PLATTFORM INDUSTRIE 4.0

Achieving Trustworthiness of Secure Supply Chains for Industrie 4.0

Wolfgang Klasen
Siemens Technology and Member of the German Plattform Industrie 4.0

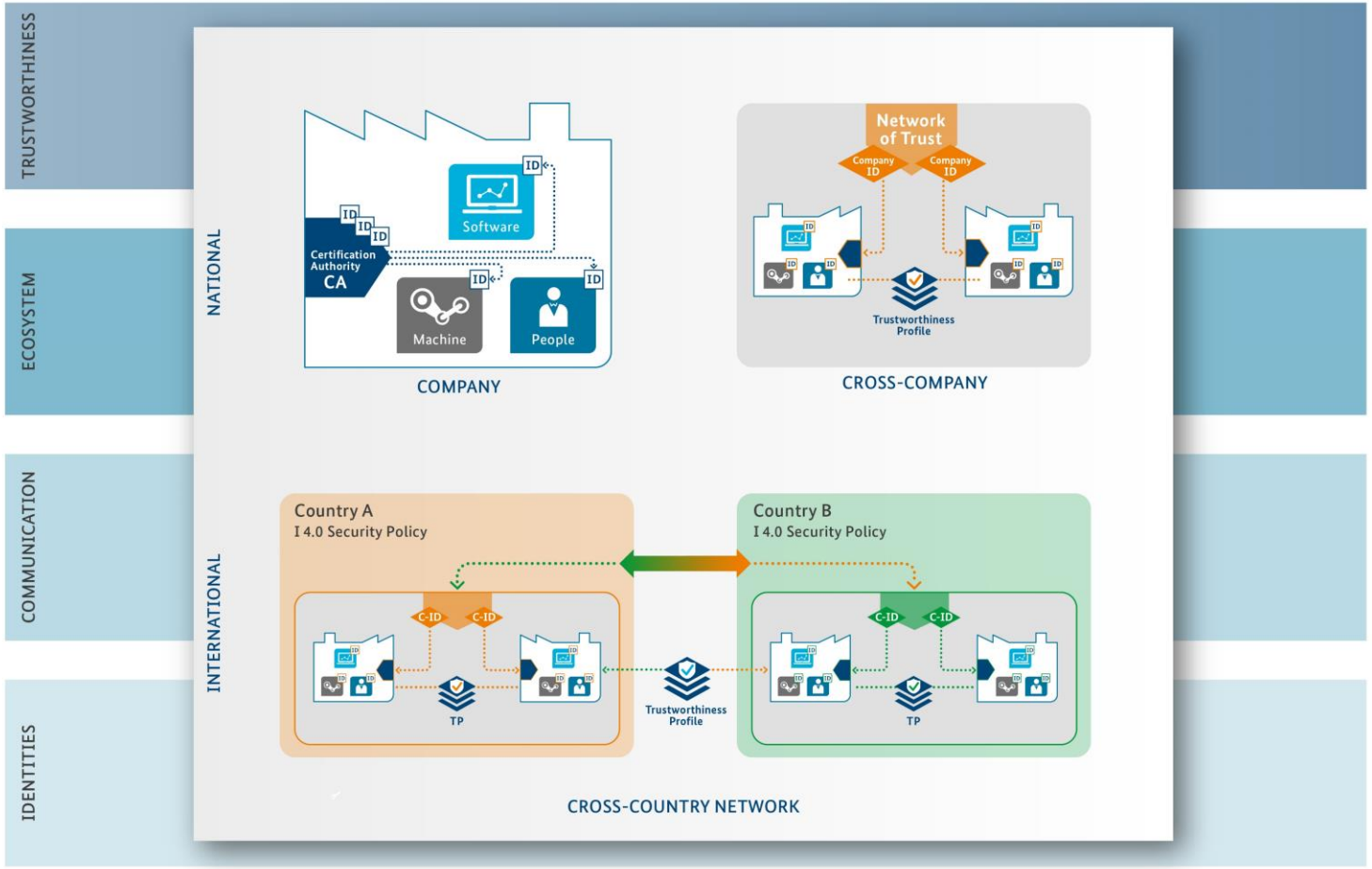
January 27, 2021

Trustworthy Global Security Infrastructure

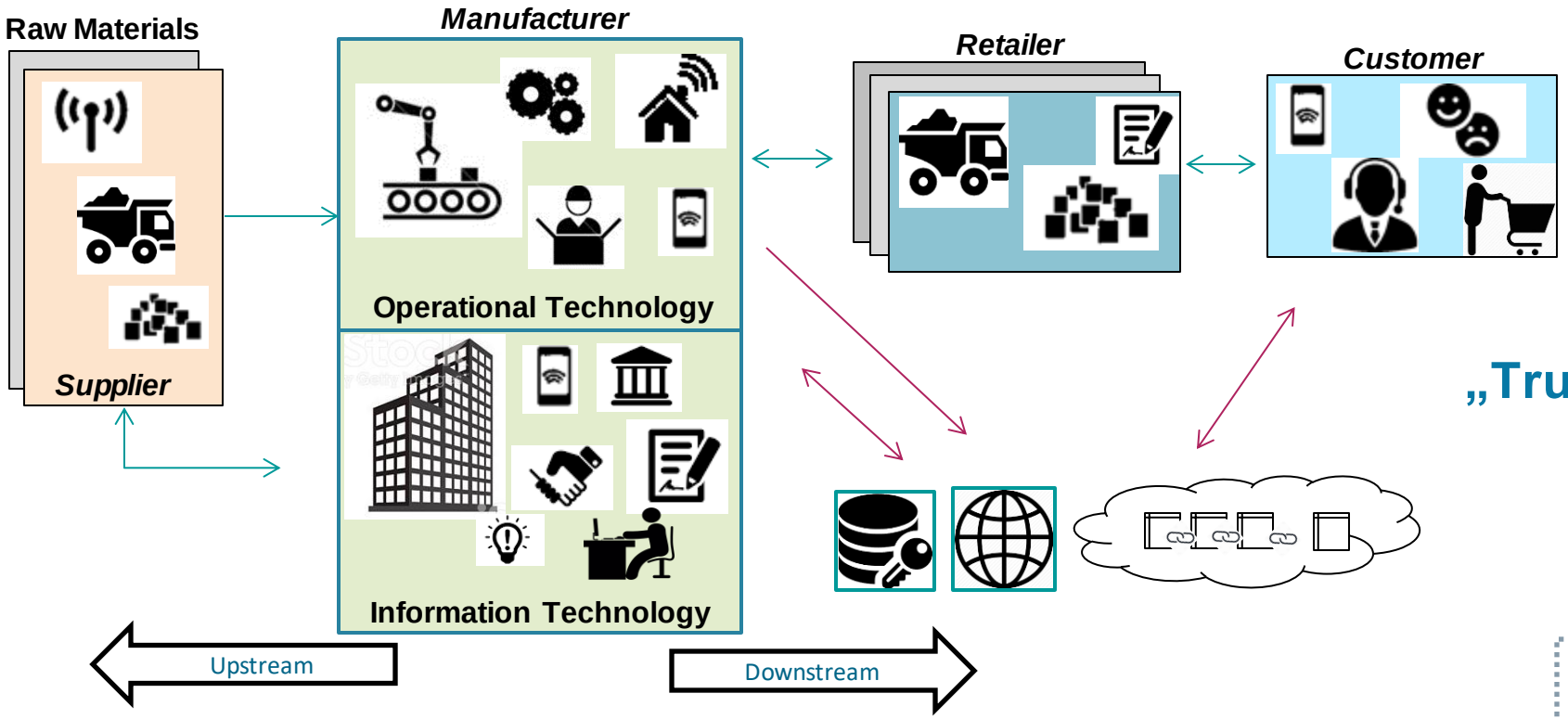
… is the prerequisite for performing secure Industrie 4.0 collaboration on a global level

... how can we trust the applicable security level of involved components, products, processes, and partners?

… how can we establish a infrastructure for secure identities?



Generic Supply Chain Scenario for Industrial IoT Systems



„Trustworthiness“?

