PLATTFORM INDUSTRIE 4.0

Webinar

Shaping a globally secure Industrie 4.0 Ecosystem

Achieving digital Trust and Trustworthiness

23. September 2020

Agenda

- **Introduction of the working group on security of networked systems of the Plattform Industrie 4.0**
  - Industrial security aspects of the German Standardization Roadmap Industrie 4.0
  - Security for Industrial IoT – The Role of Trustworthiness
  - The new Whitepaper *IIoT Value Chain Security – The Role of Trustworthiness*
  - Challenges and building blocks to achieve a trust infrastructure
  - Generic Trust Anchor API – An Enabler for Industrie 4.0 Security
- **Panel discussion (Q&A)**
- **Outlook: International Conference “Shaping a globally secure Industrie 4.0 Ecosystem”**

Introduction of the working groups

Introduction of the working group on security of networked systems of the Plattform Industrie 4.0

Reference Architectures, Standards and Norms
Chair: Kai Garrels, *ABB STOTZ-KONTAKT GmbH*

Technology and Application Scenarios
Chair: Johannes Kalhoff, *Phoenix Contact*

Security of networked systems
Chair: Michael Jochem, *Robert Bosch GmbH*

Legal Framework
Chair: Dr. Hans-Jürgen Schlinkert, *ThyssenKrupp*

Work, Education and Training
Chair: Martin Kamp, IG Metall

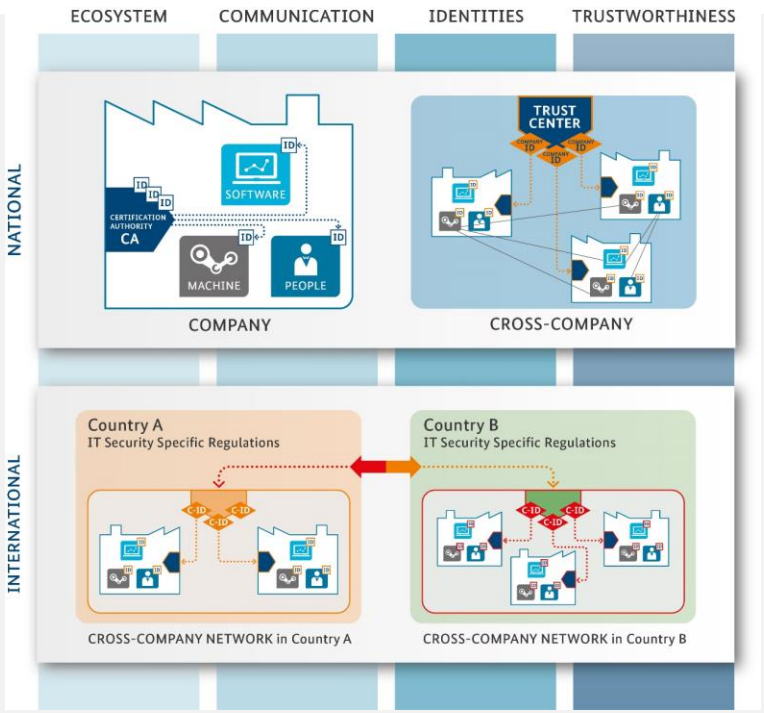
Digital Business Models in Industrie 4.0
Chair: Prof. Dr. Svenja Falk, *accenture*

Webinar Plattform Industrie 4.0
WG3 – Paradigm shift and Opportunities

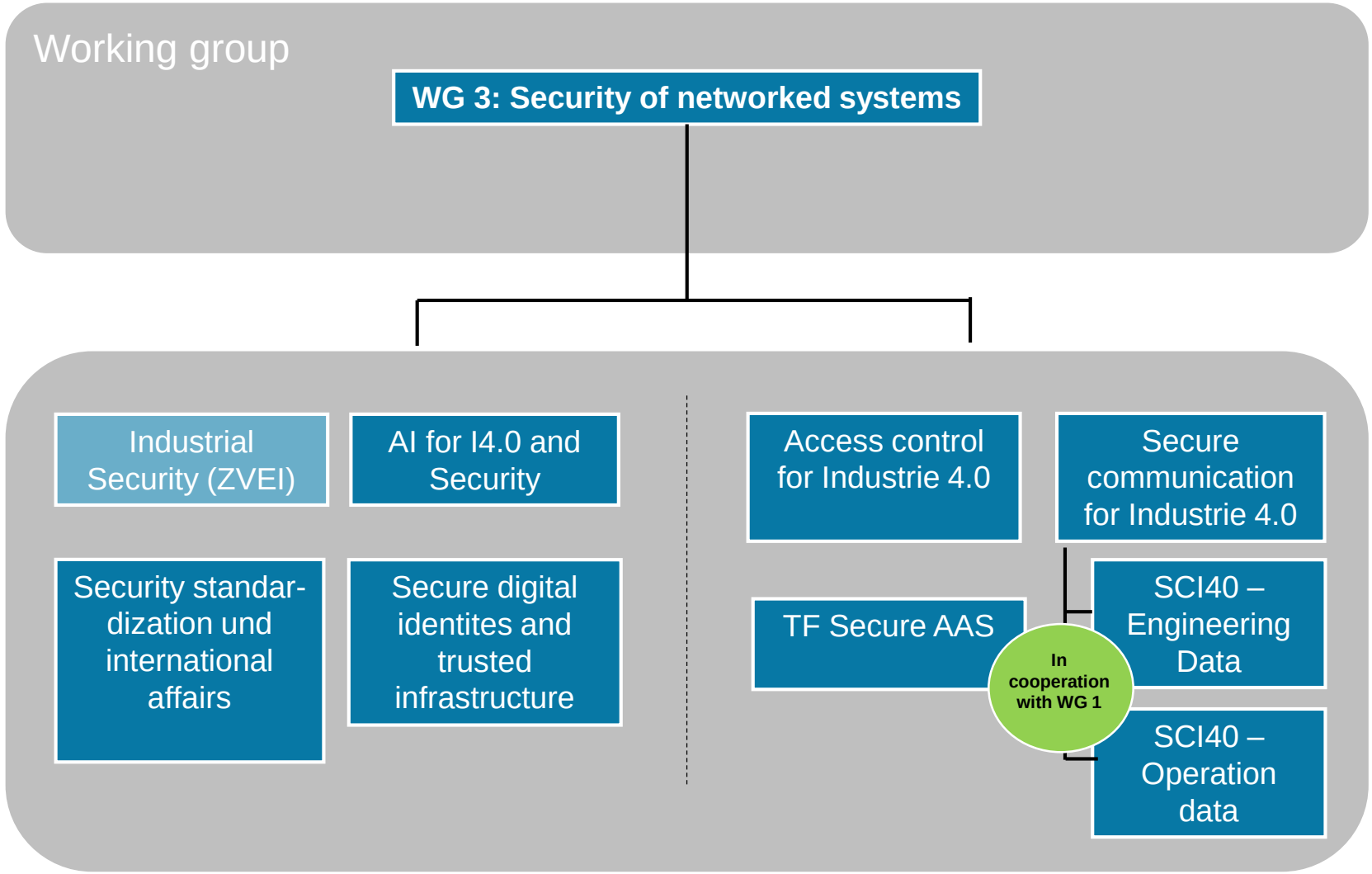
Challenge and mission:

Security as an enabler for Industrie 4.0

- Secure Ecosystems
- Secure Communications
- Secure Identities
- Trustworthiness
- Education and Vocational Training



Webinar Plattform Industrie 4.0
WG3 - Composition and working methods



Webinar Plattform Industrie 4.0

WG3 Security Publications

Handling security risks in industrial applications due to lack of explainability of AI results	Secure Retrieval of CAE Data	Access control for Industrie 4.0 components for application by manufacturers, operators and integrators	Artificial Intelligence (AI) in Security Aspects of Industrie 4.0 Introduction	Conference Report „Securing Global Industrial Value Networks – synchronizing international approaches“	Secure implementation of OPC UA for operators, integrators and manufacturers
Integrity of Data, Systems and Processes as the Core Element of Networking and Digitalization	Secure Communication for Industrie 4.0	Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0	Application scenario in practice: order-controlled production of a customised bicycle handlebar	Industrie 4.0 security in vocational and advanced training: New issues for business organisation and expertise	IT Security in Industrie 4.0

→ All WG3 publications at plattform-i40.de

Plattform Industrie 4.0
Contact Secretatiat

Thank you very much.

Plattform Industrie 4.0
Secretary

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

www.plattform-i40.de

PLATTFORM INDUSTRIE 4.0

Web-Seminar

Shaping a globally secure Industrie 4.0 Ecosystem - Roadmap for Standardizing Industrial Security -

September 23rd, 2020

Dr. Wolfgang Klasen, Siemens AG

Contents

- The Standardization Roadmap Industrie 4.0 – Version 4
- Status of Industrial Security
- Thresholds exist against implementing security
- I4.0 roadmap security recommendations for actions and applications
  - **Security infrastructure for secure inter-domain communication**
  - **Trustworthiness of the value chain / value-added network**
  - **Generic interface for security elements in embedded systems**
  - **5G Security for Industry**

Standardization Roadmap Industrie 4.0 – Version 4

STANDARDIZATION COUNCIL INDUSTRIE 4.0

"Standardization roadmaps on Industrie 4.0 are important blueprints to shape the digital ecosystem."

- **Over 60 Experts from Industry, Academia and Research involved**
- **Standard recommendations to be initiated by German standardisation bodies DKE and DIN**
- **Virtually presented on 16.07.2020 to an international audience of 180 participants from Asia, Europe and Central and South America joining the virtual presentation**
- **Shall be "Door Opener" for SME into standardization of digital manufacturing**
- **Translation work in various languages started**

Chapters

→ **3.2 Industrial Security**

→ **3.3 Privacy**

→ **3.4 Trustworthiness**

https://www.dke.de/de/arbeitsfelder/industry/die-deutsche-normungs-roadmap-industrie-4-0

Status of Industrial Security (1)

- “Industrial Security”, i.e. the **holistic protection** of information technology in production systems, as well as of machines and plants against sabotage, espionage or manipulation
- **“Security-by-Design”** accepted as a general principle
- **OT-Security is different from IT-Security**: Real-time and robustness requirements, life cycles of industrial components, requirements for the continuous availability of industrial plants,…
- Increasing need to protect industrial applications and systems directly (i.e. **security at application level**) rather than relying on network security mechanisms alone.
  In this way, **end-to-end security** or, for example, measures for know-how protection, licensing protection or data protection can be implemented >>> “Zero Trust Security”
- **Support of Artificial Intelligence** creates new security requirements, esp. “Integrity of Applications”, but also offers new opportunities for security solutions

Status of Industrial Security (2)

- **Expectation of trustworthiness along the value creation chain** has become increasingly important, need to increase trustworthiness of value creation networks in Industrie 4.0
- **Current standardization work** for Industrial Security takes place at IEC, ISO, ISO/IEC JTC1, i.e. IEC/TC65, IECEE CMC WG31, ISO TC292 WGs4,8, ISO/IEC JTC1 several groups/sub committees,…
- Technical and organizational standards need to be in **sync with regulatory requirements** (sometimes national/regional specific, various cyber security laws in development, EU Cyber Security Act)

- **IEC 62443 leading security standard for industrial automation**

Thresholds exist against implementing security……

- **Unclear contribution of security investments** to value creation: In certain sensitive areas such as critical infrastructures, however, government regulation will increasingly force the implementation of appropriate measures
- **Fear of increased system complexity** due to security measures that cannot be dealt with in conventional established processes for development and operations
- **Lack of generally applicable and industry-compatible implementation standards** for security with moderate certification efforts for trustworthy solutions
- **Lack of a global trust infrastructure**, which supports compatibility of security implementations regarding trustworthiness

