ロボット革命イニシアティブ協議会
Robot Revolution & Industrial IoT Initiative

PLATTFORM INDUSTRIE4.0

INTERNATIONAL PAPER

IIoT Value Chain Security – The Role of Trustworthiness

Imprint

Publisher
Federal Ministry for Economic Affairs
and Energy (BMWi)
Public Relations Division
11019 Berlin
www.bmwi.de

Editorial responsibility
Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Design
PRpetuum GmbH, Munich

Status
April 2020

Image credits
istockphoto / Peshkova (title)
istockphoto / artisteer (p. 3)
istockphoto / Tony Studio (p. 7)

You can obtain this and other brochures from:
Federal Ministry for Economic Affairs
and Energy (BMWi)
Public Relations
Email: publikationen@bundesregierung.de
www.bmwi.de

Central ordering service:
Tel.: +49 30 182722721
Fax: +49 30 18102722721

Contents

Figures

1. Background

In the past, Plattform Industrie 4.0, Germany and Robot Revolution & Industrial IoT Initiative (RRI), Japan, announced three common position papers, “Facilitating International Cooperation for Secure Industrial Internet of Things/Industrie 4.0” (16th March 2017, 16th May 2018, 3rd April, 2019) [1].

In line with these three common position papers, Plattform Industrie 4.0 and RRI have discussed the goal of the activity, i.e. to foster trustworthiness in increasingly digital and interconnected economies.

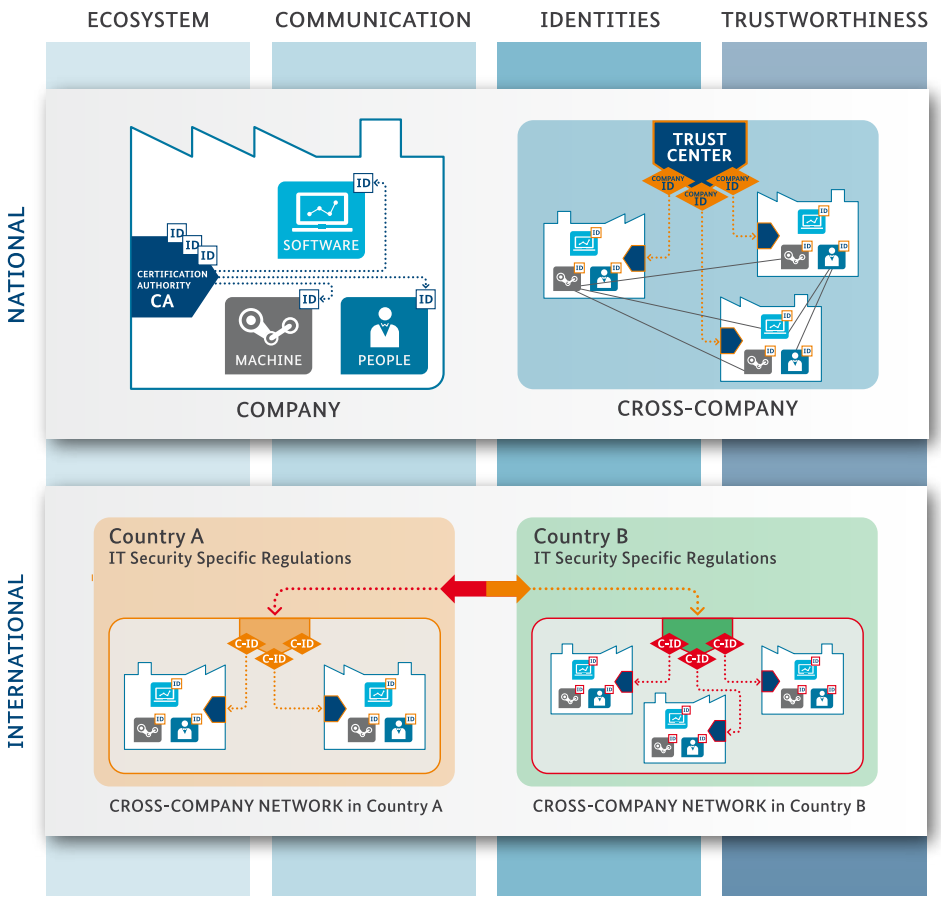
2. Introduction

Highly automated international and global collaboration of industrial production environments is a key feature of Industry 4.0 (I4.0). In various countries, local production facilities will be able to collaborate with each other in an ad-hoc and automated manner across continents. Therefore, availability of a comprehensive I4.0 ecosystem with a high-level of security integrated is an indispensable prerequisite. Trustworthiness in the context of Industrial Internet of Things (IIoT) value chain security is an integral part of it.

As shown in Figure 1, supply chains of the connected industries that are part of the I4.0 security ecosystem, must implement trustworthy collaboration infrastructure. In order to achieve the stated target, partners must be identified, and their respective trust-relevant characteristics must be determined and exchanged. For example, procurement, a process to form buyer-supplier relationships, has been done between parent companies and their subsidiaries based on their traditional relationships. However, in recent years, the business case of procurement between companies that do not have long business histories, has been globally increasing regardless of the companies' scale and geographical location.

