

TeleTrust-EBCA "PKI-Workshop" 2023

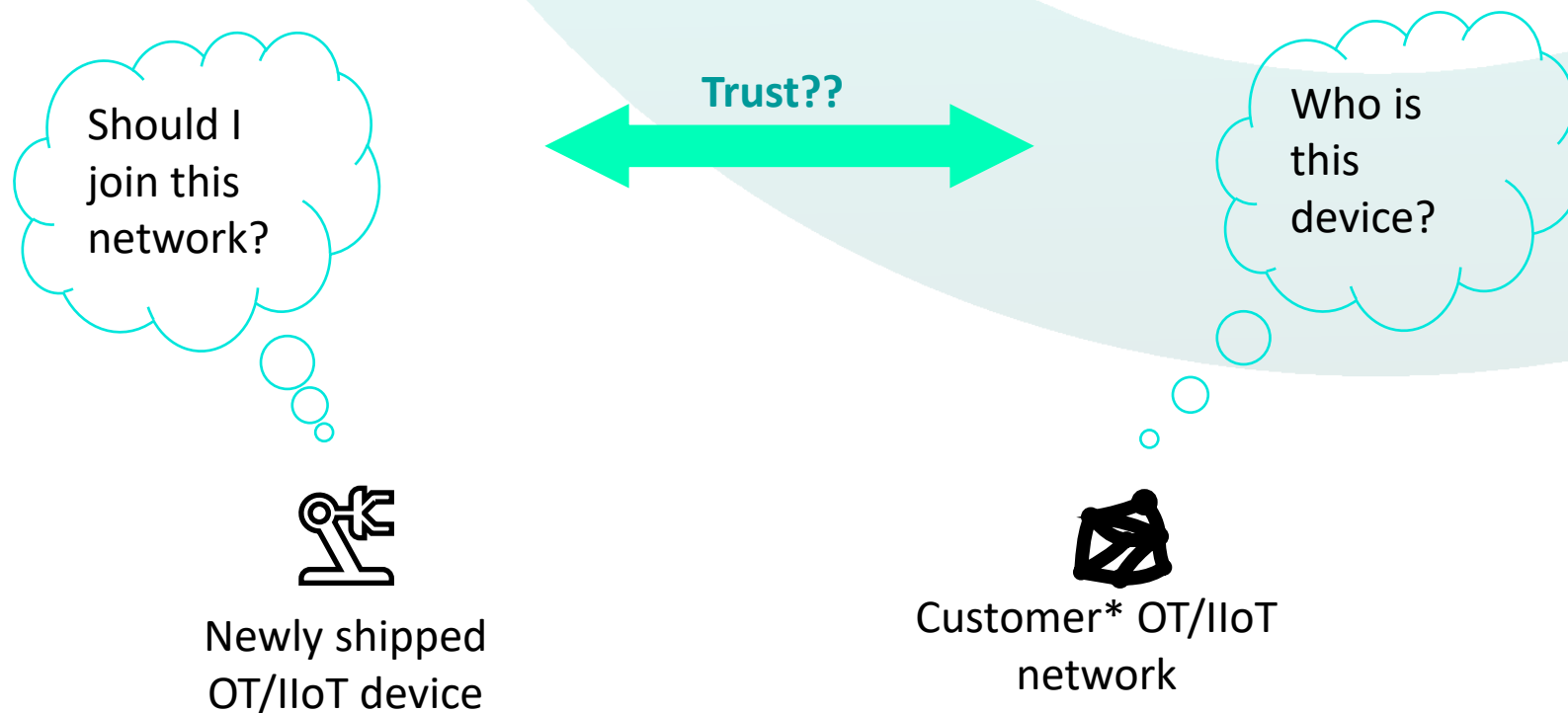
Berlin, 21.09.2023

"Entwicklung eines Secure Device Bootstrapping Backends nach RFC8995 (BRSKI / MASA)"

Rufus Buschart, Siemens

Thomas Werner, Siemens

Motivation: How to gain trust in an OT/IloT network?



