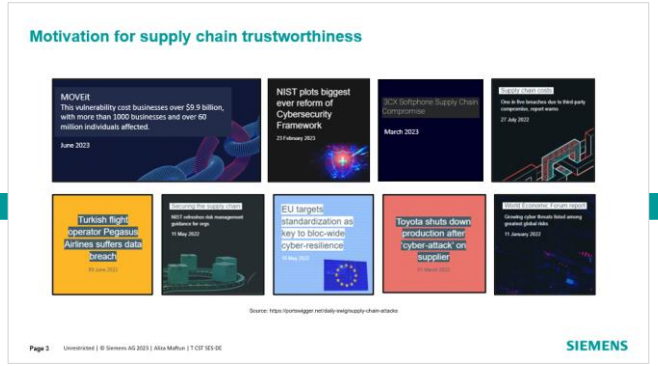
Supply Chain Trustworthiness

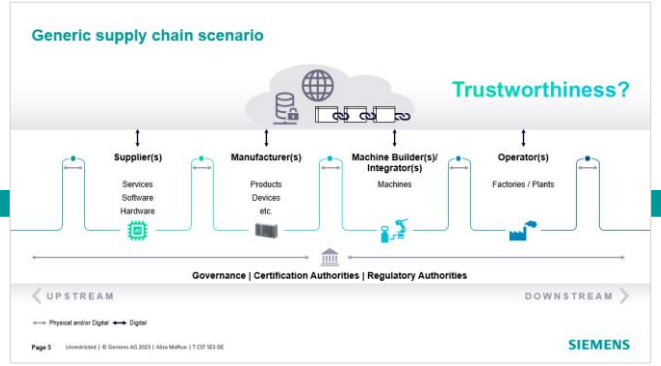
Aliza Maftun

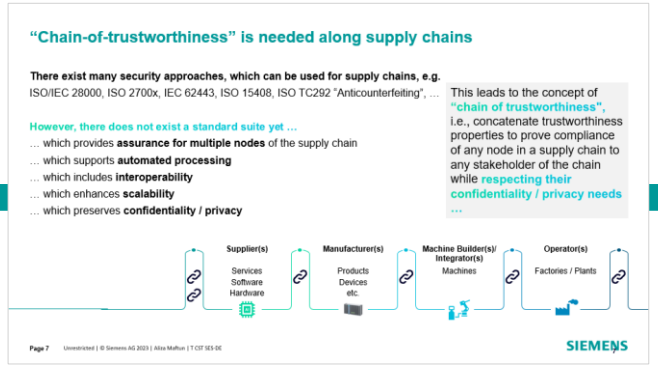
Siemens AG

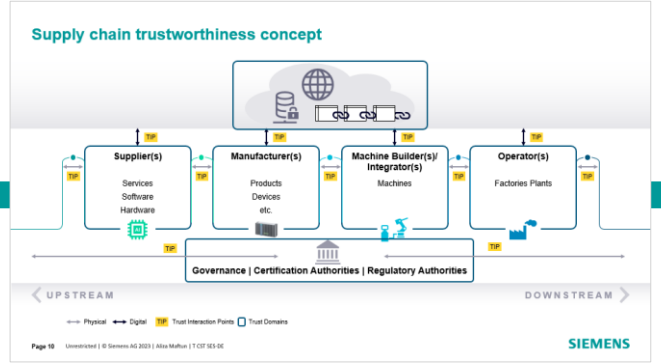
SIEMENS

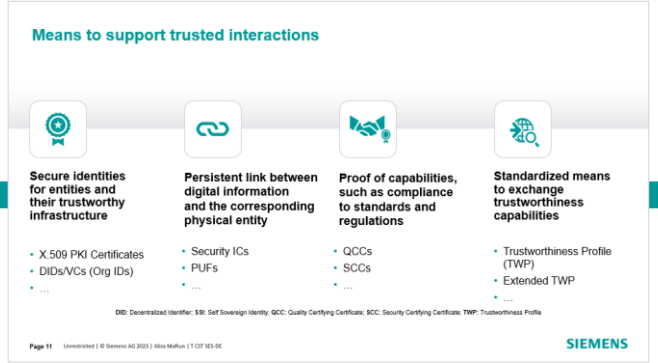
Content

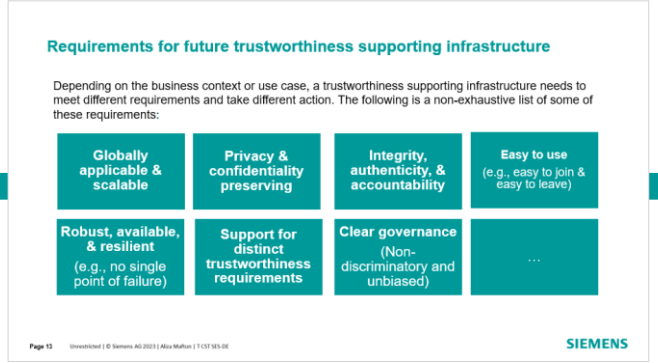