>>> Security Standardization must support to overcome these thresholds <<<

I4.0 roadmap
security recommendations for actions and applications

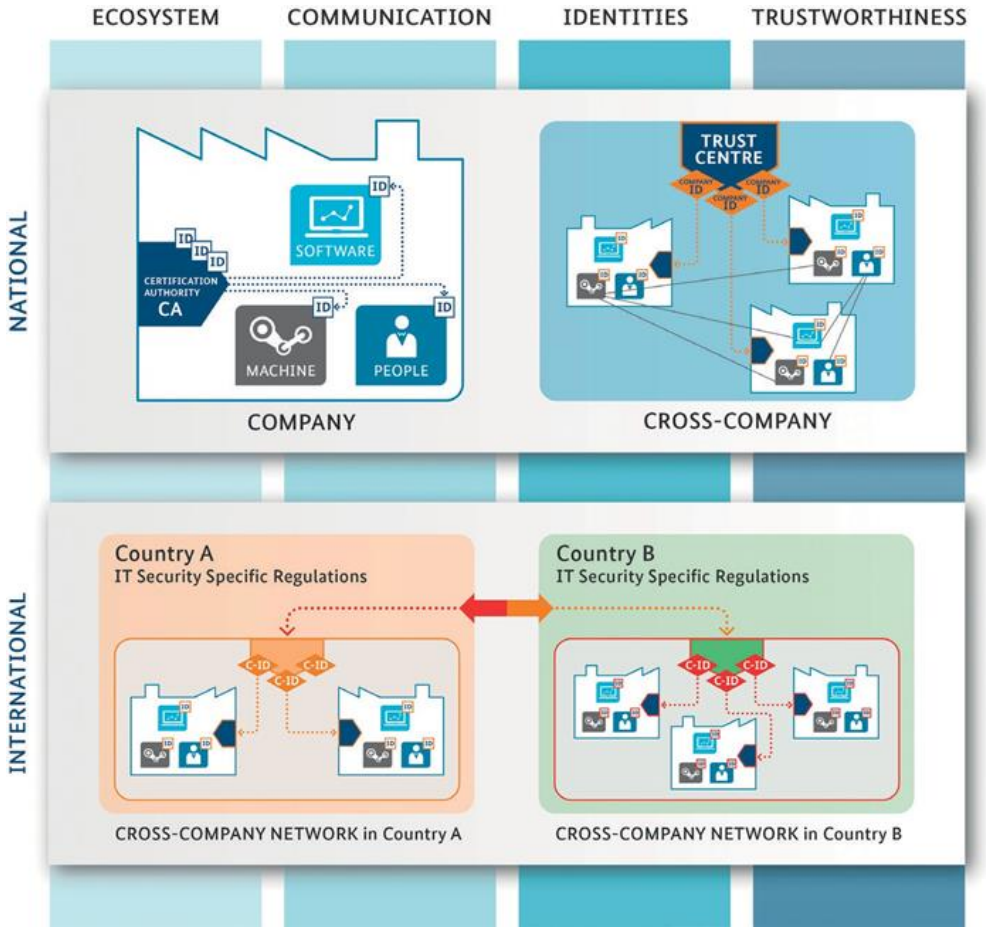
- Security infrastructure for secure inter-domain communication
- Access, roles and authorization mechanisms for Industrie 4.0
- Security for agile systems
- Trustworthiness of the value-added network
- Methods for determining the security characteristics of composite products based on the security characteristics of the contained/interacting components.
- Generic interface for security elements in embedded systems
- 5G Security for Industry
- Industrie 4.0 Security Management Processes
- Security standards for the exchange of type and instance information of administration shells
- Standardized security development process for integrators and operators
- “Security Training“ guide
- Data protection / privacy topics
- Harmonization of the EU Cybersecurity Act and New Legislative Framework

I4.0 roadmap
security recommendations for actions and applications

- Security infrastructure for secure inter-domain communication
- Access, roles and authorization mechanisms for Industrie 4.0
- Security for agile systems
- Trustworthiness of the value-added network
- Methods for determining the security characteristics of composite products based on the security characteristics of the contained/interacting components.
- Generic interface for security elements in embedded systems
- 5G Security for Industry
- Industrie 4.0 Security Management Processes
- Security standards for the exchange of type and instance information of administration shells
- Standardized security development process for integrators and operators
- “Security Training“ guide
- Data protection / privacy topics
- Harmonization of the EU Cybersecurity Act and New Legislative Framework

Security infrastructure for secure inter-domain communication

- Secure communication requires **secure identities** (identifiers and attributes) and **anchors of trust**
- Generating and administering secure identities and securing their trustworthiness needs a **Security Infrastructure**
- Requirements include factors such as **scalability**, **resilience**, **profitability**, **long-term fitness** for purpose, and (“user-related”) **trustworthiness beyond local legal jurisdictions** and independent of local jurisdictions
- **Cross-domain governance structures** to support secure Industrie 4.0 communication must be defined and standardized
- **Close cooperation of all industrial stakeholders needed**
- Use and **integration of national/regional solutions** (such as eIDAS) must be examined with the help of the regulatory authorities and tested in field trials/pilot projects



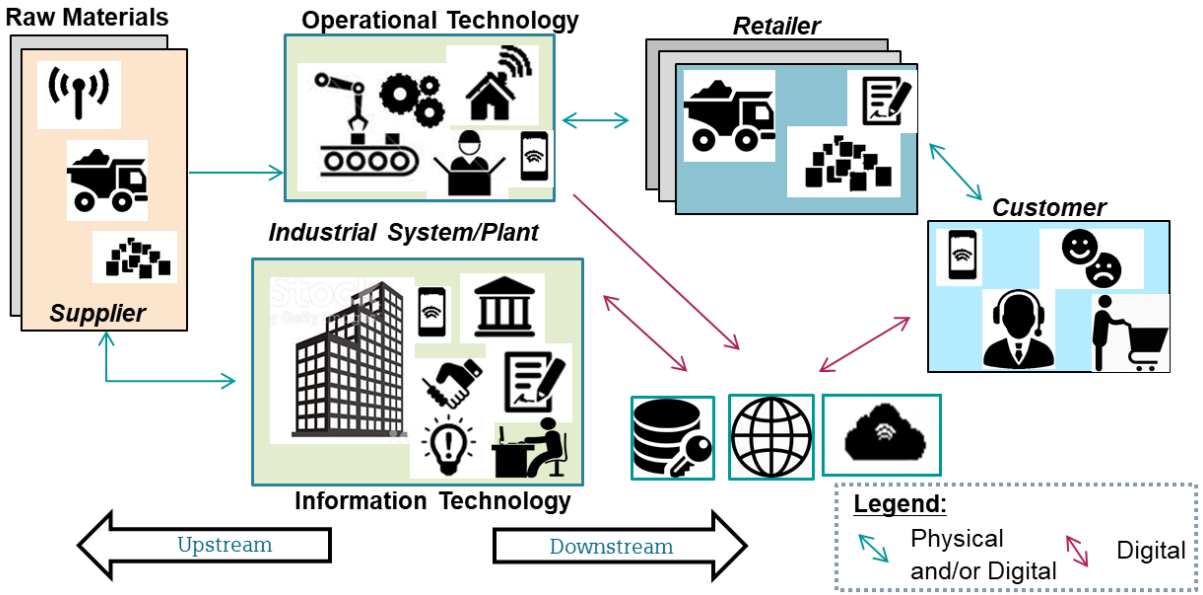
Trustworthiness of the value chain / value-added network

Various (vertical/national) approaches exist (ISO, ISO/IEC JTC1, NIST, VDI2182, …,)

White Paper by German Plattform I4.0 and Robot Revolution Initiative of Japan

Aspects of Supply Chain Security are:

- **Evaluate trustworthiness** of stake holders
- Assurance of implemented **security processes** along the supply chain
- **Integrity protection** and proof of origin, minimize counterfeiting and protect against back-doors
- **Availability and robustness** of supply chain / resilience
- Authorized access to goods and documents, **privacy of intellectual property** of stakeholders

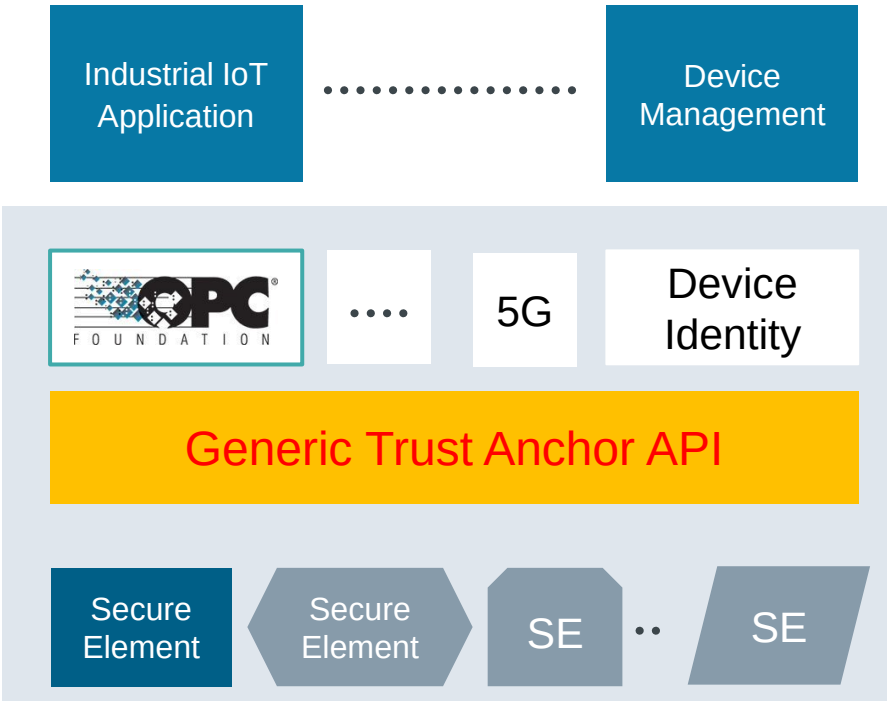


Foster digitalization and automation of measures

Generic interface for security elements in embedded systems

Established as work item within ISO/IEC JTC1 SC41

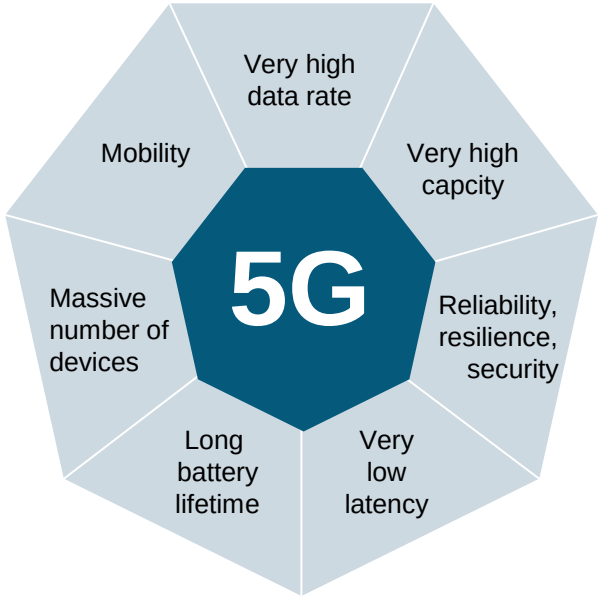
- **Supports flexible integration of different trust anchors**
- **Different physical characteristics**
  (Standalone, SoC, FPGA, integrated, firmware, trusted execution environment, …)
- **Industrial applications**
- **Multi-vendor**
- **Long-term evolution**



- **Supporting security for various Industrial IoT scenarios**
- **Addressing multiple security requirement profiles**
- **Enabling flexible and scalable integration of different trust anchor types**

Security for Industrial 5G

- 5G technology is seen as one important building block for telecommunication and also for **applications in the context of digitalization of the industry**
- It will cope with industry specific needs, like **low latency to support TSN** or **high reliability to ensure dedicated QoS**
- 3GPP is currently working on further 5G functionalities. The evolution of Stand-alone Non-Public Networks (SNPN) allows the **industry to use 5G technology locally as access technology for their networks**
- Security challenges to be addressed in 5G applications comprise beyond others:
  - **Allow existing security mechanisms of industrial devices (e.g., for provisioning or communication) via 5G user plane for the support of end-to-end security**
  - **Using credentials for 5G network access, not owned by the mobile network operator**. Allow further usage of credentials, which are already in place, e.g. based on current industrial WLAN application



Plattform Industrie 4.0 – Industrial Security

Thank you very much.

Dr. Wolfgang Klasen

wolfgang.klasen@siemens.com

Tel.: +49 173 362 362 1

Security for Industrial IoT
- The Role of Trustworthiness -

23rd Sept. 2020

Robot Revolution & Industrial IoT Initiative(RRI)
Takeshi Yoneda(Mitsubishi Electric Corporation)

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

-The goal of our activity is:
*To identify new security requirements for Industrie 4.0.
*To incorporate trustworthiness in coming interconnected economies.

-PI4.0(Germany) and RRI(Japan) announced three common position papers," Facilitating International Cooperation for Secure Industrial Internet of Things/ Industrie4.0"
(16th March 2017, 16th May 2018, 3rd April, 2019)

-PI4.0 and RRI had discussed the role of trustiness intensively during FY19 and have provided the whitepaper "IIOT Value Chain Security – The role of Trustworthiness."

