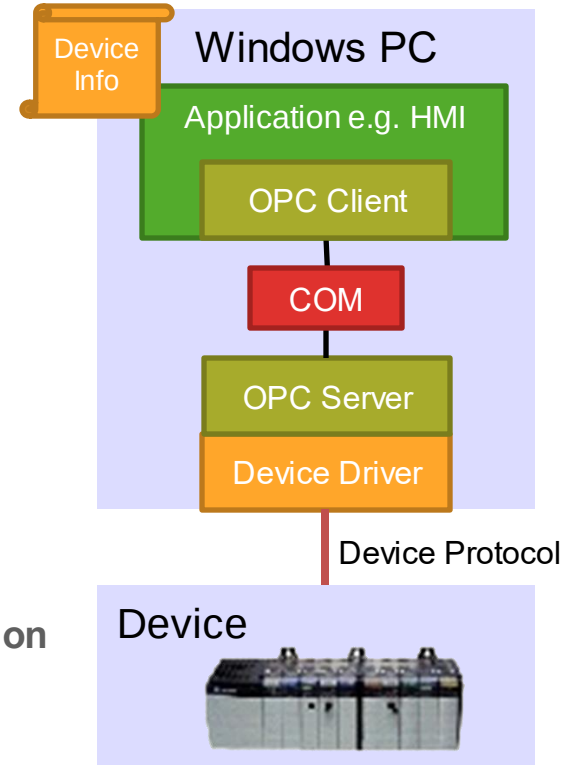
- Vendor specific APIs
- Vendor / device specific protocols
- No security
- Semantic added on application level

With OPC Classic (OLE for Process Control – since 1996)

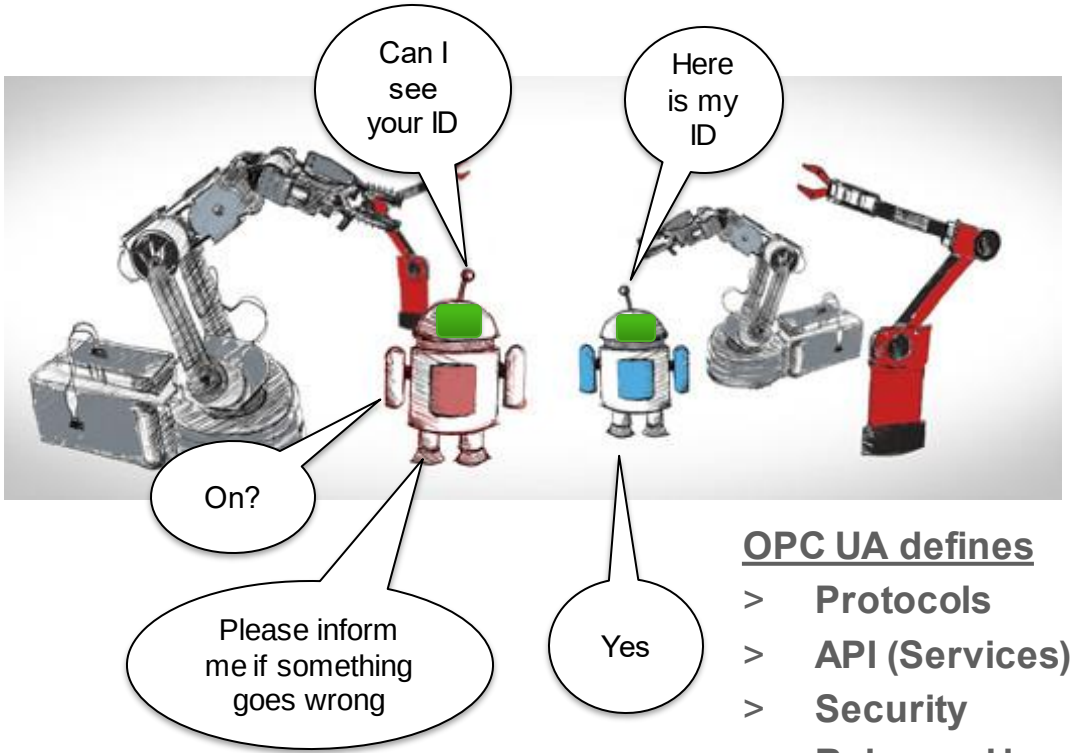


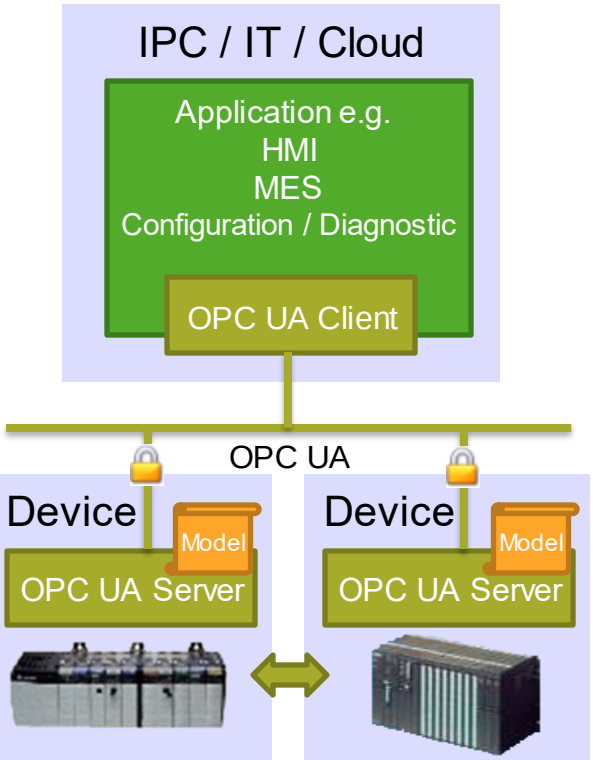
Classic OPC defines

- > Standard API
- > Windows specific protocol (COM)
- > No security
- > Semantic added on application level



With OPC Unified Architecture (since 2006)