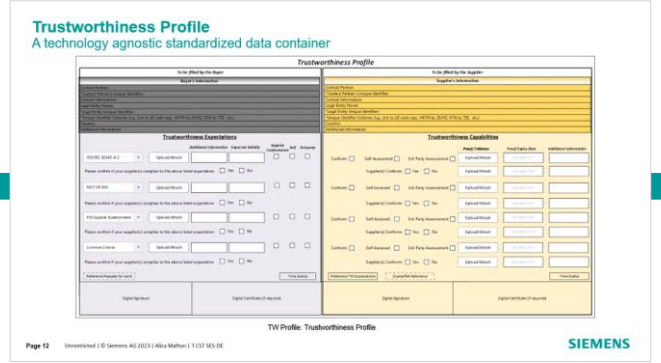


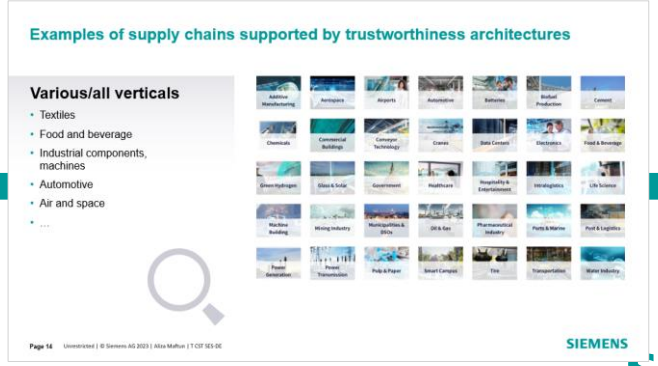












SIEMENS

Motivation for supply chain trustworthiness

Source: https://portswigger.net/daily-swig/supply-chain-attacks

SIEMENS

Demand for supply chain trustworthiness is increasing

Drivers of economy
(examples)