-Today what PI4.0 and RRI had discussed in FY19 is introduced.

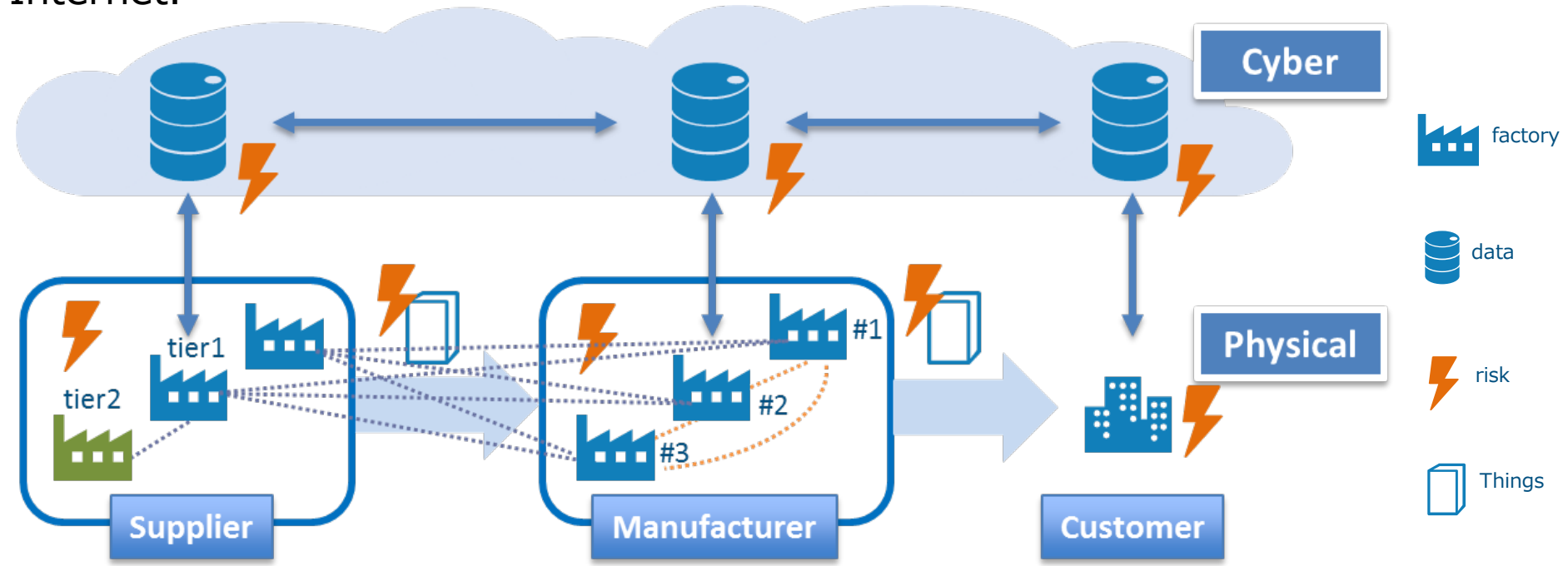
PI4.0: Plattform Industrie4.0, RRI: Robot Revolution & Industrial IoT Initiative

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

Global Value Chain

Information security has become an essential aspect of trustworthiness because manufacturers and suppliers are becoming interdependent as parties in the global value chain accelerated through the Internet.

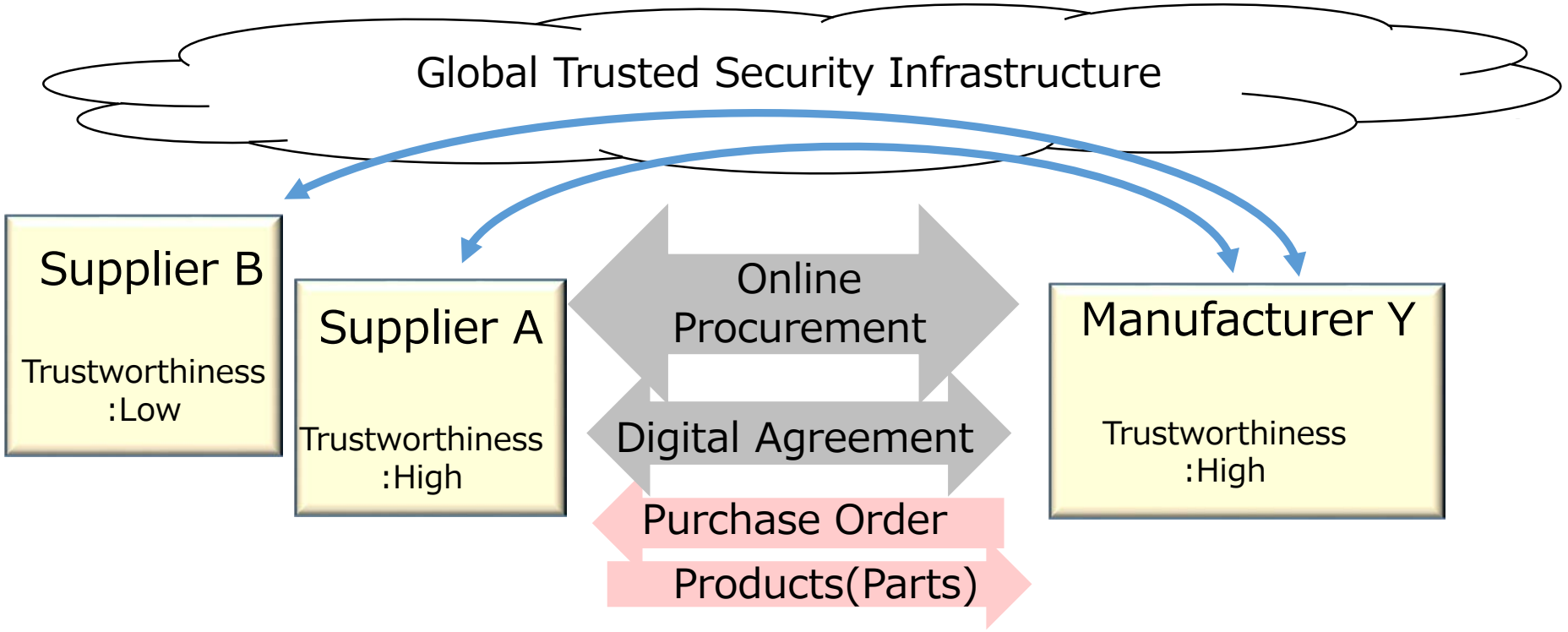
1)Needs to develop products that satisfy rapidly changing customer needs.
2)Needs to collaborate with suppliers whose products are required to develop the products.
3)Needs to find appropriate suppliers from all over the world timely though the Internet.



2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

A use case for understanding the role of trustworthiness

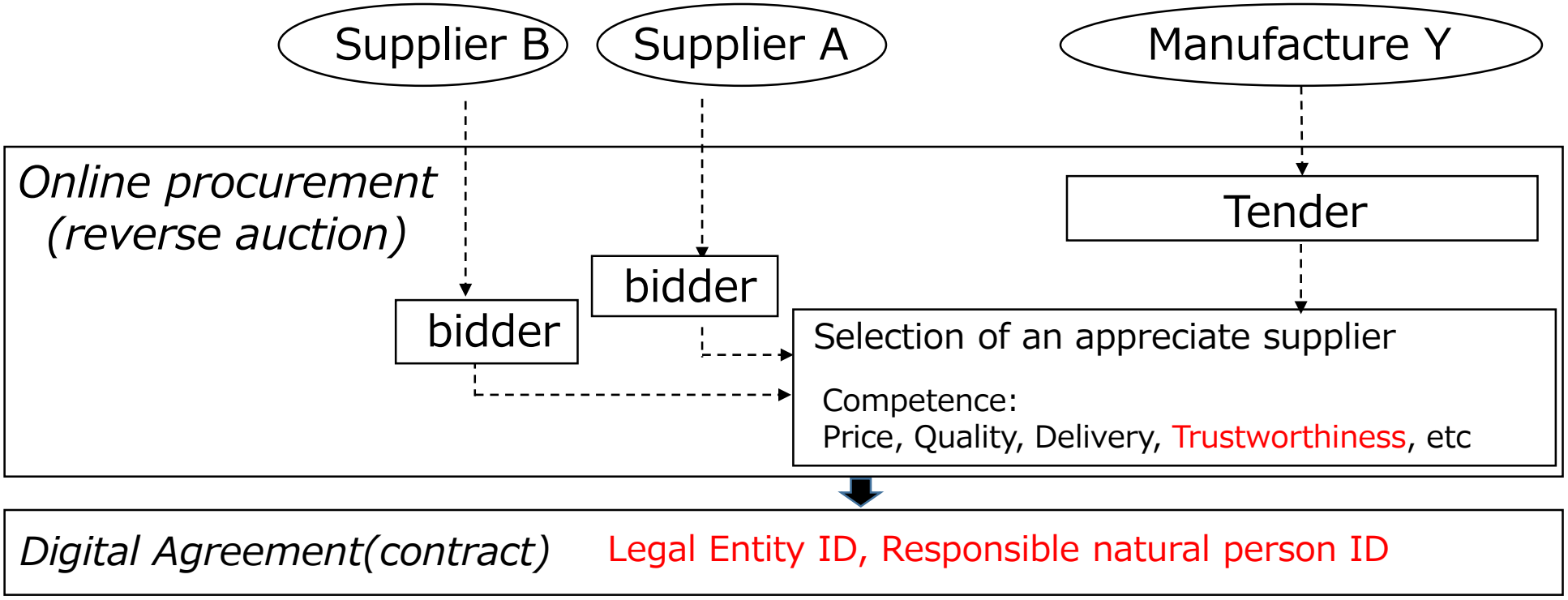
-To find an appropriate supplier, what level of trustworthiness the supplier has is crucial because the supplier would share critical information and high availability among other parties in the value chain.
-So by using online procurement as a use case, we had discussed "what is trustworthiness" ,"how to determine the party's trustworthiness" and "how parties in the value chain have the same trustworthiness level" .



2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

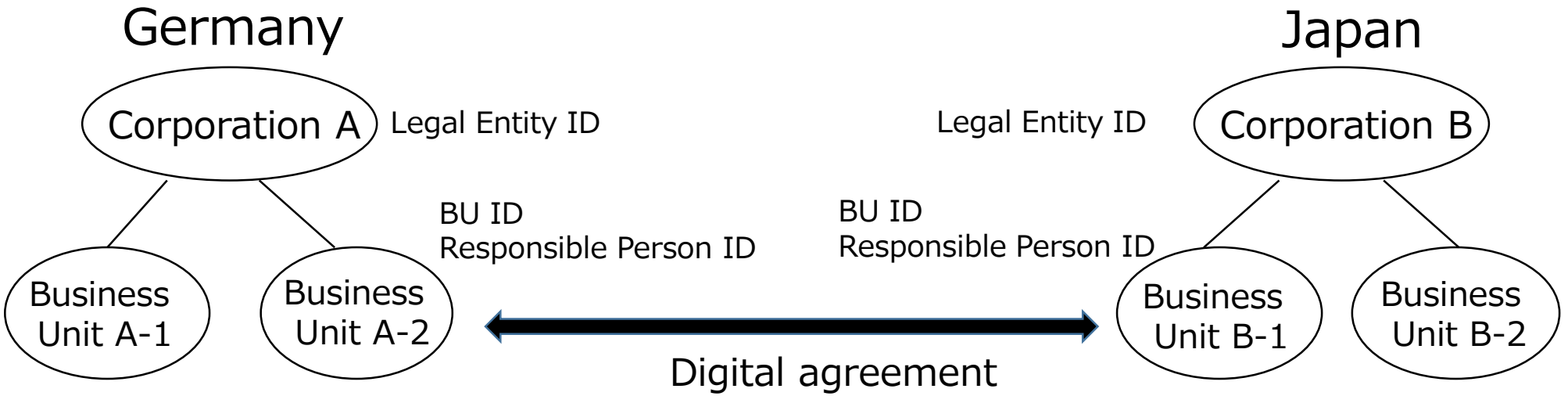
Online Procurement and Digital Agreement

- In **Online procurement** the following security aspects of the parties are the matter.
  *authenticity of parties
  *security level implemented in their organizations
  *security level of their products
- In **Digital agreement** the following security aspects are the matter.
  *authenticity of the organization as a legal entity represented by a legal entity ID
  *authenticity of the signer as a responsible natural person represented by a natural person ID



