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

PLATTFORM INDUSTRIE4.0

WHITEPAPER

IIot Value Chain Security – Trustworthiness of Data

German-Japan cooperation

Imprint

Publisher
Federal Ministry for Economic Affairs and Climate Action (BMWK)
Public Relations
11019 Berlin
www.bmwk.de

Editorial responsibility
Plattform Industrie 4.0
Bülowstraße 78
10783 Berlin

Status
April 2024

This publication is available for download only.

Design
PRpetuum GmbH, 80801 Munich

Picture credit
WrightStudio / Adobe Stock / title
Vladimir / Adobe Stock / p. 3
The Little Hut / Adobe Stock / p. 5
ipopba // Adobe Stock / p. 8
bsd_studio / vecteezy / p. 9
FrentaN / Shutterstock / p. 9
D3Damon / iStock / p. 12
Pakin / Adobe Stock / p. 14

Central ordering service for publications of the Federal Government:
Email: publikationen@bundesregierung.de
Tel.: +49 30 182722721
Fax: +49 30 18102722721

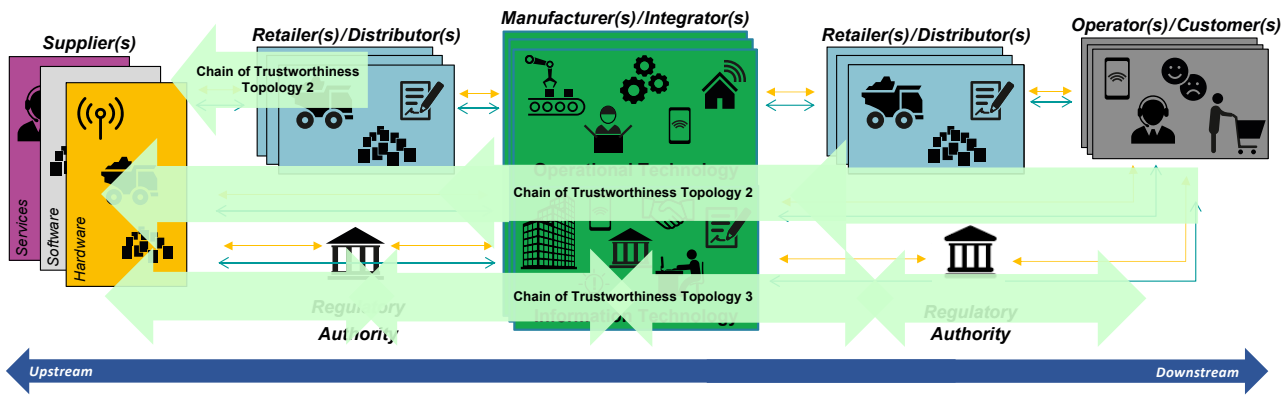
This publication is issued by the Federal Ministry of Economic Affairs and Climate Action as part of its public relations work. The publication is available free of charge. It is not for sale and may not be used by political parties or groups for electoral campaigning.

Table of contents

1. Background

Robot Revolution & Industrial IoT Initiative (RRI), Japan and Plattform Industrie 4.0, Germany, have a successful history of collaboration concentrating on supporting organizations with the establishment of trustworthy relationships, regardless of their business histories or geographical locations. Therefore, our previously published white papers elaborated the realization of trustworthiness attributes in a supply chain and the role of trustworthiness in global value chains. These white papers [8, 9] described different aspects of supply-chain trustworthiness, i.e., organization trustworthiness, product trustworthiness, and the relation between them. These white papers also emphasized the importance of chain of trustworthiness along supply and value chains (shown in Figure 1) and introduced means to achieve it.

Figure 1: Different constellations of chain of trustworthiness along supply chains



Source: Figure 4 from whitepaper on IIoT Value Chain Security-Realizing Trustworthiness Attributes for Supply Chain Elements [8]

2. Introduction

Global supply and value chains are extensively scattered with organizations located in different parts of the world. Usually, they have different processes in place, use different technologies and have different trustworthiness targets. So, it is not trivial to achieve an end-to-end trustworthiness along the entire supply chain in such a diverse setup.

In our previous publications [8, 9], the focus had been on establishing the principles of trustworthiness by elaborating on types of trustworthiness, trustworthiness topologies, and means to exchange trustworthiness expectations and capabilities along supply and value chains.

Based on our previous research on organizational and product trustworthiness, in this publication, we concentrate on researching aspects of trustworthiness of data in value networks that comprise several heterogeneous supply and value chains.