The overall goal of the present collaboration work between RRI, Japan and Plattform Industrie 4.0, Germany, is concentrated to the possibility of creating ad-hoc trustworthy relationships between companies, regardless of their business histories or their geographical locations. Therefore, in this whitepaper, the role of trustworthiness and mechanisms to assure trustworthiness between existing or potential business partners have been described.

Figure 1: Overall Scenario of I4.0-Production



3. Motivation

The whitepaper focuses on a use case, i.e. a potential supplier based in Japan wants to establish a new business relationship with a customer in Germany. 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.

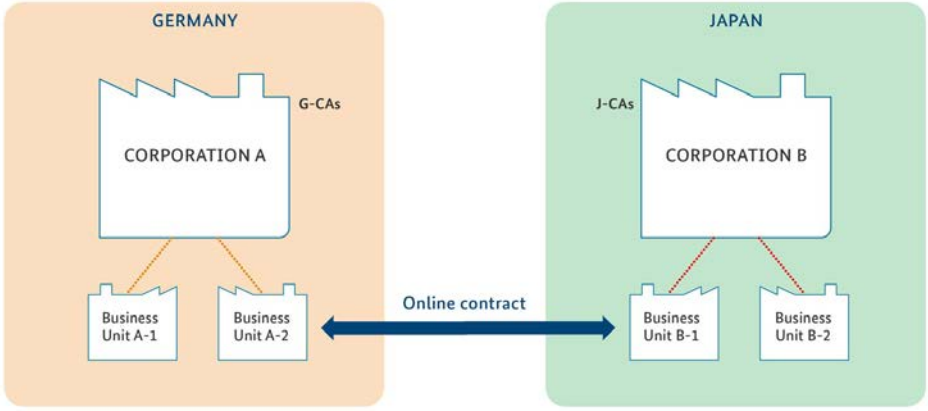
In order to achieve this target, the sub-working group AG 3, i.e. Security of Networked Systems" from Plattform Industrie 4.0 in Germany and RRI in Japan jointly postulate key issues that need to be taken into consideration for a lasting business relationship between customers and suppliers, across the two continents:

1. How to define trustworthiness in the context of supply/value chain security?

2. Which criteria can be used to determine the trustworthiness of a company and its products?

3. What kind of mechanisms are needed for assuring trustworthiness, with respect to supply/value chain security, globally?
   a. How can we ensure dynamic and quick establishment of trustworthy relationships between companies across borders?
   b. Is a single overarching global certificate-based process for delivering secure digital identities globally applicable, feasible, and economical?
      i. How can secure digital identities for companies, people, machines and software processes be issued, distributed, managed and used?
      ii. How can secure digital identities be realized across different countries in an industrial infrastructure?
      iii. How can we ensure that the secure digital identities in both countries have the same or comparable security level?
      iv. How can we check the validity of conditional trust services?
      v. How can it be ensured that digital identities are valid and are used exclusively by the authorized entities (persons, machines, SW processes) and within the scope of a defined release process of the identity?
      vi. How can such an infrastructure be operated realistically? How can a gradual introduction be made?
   c. How is (partially-) automated verification of the trustworthiness of the business partner possible without prior discussions, confidentiality agreements and business contracts?
   d. How can existing national procedures be linked internationally? Is it enough to link individual national procedures bi-nationally via "bridge" constructions? Are group constructions required?

Figure 2: Targeted Use Case-Cross-Border Business Relationships



4. Trustworthiness

Global value networks require comprehensive trustworthiness architectures covering all entities, regardless of their geographical location.

Security in I4.0 is driven by people, software, hardware, and communication processes. Global economy is supported through global supply chains where interdependency among organizations, systems, and components is increasing. Therefore, it is essential to establish their trustworthiness for healthy growth of global economy.

In order to create digital business relationships across continents, all security related entities (organizations, people, components, data, procedures, systems) and communication processes need to be trustworthy [2].

In the context of our project, the definition of the term 'trustworthiness' proposed by the ISO/IEC JTC1/WG13 [3] has been adapted as:

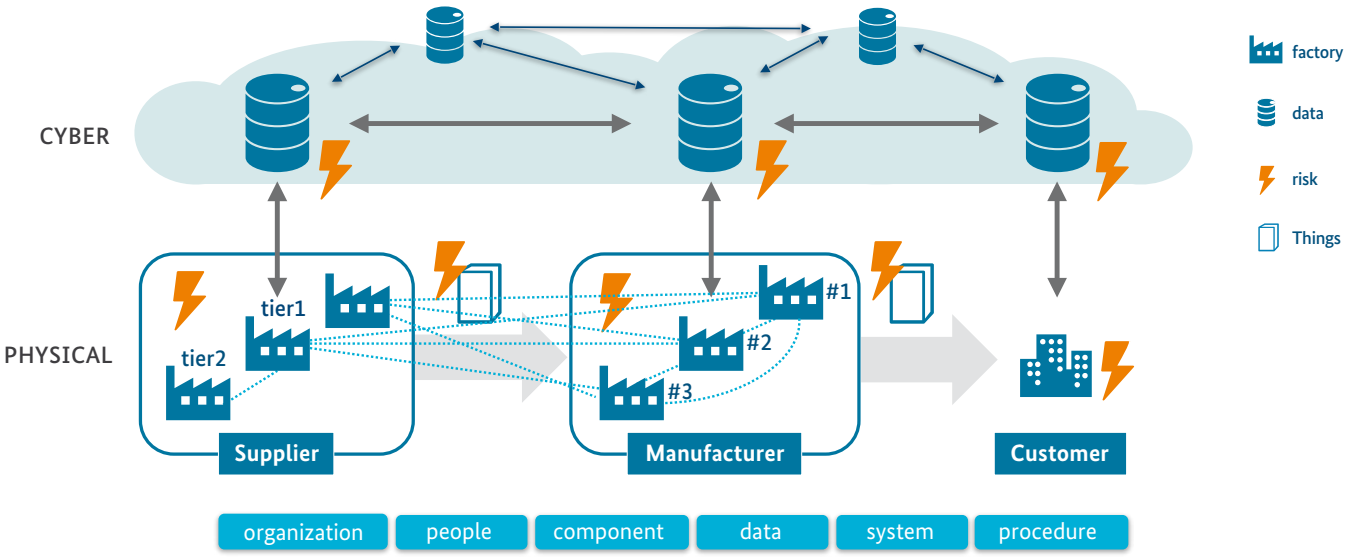
"For supply/value chain security and risk management, the term 'Trustworthiness' corresponds to the supplier's ability to meet the expectations of the potential contract partner in a verifiable way".

Depending on the use case in focus, and on the specific product, service, data, and the technology used, different characteristics would apply and would require verification to ensure the fulfilment of stakeholder's expectations. These characteristics may include authenticity, integrity, resilience, availability, confidentiality, privacy, safety, accountability, and usability.

Within the process of trustworthiness establishment, different perspectives need to be considered:

- Business perspective considers the identification of relevant business partners, determination of basis for collaboration, specifications of the products, etc.
- Legal perspective considers the negotiation and agreement for the terms of cooperation between business partners, such as Non-Disclosure Agreement (NDA), etc. It might also include clause that can be used in law courts.
- Technical processes support the collaboration between the two business partners via technical means (network, communication protocols, application, etc.). It is the realization of business and legal processes, for example, signed contracts, etc.

Figure 3: Risks in Connected Industries



The scope of this project is limited to the technical processes only, as we aim to establish a mechanism that can be leveraged to realize time-efficient and trustworthy contracts between business partners, regardless of their geographical location.

Our chosen use case (discussed in Section 3), depicts that the potential business entities usually have a contract in-place followed by the delivery of products. The trust between the business entities develop along the product lifecycle if the delivered products meet the buyer's expectations. This use case shows that regarding organizations and their products, trustworthiness has at least two (but not limited to) properties: authenticity and security. Therefore, four types of trustworthiness criteria can be deduced:

1. **Authenticity as a property of an organization's trustworthiness**
   The communication is based on the authenticity of the other party. For example, the authenticity of an organization may be assured by its globally unique ID and the corresponding digital certificate.

2. **Authenticity as a property of products' trustworthiness**
   It is the basis of trustworthiness that products are authentic (i.e. not fake). For examples, the authenticity of products can be assured by globally unique IDs and corresponding digital certificates.

3. **Security as a property of an organization's trustworthiness**
   Recently, the value of information is increasing and the means through which participants in the global supply chain securely share information are becoming crucial. So, security should be considered as a property of the organization's trustworthiness.

4. **Security as a property of products' trustworthiness**
   Nowadays, a product depends on parts and products from other parties in the global supply chain. Attackers try to exploit a weak point within the supply chain and may compromise the product or its components. So, security should be added to the property of products' trustworthiness as well as other quality expectations.

5. Mechanisms to Support Trustworthiness Assurance

5.1 Unique Identities of Organizations, Employees, Processes, and Products

In terms of organizations, each country usually has a 'unique ID for organization' assignment procedure in place. For example, companies in Japan are assigned a trusted free-for-use company ID (corporate number) by the National Tax Administration Agency (NTA). Since, companies have several business units scattered around the globe, there's a need for a procedure for assignment of globally unique IDs to each business unit. Likewise, an increasing global supply chain leads to the need of a globally unique numbering scheme for products so that they can be authenticated at any stage of their lifecycle.

Digital identities, such as contactless RFID cards, are widely used as employee identification. Access to buildings, rooms, IT-terminals, applications, etc., is based on some form of digital identification of the user. These digital identities are often based on standardized mechanisms but have not yet been formally standardized to ensure interoperability.

Likewise, machines and their components often have identifiers, such as bar code, QR code, etc., that are used for their identification along their lifecycle. Similarly, communication modules are often assigned a globally unique MAC address via a defined registration process. During operations, a time-limited identity, i.e. an IP address is assigned to the communication modules. In cryptographically secured communications, TLS or IPSec certificates are assigned to the respective MAC or IP addresses. For legitimate authentication of a unique identity, an attack-resistant association to a secret key material is always required. Till now, it is not an established practice to implement attack-resistant links in IoT devices.