2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

ID systems for online procurement



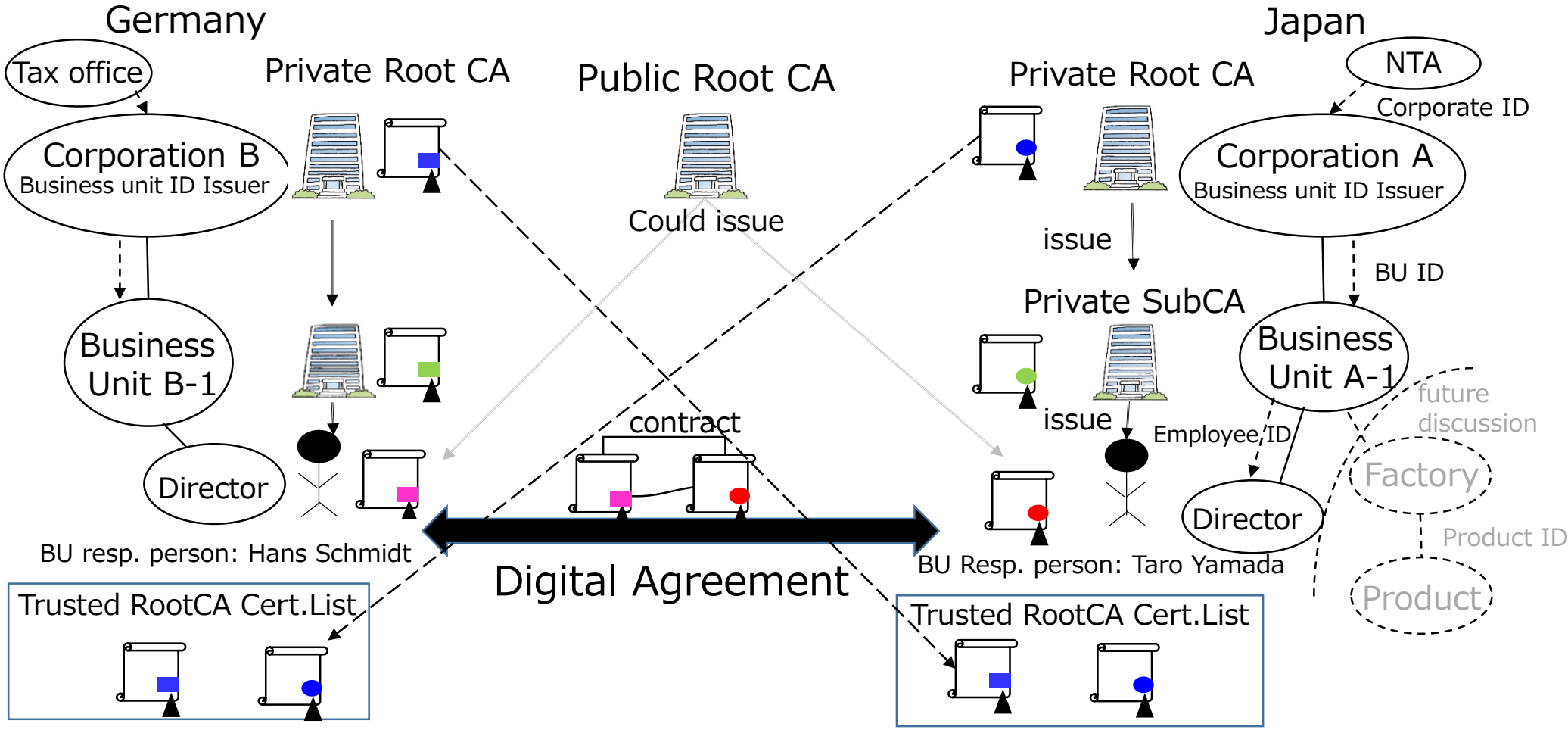
Discussion items	Germany	Japan	Technical Issus
Legal Entity ID and its provider	VATIN (USt-IdNr) The tax office	Corporate No. NTA	—
Natural person ID/BU ID and their provider	eIDAS	Employee ID Each Corp.	BU ID code system is not yet determined.
Digital Certificates for natural persons	eSignature, eIDAS	Each Corp.	Cross certification is needed.
Digital Certificates for legal entities	eSEAL, eIDAS	Each Corp.	Cross certification is needed.

NTA: National Tax Administration Agency

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

A Certificate Authority(CA) structure for online procurement

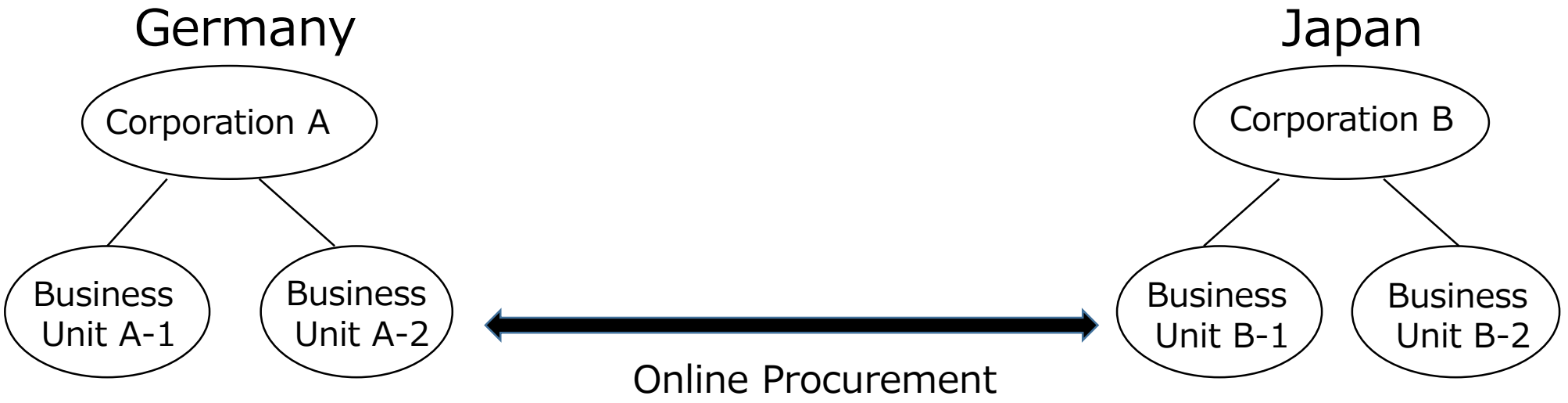
-Digital signatures of responsible persons are used for digital agreement.
-A CA structure for issuing digital certificates to responsible persons is needed for each side.
-A mechanism of trusting each other's Root CA is needed.



NTA: National Tax Administration Agency

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

Security exchanged though online procurement

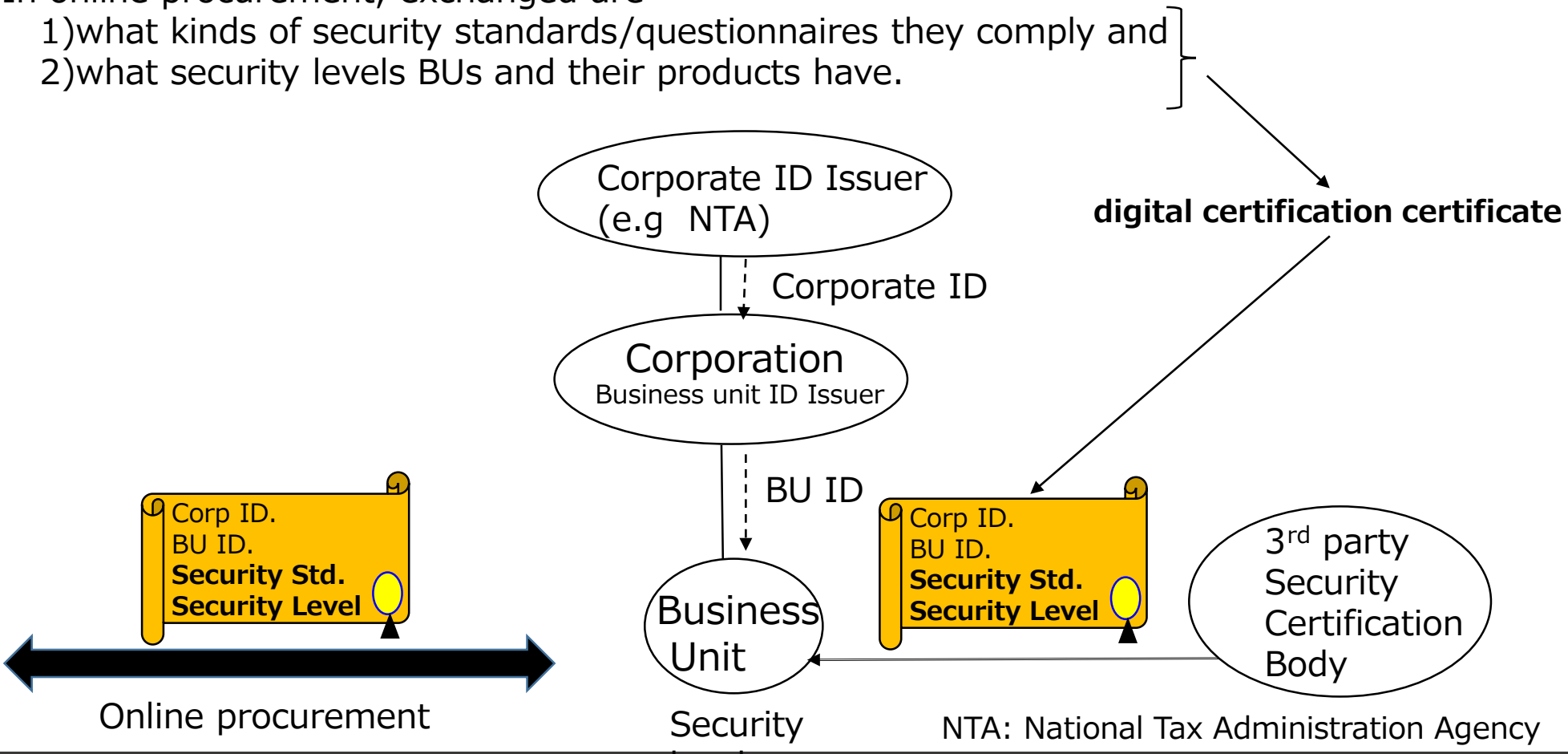


Discussion items	Germany	Japan	Technical Issus
Standards used for security(trustworthiness) assurance	ISO 27001,IEC 62443,etc		Machine readable certification certificate is not yet established
Security(Trustworthiness) level agreement	-	-	There is no agreement protocol

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

Security exchanged though online procurement

1.Corporate ID Issuers assure the existence of corporations.
2.Each corporation has responsible for assigning a BU ID to a BU.
3.Each corporation has a CA which issues digital certificates to employees with IDs and names.
4.Those certificates are used for digital signatures(by natural persons) on a digital agreement.
5.In online procurement, exchanged are
  1)what kinds of security standards/questionnaires they comply and
  2)what security levels BUs and their products have.



