Cybersecurity Challenges in Dataspaces

-Trustworthiness and Security for Value Chains -

Accomplishing Chain-of-Trust

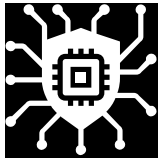
Dr. Wolfgang Klasen | Senior Advisor Security | Siemens AG

SIEMENS

Dataspaces support data sharing among organizations

Definition

A dataspace can be defined as a data ecosystem built around commonly agreed building blocks, enabling an effective and trusted sharing of data among participants to create value *



Supply and Value Chain Operation

Product Carbon Footprint (PCF)

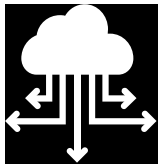
Collaborative Engineering

Use Cases

Circular Economy, DPP (Environmental and Social Standards)

Condition Monitoring

Demand & Capacity Management



Benefit

Enables cross-organizational and cross-company exchange of data, providing basis for fruitful co-operation and implementing complex data-driven use cases, also allowing data monetization

SIEMENS

**Dataspace defintion: Guidance on IoT and digital twin integrations in data spaces, ISO/IEC JTC 1/SC 41 N2335*

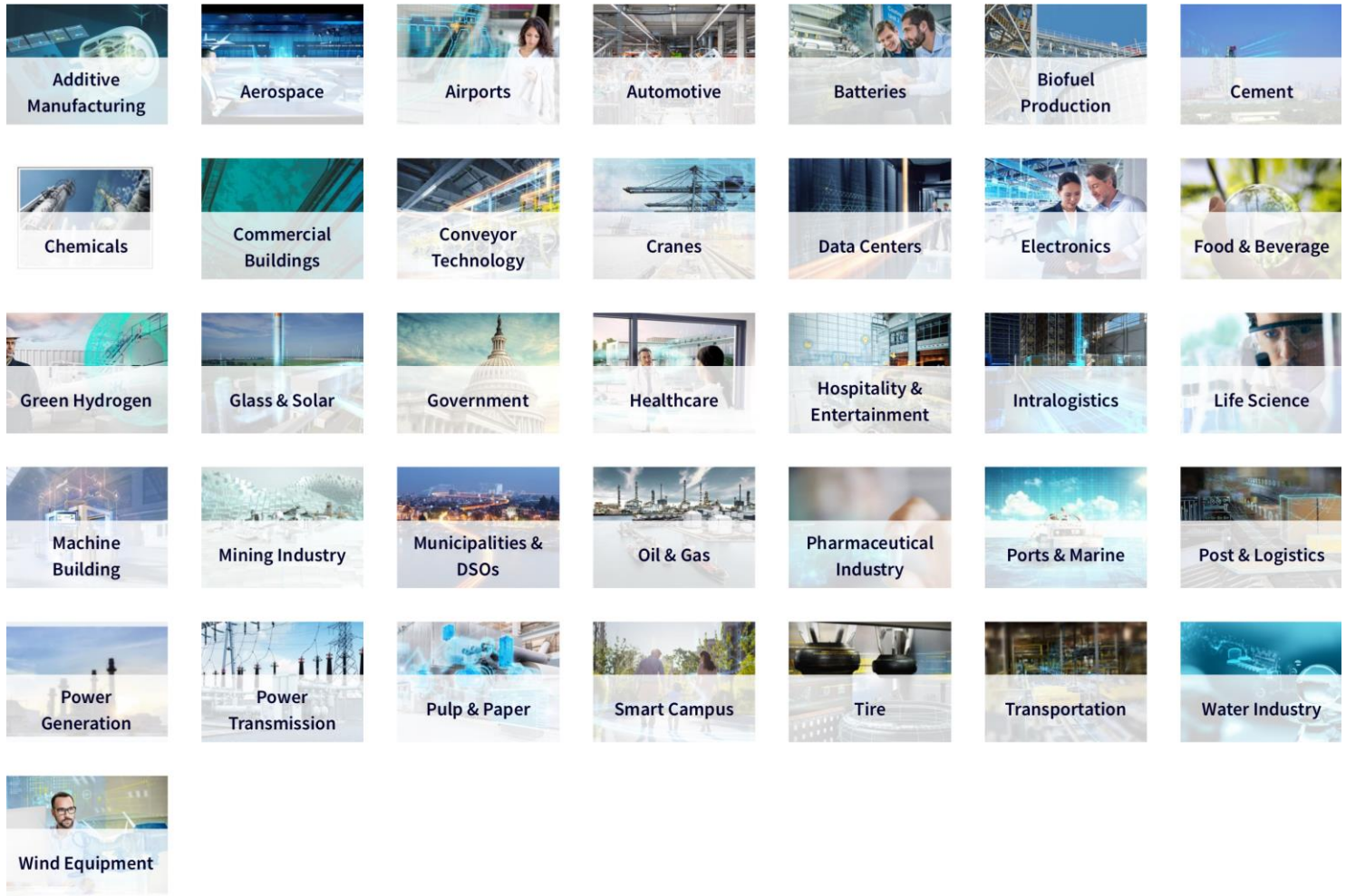
Motivation for supply chain security & trustworthiness is not new…