In the software domain, usually the operating system assigns a system-wide unique (time-dependent) ID to each process instance. A widely leveraged practice is to map software process permissions to the permissions of the executing account (e.g. system, functional user, regular user, etc.) so that the software process is instantiated only by the authorized user. The authentication of user's identity is usually based on the unique combination of a username and a password, username and PIN code, or two-factor authentication schemes.

For cross-device authentication of software processes, digital identities are often linked to X.509 certificates that are used to verify the secret key material of the software application. For example, when a process accesses a webserver via secure link, such as https, the webserver authenticates itself with an X.509 certificate. On the other hand, the unique identity of the software process is the DNS name, the IP address of the device, or the machine identity. This authentication method is currently unidirectional. In the case of OPC UA, the authentication is defined bidirectionally. In industrial environments, assignment of unique digital IDs to software processes is not an established practice although it is stressed in security standards, such as IEC-62443.

Nowadays, current development is also going in the direction of 'Self-Sovereign Identity' for contracts, in the domain of smart contracts. In this context, "smart" means verification of contract contents by the involved parties independently.

5.2 Certificates

In this white paper, the term certificate is used in two different ways; Identity Authenticating Certificate (IAC) is one that is used to authenticate public key corresponding to asymmetric cryptography and, the Security Certification Certificate (SCC) serves as a proof of certification of a product's or a process's quality. Within the realm of I4.0, secure and trustworthy value chains leverage both types of certificates.

Identity Authenticating Certificates

Industrial communicating partners leverage IACs to prove and verify there and their products' authenticity.

Digital IACs are often created and issued according to the X.509 standard that is the basis of Public Key Infrastructure (PKI). These digital certificates bind an entity's digital identity to its public key. In order to prevent fake digital certificates, trusted third parties called Certifying Authorities (CAs) digitally sign the digital certificate after verifying the authenticity of the certificate's owner, which may be an organization, an individual, a process, or any physical entity.

Nationally hosted PKI solutions exist in some countries for various purposes, such as for toll collection on federal motorways, etc. Internationally, an example of PKI integration is the usage of tachographs for heavy duty vehicles. They have an on-board unit used for recording steering and idle time.

Another application of IAC is the electronic train ticked system, e.g. in Germany. Cryptographic checksums are created during the booking and issuing of train tickets on the web and can be verified during the ticket control using special terminals or applications. In 2014, the eIDAS regulation (EC / 910/2014) [4] was adopted by the local European market. According to this regulation, electronic ID cards are issued to citizens of EU member states and could be used as a secure identity for various public online services. Other examples of certificate-based global solutions are the authenticity assurance of biometric passports that are standardized according to the ICAO 0303 worldwide, and bank cards which, however, can comply with different national or regional standards, such as EC card in Germany and the JCB card in Japan.

Security Certification Certificates

In the context of I4.0, SCCs are leveraged (and may be displayed) to certify the quality levels of products, equipment, or manufacturing processes according to internationally recognized ISO or IEC standards such as ISO27000x, IEC 62443. While establishing secure communication between business partners, SCC can be used to assess the trustworthiness of the communicating entities. Currently, SCCs are leveraged usually in printed form. The printed certificates have security features, such as stamps, holograms, etc. to ensure their authenticity. These certificates cannot be used electronically in an easy and reliable way. For the future, technology is needed to support digital SCCs that can prove their authenticity and that cannot be replicated by unauthorized entities.

5.3 Useful Trustworthiness Standards and Frameworks for the Chosen Use Case

Since the scope of the project is widespread and covers a broader spectrum of establishing trustworthiness between potential business partners, various standards have been reviewed that are applicable at various stages.

At the beginning of the project, ETSI 319 412 series [5], CA browser forum baseline requirements, ISO 27002, ISO 17065, RFC 3647, and NIST SP 800 63-3 have been taken into consideration. These standards and requirements have been considered from the perspective of realizing trust services for the business partners. The following diagram (Figure 4) depicts relationship between the reviewed standards.

Later, widely known standards and frameworks that support establishment of security in industrial environments have been reviewed. Recently, it has been noted that in security standards there's an additional focus on defining security levels for organizations and components, such as NIST CSF and METI CPSF. Additionally, it has been observed that most security standards define types of security levels in different ways, as depicted in the following diagram (Figure 5).

Different types of security levels can be employed to evaluate trustworthiness of other business partners. For instance:

- an organization's security maturity can be estimated using the organizational security levels defined according to VDA-ISA and CPSF.
- or a product's security level that depicts the quality measurements regarding the assurance of requirements in the **product development process**, according to VDA-ISA, IEC 62443, ISO / IEC 15408.