3. Motivation

In Europe, a new regulation is being introduced, i.e., Eco-design for Sustainable Products Regulation (ESPR) [1]. This regulation introduces a digital product passport that will provide information about products' environmental sustainability. It is intended that the information will be easily accessible by scanning a data carrier, and it will include attributes such as durability, repairability, recycled content, availability of spare parts, etc. Under the ESPR, information related to products is digitalized, and the services using information about products are expected to become increasingly common in the future, such as battery's remaining value assessment services, predictive maintenance services, etc. It should help consumers and businesses to make informed choices when purchasing products, manufacturing, operation, utilization, and recycling/reuse to increase transparency about the impact of product lifecycles on the environment. The digital product passport should also help public authorities to perform checks and controls in an efficient manner [1]. In the future, following the industry 4.0 ideology, it will be more common to exchange information related to digitized products directly from machine to machine, without human intervention in supply chains, value chains, and value networks. In this context, stakeholders' need to ensure the trustworthiness of data itself are important.

Considering ESPR regulation and circular economy, we aim to analyze the trustworthiness of data (related to products) not only until the product placement on the market, but also during the product lifecycle, such as operation, utilization, recycling, and reusing, etc.

In previous publications [8, 9], we introduced the establishment of organization and product trustworthiness by exchanging trustworthiness expectations and capabilities. In this publication, we go a step deeper and examine the trustworthiness of data in value networks that comprise supply and value chains and the aspects of trustworthiness of data itself. It is essential as various sorts of data are being exchanged in supply and value chains, such as Product Carbon Footprint (PCF) values, configurations, health checks, etc., that have a certain overall impact on trustworthiness.

4. Terminologies: Trustworthiness of data for value networks

Global supply and value chains are extensively scattered with organizations located in different parts of the world. Usually, they have different processes in place, use different technologies and have different trustworthiness targets. So, it is not trivial to achieve an end-to-end trustworthiness along the entire supply chain in such a diverse setup.

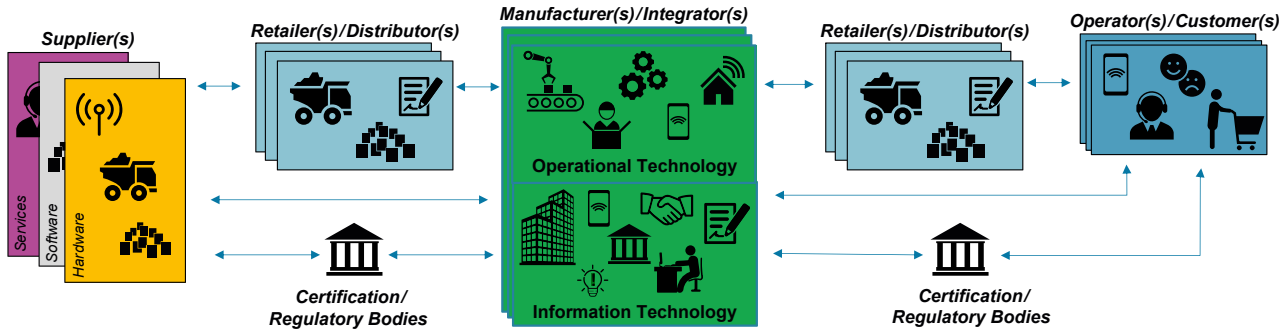
In our previous publications [8, 9], the focus had been on establishing the principles of trustworthiness by elaborating on types of trustworthiness, trustworthiness topologies, and means to exchange trustworthiness expectations and capabilities along supply and value chains.

Based on our previous research on organizational and product trustworthiness, in this publication, we concentrate on researching aspects of trustworthiness of data in value networks that comprise several heterogeneous supply and value chains.

Terminologies describing different interactions along a product lifecycle are often not understood in the same manner. Therefore, this white paper uses the following terminologies as per their standardized definitions:

- 'Supply chain' has been defined in many standards, such as ISO 18495, ISO 22095, etc. For the context of our work, we concentrate on the definition provided by ISO 28001, i.e., the supply chain is the linked set of resources and processes that upon placement of a purchase order begins with the sourcing of raw materials and extends through the manufacturing, processing, handling and delivery of goods and related services to the purchaser. (Note 1 to entry: The supply chain may include vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers, and other entities involved in the manufacturing, processing, handling and delivery of the goods and their related services.)