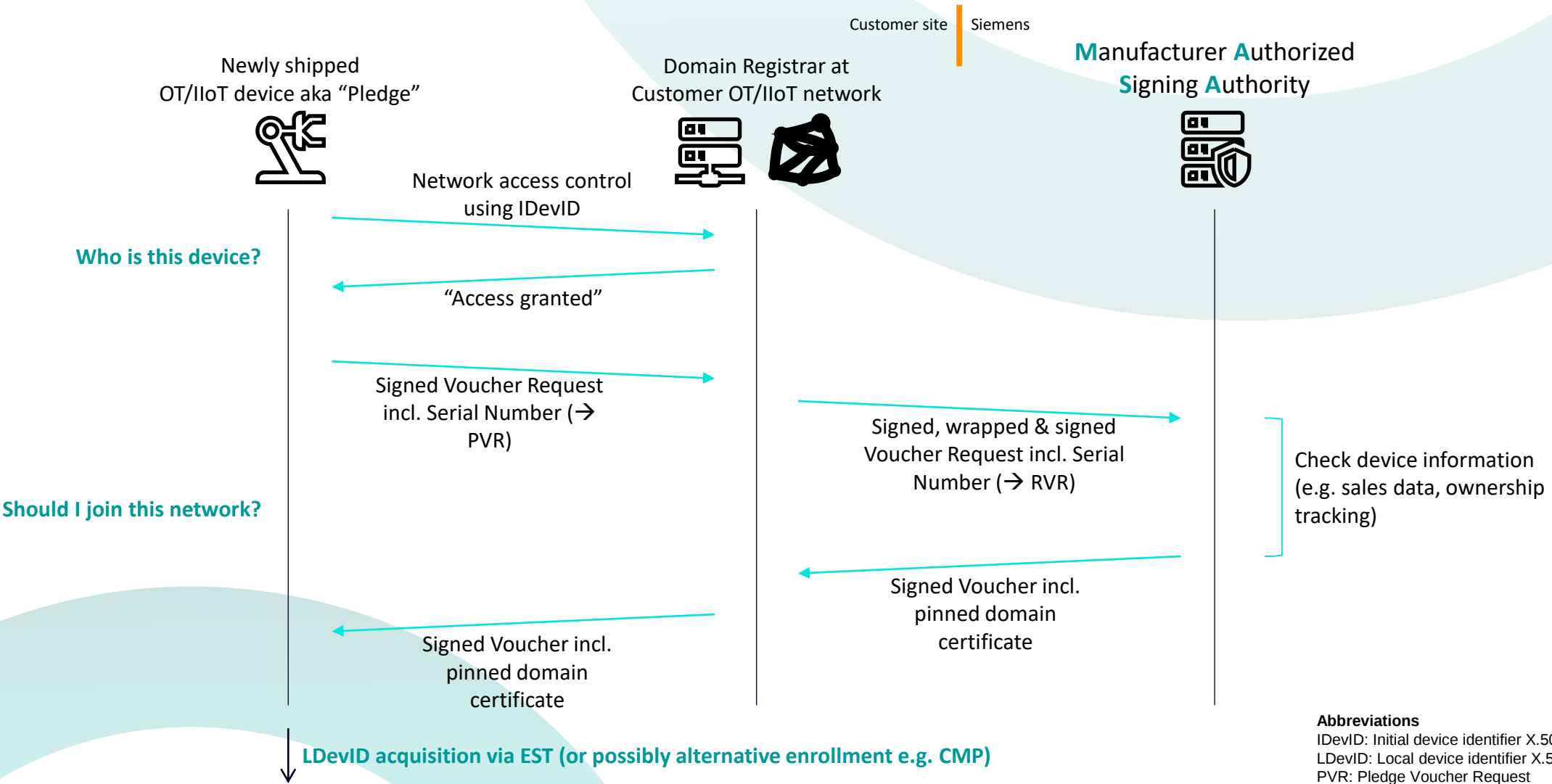
Traditional approach: TOFU – Trust On First Use

* Can be Siemens internal or external

But:

never trust  always verify

Trust generation acc. RFC8995 / Bootstrapping Remote Secure Key Infrastructure (BRSKI)



Abbreviations
IDevID: Initial device identifier X.509 certificate
LDevID: Local device identifier X.509 certificate
PVR: Pledge Voucher Request
RVR: Registrar Voucher Request

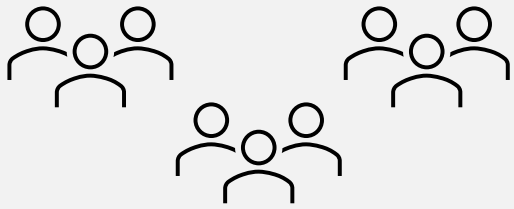


Page 4 Public | © Siemens 2023 | Buschart R., Werner T. | 2023-09-21

Bootstrapping / Onboarding Specifications



Zero-Touch Onboarding is specified in **different standardization bodies** and industrial consortia



Onboarding solutions have been investigated **based on interest** of different industries & markets.

