PLATTFORM INDUSTRIE 4.0

Web-Seminar

Shaping a globally secure Industrie 4.0 Ecosystem

IIoT Value Chain Security- The Role of Trustworthiness

Whitepaper 2020

14th October 2020

Agenda

- RRI(Japan) & PI4(Germany) collaboration, The goal of our activity
- White Paper (IIOT Value Chain Security –The Role of Trustworthiness) 2020
- Next Steps
- Security questionnaires for suppliers
- RRI Next Steps

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.

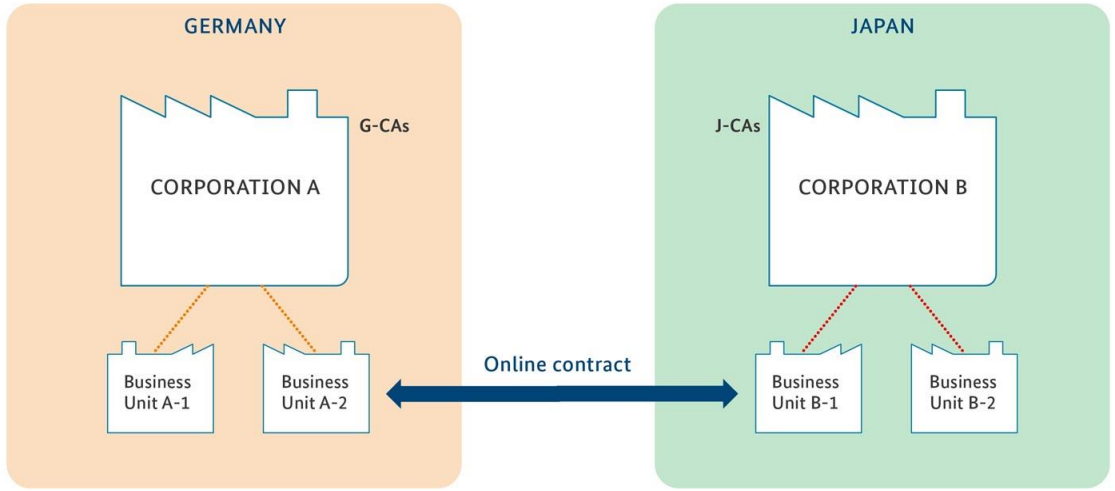
https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.html

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

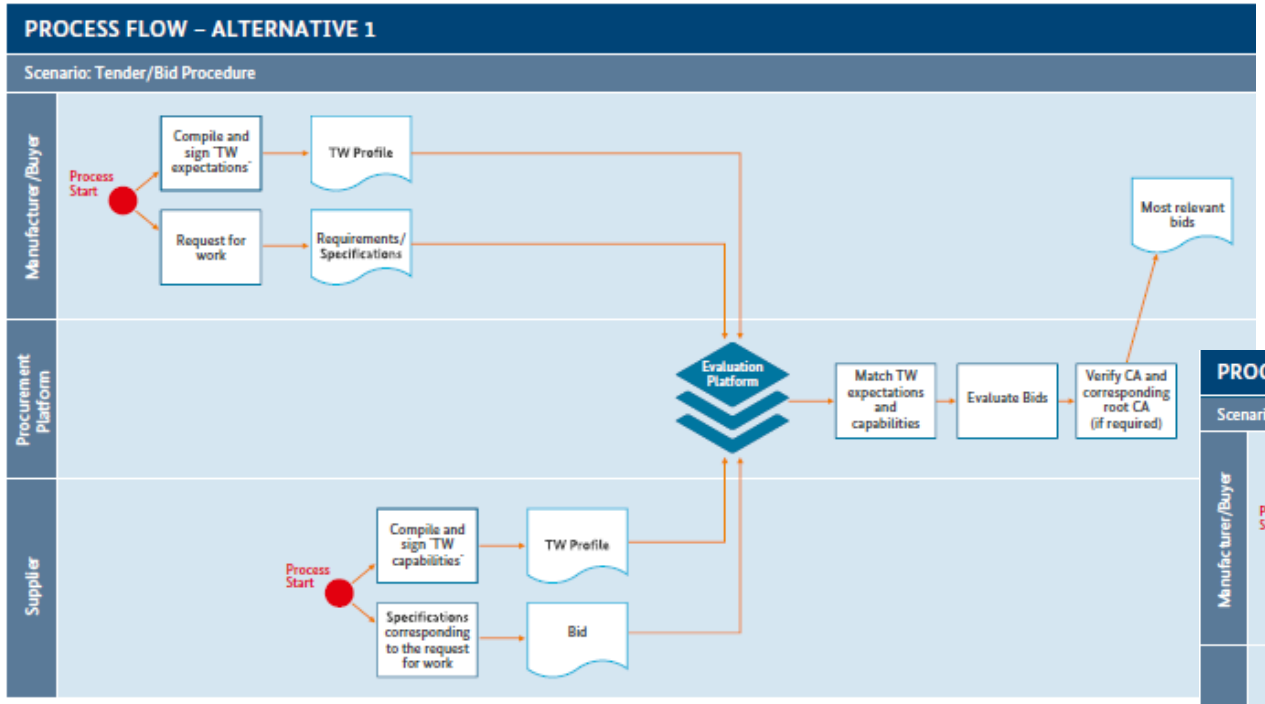
- Identity Authenticating Certificates such as X.509 PKI, eIDAS, etc.
- Security Certification Certificates, such as ISO 2700x certificates, IEC 62443 certificates, etc.