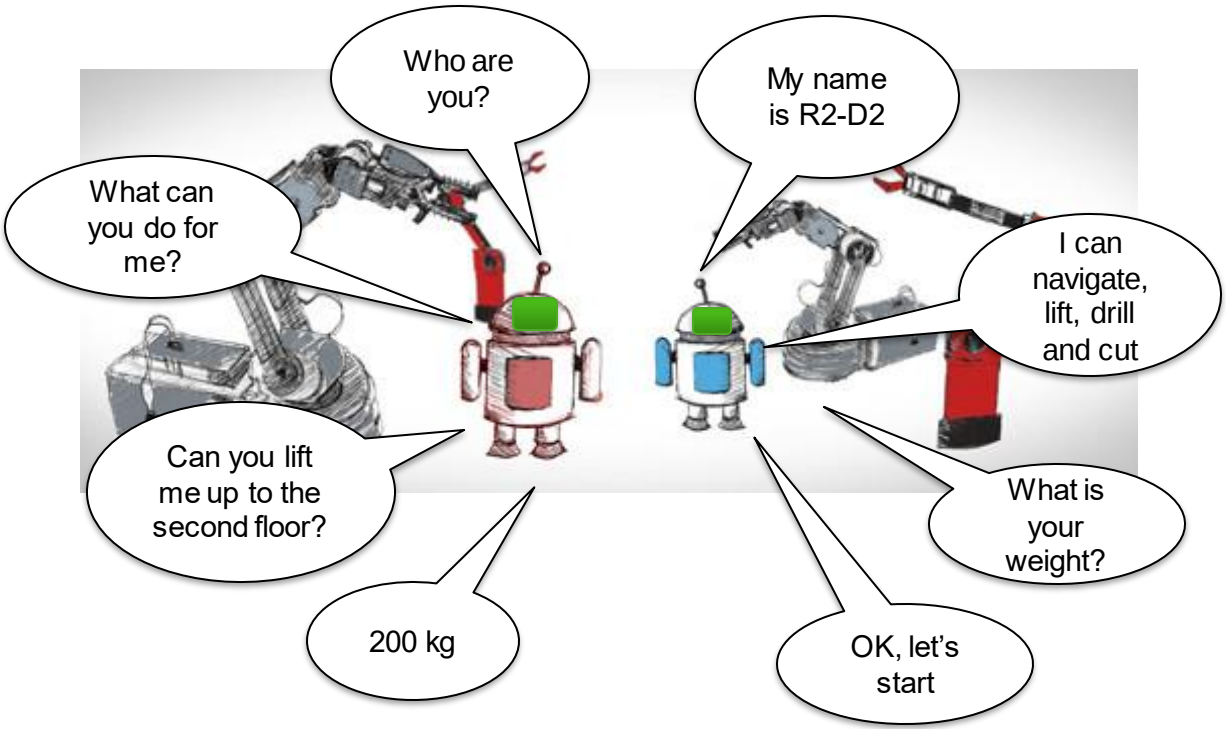


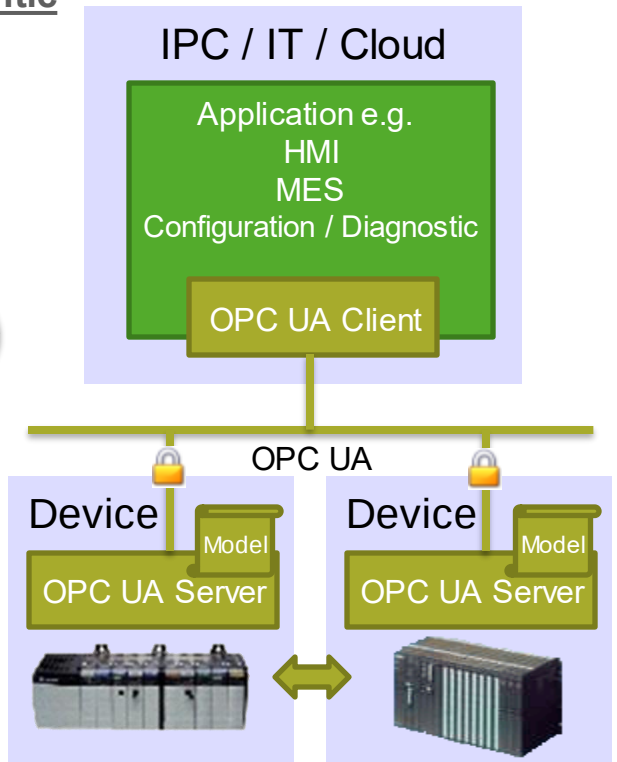
OPC UA defines

- > **Protocols**
- > **API (Services)**
- > **Security**
- > **Rules and language to add semantic**

With OPC UA Information Models

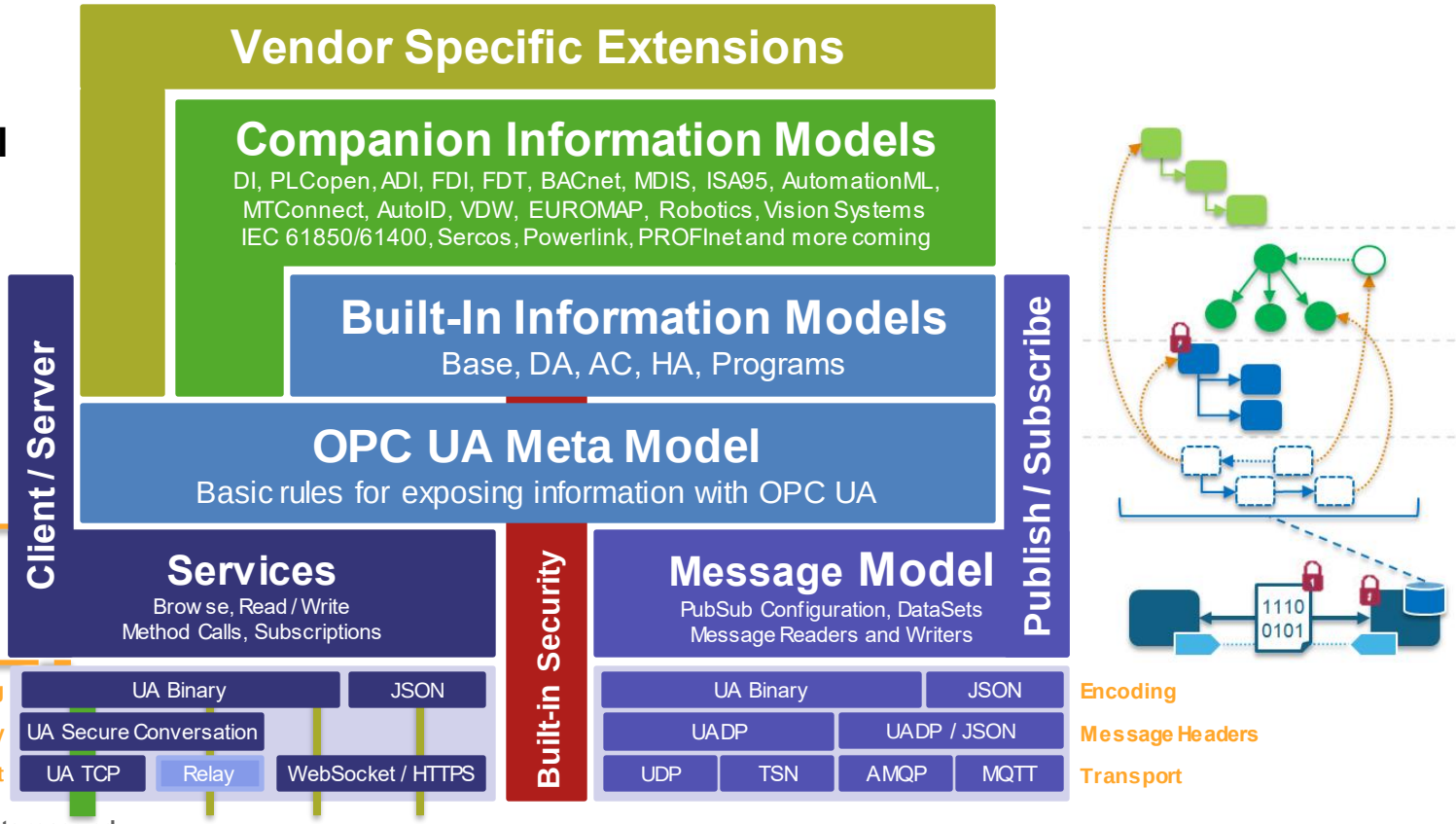
OPC UA defines use case, machine or device specific semantic