Figure 4: Standards and Frameworks That Support Trustworthiness

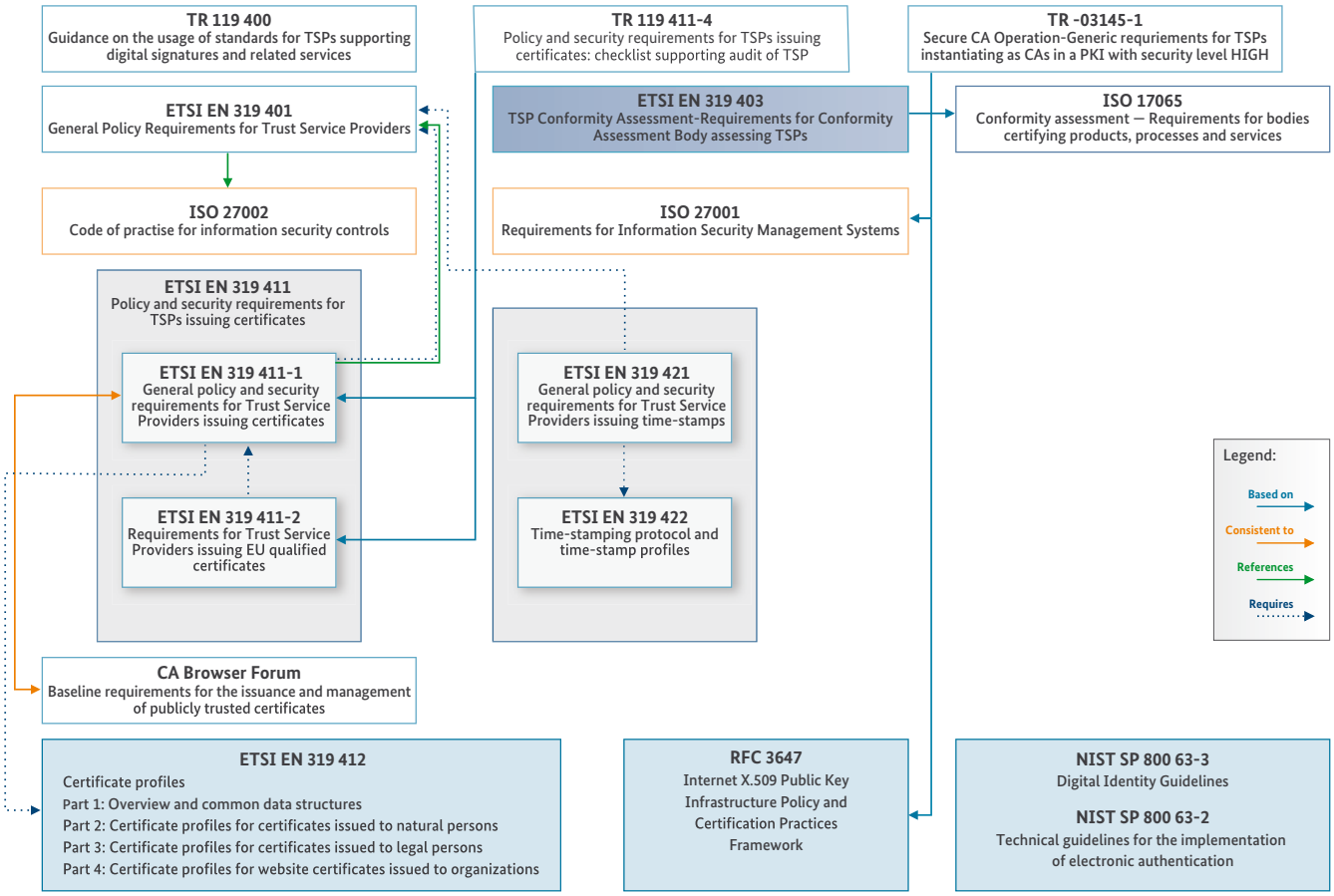


Figure 5: Different Security Standards Defining Various Security and Maturity Levels

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)* BR/RE**	SL (4 levels)
VDA-ISA	Maturity Level (6 levels)	Required level (5 expressions)	
ISO/IEC 15408	—	CC EAL(7 levels)	
ISACA COBiT5	Process Capability Level (6 levels)	—	

6. Trustworthiness Expectations and Capabilities Exchange Protocol

6.1 Overview

During the course of collaboration between Plattform Industrie 4.0 and RRI, a demonstrator has been proposed. This demonstrator intends to realize the overall goal of the collaboration work, i.e. to establish ad-hoc trustworthy relationships between companies and business partners, regardless of their geographical location, business history, etc.

In the progressing era of global supply chains, our primary focus is organizational trustworthiness in the realm of online contracts and e-procurement processes. Before designing the demonstrator, various existing procedures, technologies and relevant standards have been reviewed and the currently existing infrastructure in both the countries, i.e. Germany and Japan, has been thoroughly understood. Additionally, already existing procurement solutions and platforms, such as SAP Ariba, Open Procurement, SupplyOn etc. have been thoroughly reviewed.

6.2 Conceptual Design

In this white paper, a "Trustworthiness Expectations and Capabilities Exchange Protocol" (TECEP) is proposed as a technical solution to be used for trustworthiness negotiation and exchange between peers.

It can be considered as a support to the risk-based approach to determine the trustworthiness of a supplier and the respective product. The TECEP comprises exchange, comparison and evaluation of a supplier's trustworthiness capabilities based on the buyer's trustworthiness expectations.