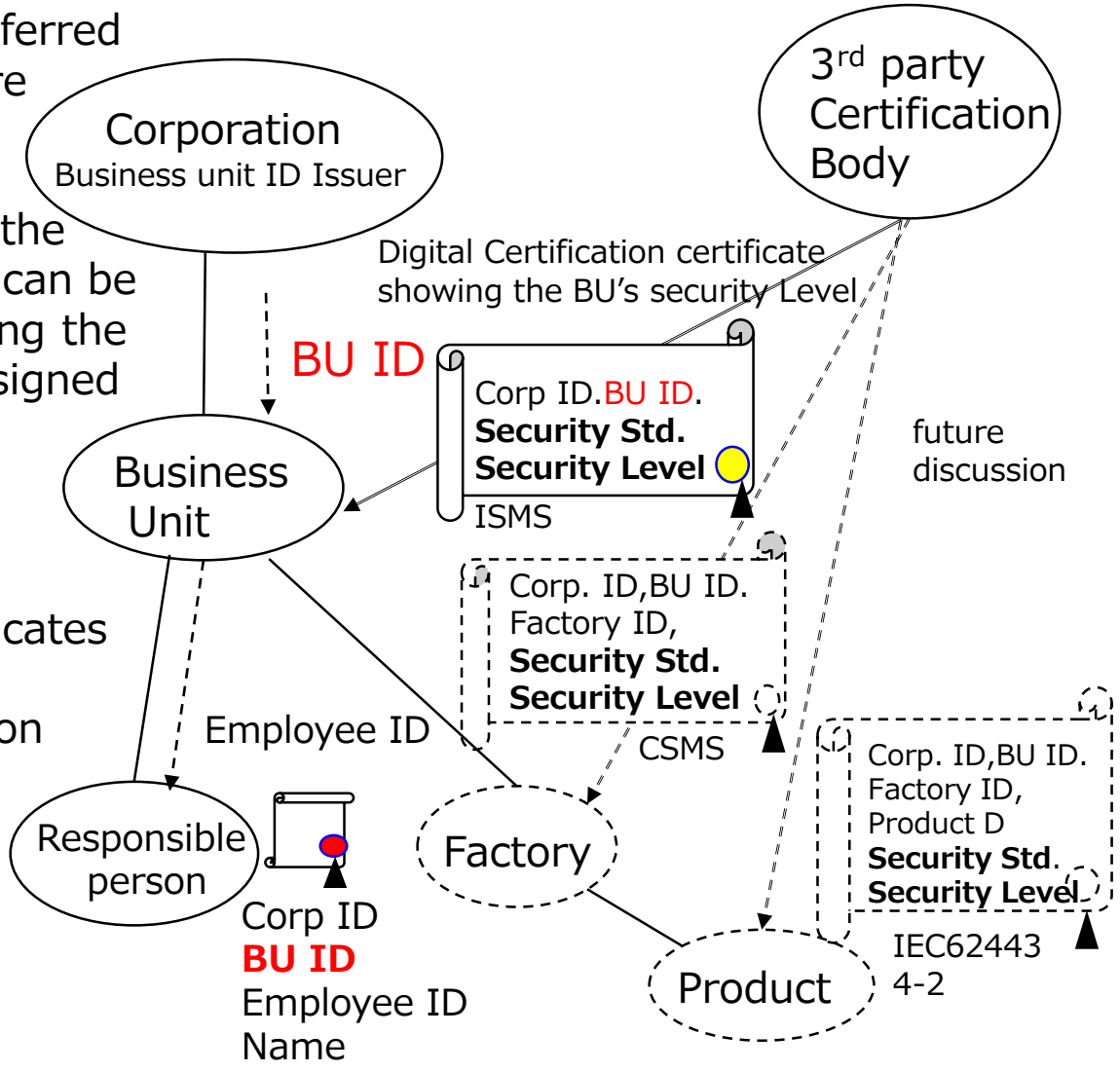
2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

IDs and digital certification certificates

1. A Corp.ID should be globally unique and trusted, because they are used and referred to in various economic activities, where corporation identification is critical.

2. A BU ID should be globally unique for the same reason. Such global uniqueness can be achieved, for example, by concatenating the unique global Corp.ID and a BU ID assigned uniquely within the corporation.

3. BU IDs would be used in at least two different applications.
   1) BU IDs included in the digital certificates used for digital agreements.
   2) BU IDs included in digital certification certificates.

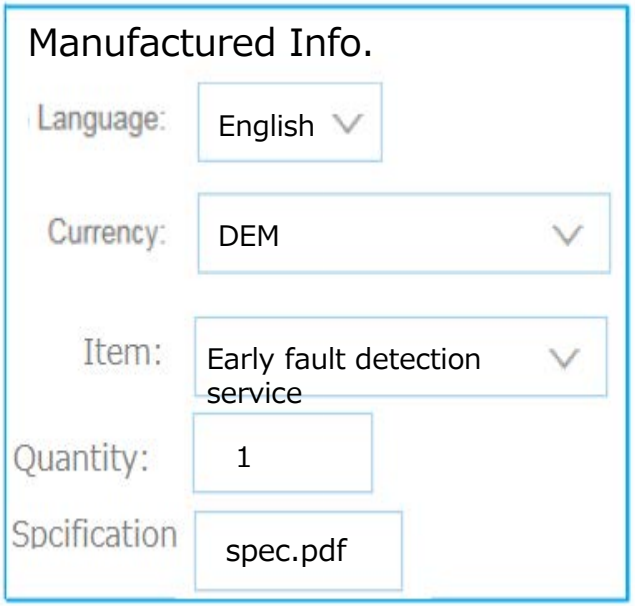


2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

A Sample GUI for Online Procurement

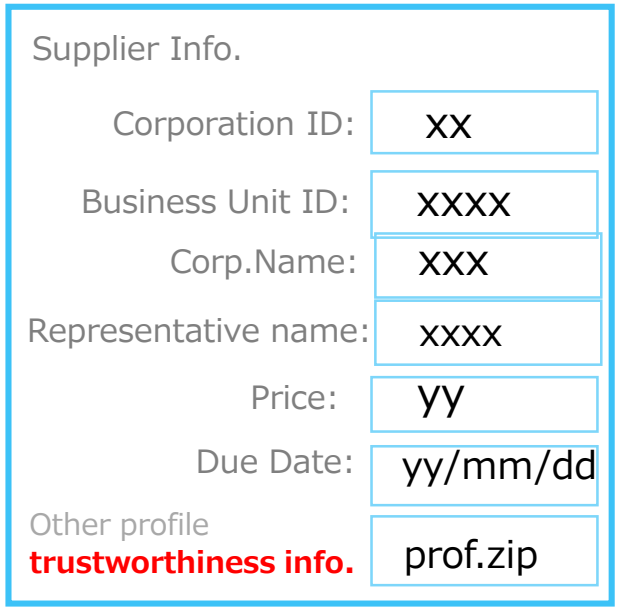
After assigning IDs and Digital certificates to corporations/BUs/responsible persons, manufactures and suppliers can participate in online procurement.

Request for work



Manufacture(tender) side

Submission to bid



Supplier(bidder) side

Supplier selection

Manufacture(tender) side

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

A sample security requirements for online procurement

ISO 27001: Protection of development environment in supplier
IEC 62443: Implementing security of product in suppliers' development process

Organization Trustworthiness: ISO 27001 + Supply chain security

1. Information Security Policy	**(ISO 27001 A.5)**
2. Organization of Information Security	**(ISO 27001 A.6)**
3. Human Resources Security	**(ISO 27001 A.7)**
4. Asset management	**(ISO 27001 A.8)**
5. Access Control	**(ISO 27001 A.9)**
6. Cryptography	**(ISO 27001 A.10)**
7. Physical and Environmental Security	**(ISO 27001 A.11)**
8. Operations Security	**(ISO 27001 A.12)**
9. Communications Security	**(ISO 27001 A.13)**
10. System acquisition, development and maintenance	**(ISO 27001 A.14)**
11. Supplier Relationships	**(ISO 27001 A.15)**
12. Information Security Incident Management	**(ISO 27001 A.16)**
13. Information Security Aspects of Business Continuity Management	**(ISO 27001 A.17)**
14. Compliance	**(ISO 27001 A.18)**
15. Supply chain security	**(NIST CSF and CPSF)**

- Clarify, manage and continuously improve the role of the organizations in the supply chain
- Specify how to manage the components produced by the organization's supply chain

System/Component Trustworthiness: IEC 62443 3-3,4-1,4-2

- Integrity in Product Lifecycle
- Document/Secure Configuration, Testing for Security Vulnerabilities, Prevention of Undocumented Functions, Back Doors and Easter Eggs, Provide additional documents and so on (T.B.D).

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

Security levels used for online procurement

Types of security levels are categorized the following:
*Level of Maturity
*Level of Security: (A) Organization (B) System/Component (Technical)

Document	Type of security levels		
	Maturity	Security	
		Organization	System/Component (Technical)
NIST CSF	Framework Implementation Tier (4 levels)		–
NIST SP800-82 (FISMA)	–	ICS Impact level (3 levels)	
METI CPSF	–	Measure Requirement (3 levels)	
ISA/IEC 62443	ML (5 levels)	ISO/IEC directive verbal form(2 levels)	SL (4 levels)
VDA-ISA	Maturity Level (6 levels)	Required level (5 expressions)	
ISO/IEC 15408	–	CC EAL(7 levels)	
ISACA COBiTS	Process Capability Level(6 levels)		

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

Next Step

- RRI is developing a security requirements questionnaire for suppliers in FY2020 based on Cyber/Physical Security Framework issued by METI, Japan.

- We expect the questionnaire would be standardized and the answer for the questionnaire would be evaluated and digitally signed by 3rd party security certification bodies.

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

Thank you!

2020 Copyright Robot Revolution & Industrial IoT Initiative, All Rights Reserved.

PLATTFORM INDUSTRIE 4.0

Web-Seminar

Shaping a globally secure Industrie 4.0 Ecosystem

IIoT Value Chain Security – The Role of Trustworthiness

Whitepaper 2020

23. September 2020

Agenda

- **Introduction of the working group on security of networked systems of the Plattform Industrie 4.0**
  - Industrial security aspects of the German Standardization Roadmap Industrie 4.0
  - Security for Industrial IoT – The Role of Trustworthiness
  - **The new Whitepaper *IIoT Value Chain Security - The Role of Trustworthiness***
  - Challenges and building blocks to achieve a trust infrastructure
  - Generic Trust Anchor - a new API standard to create a root of trust
- **Panel discussion (Q&A)**
- **Outlook: International Conference “Shaping a globally secure Industrie 4.0 Ecosystem”**

Introduction

Plattform Industrie 4.0, Germany and Robot Revolution Initiative, Japan had been collaborating since 2017 on topics concerning security of Industrial IoT (IIoT) and Industry 4.0 use cases.

This whitepaper is the result of collaboration activities in 2019.

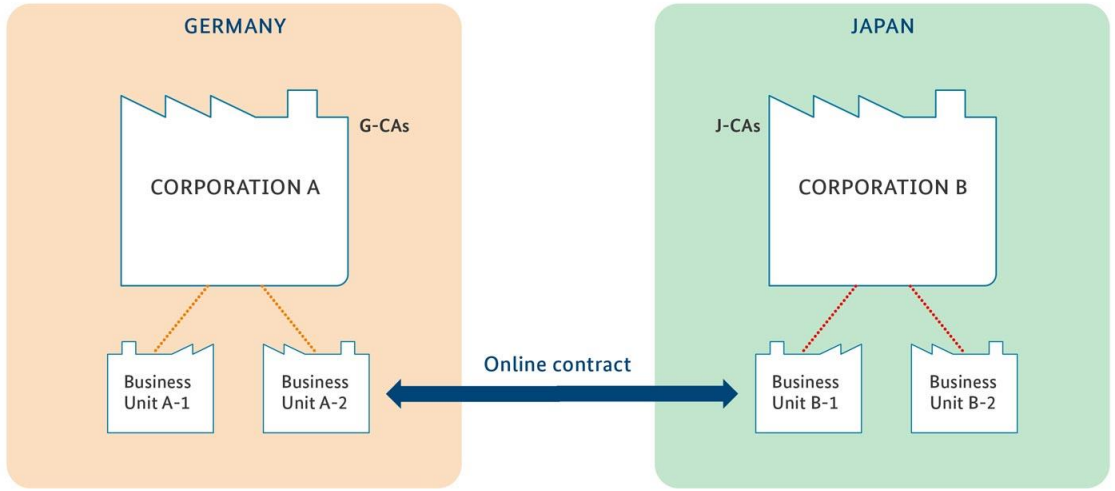
The overall aim of the whitepaper is to provide considerations and possibilities for supporting ad-hoc trustworthy relationships between companies, regardless of their business histories or their geographical locations.

Motivation

Consider a manufacturer in Germany that wants to establish a new business with a potential supplier based in Japan. They do not have a business history, i.e. they have not worked together on any joint projects in the past.

At this stage, they require support for quick and trustworthy collaboration.

The aim of this activity is to provide support to companies so that they can find trustworthy collaboration partners easily and can establish trustworthy relationships on-the-go.



Main Considerations

Key Issues:

- How to define trustworthiness in the context of supply/value chain security?
- Which criteria can be used to determine the trustworthiness of a company and its products?
- What kind of mechanisms are needed for assuring trustworthiness, with respect to supply/value chain security, globally?

Trustworthiness

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

“For supply/ value chain security and risk management, 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.

For the selected use case, the following trustworthiness criteria have been deduced:

- *Authenticity as a property of an organization’s trustworthiness*
- *Authenticity as a property of products’ trustworthiness*
- *Security as a property of an organization’s trustworthiness*
- *Security as a property of products’ trustworthiness*

Ingredients for Trustworthiness Negotiation

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, such as barcodes, etc.