OPC Unified Architecture – The Big Picture

OPC UA is much more than a protocol

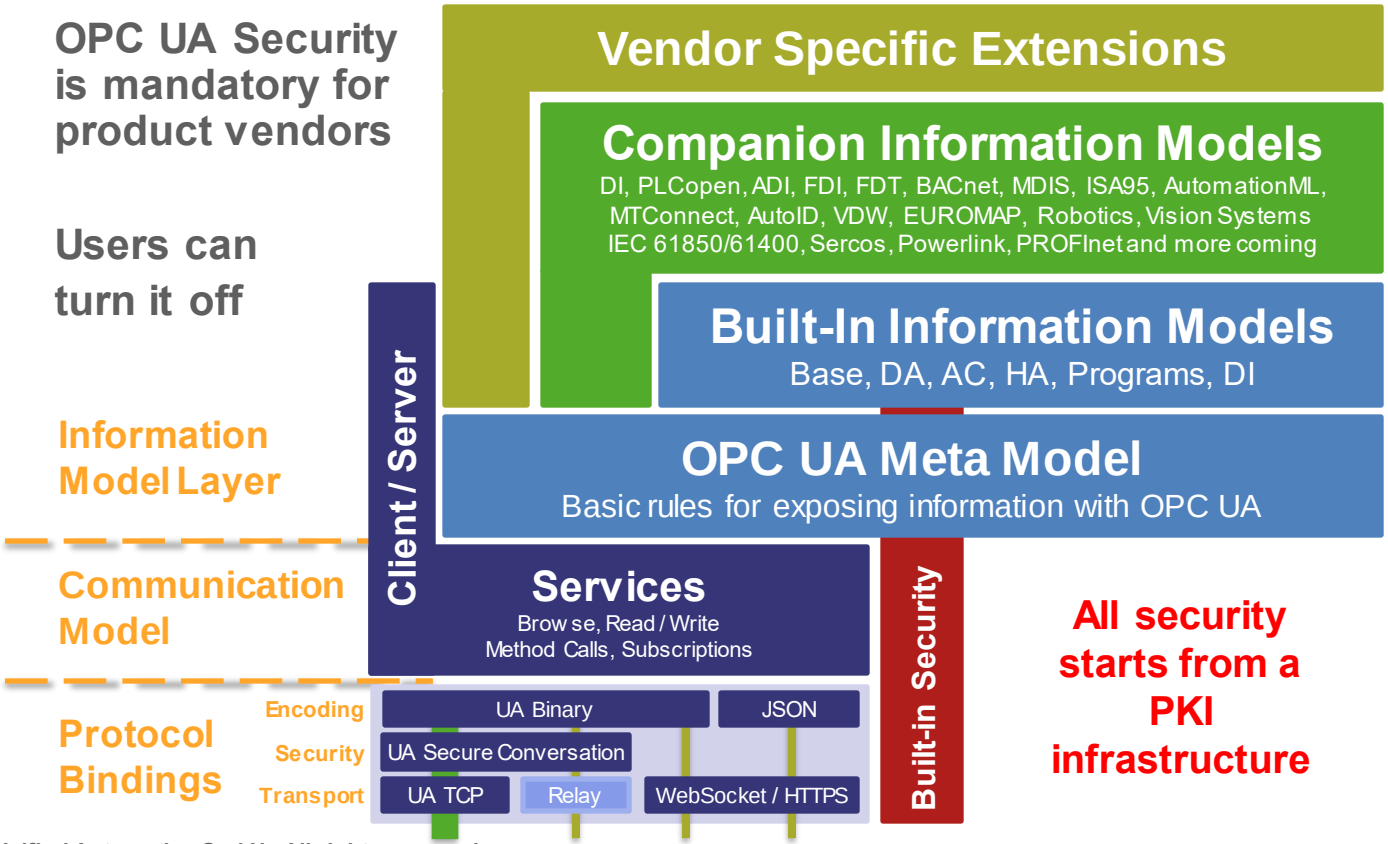


Unified Automation

OPC UA Client / Server Security

OPC UA Security is mandatory for product vendors

Users can turn it off



All security starts from a PKI infrastructure

Security built-in to different levels

Protocol Security

- Application authentication PKI / Certificate based
- Message signing
- Message encryption