The following figures show two possible alternatives of the TECEP. The first alternative (shown in Figure 6) depicts a bidding system in which the buyer publishes the request-for-work along with his trustworthiness expectation on an independent platform. On the other hand, the supplier responds with his bid along with his trustworthiness capabilities to the platform. Based on the pre-defined set of rules, the platform evaluates the request-of-work(s) and the corresponding bids, trustworthiness expectations and corresponding trustworthiness capabilities and forwards the most relevant ones to the respective buyer for further business.

The second alternative (shown in Figure 7) eliminates the need of an independent platform and depicts the 1:1 business relationship. It shows that the buyer sends his request-of-work along with his list of trustworthiness expectations

Figure 6: Trustworthiness Expectations and Capabilities Exchange Protocol – Alternative 1

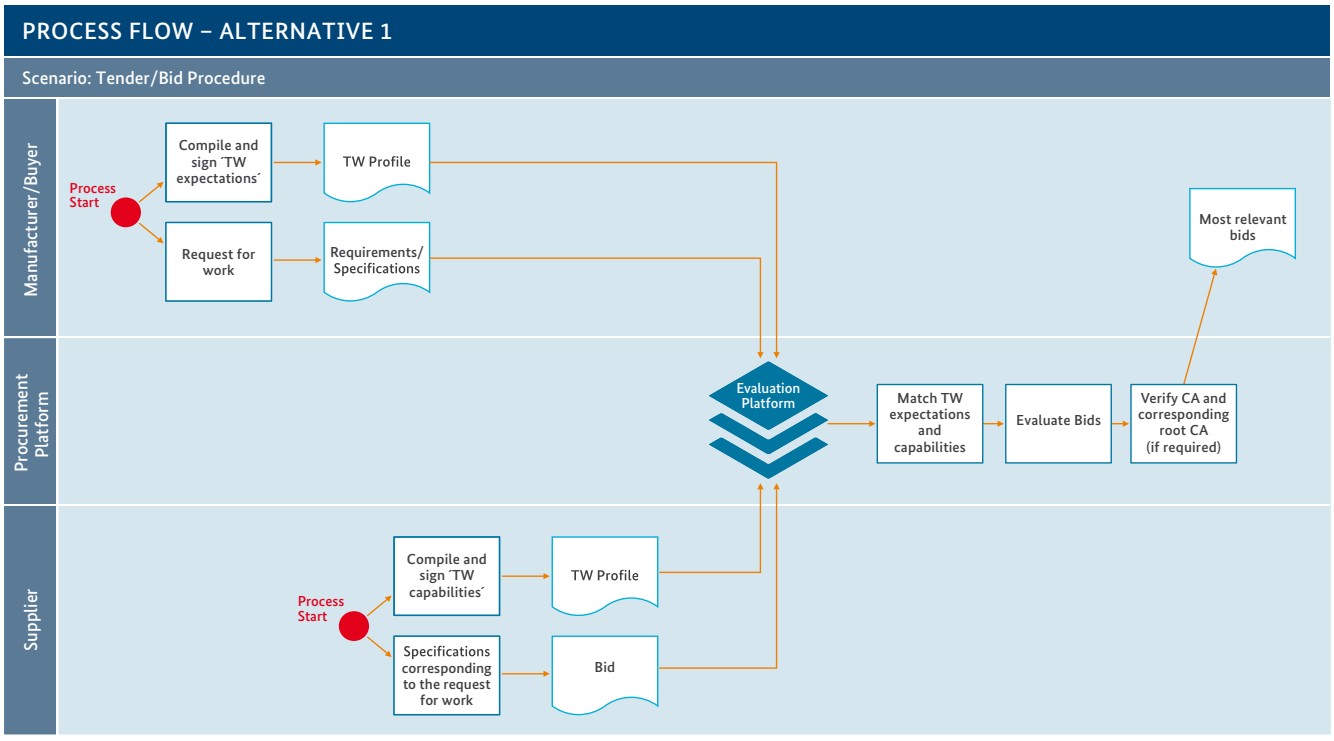
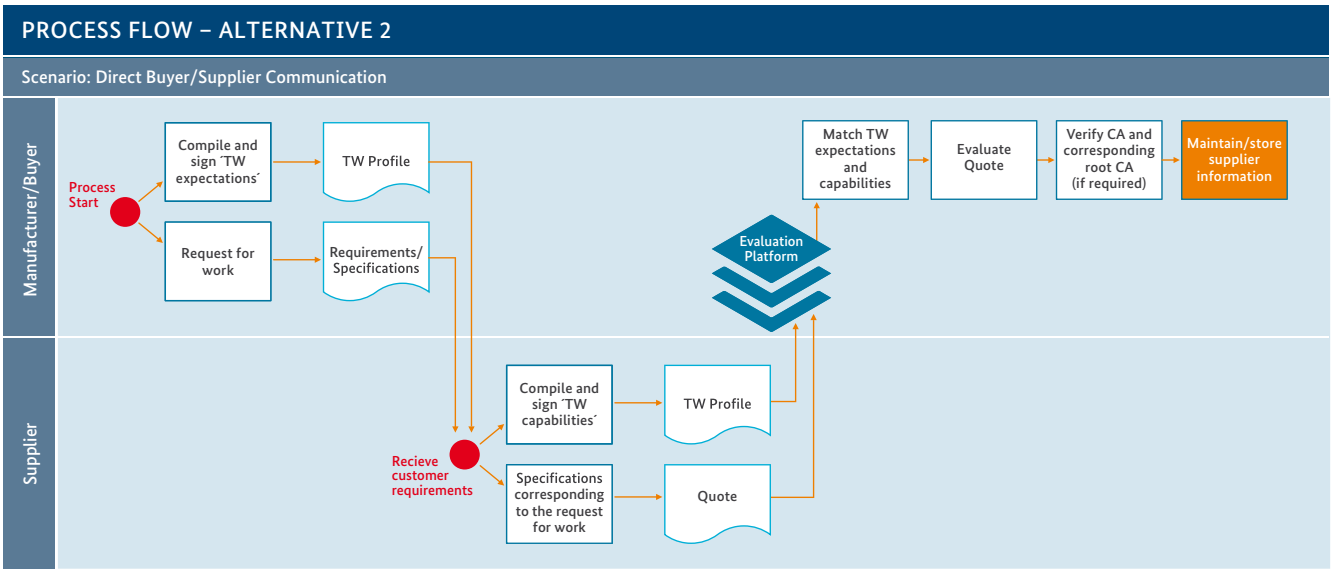