Customer needs/values

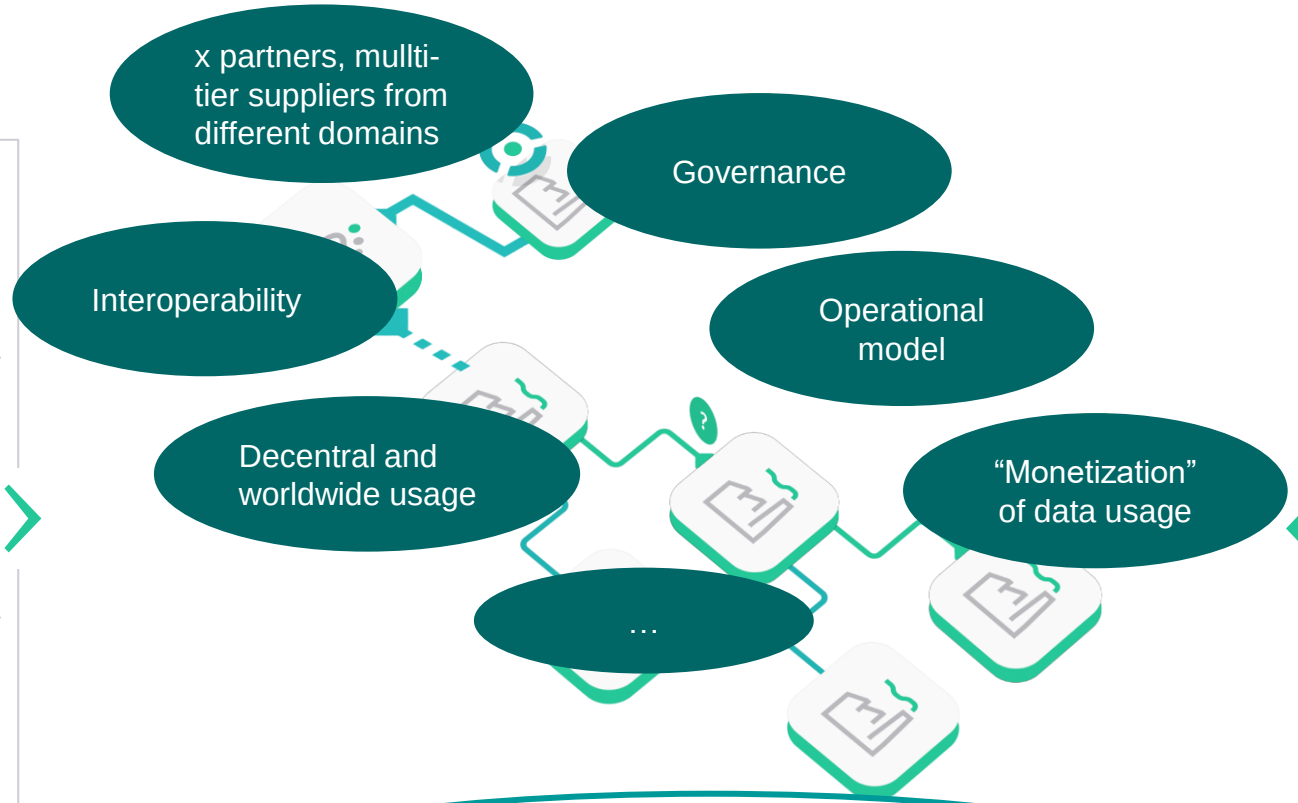
Market needs

Public needs/values

- Responsibility
- Sustainability

Regulations

- Data act
- Dig. product pass



Trustworthiness along the supply chain, with multiple (unknown) entities, is needed

… reflected by companies
(examples)

Company values

Comp. advantage

- Resilience, Supply chain tech. sovereignty

Technology

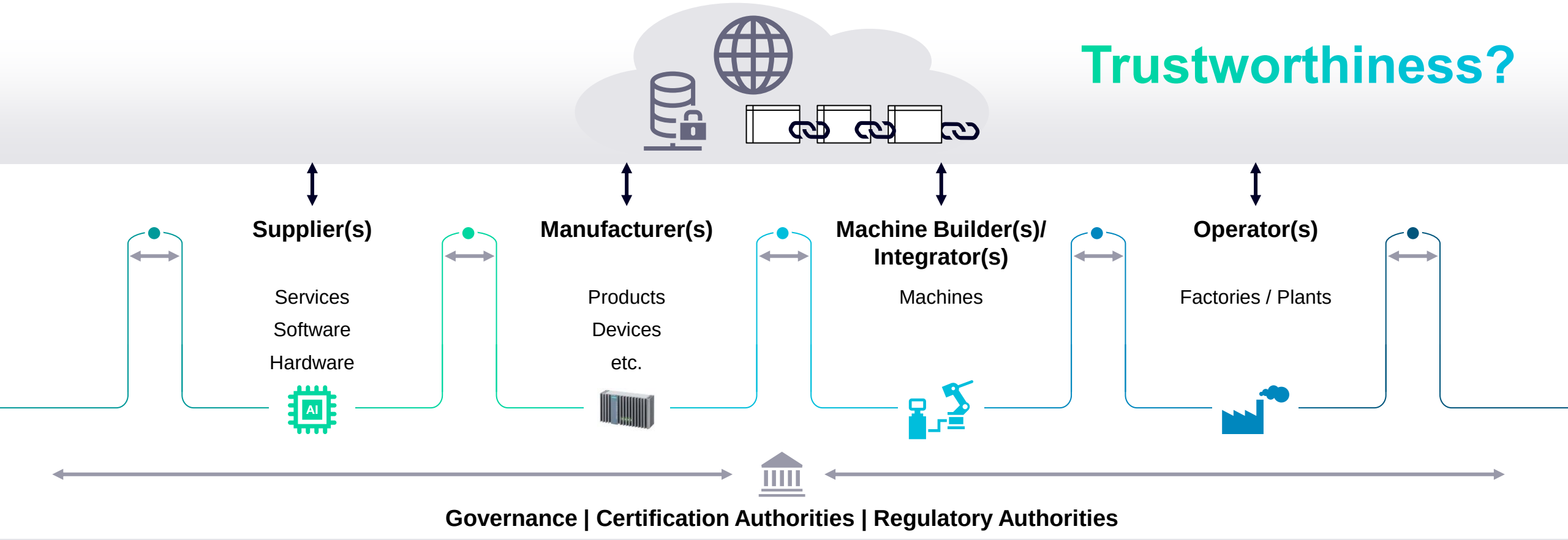
- Central, decentral or distributed

Business strategy

- New improved businesses
- Partner network

SIEMENS

Generic supply chain scenario



Physical and/or Digital ⟷ Digital

SIEMENS

What is supply chain trustworthiness?