IETF anima BRSKI – Bootstrapping Remote Secure Key Infrastructure RFC 8995 – plus enhancements: BRSKI-AE, BRSKI-PRM, JWS-Voucher, Constrained-Voucher

FIDO Device Onboard Specification (FDO)

OPC Foundation - OPC-UA – Part 21: Device Onboarding

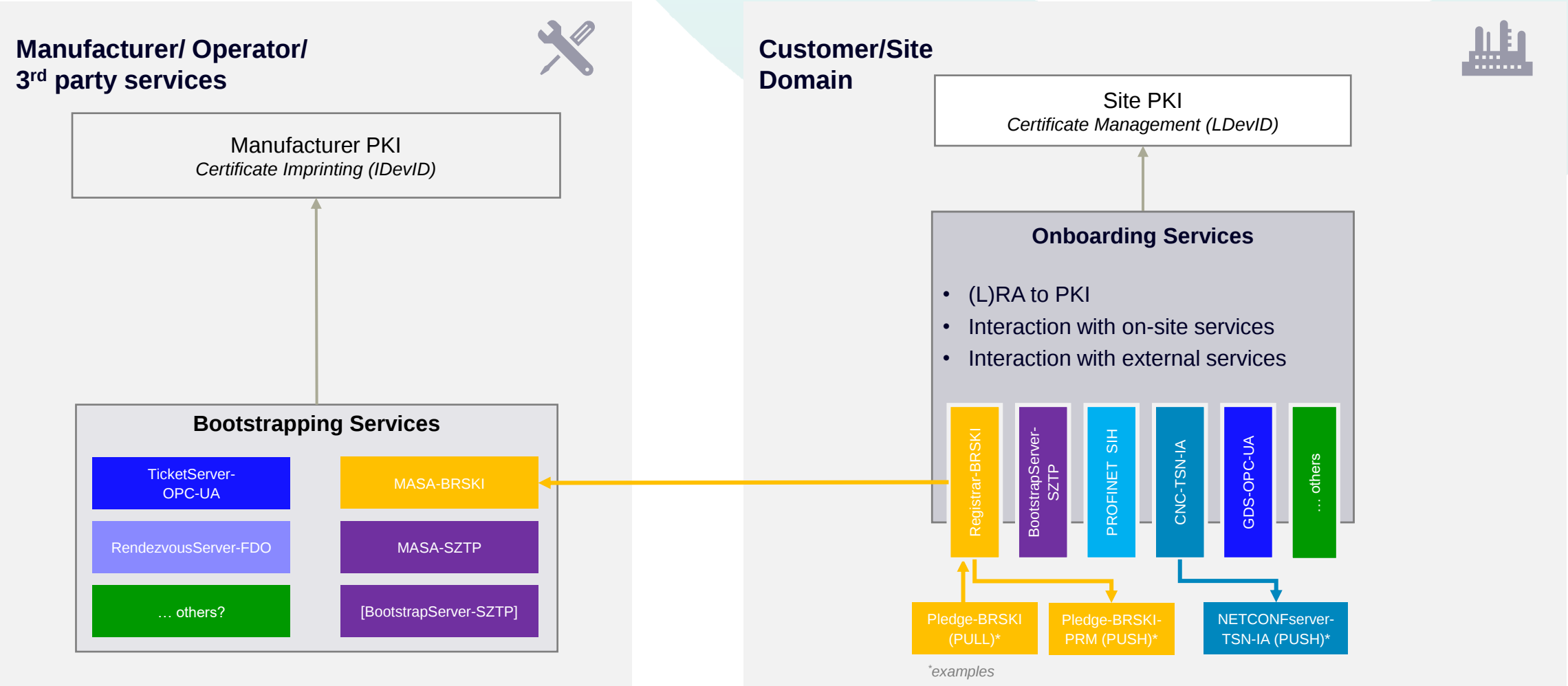
PROFINET (native) – PROFINET Specification, IEC 61158

IEC/IEEE - TSN-IA – TSN Profile for Industrial Automation – IEC/IEEE 60802 (based on netconf/YANG: RFC 6241, RFC 6020, RFC 8342)