Legend:
Physical and/or Digital
Digital

Trustworthiness

Definition of Trustworthiness according to ISO/IEC JTC1 WG 13 Working Draft:

„Ability to meet stakeholders expectations in a demonstrable, verifiable and measurable way"

Notes:

- Depending on the context or sector, and also on the specific product or service, data, and technology used, different characteristics apply and need verification to ensure stakeholders expectations are met.
- Characteristics of trustworthiness include, for instance, reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability and accuracy.
- Trustworthiness is an attribute that can be applied to services, products, technology, data and information as well as, in the context of governance, to organizations.

Trustworthiness of Secure Supply Chains for Industrie 4.0

In the context of our work, the definition of the term ‘trustworthiness’ proposed by the ISO/IEC JTC1/WG13 has been adapted as:

“For supply/value chain security, the term ‘Trustworthiness’ corresponds to the supplier’s ability to meet the expectations of the potential contract partner in a verifiable way”.

Depending on the use case and on the specific product, different characteristics would apply to fulfil stakeholder’s expectations. These characteristics may include authenticity, integrity, resilience, availability, confidentiality, privacy, safety, accountability, and usability.

Trustworthiness Targets regarding Security within a Supply Chain (generic approach)

Assess/monitor the security properties of suppliers via questionnaires and mechanisms

Integrity and authenticity of the product along its lifecycle. Appropriate measures shall be taken in case of a breach

Fulfill baseline cybersecurity supply chain requirements

(e.g. “Charter of Trust”)

- Data Protection
- Security Policies
- Incident Response
- Site Security
- Access, Intervention, Transfer & Separation
- Integrity & Availability
- Support
- Training
- …

Ensure security properties and compliance to security standards and regulations by multiple nodes (suppliers) along the supply chain

Security compliance of the leveraged third-party components in products along their security life cycle (includes processes for fixing vulnerabilities)

What are the problems?

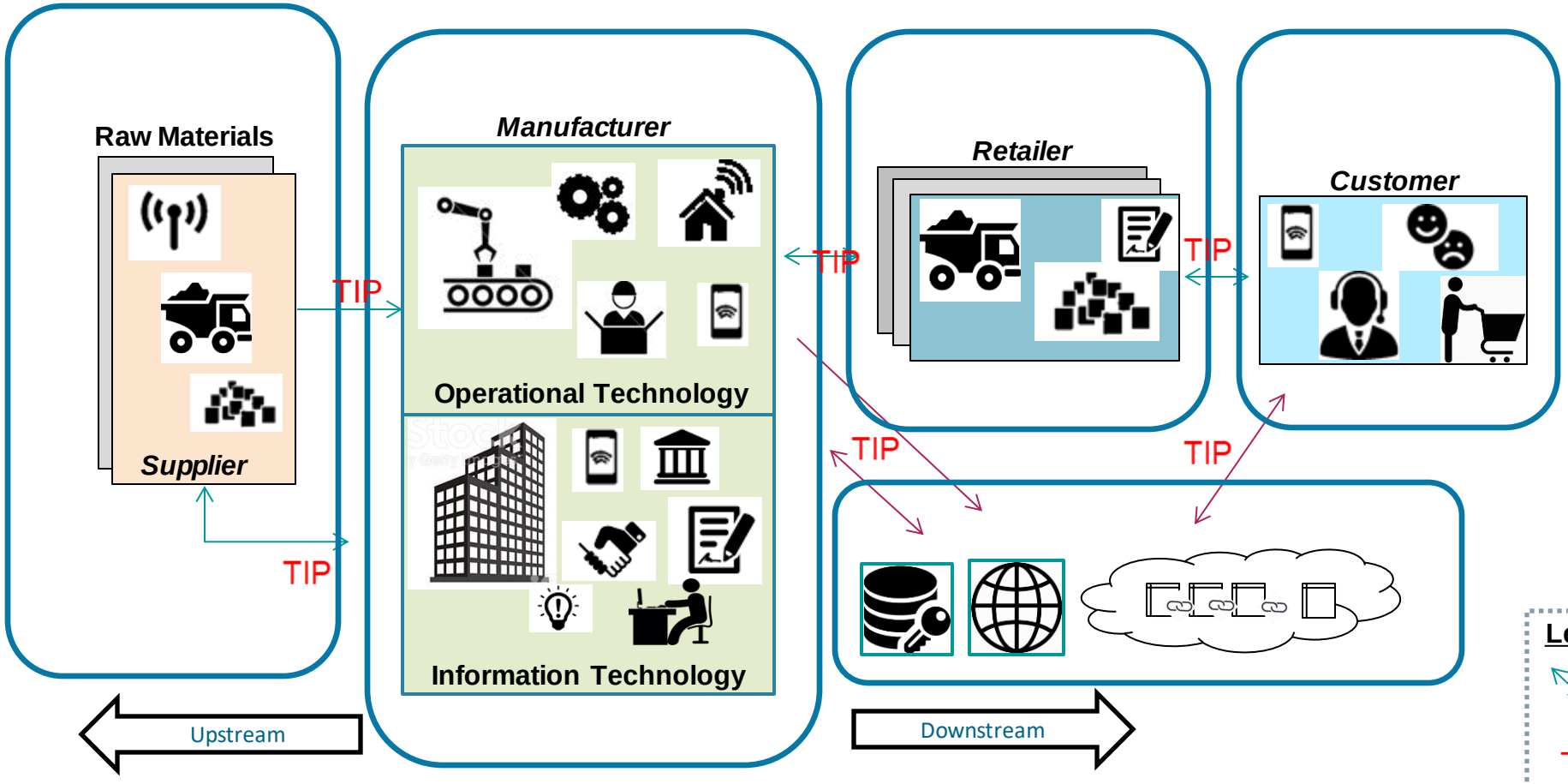
- How can Trustworthiness of Security properties be established and measured along the supply chain?
- What are feasible standards and processes?
- Can we use exisiting standards or do we need new ones?
- How to deal with security requirements specfic to an industrial vertical or to a special business case?