In the context of supply chain, the definition of the term “trustworthiness” proposed by the ISO/IEC JTC1/WG13 has been adapted as

Trustworthiness corresponds to the ability of a stakeholder to make its **claims verifiable**, between immediate or along multiple entities in a supply chain

Notes

01 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.

02 Characteristics of trustworthiness include reliability, availability, resilience, security, privacy, safety, accountability, transparency, integrity, authenticity, quality, usability, sustainability or environmental properties (CO_2 footprint), compliance to local or national regulations (German “Lieferkettengesetz”), etc.

03 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.

“Chain-of-trustworthiness” is needed along supply chains

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 provides **assurance for multiple nodes** of the supply chain

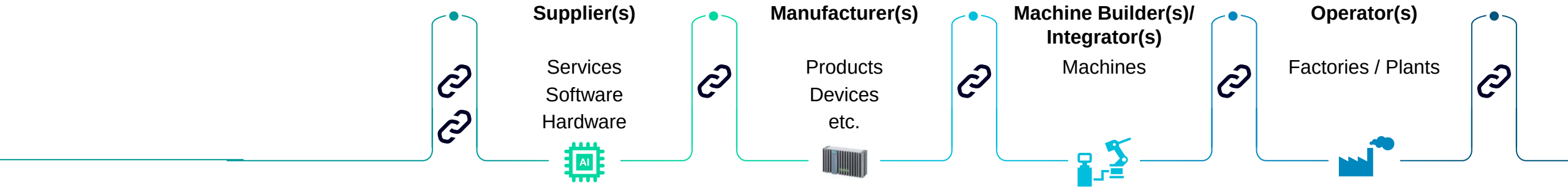
… which supports **automated processing**

… which includes **interoperability**

… which enhances **scalability**

… which preserves **confidentiality / privacy**

This leads to the concept of **“chain of trustworthiness",** i.e., concatenate trustworthiness properties to prove compliance of any node in a supply chain to any stakeholder of the chain while **respecting their confidentiality / privacy needs …**