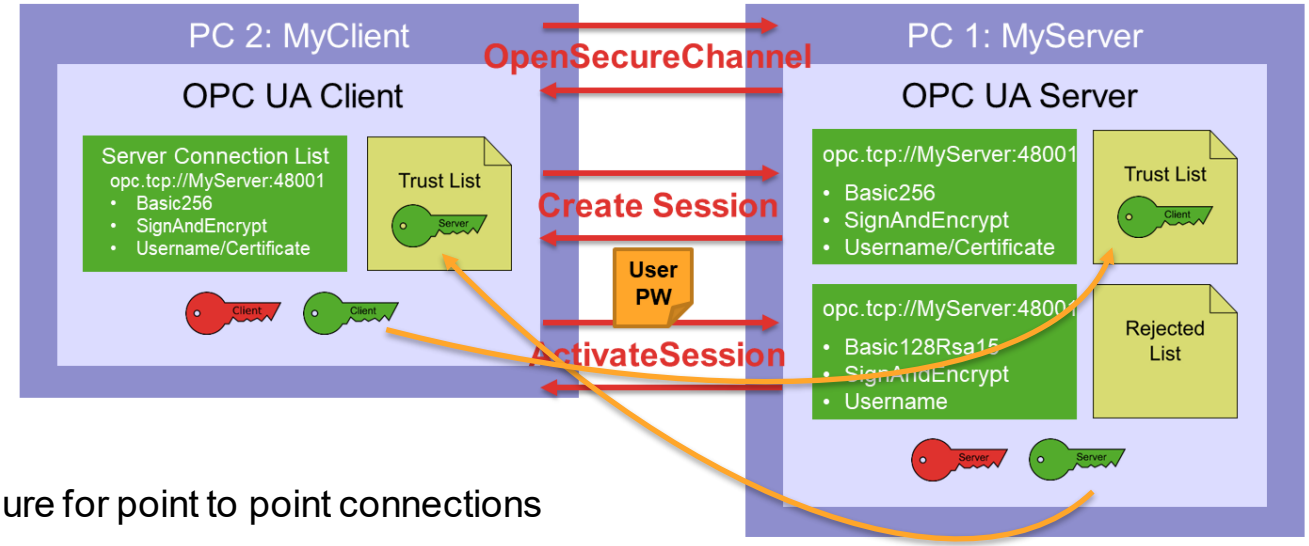
User Security

- User Authentication
  - Anonymous
  - User / Password
  - User Certificate
  - Web tokens (JWT)
- User Authorization
  - Role based
  - Permissions down to node attributes

Application Level

- Audit events for all security relevant client actions, write and method calls

OPC UA Security with self-signed Certificates



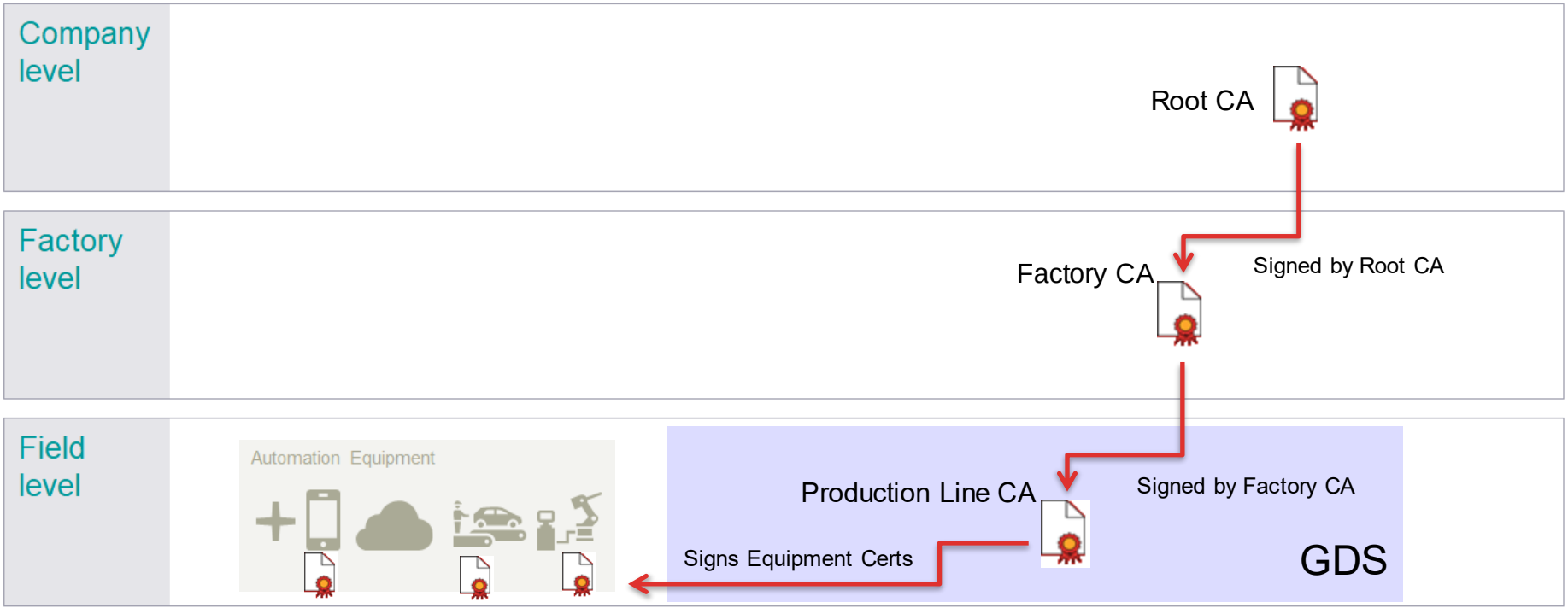
Pro

- Easy to configure for point to point connections

Con

- No automatic update of certificates
- No central management – no central revocation of certificates
- Not manageable for many clients talking to many servers

Certificate Authority (CA) Certificate Chains



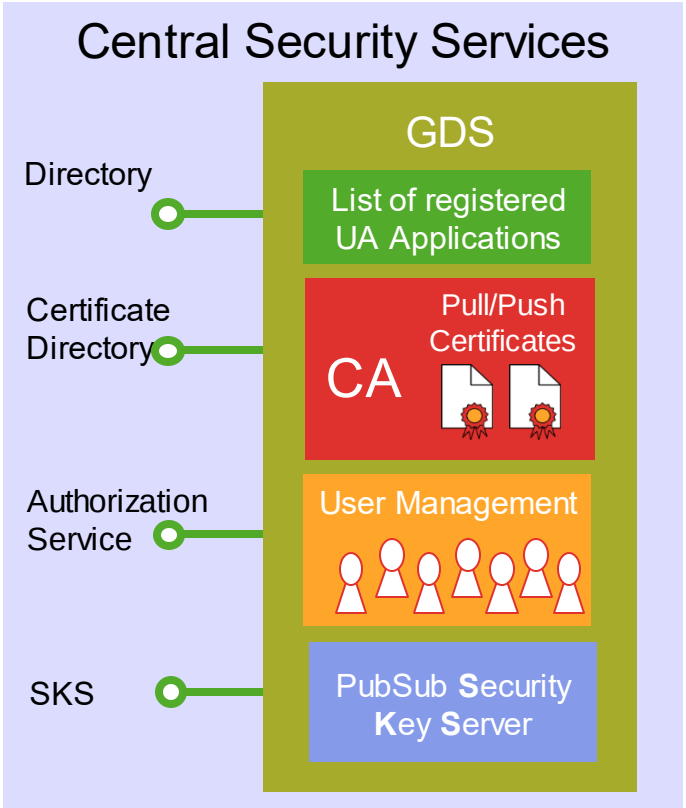
Global Discovery Server (GDS)