Figure 7: Trustworthiness Expectations and Capabilities Exchange Protocol – Alternative 2



directly to the supplier. The supplier replies with the corresponding quote and his trustworthiness capabilities. As discussed later in this chapter (section 6.46.4 Evaluation), the buyer evaluates the received quote and corresponding trustworthiness capabilities and leverages them as basis for further relationships with the corresponding supplier.

The target of TECEP is to support automation of the existing process of supplier (and/or product) qualification and selection in order to evaluate the supplier's trustworthiness. This can be realized by the exchange of the trustworthiness profile, introduced in the following section.

6.3 Trustworthiness Profile

It can be considered as a standardized container that can be realized irrespective of the base communication technology, as shown in Figure 8. The granularity of trustworthiness expectations is flexible and depends on the business provider's requirements. For instance, the buyer may demand for IEC62443-4-2, etc. For the buyer, the trustworthiness profile (TWP) also provides provision of marking mandatory expectations and defining the expected validity of the demanded supplier's trustworthiness capabilities. As an additional information, the buyer can specify the type of proof he/she requires, for example, a digital certificate, documentation, etc.

Likewise, the supplier can attach the required proof, for example, a .pdf file, digital certificate, link to the proof, etc., depending on the requirement specified by the buyer. In case of time-dependent proofs, e.g., certificate valid for a particular duration, etc., the proof-expiry date needs to be entered.

The TWP leverages cryptographic mechanisms to ensure integrity of the trustworthiness expectations and corresponding trustworthiness capabilities. It includes digital signatures and digital certificates of the involved parties.

At present, buyers often leverage customized questionnaires for evaluating their supplier's security levels. The proposed TWP provides flexibility to include customized questionnaires as well. Additionally, it will be useful to have a common TWP across an industrial vertical.

6.4 Evaluation

Once the buyer receives the filled TWP from the supplier, either an automated or a manual procedure can be used to compare and evaluate the trustworthiness capabilities corresponding to the defined trustworthiness expectations. If required, the buyer and the supplier may negotiate their expectations and capabilities using the proposed TWP.

In case of an automated evaluation of the TWP, each company can design and leverage its own evaluation procedure. For example, the buyer can classify his trustworthiness expectations in 'must haves', 'should haves' and 'good to haves'. An algorithm can be implemented to select the supplier that fulfils all 'must have's, then 'should have's and so on. Based on the buyer's requirements, more complex Artificial Intelligence (AI) based tools can also be used in addition to a TWP evaluation.

The degree of trust in further relationships between buyers and suppliers maybe based on the negotiation and evaluation of the exchanged TWP. In the future, TWPs can be maintained using distributed ledger technologies by buyers to establish trustworthiness traceability along the value chain.