Possible topologies for chain of trustworthiness along supply chains

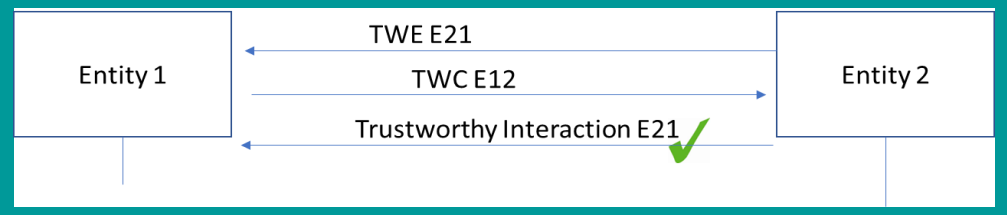


Figure 1 Unilateral trustworthiness

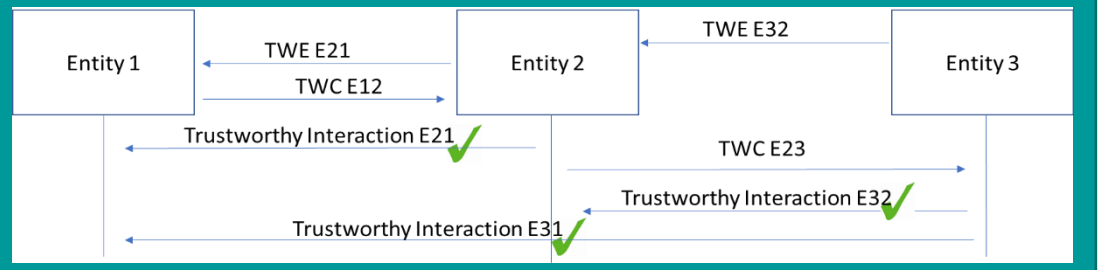


Figure 2 Unilateral trustworthiness propagation

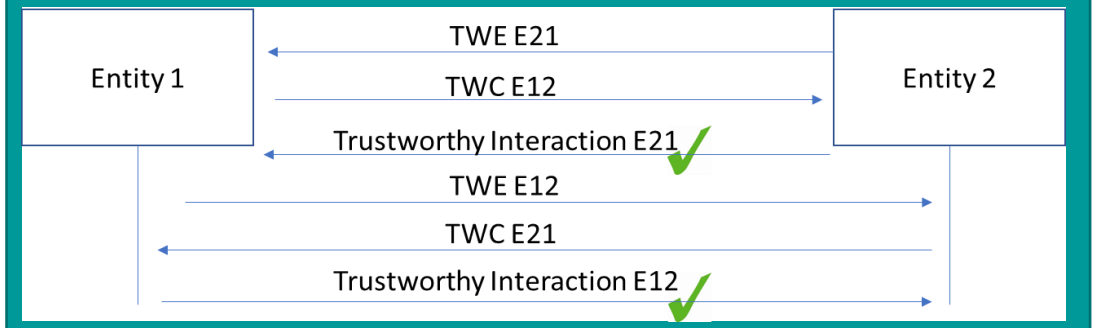


Figure 3 Bilateral trustworthiness

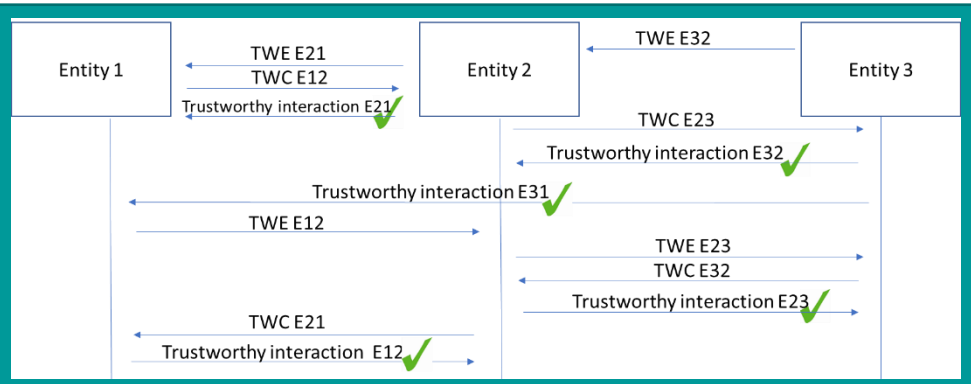


Figure 4 Bilateral trustworthiness propagation

SIEMENS

ISO 22373 – Framework for supply chain trustworthiness

A standardized approach to achieve end-to-end trustworthiness across supply chains

ISO TC 292 - Security and Resilience

Scope: Standardization in the field of security to enhance the safety and resilience of society.