Certificates

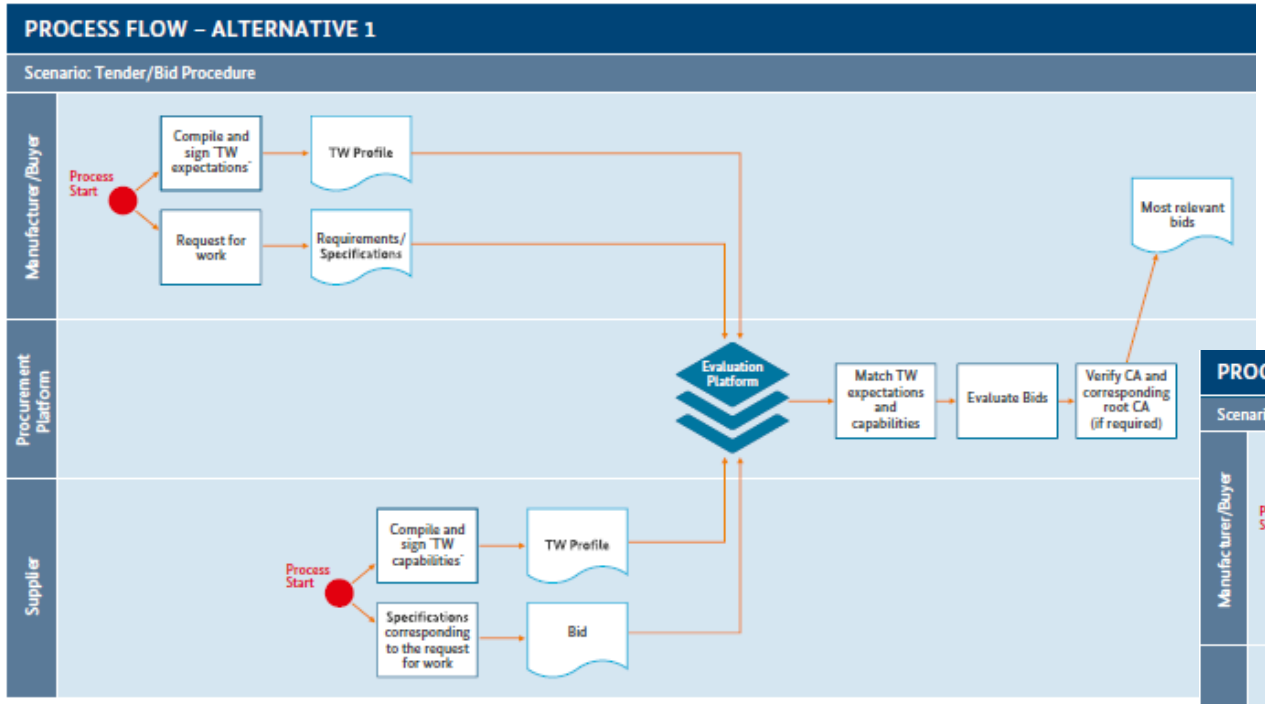
- Identity Authenticating Certificates such as X.509 PKI, eIDAS, etc.
- Security Certification Certificates, such as ISO 2700x certificates, IEC 62443 certificates, etc.

Standards and Frameworks

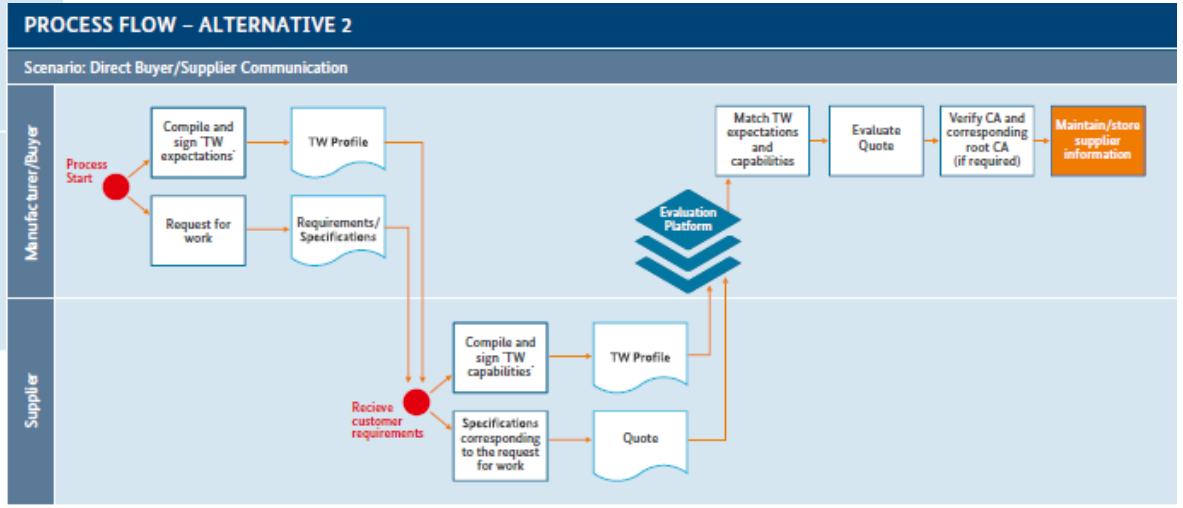
- ETSI 319 412 series
- ISO/IEC 62443-x-x
- METI CPSF
- NIST CSF
- …

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.

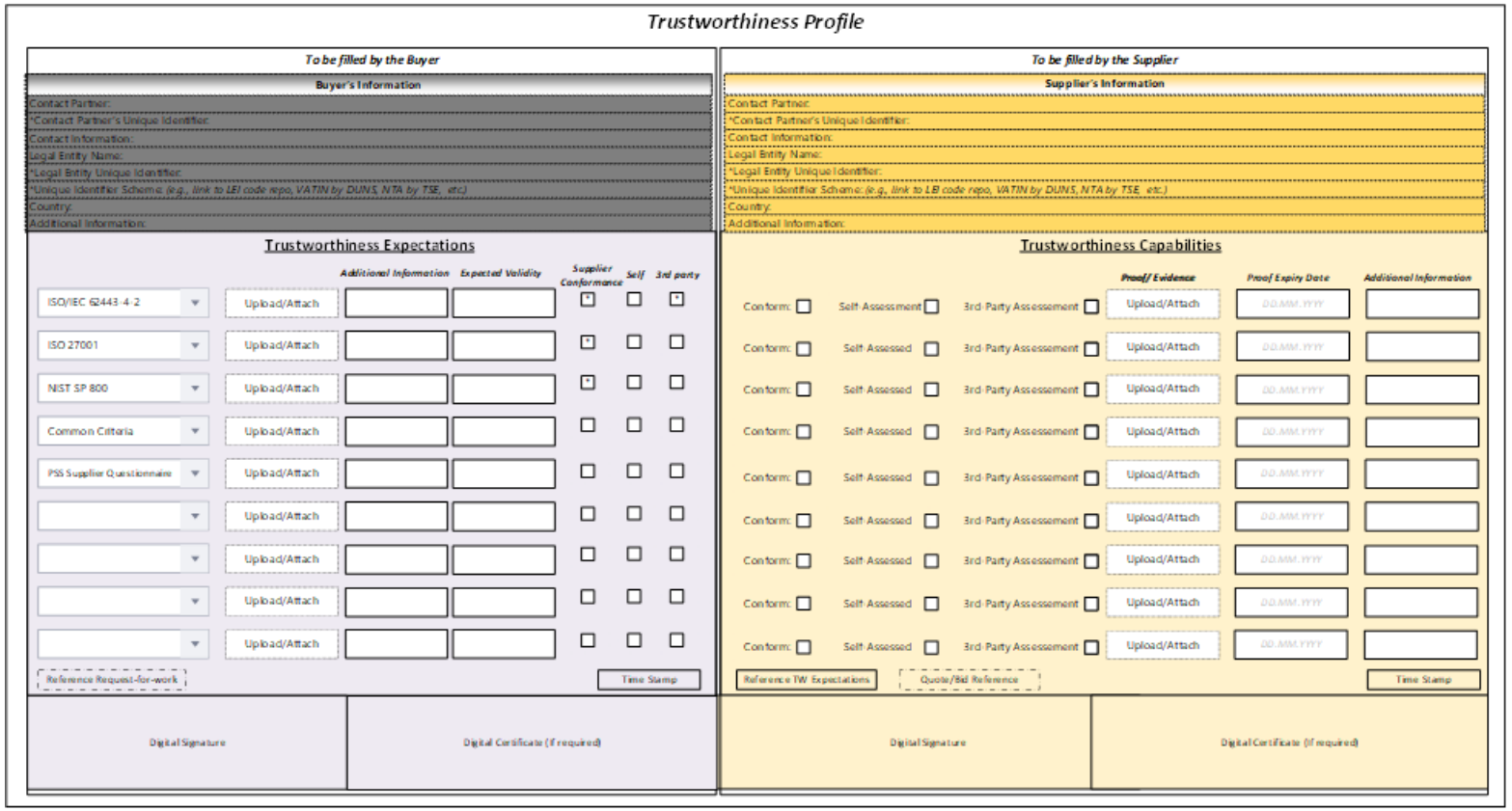


Trustworthiness Profile

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



Next Steps

- TECEP Demonstrator
- Machine-to-machine secure communication aspects
- Automated procedures for the development and evaluation of the Trustworthiness Profile
- Digitalization of machine-readable Security Certification Certificates

Thank you very much.

Aliza Maftun

aliza.maftun@siemens.com

Tel.: +49 (152) 03315778

PLATTFORM INDUSTRIE 4.0

Web-Seminar

Shaping a globally secure Industrie 4.0 Ecosystem

Achieving digital Trust and Trustworthiness

23. September 2020

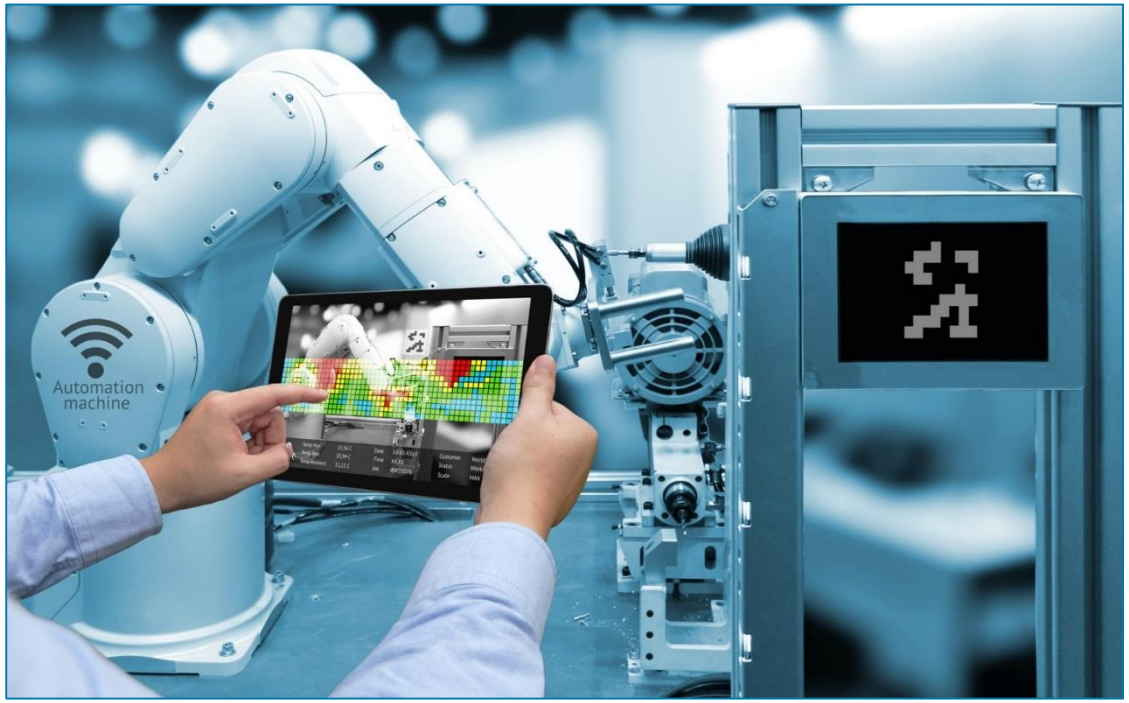
Agenda

- Introduction of the working group on security of networked systems of the Plattform Industrie 4.0
  - Industrial security aspects of the German Standardization Roadmap Industrie 4.0
  - Security for Industrial IoT – The Role of Trustworthiness
  - The new Whitepaper *IIoT Value Chain Security - The Role of Trustworthiness*
  - **Challenges and building blocks to achieve a trust infrastructure**
  - Generic Trust Anchor API – An Enabler for Industrie 4.0 Security
- Panel discussion (Q&A)
- Outlook: International Conference “Shaping a globally secure Industrie 4.0 Ecosystem”