SIEMENS

Examples of supply chains to be supported by trustworthiness architectures

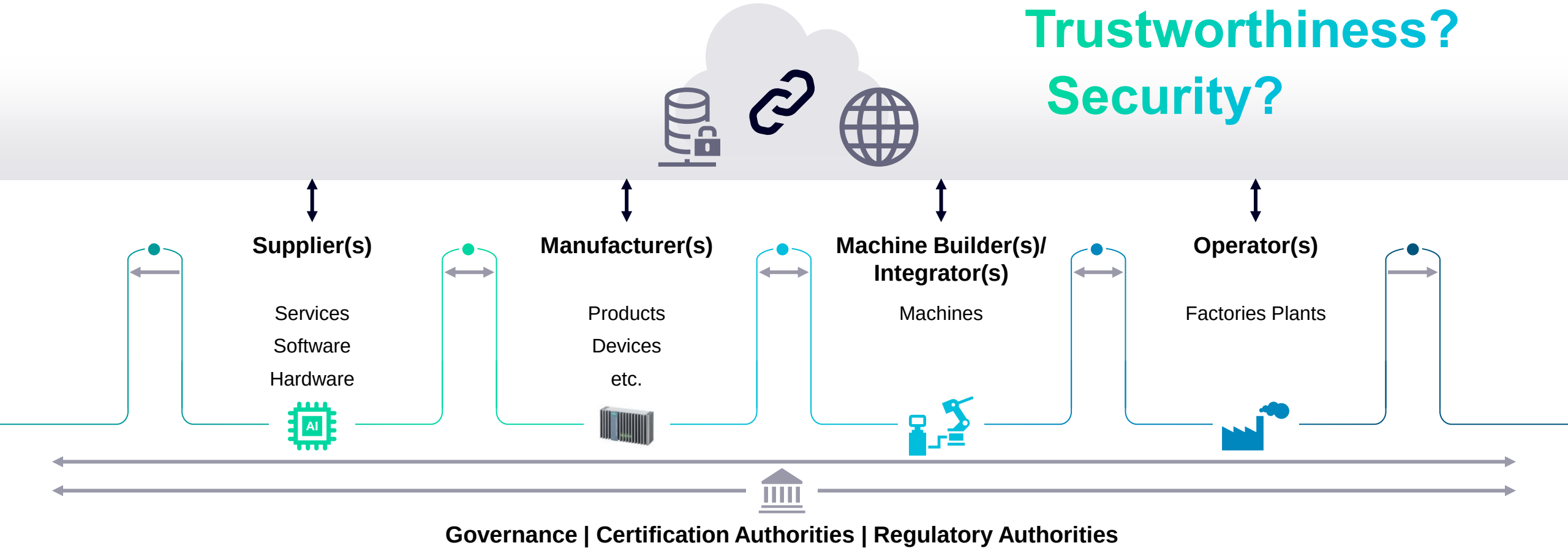
Various/all verticals

- Textiles
- Food and Beverage
- Industrial components, machines
- Automotive
- Air&Space
- …



SIEMENS

Industrial Supply & Value Chain Operation is a typical use case in Data Space



Physical and/or Digital Digital

SIEMENS

How to define supply chain Trustworthiness on top of Security?

Definition of Trustworthiness in the context of supply chains based on the working definition by ISO/IEC JTC1 WG13

“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, for instance, reliability, availability, **resilience**, **security**, privacy, **safety**, accountability, transparency, integrity, authenticity, quality, usability, accuracy, **sustainability**, compliance to applicable standards and regulations, 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.

04 Verifiability includes measurability and demonstrability by means of objective evidence.

How to define supply chain Trustworthiness on top of Security?

Definition of Trustworthiness in the context of supply chains based on the working definition by ISO/IEC JTC1 WG13

“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.