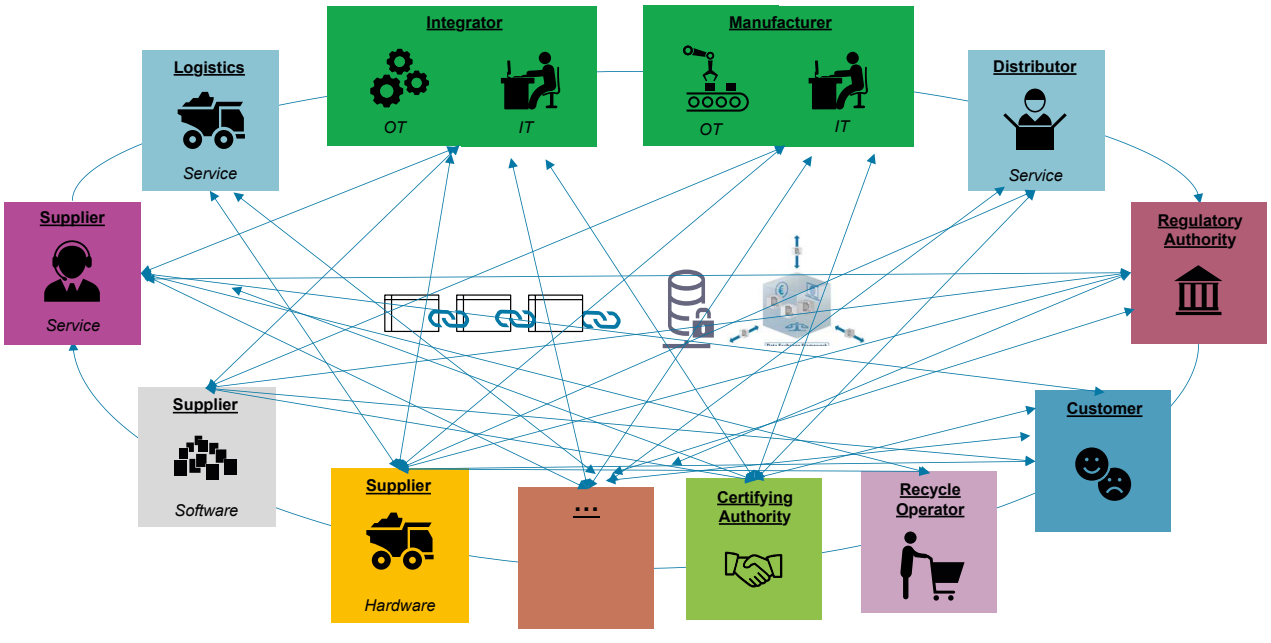
Figure 2: Example of a generic supply chain



Source: Based on Figure 1 from whitepaper on IIoT Value Chain Security - Realizing Trustworthiness Attributes for Supply Chain Elements [8]

- Likewise, 'value chain' has been defined in various standards like ISO 32210, ISO 59010, etc., we take the one defined in ISO 26000, i.e., the value chain is the entire sequence of activities or parties that provide or receive value in the form of products or services. (Note 1 to entry: Parties that provide value include suppliers, outsourced workers, contractors, and others. Note 2 to entry: Parties that receive value include customers, consumers, clients, members, and other users). A supply chain can be considered as a subset of a value chain, and the value chain means all activities and processes that are part of the product life cycle, including re-manufacturing, refurbishing, etc.