Working Group 4 - Authenticity, integrity and trust for products and documents

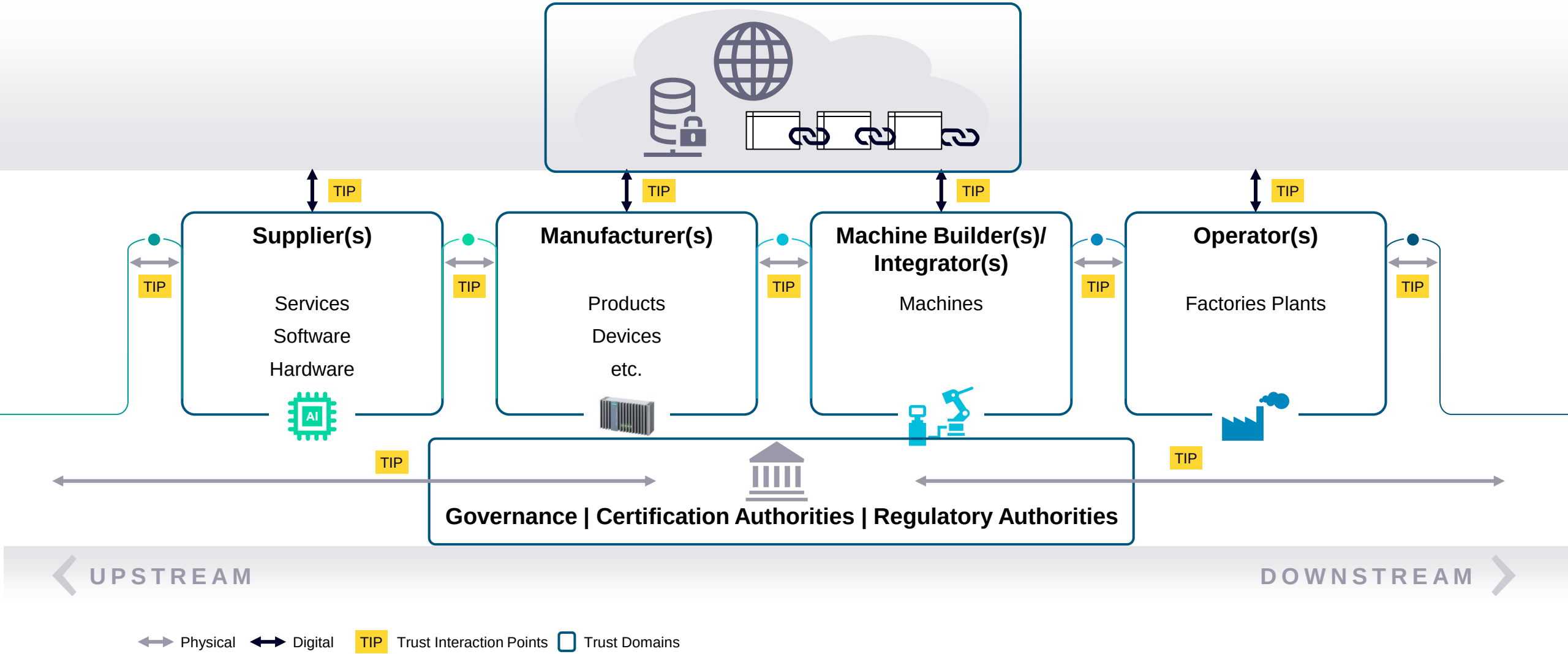
This Working Group is responsible for drafting standards in the field of fraud countermeasures and controls.

ISO 22373:

- provides **guidelines**
- applicable to **all organizations**, regardless of their type, size, or nature
- **Technology-agnostic** and can leverage existing and upcoming technologies like PKI, W3C verifiable credentials, etc.
- focuses on ensuring **scalability** and **interoperability**

SIEMENS

Supply chain trustworthiness concept



Physical | Digital | TIP Trust Interaction Points | Trust Domains

SIEMENS

Means to support trusted interactions

Secure identities for entities and their trustworthy infrastructure

- X.509 PKI Certificates
- DIDs/VCs (Org IDs)
- …

Persistent link between digital information and the corresponding physical entity