Standards and Frameworks

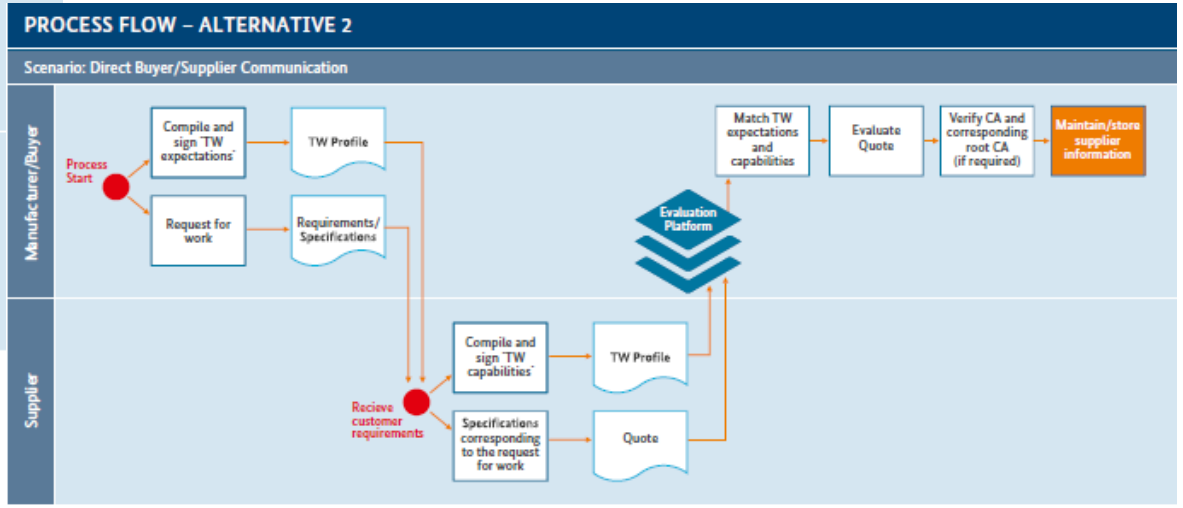
- ETSI 319 412 series
- ISO/IEC 62443-x-x
- METI CPSF
- NIST CSF
- …

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.