GDS – OPC UA defined Security Services

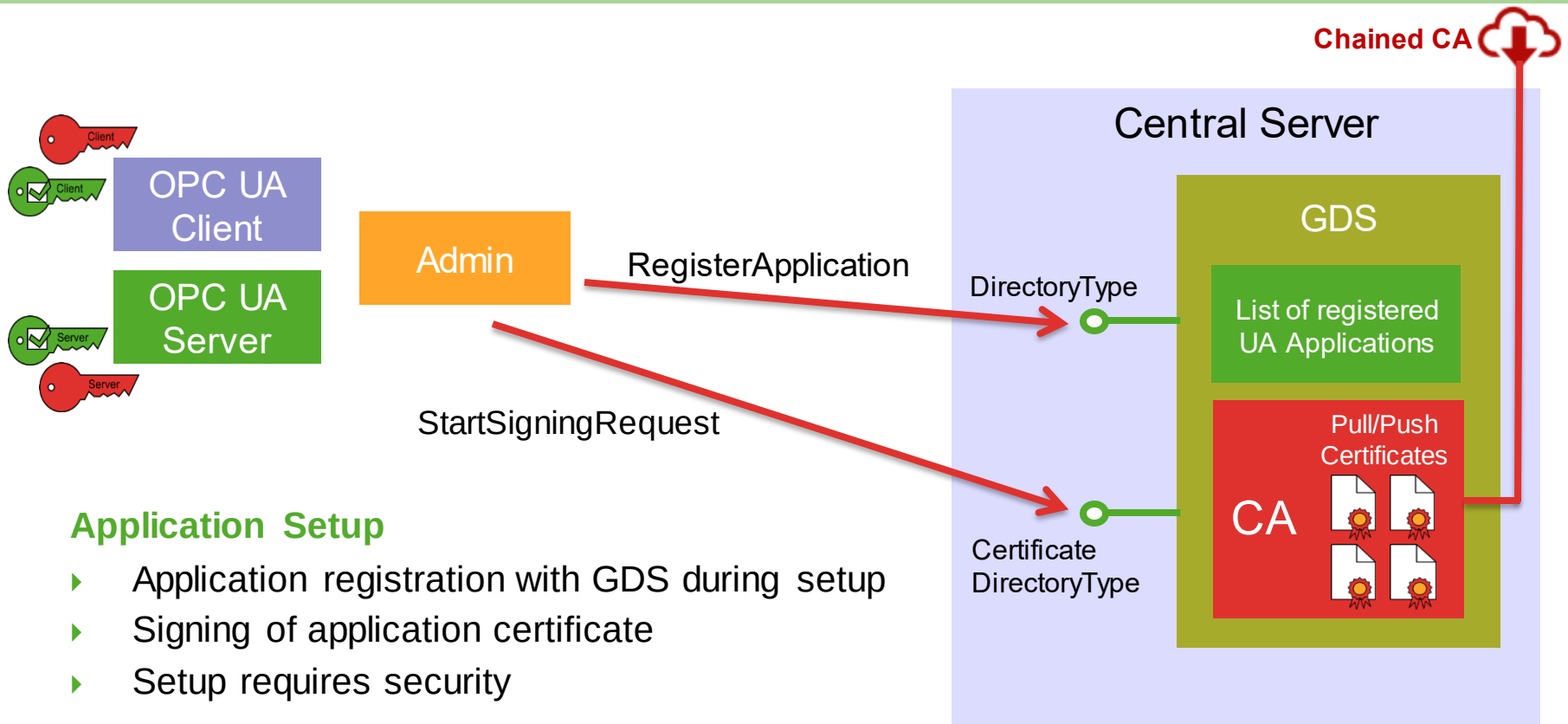
- Full OPC UA Server (all OPC UA security features)
- **OPC UA Part 12 - Discovery and Global Services**
- Provides different UA security management services
  - OPC UA server discovery
  - Public Key Infrastructure (PKI) for certificate management
  - PubSub Security Key Server (SKS)
  - User management
- PKI is base for **ALL** security features

GDS as Certificate Authority for PKI

- Frontend to CA for certificate management
- Certificate signing
- Trust list and revocation list distribution
- Automated certificate renewal



GDS – Application Setup



Application Setup

- Application registration with GDS during setup
- Signing of application certificate
- Setup requires security