- Security ICs
- PUFs
- …

Proof of capabilities, such as compliance to standards and regulations

- QCCs
- SCCs
- …

Standardized means to exchange trustworthiness capabilities

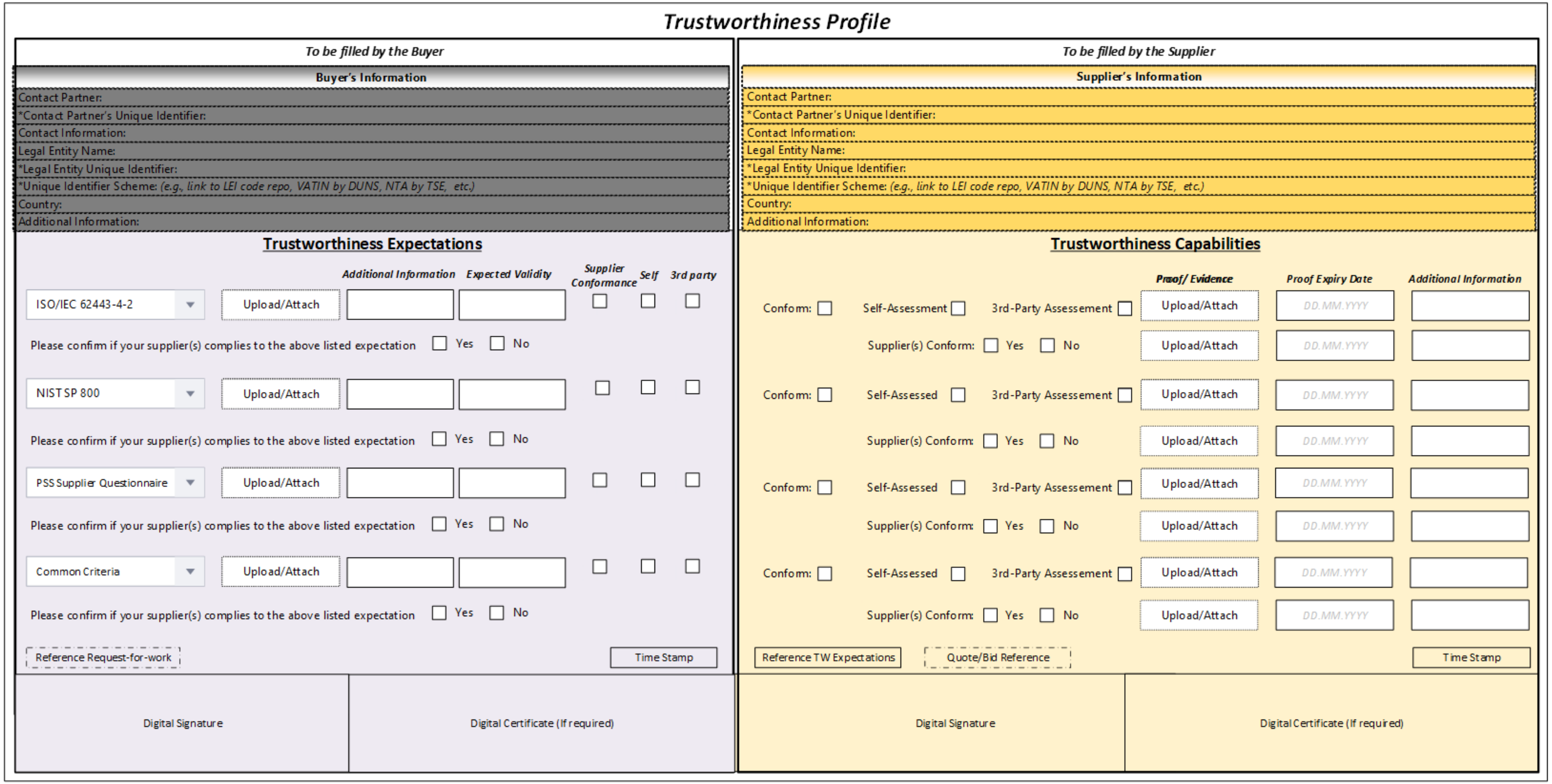
- Trustworthiness Profile (TWP)
- Extended TWP
- …

DID: Decentralized Identifier; **SSI:** Self Sovereign Identity; **QCC:** Quality Certifying Certificate; **SCC:** Security Certifying Certificate; **TWP:** Trustworthiness Profile

SIEMENS

Trustworthiness Profile

A technology agnostic standardized data container



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			☐	☐	☐
NIST SP 800 ▾	Upload/Attach			☐	☐	☐
PSS Supplier Questionnaire ▾	Upload/Attach			☐	☐	☐
Common Criteria ▾	Upload/Attach			☐	☐	☐

After each row: Please confirm if your supplier(s) complies to the above listed expectation ☐ Yes ☐ No

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	
Supplier(s) Conform: ☐ Yes ☐ No	Upload/Attach	DD.MM.YYYY	
Conform: ☐ Self-Assessed ☐ 3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Supplier(s) Conform: ☐ Yes ☐ No	Upload/Attach	DD.MM.YYYY	
Conform: ☐ Self-Assessed ☐ 3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Supplier(s) Conform: ☐ Yes ☐ No	Upload/Attach	DD.MM.YYYY	
Conform: ☐ Self-Assessed ☐ 3rd-Party Assessement ☐	Upload/Attach	DD.MM.YYYY	
Supplier(s) Conform: ☐ Yes ☐ No	Upload/Attach	DD.MM.YYYY	

Reference TW Expectations
Quote/Bid Reference
Time Stamp

Digital Signature
Digital Certificate (If required)

TW Profile: Trustworthiness Profile

Requirements for future trustworthiness supporting infrastructure

Depending on the business context or use case, a trustworthiness supporting infrastructure needs to meet different requirements and take different action. The following is a non-exhaustive list of some of these requirements:

Globally applicable & scalable

Privacy & confidentiality preserving

Integrity, authenticity, & accountability

Easy to use
(e.g., easy to join & easy to leave)

Robust, available, & resilient
(e.g., no single point of failure)

Support for distinct trustworthiness requirements

Clear governance
(Non-discriminatory and unbiased)