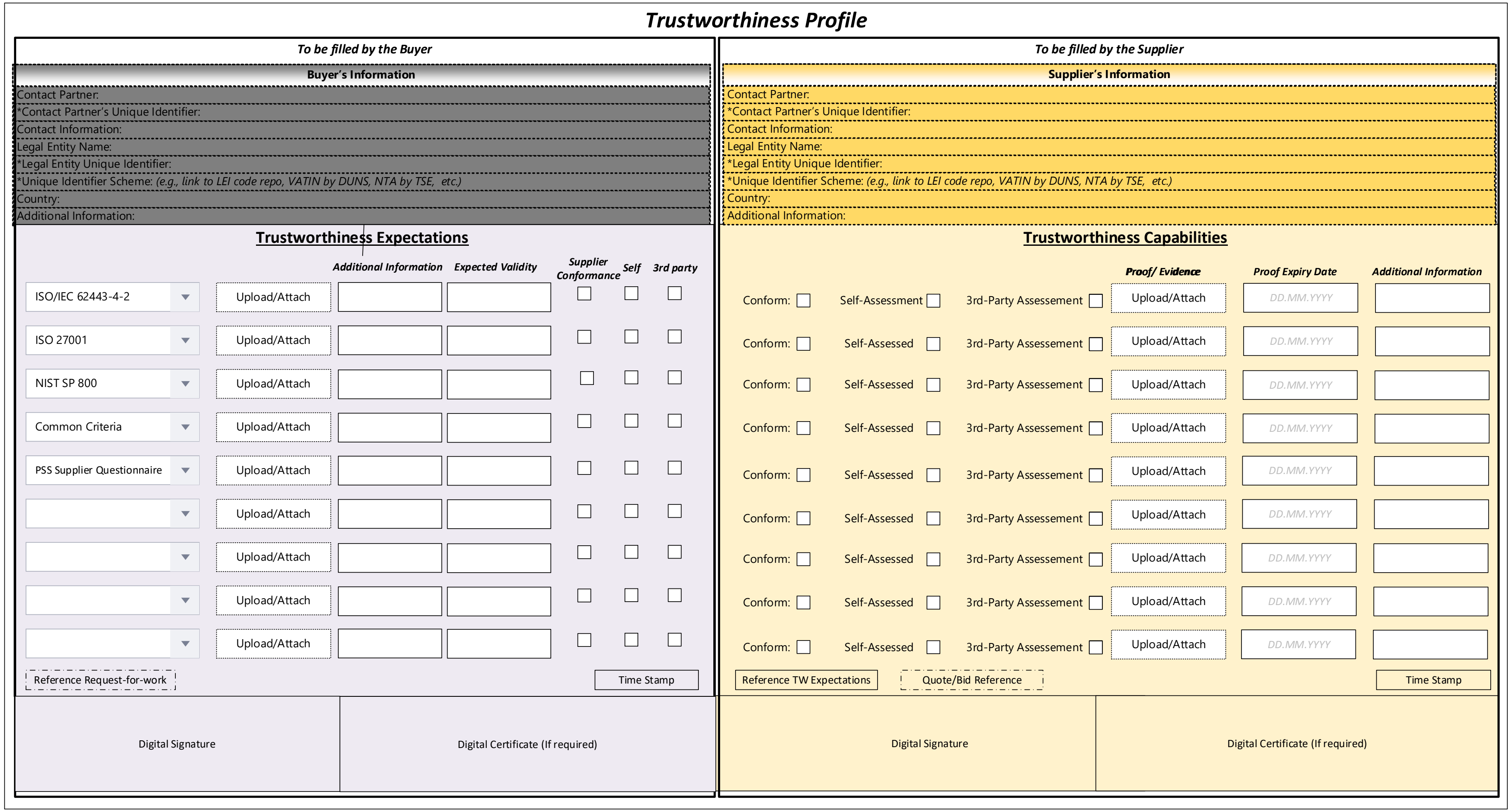


Trustworthiness Profile

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


Trustworthiness Profile

To be filled by the Buyer

Buyer's Information

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

Trustworthiness Expectations

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

Reference Request-for-work | Time Stamp

Digital Signature | Digital Certificate (If required)

To be filled by the Supplier

Supplier's Information

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

Trustworthiness Capabilities

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

Reference TW Expectations | Quote/Bid Reference | Time Stamp

Digital Signature | Digital Certificate (If required)

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