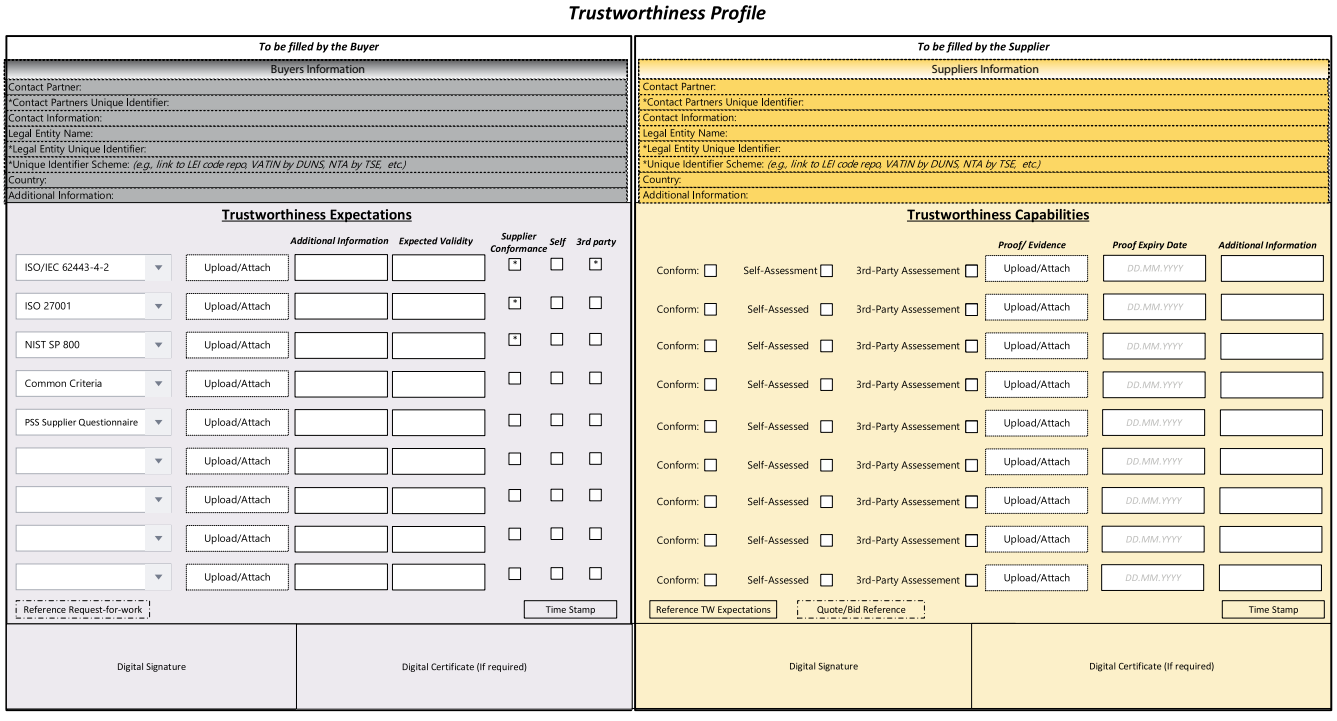
6.5 Scalability and Interoperability of the TECEP

As described in Section 6.3, the TWP provides a container format that can be leveraged to consolidate trustworthiness expectations and capabilities of the potential business partners. For the future, RRI and Plattform Industrie 4.0 propose to standardize the TWP as it can serve as an efficient basis for the determination of trust in new and existing business relationships. A standardized TWP format might lead to the establishment of standardized TWPs for various industry verticals. This may lead to the increased utilization of Federated Identity Management (FIM). FIM is an arrangement between multiple organizations to allow their users use the same identification data for various uses across the network of organizations that are part of the group.

In order to protect integrity of the exchanged TWP, cryptographic measures such as digital signatures are proposed. In the future, if TWPs are widely exchanged and maintained, they can be used to trace trustworthiness of the buyers and suppliers.

Currently, most of the organizations have their own customized procedure for supplier selection, which is usually manual. We expect that the widespread utilization of the standardized TECEP and TWP would help in automating the procurement process leading to automated supplier selection leveraging automated TWP evaluation mechanisms.

Figure 8: Proposed Trustworthiness Profile



7. Future Work

Contrary to IACs, certificates used for assuring quality of organizations and products are usually available in printed form. For example, audit companies issue a manually signed printed certificate to the audited company. These printed certificates have security technologies integrated, such as non-replicable inks, special holograms, etc. The future collaboration activities, between RRI and Plattform Industrie 4.0, will also discuss the digital SCC structure, that cannot be faked or copied by unauthorized entities.

In the future, collaboration activities between RRI and Plattform Industrie 4.0 plan to realize the TWP in a demonstrator, which would provide a standardized basis for establishing digitalized trustworthy relationships between buyers and suppliers. AI based algorithms may be considered to devise industrial vertical or use case relevant TWPs automatically. Further, consideration may be given to automated procedures for TWP evaluation in the most efficient manner. RRI intends to research on existing security requirements and derive a common set of security questionnaires for suppliers.

8. References

[1] https://www.jmfrri.gr.jp/document/library/1105.html

[2] https://www.meti.go.jp/english/press/2019/0418_001.html

[3] https://www.iso.org/committee/45020.html

[4] https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014

[5] https://portal.etsi.org/TB-SiteMap/ESI/Trust-Service-Providers

AUTHORS

Kitamura Atsushi, Robot Revolution & Industrial IoT Initiative; Vanessa Bellinghausen, Bundesamt für Sicherheit in der Informationstechnik; Junya Fujita, Hitachi Ltd.; Ayaji Furukawa, Toshiba Corporation; Dr. Lutz Jänicke, Phoenix Contact GmbH & Co Kg; Michael Jochem, Robert Bosch GmbH; Dr. Wolfgang Klasen, Siemens AG; Aliza Maftun, Siemens AG; Prof. Tsutomu Matsumoto, Yokohama National University; Masue Shiba, Toshiba Corporation; Nobuaki Suzuki, Toshiba Corporation; Thomas Walloschke, Industrie KI GmbH; Steffen Zimmermann, VDMA e.V.; Tsutomu Yamada, Hitachi Ltd.; Dr. Takeshi Yoneda, Mitsubishi Electric Corporation

www.plattform-i40.de