Baseline situation

- More and more data will be collected, analysed and exchanged (Sensor-Data, Big Data, AI-Data)

- This exchange of data happens
  - multilateral,
  - increasingly automated and
  - across company boundaries



Source: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Introduction trust infrastructure

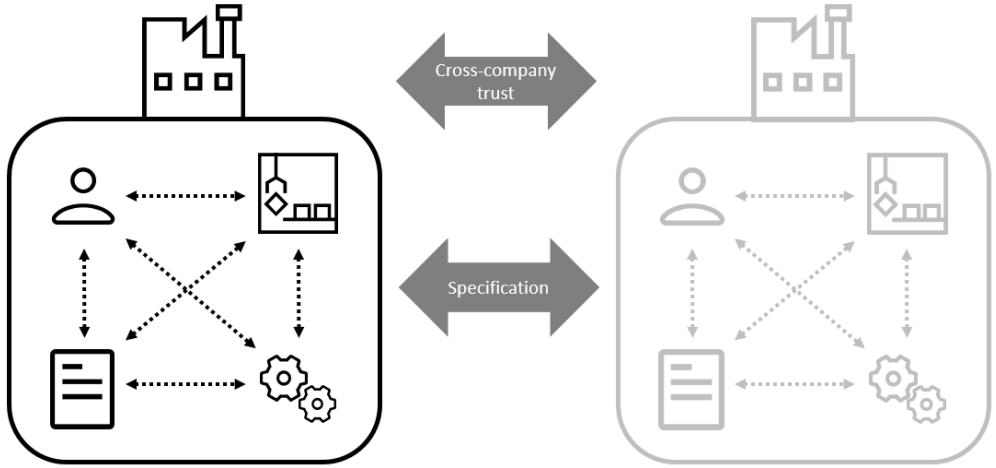
- Entities should be able to interact, in a trustworthy manner, across companies (trustworthy value chain)
- Secure communication, access control and Secure Digital Identities (SDI) are essential to achieve mutual trust
- A Trust infrastructure enables I4.0-entities to exchange proofs of trust

A **'Secure Digital Identity'** is a unique identity with further security attributes to achieve a reliable and trustworthy authentication of an entity.

Source: Sichere Identitäten (Plattform Industrie 4.0, 2016)

Challenges to achieve a trust infrastructure

- Organizational and technical measures to achieve trustworthiness need to be interoperable
- A Common understanding of these measures is essential
- Procedures and processes for creation, verification and validation of trustworthiness should be increasingly automated



Excursus in definition of trustworthiness regarding I4.0-value chains

"For supply/ value chain security and risk management, the term **'Trustworthiness'** corresponds to the supplier's ability to meet the expectations of the potential contract partner in a verifiable way".

Source: WhitePaper_I4.0CrossBorderCommunication_German_Japan

Requirements for a trust infrastructure

- Security requirements of integrity, confidentiality and availability need to be realized
- Processes and standards are required to link different CAs[1]
- Requirements to achieve trustworthiness need to be appropriate and interoperable
- National and transnational requirements need to be accomplished e.g. regulatory requirements

Source: Bundesamt für Sicherheit in der Informationstechnik (BSI)

1) CA = Certificate Authority

Building Blocks for a trust infrastructure

Public Key Infrastructures

Exchange of cryptographic keys

International unique identifiers

eIDAS-regulation (EU-regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014)

Identity Authenticating Certificates (IACs)[2]

Security Certification Certificates (SCCs)[3]

2) IAC = certificate used to to authenticate a public key corresponding to asymmetric cryptography (Source: WhitePaper_I4.0CrossBorderCommunication_German_Japan)
3) SCC = certificate that serves as a proof of certification of a product's or a process's quality (Source: WhitePaper_I4.0CrossBorderCommunication_German_Japan)

eIDAS-regulation No 910/2014 of 23 July 2014

Electronic **I**dentification, **A**uthenication and trust **S**ervices **„eIDAS“:**

- Chapter II: electronic identification means
- Chapter III: Trust Services
- Deployment of qualified electronic seals and qualified electronic signatures
- Trusted Lists (eIDAS article 22): notified, published and updated by EU Commission
- Key principal: mutual recognition of different existing procedures in the European Economic Area (EEA), with 510+ million citizens and 28 Member States; NOT a technical harmonization!

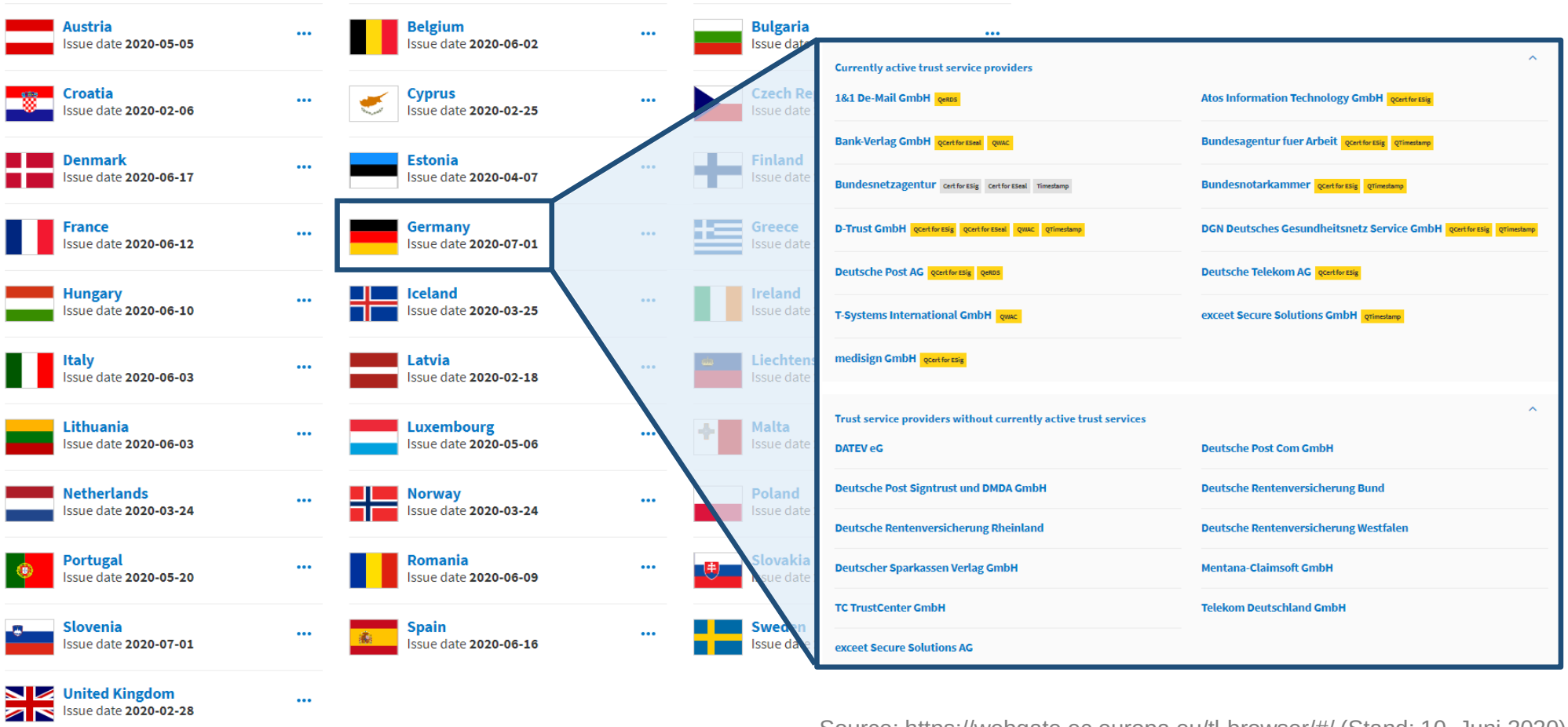
→ Possible approach for I4.0: mutual cross-company recognition of SDIs

eIDAS is based on four pillars

Identity Provider (IDP)	Service Provider (SP)	Attribute Provider (AP)	National eIDAS node operator
• IDP provides trust service • also named Trusted List Browser	• SP provides online service • e.g. I4.0 industrie parties, incl. outsourcing parties	• AP provides additional information • e.g. along the I4.0 ABAC approach	• Nodes used as national gateway to other countries[2] • e.g. for I4.0 cross-company value chains

2) To create interoperability on eIDAS nodes, a technical specification is published/available form EC, DG CNECT.

Trusted List Browser regarding member states



Source: https://webgate.ec.europa.eu/tl-browser/#/ (Stand: 10. Juni 2020)

Advantages of eIDAS

- Definition and qualification of trust services
  - Creation, verification and validation of seals, signatures, timestamps and website certificates
  - Preservation services for signatures
  - Electronic registered delivery services
- Trust services can be automatically checked against trusted lists
- Quality of trust services can be transparently identified
- Interoperability: Many standards have been developed the recent years by ETSI regarding requirements and certification for different stakeholders
- Trusted lists support mutual recognition among all member states

Achieving digital Trust and Trustworthiness

Q&A

Plattform Industrie 4.0
Contact Secretatiat

Thank you very much.

Plattform Industrie 4.0
Secretariat

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

www.plattform-i40.de

PLATTFORM INDUSTRIE 4.0

Web-Seminar

Generic Trust Anchor API

An Enabler for Industrie 4.0 Security

Björn A. Flubacher

Federal Office for Information Security (BSI)

23. September 2020

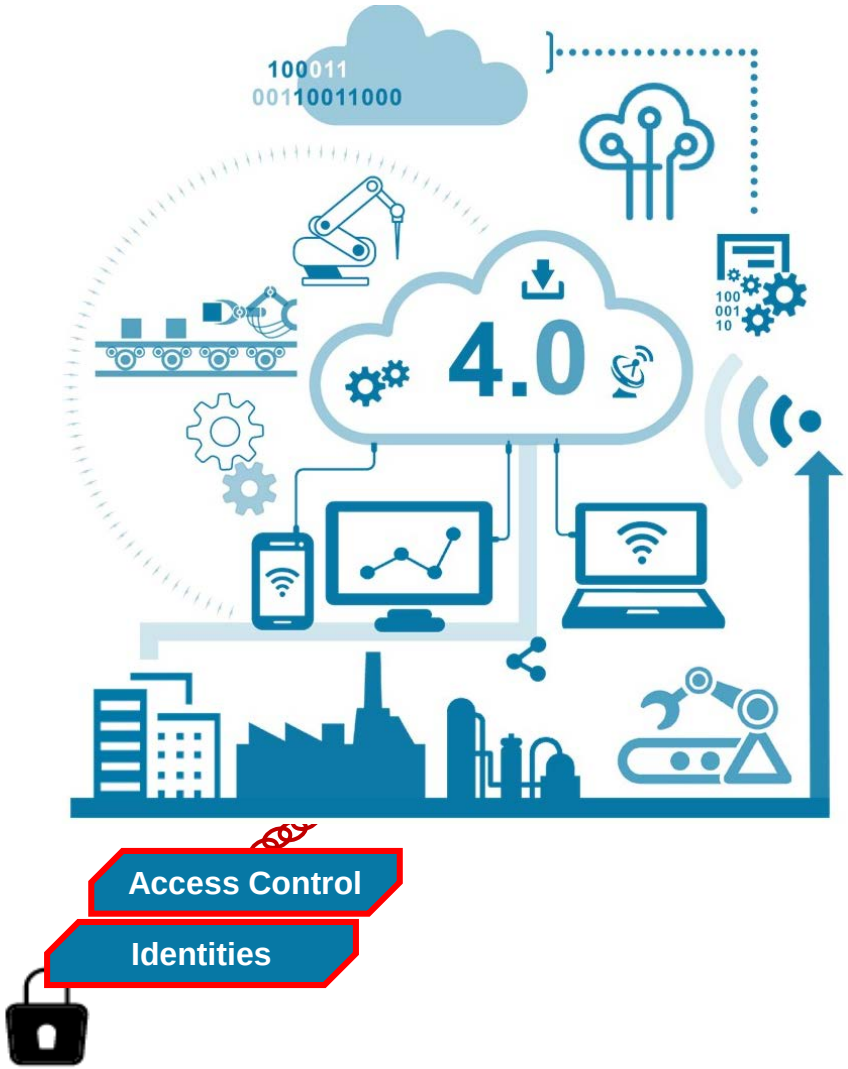
Industrie 4.0 requires Security

Security Architectures rely on Trust Anchors

- Root Certificate
- Secure Element

Purpose of a Secure Element (SE):