Figure 3: Example of a generic value chain

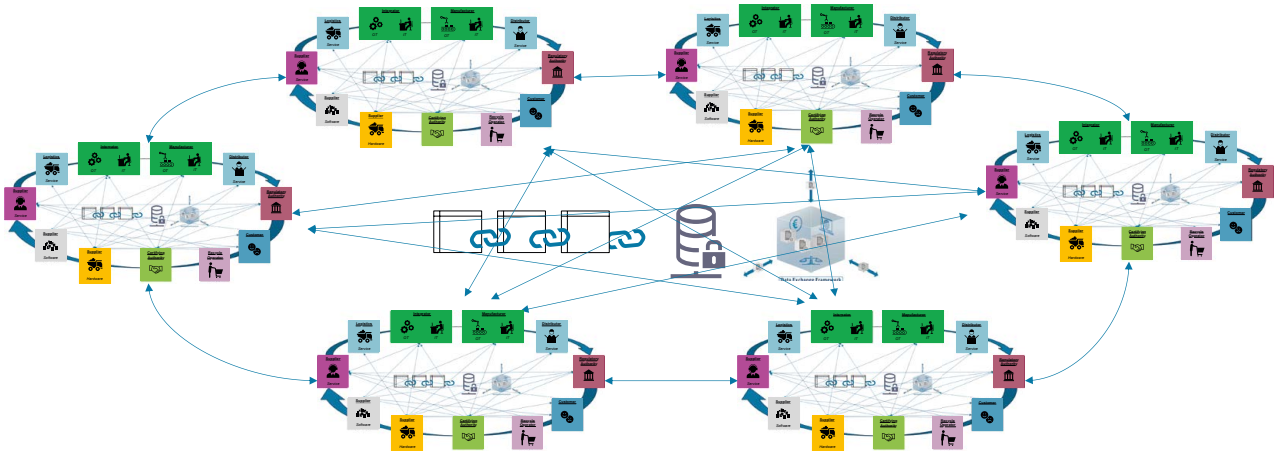


Source: Cooperation of Plattform Industrie 4.0 and RRI

- Moreover, we use the term 'value network' as defined in ISO 59010, i.e., a value network is a network of interlinked value chains and interested parties or stakeholders.

In the current global economic activities, not only the cooperation of companies, but also various value and supply chains are interlinked to promote businesses, represented by a value network. Therefore, a value network can comprise of different value and supply chains.

Figure 4: Example of a generic value network



Source: Cooperation of Plattform Industrie 4.0 and RRI

Value networks, which are connected to different supply and value chains, require common rules, protocols, and product data formats supported by the trustworthiness infrastructure.

- As per ISO/IEC 25019:23 [7], 'trustworthiness' is defined as the extent to which users and stakeholders have confidence that their expectations are met in a verifiable way. In regard to value chain and value networks, trustworthiness can have the following aspects:
  - Trustworthiness between organizations within a supply or value chain or in different supply or value chains
  - Trustworthiness of products and components
  - Trustworthiness of information/data related to components, products, and organizations. Trustworthiness of data can be understood as the extent to which a stakeholder can assure transparency regarding the implementation of data usage rights and/or obligations, and/or the traceability of the flow.
  - Trustworthiness of services, processes, and technology being leveraged by users and stakeholders
  - Trustworthiness of means of exchanging trustworthiness-relevant information within different stakeholders in supply or value chains (i.e., value network).

Our last two white papers [8, 9] focused on the first two aspects, listed above. In this white paper, we will focus on the trustworthiness of data (the last three above-mentioned aspects). Moreover, depending on the use case or business context, different attributes define trustworthiness. These attributes may include authenticity, integrity, resilience, accountability, confidentiality, privacy, safety, traceability, compliance with social regulations, conformance with applicable standards, etc.

5. Trustworthiness of data

5.1 Leveraging the trustworthiness profile for data trustworthiness

In our last two white papers [8, 9], we introduced the trustworthiness concept, which helps identify distinct trust domains along a supply or value chain. A Trust Domain (TD) can be defined as a domain with a specified authority that determines its present and targeted trustworthiness attributes for an entity or a set of entities in a supply chain, value chain or value network [9]. Once the trust domains (TDs) are identified, they can establish trustworthy interactions with one another based on the exchanged trustworthiness expectations (TWEs) and their corresponding trustworthiness capabilities (TWCs), i.e., a list of verifiable claims, in form of the trustworthiness profile (TWP) and the extended trustworthiness profile. TWP is a standardized and interoperable structure comprising of TWEs and TWCs.

In this white paper, our research focus is towards the trustworthiness of product-related data. Trustworthiness of such data can be defined as an extent to which a stakeholder can assure transparency regarding the implementation of data usage rights and/or obligations, and/or the traceability of the flow of the process, including generation, processing, and utilization of data are ensured as intended. Extending on the concept of TWP, in this white paper we propose that not only entities in the supply chain, but also entities in the value chain and value network can also communicate data-usage rights along with TWEs and TWCs. Data-usage rights can be communicated as part of the TWE or as an independent TWE. For example, the data provider can present its data usage terms and conditions as a TWE, whereas the data user can return a TWC confirming agreement to the TWE.

Since TWCs are comprised of verifiable claims corresponding to the TWE, they may include different technologies, such as unique IDs realized via secure elements, Physical Unclonable Functions (PUFs), etc., to ensure the integrity of data (e.g., by using digital signatures). Additionally, the TWCs may include rules regarding the usage of data in form of contracts and certifications.