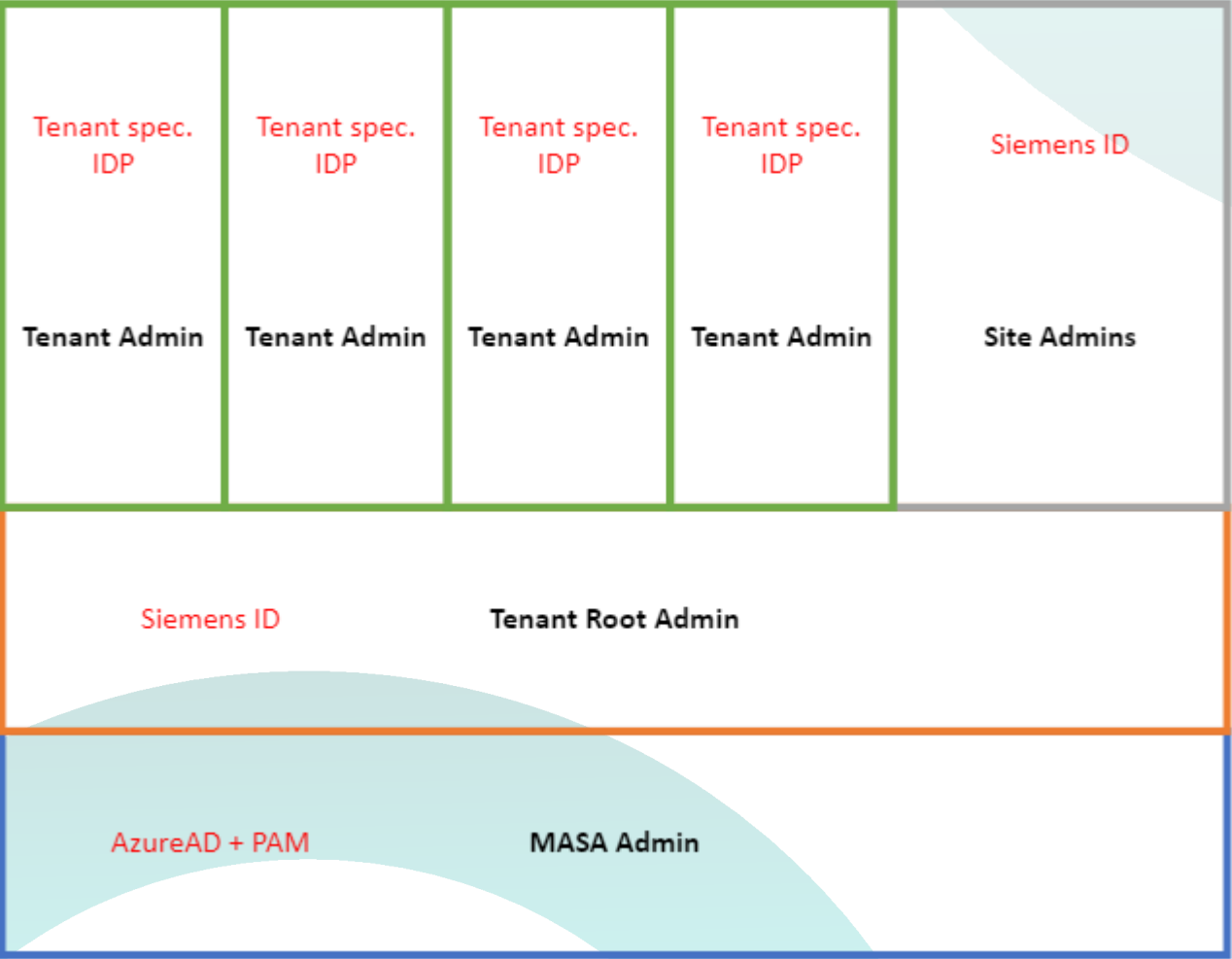
IETF netconf SZTP – Secure Zero Touch Provisioning RFC 8572

Further solutions are evolving, to be analyzed and considered in more detail – EAP bootstrapping, Matter, ...

Blueprint for Zero-Touch Onboarding architecture ensures modular, “pluggable” functionalities and services



MASA-as-a-Service developed by Siemens



Personas:

MASA Admin: Employee of Siemens operating the MASA system

Tenant Root Admin: Employee of a pledge manufacturer, responsible for setting up a tenant

Tenant Admin: Employee of a pledge manufacturer, configuring operative data in the tenant

Site Admin: Employee of a company that owns a pledge



Live demonstration

Disclaimer



© Siemens 2023

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.



Contact

Published by Siemens IT & T

Rufus J.W. Buschart
IT Project Manager

E-mail: rufus.buschart@siemens.com

Thomas Werner
Senior Key Expert Zero-Touch Onboarding

E-mail: thomas-werner@siemens.com