- Protect data from unauthorized manipulation or disclosure, e.g. Identities (actually Private Keys)
- Provide evidence/trust that crytographic functions execute as expected



SE : Trust Anchor

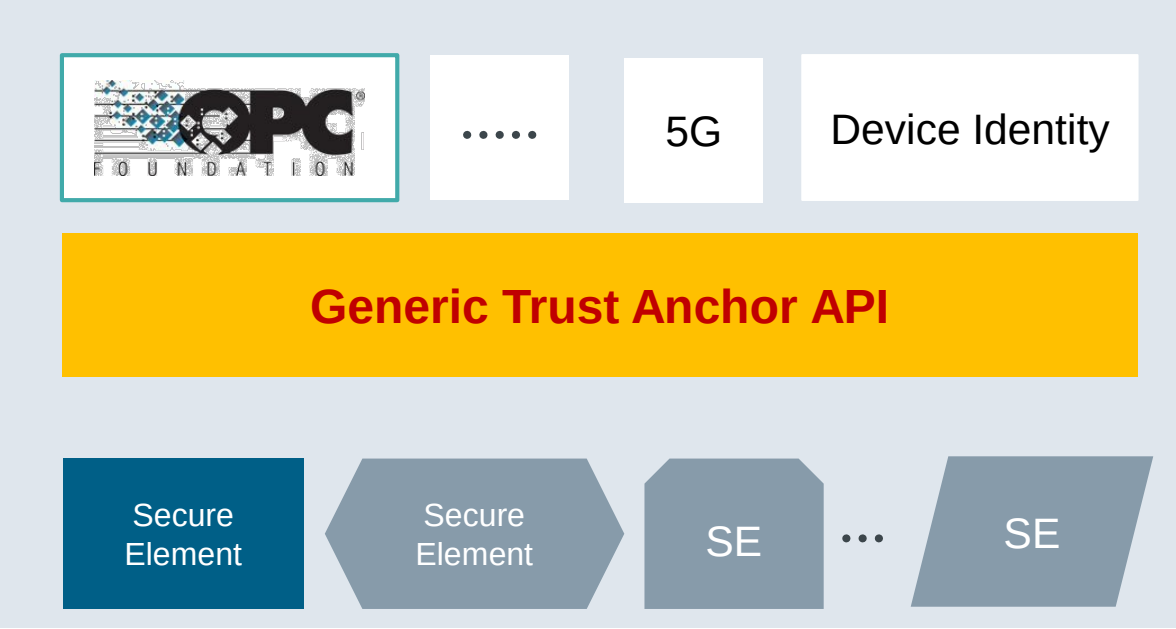
Controlling a SE is challenging

Interdisciplinary knowledge needed:

- **Security background (strong)**
- **Low-Level programming**
- **SE command structure**

➢ **Experts for SEs are rare**

A High-level API for SEs in Embedded Systems



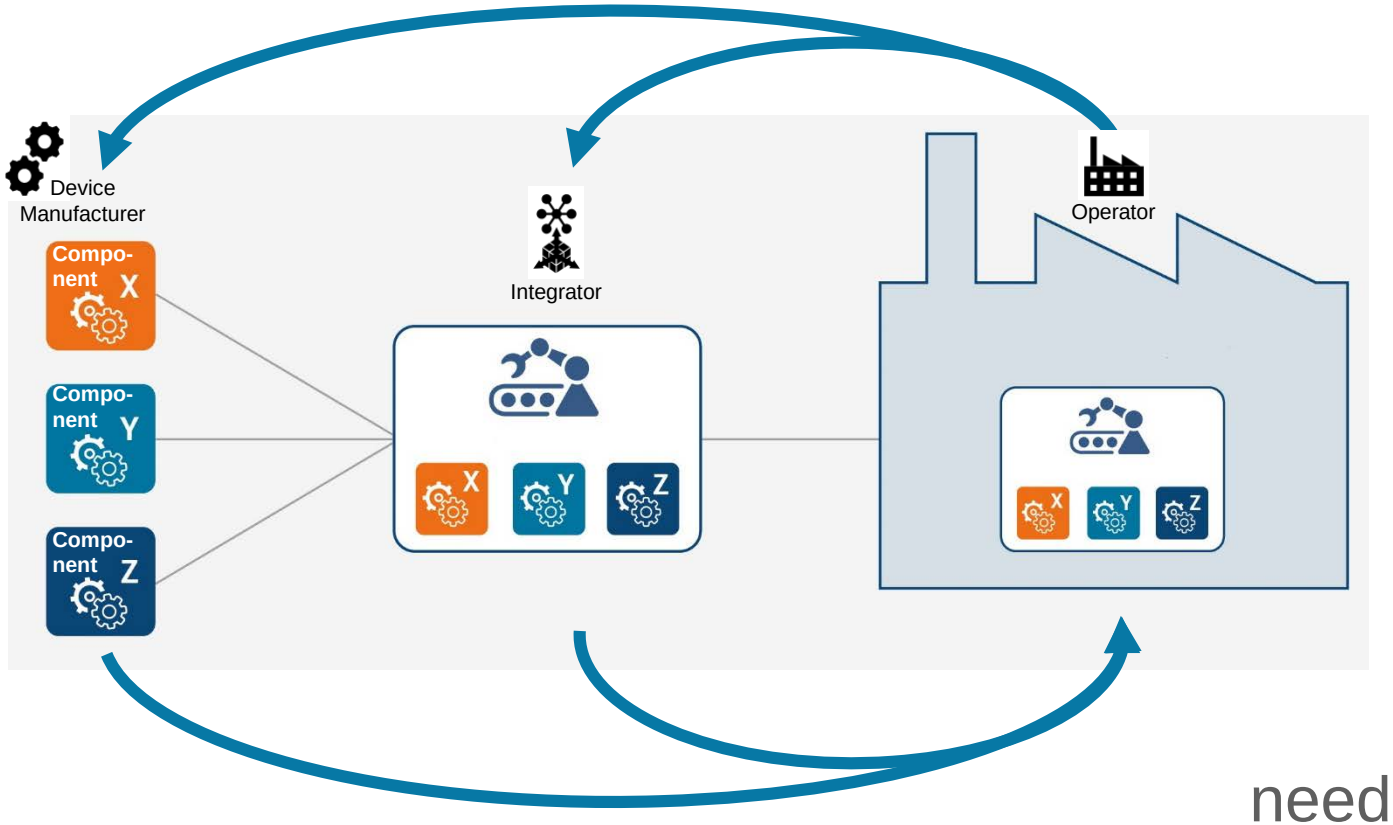
Intended for various…

- Industrial Applications
  - 5G
  - OPC UA
  - …
- Secure Elements

Supporting security for various Industrial IoT scenarios

Identity & Access Management

Supporting security for various Industrial IoT scenarios



Collaborative Condition Monitoring (CCM)

Pay-per-Use

Provisioning

Manufacturing as a Service

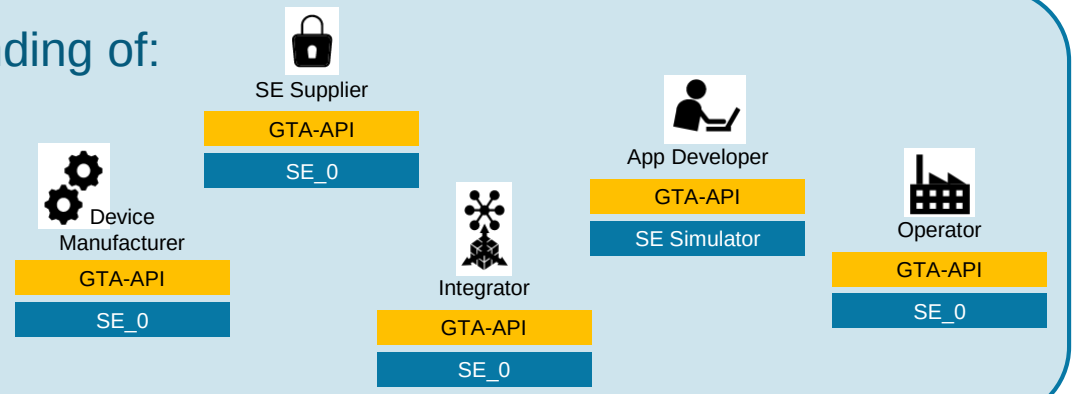
Remote Service

➢ **Multiple Stakeholder**
need to manage their Credentials
(e.g. passwords) on the same IIoT-Component

Not only Simplifies Handling of SEs …

Makes a Framework by common understanding of:

- IIoT Scenarios
- Stakeholders
- Access Rights
- Security Requirements



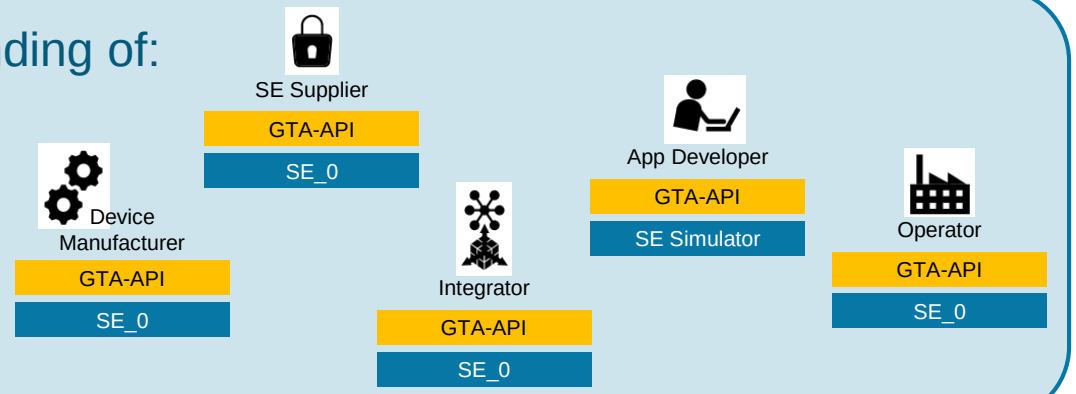
Interoperability on a Higher Level

- between Stakeholders/Participants in Value-creation chain
- on Business Level
  - ➢ Clear Contract Conditions
    - ➢ Enables autonomous Conclusion of Contracts

Not only Simplifies Handling of SEs …

Makes a Framework by common understanding of:

- IIoT Scenarios
- Stakeholders
- Access Rights
- Security Requirements



Interoperability on a Higher Level

- between Stakeholders/Participants in Value-creation chain
- on Business Level
  - ➢ Clear Contract Conditions
    - ➢ Enables autonomous Conclusion of Contracts

secure, open and dynamic Industrie 4.0

Standardisation Progress

TS - Technical Specifications
CD – Committee Draft

NA 43-01-41-02 AK

ISO/IEC JTC 1/SC 41
TS 30168 „GTA API for IIoT-Devices“
May 8, 2020

planned for
June 6, 2021

Contact

Thank you very much.

Björn A. Flubacher

bjoern.flubacher@bsi.bund.de

Tel.: +49 22899 9582-6402

PLATTFORM INDUSTRIE 4.0

Webinar

Shaping a globally secure Industrie 4.0 Ecosystem

Achieving digital Trust and Trustworthiness

23. September 2020

Agenda

- **Introduction of the working group on security of networked systems of the Plattform Industrie 4.0**
  - Industrial security aspects of the German Standardization Roadmap Industrie 4.0
  - Security for Industrial IoT – The Role of Trustworthiness
  - The new Whitepaper *IIoT Value Chain Security – The Role of Trustworthiness*
  - Challenges and building blocks to achieve a trust infrastructure
  - Generic Trust Anchor API – An Enabler for Industrie 4.0 Security
- **Panel discussion (Q&A)**
- **Outlook: International Conference “Shaping a globally secure Industrie 4.0 Ecosystem”**

Outlook

International Conference

Shaping a globally secure Industrie 4.0 Ecosystem

How to enable international interoperable security policies?

from January 28th – 29th 2021

at the

Federal Ministry for Economic Affairs and Energy (in Berlin, Germany)

Webinar Plattform Industrie 4.0
Outlook

- In **2018**, 140 international private sector and political leaders came together to discuss, how we can secure global industrial value networks.
- In **2021**, once again, we will bring together international top-level stakeholders and decision makers from industry, governments and regulatory bodies for two days of dialogue and discussion.
- A **Call for Papers** is open until October 7th 2020

Plattform Industrie 4.0
Contact

Thank you very much.

Plattform Industrie 4.0
Secretary

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

www.plattform-i40.de