Standardization Bodies and Consortia regarding Supply Chain Security

With respect to supply chain security and trustworthiness, following is a non-exhaustive list of standardization bodies and consortia that shall be considered:

ISO, IEC ISO/IEC JTC1	CEN/CELEC	DIN/DKE, other NSBs	ITU	ETSI
IETF	ENISA	NIST	NEMA	VDA
Global Semiconductor Alliance	IIC	Plattform Industrie 4.0	Charter of Trust	…

Trust Domains and Trust Interaction Points



Ingredients for Trustworthiness Negotiations at Trust Interaction Points

Identities …

- of organizations, such as NTA, etc.
- of employees, such as usernames, email addresses, PKI certificates, etc.
- of processes, such as the unique process ID assigned by the operating systems, etc.
- of products and components, such as barcodes, etc.

Certificates

- Identity Authenticating Certificates such as X.509 PKI, eIDAS, etc.
- “Security Certification Certificates”, such as ISO 27001 certificates, IEC 62443 certificates, ISO/IEC 15408 certificates, etc.

Standards and Frameworks

- IEC 62443-x-x
- ISO 27001
- METI CPSF
- NIST CSF
- ISO 21434
- TISAX
- ISO/IEC 15408-x
- …

PLATTFORM INDUSTRIE 4.0

Trustworthiness Profile

A standardized container that can be realized irrespective of the base communication technology

The granularity of trustworthiness expectations is flexible and depends on the business provider's requirements

The Trustworthiness Profile leverages cryptographic mechanisms to ensure integrity of the exchanged information

Trustworthiness Profile

To be filled by the Buyer

Buyer's Information

Contact Partner:
*Contact Partner's Unique Identifier:
Contact Information:
Legal Entity Name:
*Legal Entity Unique Identifier:
*Unique Identifier Scheme: *(e.g., link to LEI code repo, VATIN by DUNS, NTA by TSE, etc.)*
Country:
Additional Information:

Trustworthiness Expectations

		Additional Information	*Expected Validity*	*Supplier Conformance*	*Self*	*3rd party*
ISO/IEC 62443-4-2	Upload/Attach			☐	☐	☐
ISO 27001	Upload/Attach			☐	☐	☐
NIST SP 800	Upload/Attach			☐	☐	☐
Common Criteria	Upload/Attach			☐	☐	☐
PSS Supplier Questionnaire	Upload/Attach			☐	☐	☐
	Upload/Attach			☐	☐	☐
	Upload/Attach			☐	☐	☐
	Upload/Attach			☐	☐	☐
	Upload/Attach			☐	☐	☐