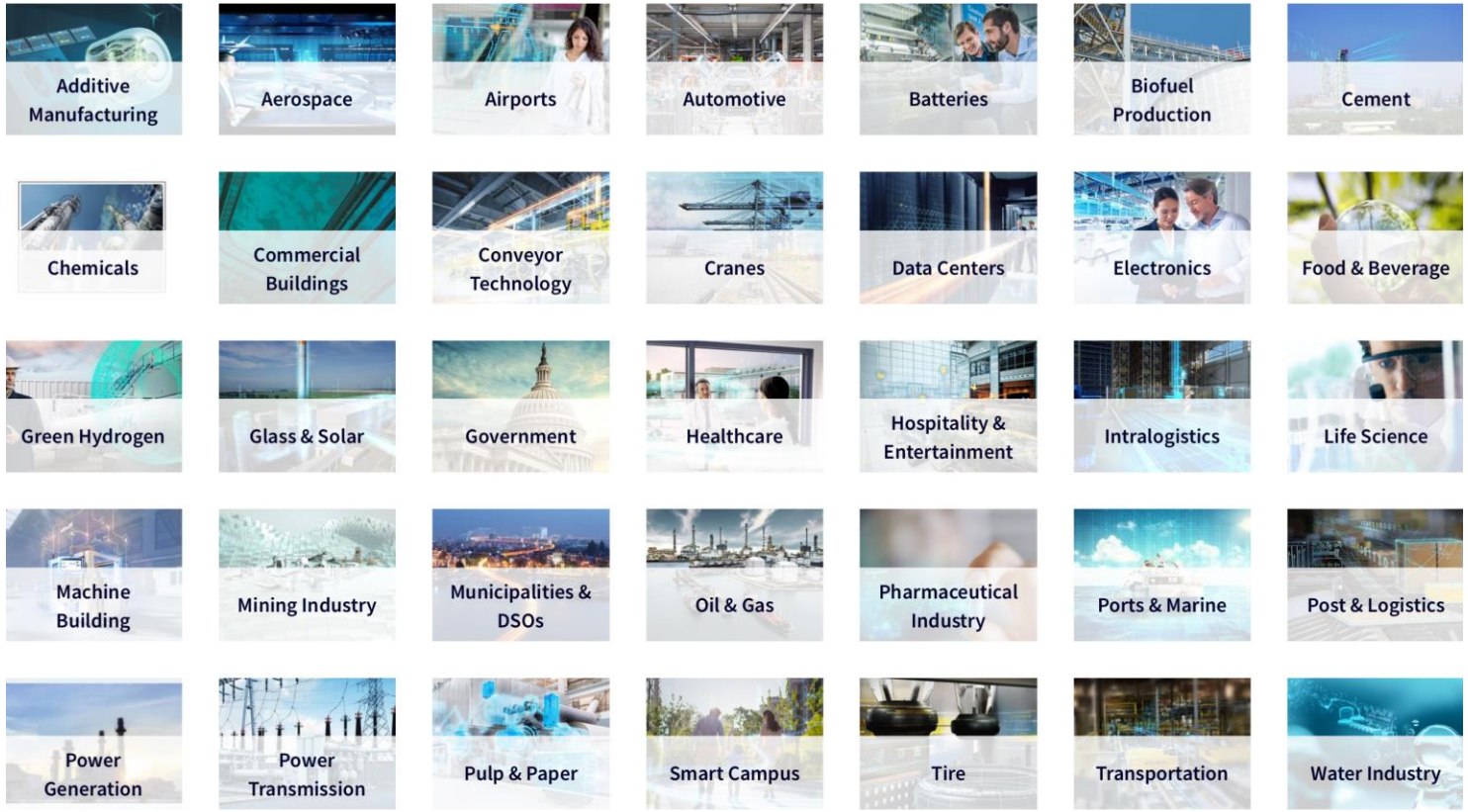
…

SIEMENS

Examples of supply chains supported by trustworthiness architectures

Various/all verticals

- Textiles
- Food and beverage
- Industrial components, machines
- Automotive
- Air and space
- …



SIEMENS

Thank you for your attention

Please feel free to share your thoughts, questions, comments, etc.

Contact Information:

Aliza Maftun

Senior Key Expert – Supply Chain Security

T CST SES-DE

Siemens AG

E-mail aliza.maftun@siemens.com

SIEMENS