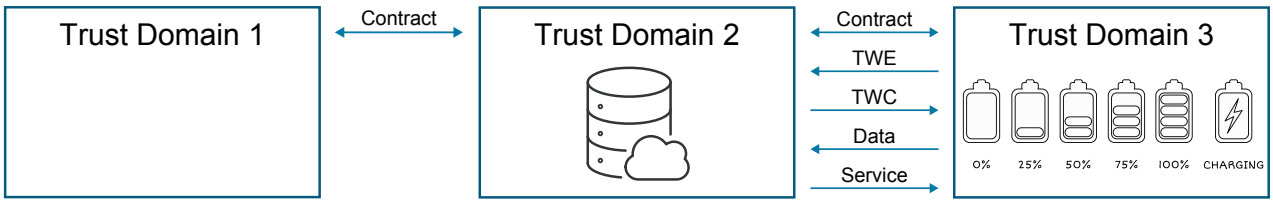
5.2 Trustworthiness of data derived from products

In value chains, or value networks, more and more services using data derived from products are being introduced. Therefore, it is important for consumers of products and the corresponding data to verify its trustworthiness and confirm the reliability of the service based on product data. In the context of this white paper, we consider the following aspects:

- Data is not always stored within the organization or products. For example, products are physically with the user, but the data is stored in the cloud, owned by another provider (Figure 5).
- Another use case is when both products and data are physically hosted by an entity other than the data or product user, and the user only receives services based on the product and its data (Figure 6).
- Data providers also need to verify data users' capabilities to meet the data providers´ trustworthiness expectations (Figure 7).
- Examples of TWE when diverse stakeholders in the value chain are involved (Figure 8).

There are some scenarios where the product is in a trust domain, while the data generated by the product is part of another trust domain. Hence, the product might have different trustworthiness attributes compared to the data generated by it. This scenario is shown in Figure 5, where the product (e.g., battery) is part of TD3 and the data generated by the product is stored in TD2 (e.g., cloud server). Since TD3 owns and manages the product, it receives the data-based services from TD2 with machine-to-machine (M2M) communication without human interruption and wants to ensure that it is trustworthy.

Figure 5: Product and corresponding data in different trust domains

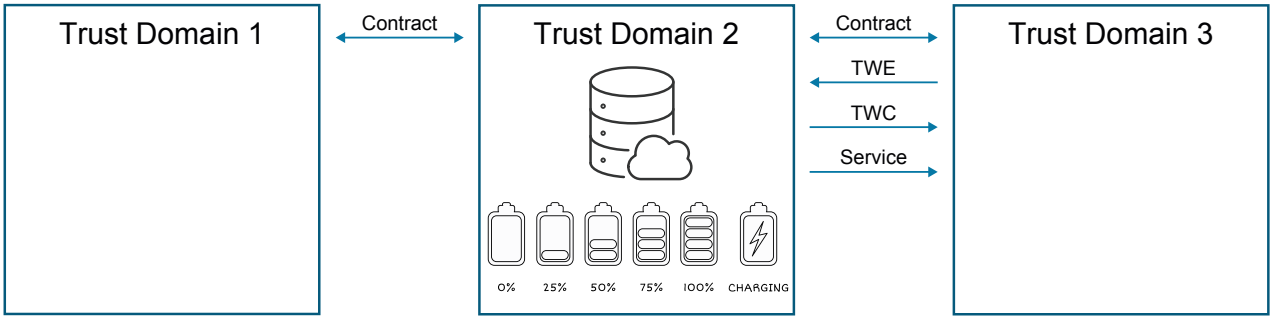


Source: Cooperation of Plattform Industrie 4.0 and RRI

In such scenarios, it is important to ensure that there is a strong, persistent binding between the product and its generated data, regardless of the trust domain it is residing in, especially to achieve greater trustworthiness. Binding between the product and its generated data can be accomplished by various mechanisms, as well as by combining various mechanisms.

Moreover, there are scenarios where the product and its data are in a TD (TD2) other than the TD (TD3) that owns the product, as shown in Figure 6. For example, there are scenarios where a machine is leased on a pay-per-use basis to another company. TD3 only receives some services based on the data produced by the product, and it needs to ensure the trustworthiness of this data.

Figure 6: Product and corresponding data in same trust domain



Source: Cooperation of Plattform Industrie 4.0 and RRI

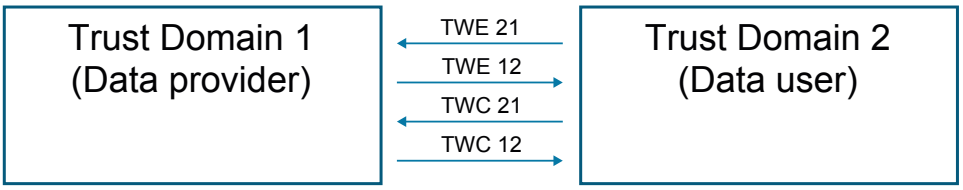
Compared to the last scenario, it is also essential to comply with TWEs with the help of contracts (guarantee that the data can be used within the described scope and confirm that the data is from the guaranteed source), and information about the manufacturer must be included. That case might often happen in the recycle and re-use phase. Stakeholders want to know the value of the products correctly based on the data derived from products. Each time the expectation (TWE) changes (operation stage, recycling state, etc.), TWC needs to be verified to adjust the TWE, and the required level of trustworthiness might differ in each phase, during its lifecycle, such as operation, utilization, recycling, and reusing, etc.