GDS – Application Security Update – PULL

Pull

- Applications are clients for GDS

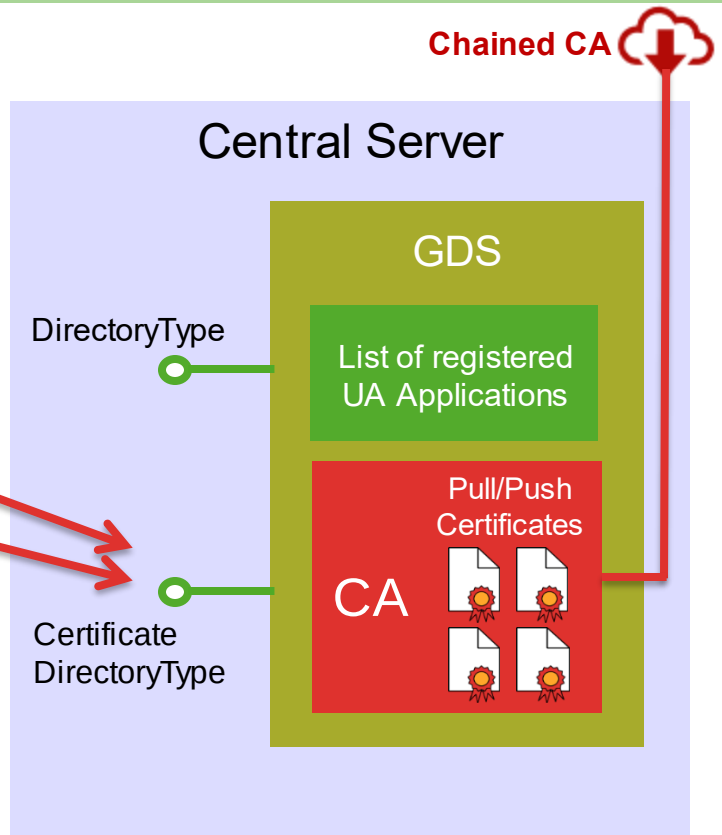
OPC UA Client

OPC UA Server

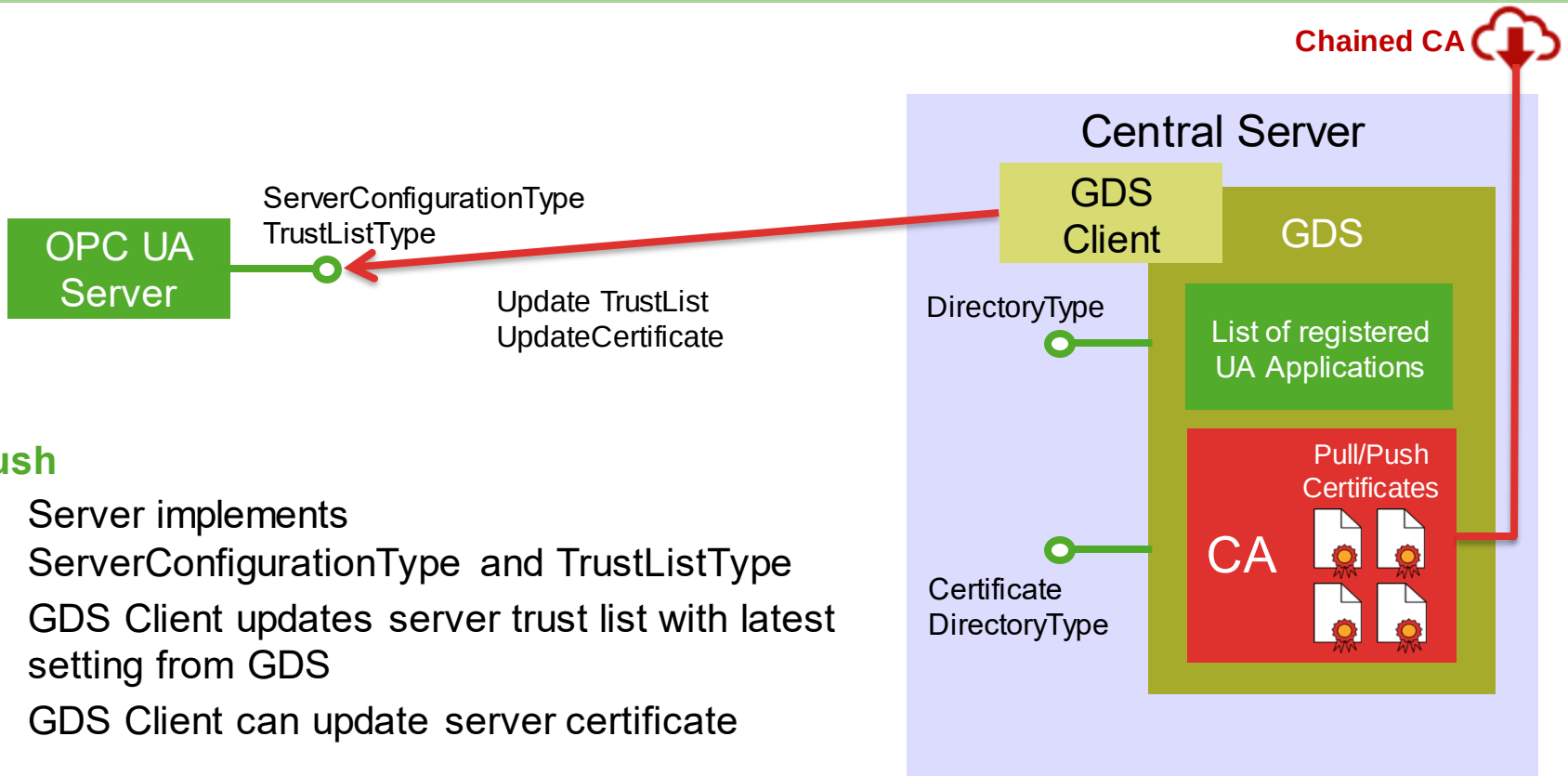
GetTrustList

Application Security Update

- Frequent update of trust list and CA revocation list
- Update requires security



GDS – Application Security Update – PUSH



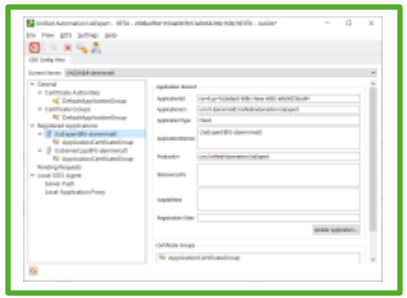
Push

- Server implements ServerConfigurationType and TrustListType
- GDS Client updates server trust list with latest setting from GDS
- GDS Client can update server certificate