Reference Request-for-work | Time Stamp

Digital Signature | Digital Certificate (If required)

To be filled by the Supplier

Supplier's Information

Contact Partner:
*Contact Partner's Unique Identifier:
Contact Information:
Legal Entity Name:
*Legal Entity Unique Identifier:
*Unique Identifier Scheme: *(e.g., link to LEI code repo, VATIN by DUNS, NTA by TSE, etc.)*
Country:
Additional Information:

Trustworthiness Capabilities

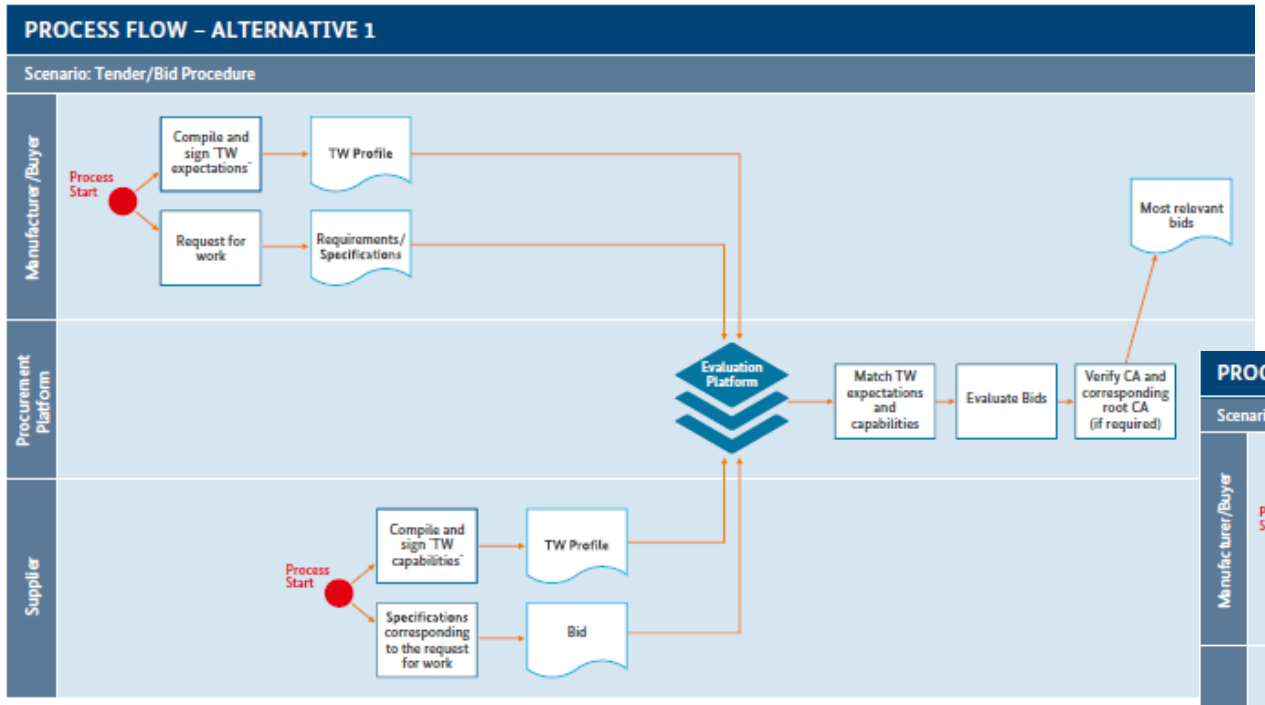
			Proof/ Evidence	*Proof Expiry Date*	*Additional Information*
Conform: ☐	Self-Assessment ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Conform: ☐	Self-Assessed ☐	3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	