Under the current ESPR, it is asked to easily access the digitalized information about the product and its life cycle by scanning a data carrier, such as a watermark or a quick response (QR) code. However, to increase trustworthiness, persistent binding of the product information to the corresponding product shall be maintained throughout the product life cycle and can be used to verify its authenticity and reliability.

There are also some scenarios where mutual exchange of TWEs regarding the use of exchanged data is required. For example, when a data provider is asked to provide its TWCs corresponding to certain TWEs, then this data provider can also provide its TWEs first to the other entity regarding the usage of its TWCs, and it will only share its TWCs once the other data provider provides its TWCs regarding data handling.

Alternatively, the data provider creates and returns a TWC adapted to the contents of the data user's TWC. For example, if the data user's TWC indicates that the data user can keep the acquired data confidential, the data provider can provide data that it does not want to publicly display as TWC. On the other hand, if a data user needs to disclose a data provider's TWC, the data provider will provide a TWC that can be publicly disclosed.

Figure 7: Mutual exchange of trustworthiness expectations and capabilities regarding data usage

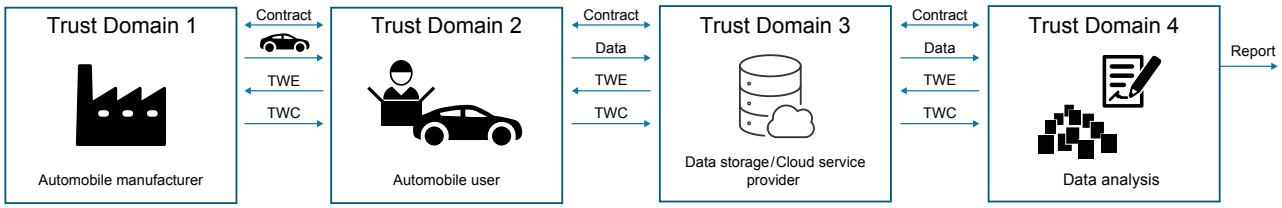


Source: Cooperation of Plattform Industrie 4.0 and RRI

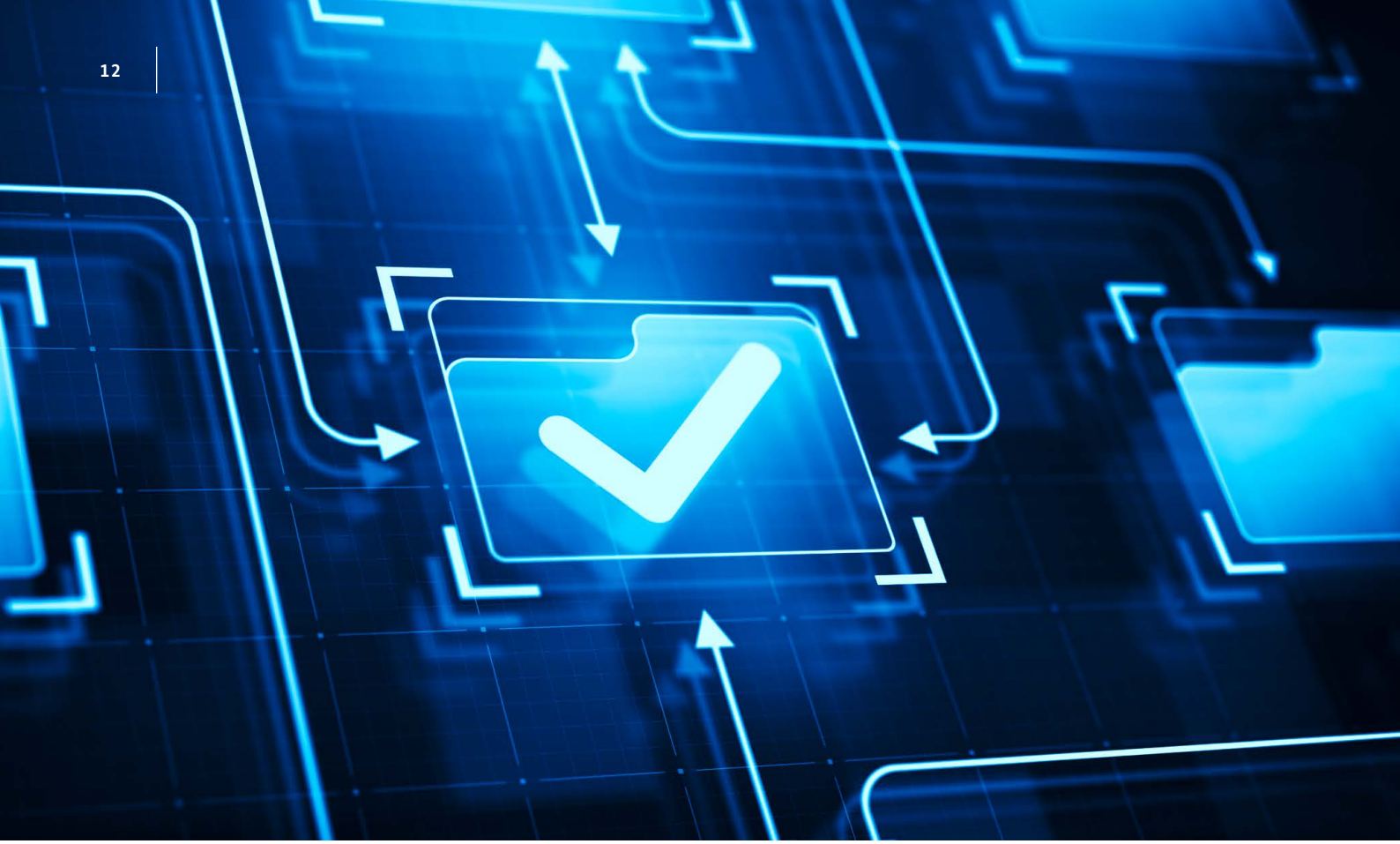
Moreover, there are some scenarios where the data is collected and exchanged along a value chain without the identification of relevant trust domains. One such use case is known for the calculation and reduction of PCF values in an automotive environment. For example, a study [6] done in Japan collected and analyzed the driving data of cars and how they are used in the market, such as the impact of usage of air conditioning, driving style, etc. As a result, it was reported that, in 2022, a reduction of 308,000 tons of CO_2 could be achieved in Japan. This was achieved using the following steps:

- Automobiles were transferred from the automobile manufacturer to the automobile user under a predetermined legal contract. The TWE of the automobile user was that the vehicle has the prescribed functions (vehicle size, fuel consumption, running, turning, stopping, etc.). The TWC provided by the manufacturer was that the vehicle was manufactured using a predetermined process (designer, manufacturer, inspector, or tool, etc.) and that the vehicle has the capability to communicate driving data to the specified cloud service provider without leakage or tampering.
- Driving data was transferred from the automobile to the specified cloud service based on a predetermined contract. The TWC of the cloud service provider was that there is no spoofing or tampering of data received from the vehicle.
- Stored driving data was transferred from the cloud service provider to the data-analysis company based on a predetermined contract. The TWE to the data-analysis company was to ensure the confidentiality, integrity, and availability of driving data during the accumulation period.
- So-called ESG reports (Environmental, Social, and Governance practices of an organization) were generated and published by the data-analysis companies without any specific contract. The TWE of the report user was that the ESG reports were derived from trustworthy information. The corresponding TWC of the data-analysis companies was that the appropriate data was analyzed using the appropriate processes.

Figure 8: Automobile use case



Source: Cooperation of Plattform Industrie 4.0 and RRI



6. Digital product passport for value network trustworthiness

In order to make trustworthy interactions in a value network, we need a common trustworthiness framework which ensures interoperability between heterogeneous systems. One such framework is introduced in ISO 22373 [2].

In Europe, a Digital Product Passport (DPP) system will introduce a regional realization of an infrastructure to support the exchange of product-related information in a value network, although it is so far limited to regulatory requirements originating from ESPR [1].

In the context of Industry 4.0, a DPP 4.0 is being developed (demonstrated by ZVEI [5]) based on the Digital Name Plate (DNP 4.0 standardized under DIN VDE V 0170-100 [3]) and the Asset Administration Shell (AAS) [4]. DPP 4.0 comprises of submodels that include information that is partially freely available (shown in green in Figure 9), and some part of that information can be accessed by authorized entities only (shown in red in Figure 9).