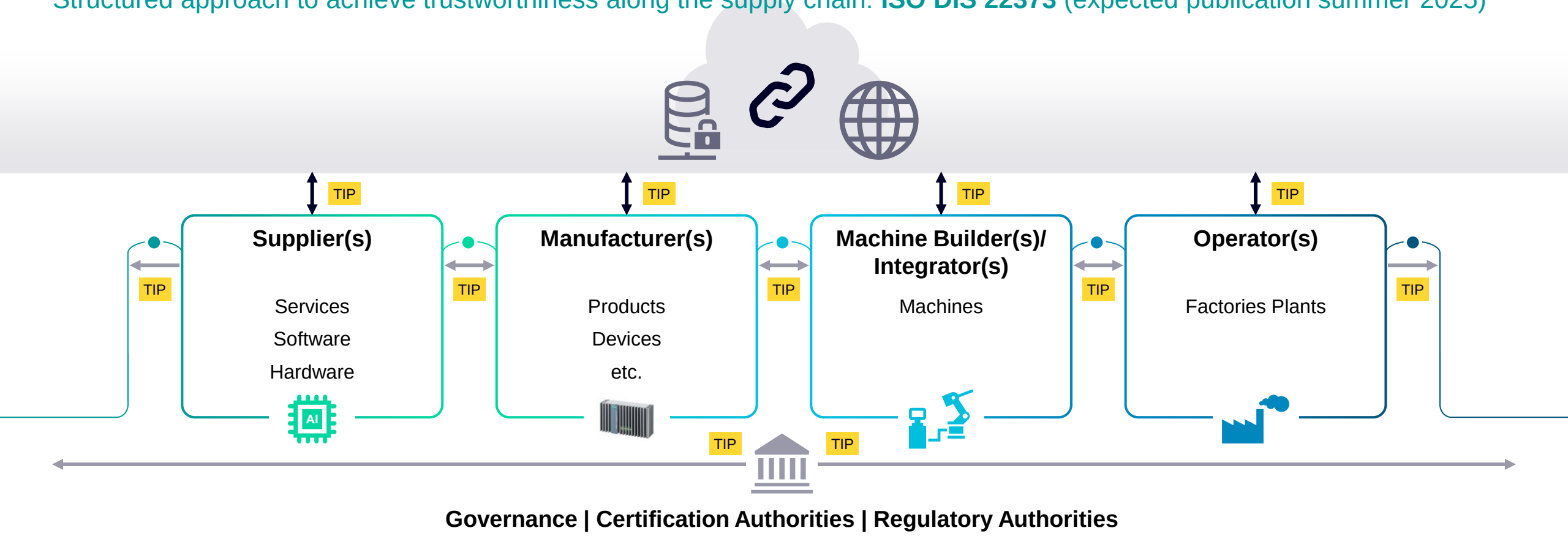
02 Characteristics of trustworthiness include, for instance, reliability, availability, **resilience**, **security**, privacy, **safety**, accountability, transparency, integrity, authenticity, quality, usability, accuracy, **sustainability**, compliance to applicable standards and regulations, etc.

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.

04 Verifiability includes measurability and demonstrability by means of objective evidence.

Trustworthiness architecture

Structured approach to achieve trustworthiness along the supply chain: **ISO DIS 22373** (expected publication summer 2025)



Means to support Trusted Interactions... What functions are necessary for Chain-of-Trust?

Secure Identities for Entities

- X.509 PKI Certificates
- DIDs/SSIs
- …

Persistent link between digital information and the corresponding physical entity

- Security ICs
- PUFs
- …

Proof of compliance to standards and regulations

- QCCs
- SCCs
- …

Standardized means to exchange TW capabilities

- TWP
- Extended TWP
- …

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

Means to support Trusted Interactions... What functions are necessary for Chain-of-Trust?

Wallet

Secure Identities for Entities

- X.509 PKI Certificates
- DIDs/SSIs
- …

Persistent link between digital information and the corresponding physical entity

- Security ICs
- PUFs
- …

Proof of compliance to standards and regulations

- QCCs
- SCCs
- …

Standardized means to exchange TW capabilities

- TWP
- Extended TWP
- …

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

Governance to essential for Trustworthiness & Security supporting infrastructure

Definitions of Governance:

- Governance: system by which organizations are directed and controlled ISO/IEC 24533-2
- Governance: human-based system comprising directing, overseeing and accountability (ISO/IEC 38500)
- Governance of information security: system by which an organization's (3.50)information security (3.28) activities are directed and controlled ISO/IEC 27000:2018(en)
    - Note 1 to entry: This process is closely linked to the notions of data ownership and stewardship.
    - Note 2 to entry: This definition is adapted from Reference [22].ISO/TR 14872:2019(en)
- Governance of IT: system by which the current and future use of IT is governed ISO/IEC 38500
- Data governance: process focused on managing the quality, consistency, usability, security, and availability of information
- Data governance: process focused on managing the quality, consistency, usability, security, and availability of information ISO/TR 14872:2019(en)
    - Note 1 to entry: This process is closely linked to the notions of data ownership and stewardship.
    - Note 2 to entry: This definition is adapted from Reference [22].
- Data governance: process of overall management of the availability, usability, integrity, and security of the data employed in an enterprise assuring that the decision-making process prioritizes investments, allocates resources, and measures results
    - Note 1 to entry: Data governance is a component of the information governance (3.1.13).ISO 5477:2023(en)

European JRC: Data governance consists of norms, principles and rules governing various types of data and their use. In general, it is understood as the correct management and maintenance of data assets and related aspects, such as data rights, data privacy, and data security, among others. It refers not only to regulations (i.e., the set of rules of a legislative nature established by policy makers), **but also to the relations, processes and socio-technical arrangements established by multiple social actors to manage data. It encompasses the social, economic, political, and cultural factors that explain how data is accessed and controlled by a multitude of actors.**

➢ https://wikis.ec.europa.eu/spaces/jrcdataspaceswiki/pages/78709313/3.+Governance

SIEMENS

Governance to essential for Trustworthiness & Security supporting infrastructure

Definitions of Governance:

- Governance: system by which organizations are directed and controlled ISO/IEC 24533-2
- Governance: human-based system comprising directing, overseeing and accountability (ISO/IEC 38500)
- Governance of information security: system by which an organization's (3.50)information security (3.28) activities are directed and controlled ISO/IEC 27000:2018(en)
    - Note 1 to entry: This process is closely linked to the notions of data ownership and stewardship.
    - Note 2 to entry: This definition is adapted from Reference [22].ISO/TR 14872:2019(en)
- Governance of IT: system by which the current and future use of IT is governed ISO/IEC 38500
- Data governance: process focused on managing the quality, consistency, usability, security, and availability of information
- Data governance: process focused on managing the quality, consistency, usability, security, and availability of information ISO/TR 14872:2019(en)
    - Note 1 to entry: This process is closely linked to the notions of data ownership and stewardship.
    - Note 2 to entry: This definition is adapted from Reference [22].
- Data governance: process of overall management of the availability, usability, integrity, and security of the data employed in an enterprise assuring that the decision-making process prioritizes investments, allocates resources, and measures results
    - Note 1 to entry: Data governance is a component of the information governance (3.1.13).ISO 5477:2023(en)

European JRC: Data governance consists of norms, principles and rules governing various types of data and their use. In general, it is understood as the correct management and maintenance of data assets and related aspects, such as data rights, data privacy, and data security, among others. It refers not only to regulations (i.e., the set of rules of a legislative nature established by policy makers), **but also to the relations, processes and socio-technical arrangements established by multiple social actors to manage data. It encompasses the social, economic, political, and cultural factors that explain how data is accessed and controlled by a multitude of actors.**

➢ https://wikis.ec.europa.eu/spaces/jrcdataspaceswiki/pages/78709313/3.+Governance

SIEMENS

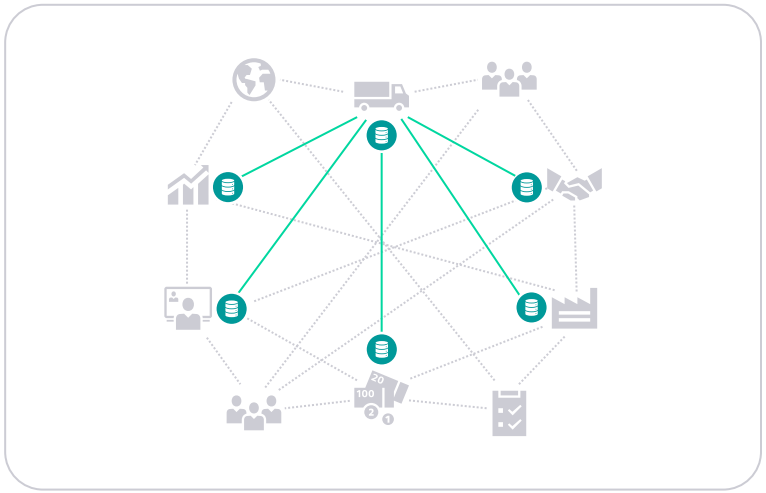
Governance along the Supply/Value Chain Data Space has to ensure:

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

- **Robustness, availability, and resilience, e.g.: no single point of failure, future proof**
  - Chain of trustworthiness must be adaptable and resilient to any (single) point of failure; flexibility to future requirements (PQC,…)
- **Scalability**
  - Trustworthiness infrastructure must be applicable to the global market and user community.
- **Privacy / confidentiality preserving**
  - The infrastructure must be able to specify and control access to any data to protect the business against attacks.
- **Integrity, authenticity, accountability**
  - The integrity and authenticity of information throughout supply chain must be verifiable to any relevant supply chain stakeholder.
- **Support of different trust levels**
  - Trust levels are not for free and must be founded by the business case that uses them.
    Therefore, different industries may want to support different trust levels.
- **Easy to use, easy to join, and easy to leave**
  - Participants should be able to use/join the chain of trustworthiness environment easily (with by low effort and cost).
  - From the perspective of the infrastructure administrator, the cost of building and operating the infrastructure is also important.
- **…**

Building blocks for Trustworthiness Infrastructure & Root(s) of Trust

Bilateral Trust



Centralized Trust

Decentralized Trust

- Use existing solutions, where possible and combine different technologies
- PKI-based infrastructures (ISO/IEC 9594-8/X.509): eIDAS, Browser Forum, Privately controlled industrial PKIs
- W3C based building blocks: DIDs, VCs
- “Wallets” are realizing secure and trustworthy interactions according to defined Governance

SIEMENS

Some security challenges are…

- **Sufficient security management level in each participating domain**
  - Vulnerability management for all components
  - Timely and efficient incidence management
  - Cooperation between different security domains
- **Interoperable and agile usage of Cryptography: different regions may have different regulations**
- **Long term capability of infrastructure:**
  - Migration to Post Quantum Security will become necessary
  - Additional/new use cases need technical adjustments
- **Robustness against failure of single building blocks**
  - No single point of failure (SPOF)
  - Technical failures
  - Political failures
- **Secure join and leave of participants**
- **Continuous compliance control and enforcements**
- **…**

SIEMENS

EU Regulation for Electronic Identification, Authentication, and Trust Services, eIDAS

eIDAS stands for **E**lectronic **I**dentification, **A**uthentication, and Trust **S**ervices. It is a set of rules by the European Union to make electronic transactions more secure and trustworthy across Europe.

Key Features

- **Better Security**: Stronger measures to protect your data and prevent fraud.
- **Digital Wallets**: New digital wallets for EU citizens to store and use their digital identities safely.
- **Trust Services:** Includes trust services like electronic signatures, seals, timestamps, website authentication certificates, etc.
- **Improved Interoperability**: Ensures that digital solutions work smoothly across different EU countries

Why is it important?

- **Standardization:** Creates a common framework for digital identities and trust services across Europe.
- **Encourages Use:** Makes it easier and safer for people and businesses to use digital identities.
- **Supports Digital Market:** Helps build a secure digital market by ensuring reliable electronic identification and trust services.

Business-to-Business/Consumer Use Cases

- **Electronic Signatures:** Businesses can use secure electronic signatures for contracts, agreements, and transactions, reducing paperwork and speeding up processes
- **Identity Verification:** Companies can verify identities of partners and clients efficiently, ensuring secure and trustworthy interactions
- **Streamlined KYC Processes:** Know Your Customer (KYC) processes can be streamlined using digital identities, making it easier for businesses to comply with regulations

Business/Consumer to Government Use Cases

- **Access to Public Services:** Governments can provide citizens with secure access to public services, like healthcare, education, and social benefits, using digital identities
- **Secure Communication:** Government agencies can communicate securely with businesses and citizens, ensuring confidentiality and integrity of sensitive information
- **Digital Identity Wallets:** Citizens can use digital wallets to interact with government services, making processes like tax filing and license renewals more efficient

SIEMENS

Usage of DIDs and VCs

DID

Decentralized Identifier

A portable, new type of URL-based identifier associated with an entity. It enables verifiable, decentralized digital identity.

VC

Verifiable Credential

Set of tamper-evident claims about a “subject” and metadata that crypto-graphically prove who issued it.

Benefits of leveraging DIDs and VCs

Support realization of secure identities of entities in a flexible & convenient manner	Enable trustworthy secure identities infrastructure	No single point of failure	Support digitalization and automation along the supply chain
Enhance privacy and confidentiality protection	Support track and trace solutions	Help enhance transparency and accountability	…

SIEMENS

Contact

Dr. Wolfgang Peter Klasen
Siemens FT RPD CST SES
Senior Advisor Security

Mobile +49 173 362 362 1

E-mail wolfgang.klasen.ext@siemens.com

SIEMENS