Reference TW Expectations | Quote/Bid Reference | Time Stamp

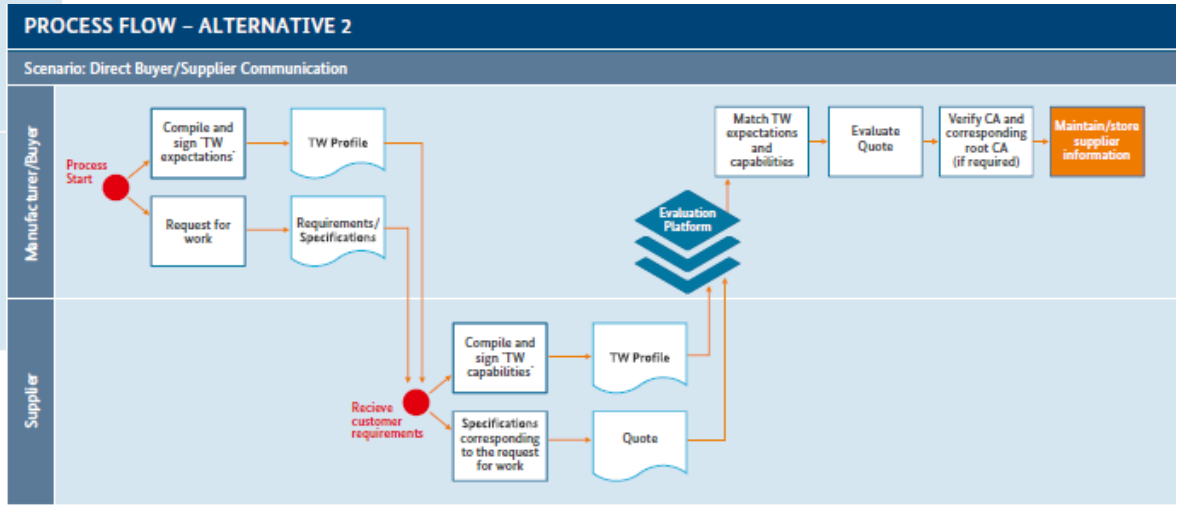
Digital Signature | Digital Certificate (If required)

Trustworthiness Expectations and Capabilities Exchange Protocol

The white paper introduces a “Trustworthiness Expectations and Capabilities Exchange Protocol” (TECEP) as a technical solution to be used for trustworthiness negotiation and exchange between participating peers.



The TECEP supports automation of the existing supplier (and/or product) qualification and selection process as well.



White Paper: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/IIoT_Value_Chain_Security.html

“Chain of Trust” is needed

There exist many security approaches, which can be used for supply chains, e.g.:

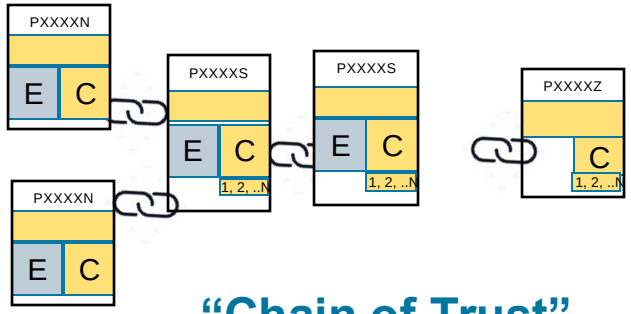
ISO/IEC 28000, ISO 2700x, IEC 62443, ISO 15408, ISO TC292 „Anticounterfeiting“,….

However, there does not exist a standard suite yet

- which establishes & measures Trustworthiness of Security properties along the supply chain
- which includes interoperability
- which provides assurance for several nodes of the supply chain
- which supports automated processing

Trustworthiness profile as basic building block for the chain of trust

to provide trustworthiness information at any node



“Chain of Trust”

Summary and next steps

- Trustworthiness of Secure Supply Chains is a prerequisite for performing secure Industrie 4.0 collaboration on a global level
- Existing work, such as the “Trustworthiness Profile”, addresses the “single” supplier-manufacturer relation
- Future activities need to support the establishment of “Chains of Trust” along the value chains of industry

Thank you very much!

Wolfgang Klasen

wolfgang.klasen@siemens.com

Tel.: +49 173 362 362 1

Plattform Industrie 4.0
Contact the Secretariat

Plattform Industrie 4.0
Secretariat

Bülowstraße 78, 10783 Berlin
Tel.: +49 30 2759 5066-50
geschaeftsstelle@plattform-i40.de
www.plattform-i40.de