Unified Automation

UaGDS Product Components

UaGDS Config Tool



Configuration using OPC UA

Unified Automation defined

Standard Interfaces

UaGDS Service

GDS management

Directory

Registered UA Applications

PULL

Certificates

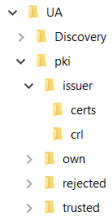
CA

Pull/Push Certificates

Root CA

Pull

OPC UA Applications with GDS support



OPC

Push

PUSH

GDS Client

TrustListType
ServerConfigurationType

UaGDS

UaGDS integration with Keyfactor PKI

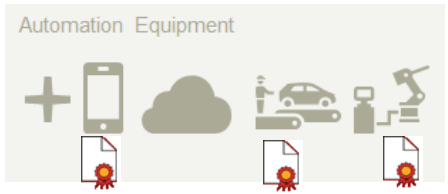
Company level

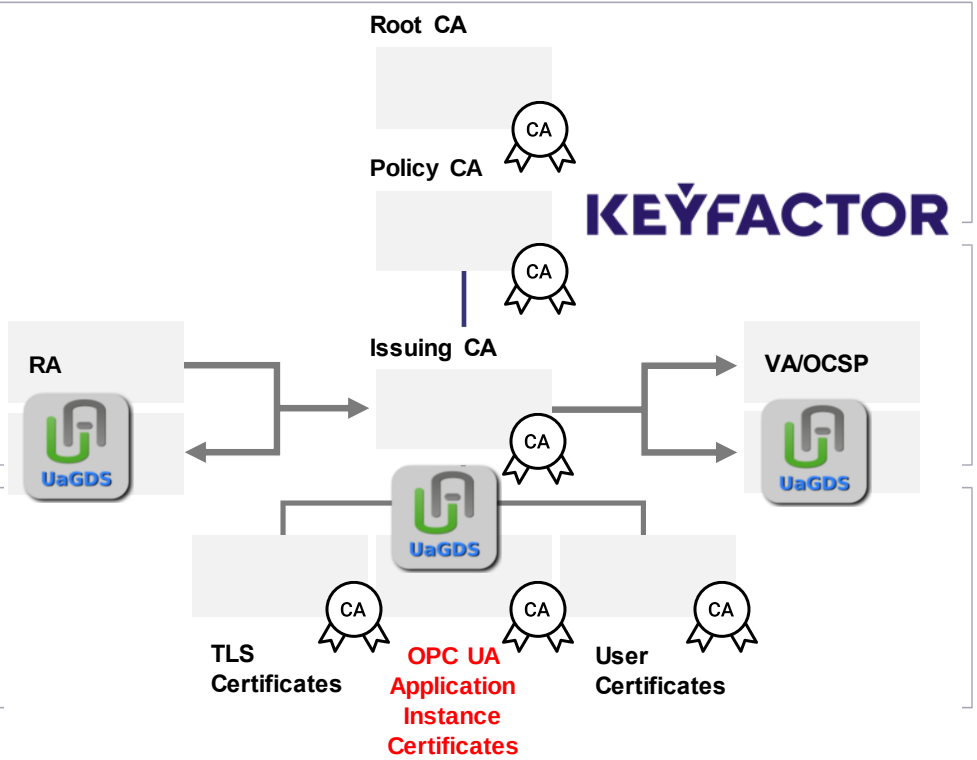
UaGDS

- Manages OPC UA Applications
- Forward certificate signing requests to Keyfactor PKI
- Distribute signed certificates
- Distribute revocation lists
- Optional online revocation check

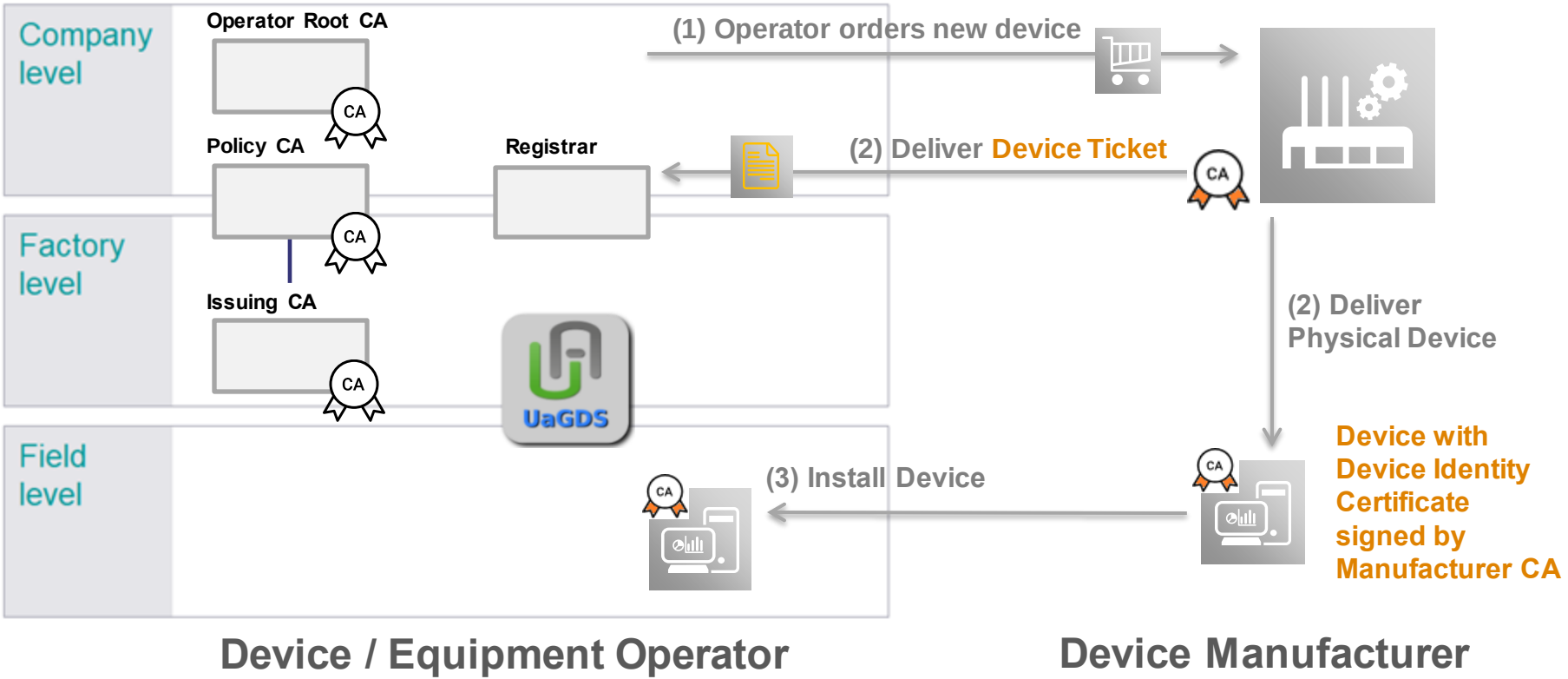
Factory level

Field level

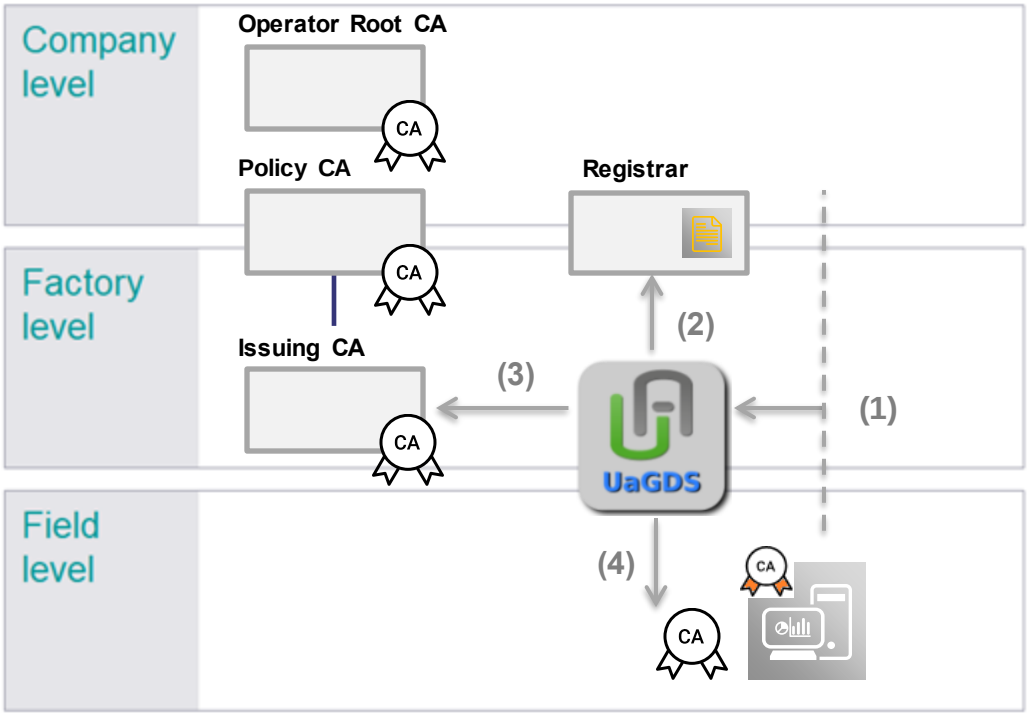




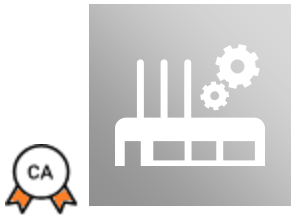
New OPC UA Part 21 – Device Onboarding



New OPC UA Part 21 – Device Onboarding



Device / Equipment Operator



Automated Device Onboarding by Operator

(1) Device Registration at GDS
  (a) During delivery of ticket
  (b) During device installation

(2) Validate Device with Registrar

(3) Create singed OPC UA Application Certificate(s)

(4) Install Operator Certificate on Device

(5) Optional Device Software Update

Summary

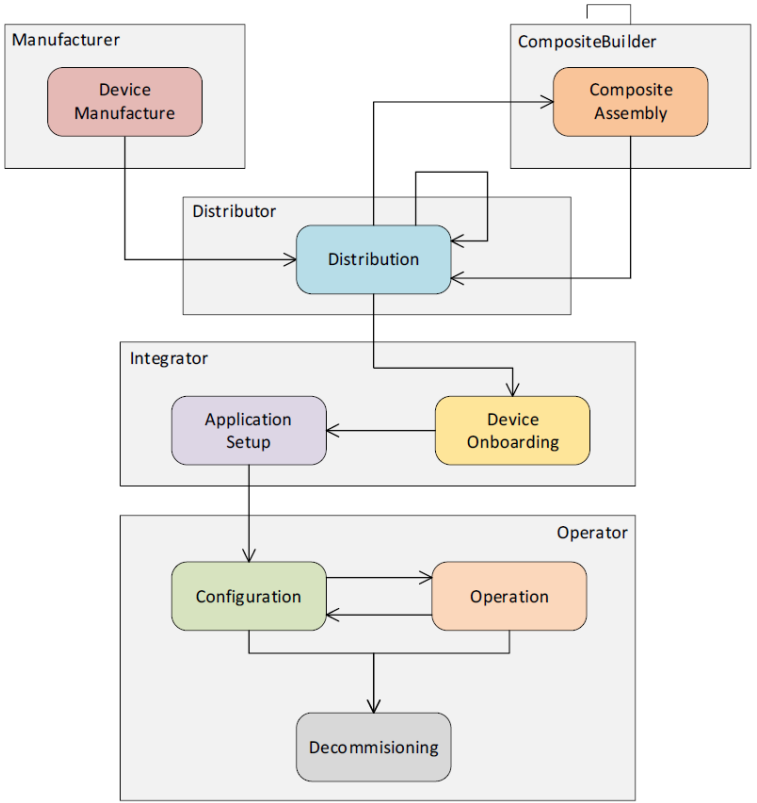
OPC Unified Architecture

- Multivendor industrial interoperability standard
- Strong focus on security features
- Concepts for central PKI and security management
- Secure device lifecycle

Unified Automation UaGDS and Keyfactor PKI

- Integration of GDS features in all OPC UA SDKs
- Product implementation of standardized central OPC UA security services
- Integration with operator PKI systems like Keyfactor

Enables and simplifies Certificate and Security Management for Industrial IoT



Open Industrial PKI

Andreas Philipp

Senior Business Development Manager IoT

Keyfactor

Florian Handke

Smart Production Engineer

Campus Schwarzwald

Secure industrial assets with X.509 certificates

Free, managed & open CA service for:

- Client-Server certificates
- Code Signing
- Device Identities

Open industrial PKI **in a nutshell**

free

Anyone in the **industrial sector** (device manufacturers, service providers, machine builders, operators) can request X.509 certificates for **free of charge.**

defined

We support current **standard interfaces** (e.g. EST, CMP). Provide a **certificate policy**, **knowledge base**, **code repo** with examples, configurations and best practices

transparent

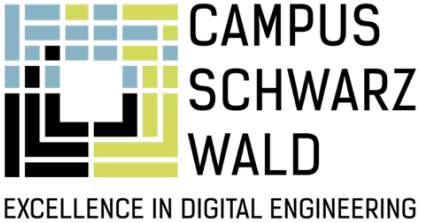
We provide **managed certificates**. CRLs are publicly available. Access only via **registration process**.

ease of use

We supply **pre-defined profiles** for the majority of industrial use cases such as OPC UA, MQTT, VPN etc.

Operation and support

Open industrial PKI is jointly operated by **Campus Schwarzwald** and **Keyfactor**



Want to **support** Open industrial PKI? Please contact us!

www.**open-industrial-pki**.org