Figure 9: Components of a DPP 4.0 [5]

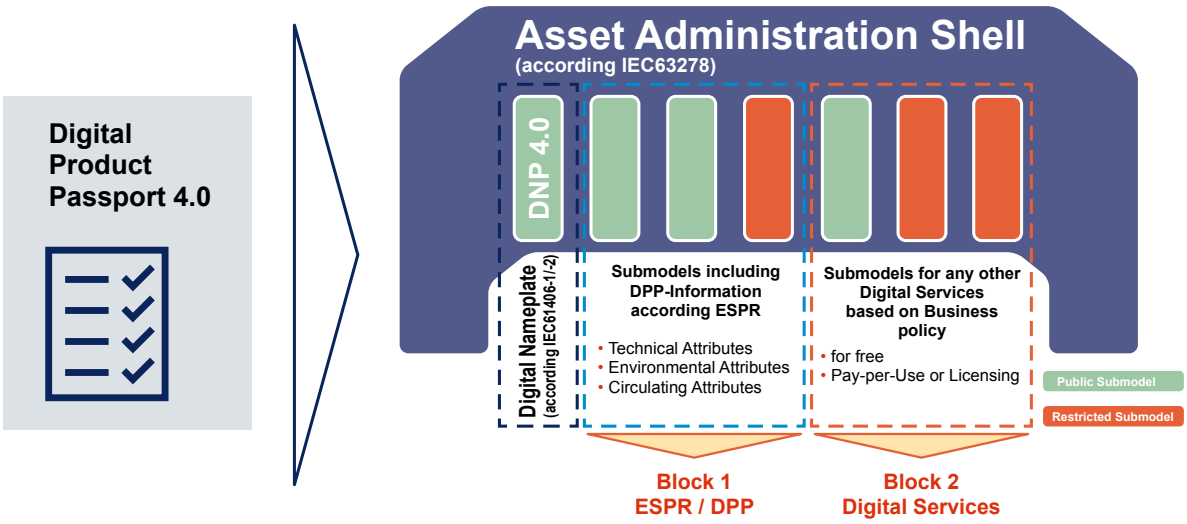


Figure 9: Source: Figure from ZVEI, DPP4.0 Big Picture [5]

A DPP is specific to a product and, hence, ideally originates from a supply chain, and it can be carried over to a value chain in a value network. To achieve trustworthiness along global value networks, a similar interoperable construct is required, and a standardized format for DPP can be a very viable option.

From a trustworthiness perspective, a DPP can contain information about a product that provides proof of its trustworthiness capabilities. Depending on the use case or business context, a product can disclose certain parts of the DPP to the required stakeholders based on their trustworthiness expectations.

ESPR [1] is going to establish a DPP that provides access to data related to a distinct product or type of product, providing relevant information to stakeholders in a value network, especially to users and regulators. If a stakeholder intends to use the DPP-based infrastructure for ensuring trustworthiness (for use cases independent of ESPR regulation as well), then, among others, the following aspects must be considered:

- Persistent binding between the product and its DPP
- Secure and reliable access control, especially for restricted information
- DPP not being a single point of failure, for example, for the manipulation or deletion of product related information
- Availability of cryptographically verifiable proofs along the whole life cycle
- Means to ensure integrity, authenticity, and accountability.

Requirements from the market that are independent of the regulatory requirements will determine the trustworthiness-related requirements that stakeholders along a value chain have to fulfill. The trustworthiness expectations of a trustworthiness profile may be determined by certain market requirements concerning a specific project. They may not be identical to the requirements derived from regulations.

7. Summary and next steps

The white paper emphasizes the importance of the trustworthiness of data for ensuring trustworthiness along supply chains, value chains, and value networks. Data, i.e., derived from products, is especially considered essential for establishing the trustworthiness of products, which is crucial for conformance to upcoming regulations as well, such as ESPR. The white paper also establishes a common understanding of trustworthiness-related terminologies in supply chains, value chains, and value networks. Finally, the white paper focuses on different aspects of data usage that can have different trustworthiness expectations and corresponding capabilities.

In the future, we intend to go deeper into the realization of specific aspects of data trustworthiness, such as exploring means to ensure persistent and reliable binding between a product and its data, etc. Additionally, use cases will be considered to analyze scenarios based TWEs and TWCs, especially regarding the trustworthiness of data from a value-network perspective.

8. References

[1] European Commission, Ecodesign for Sustainable Products Regulation, https://commission.europa.eu/energy-climate-change-environment/standards-tools-and-labels/products-labelling-rules-and-requirements/sustainable-products/ecodesign-sustainable-products-regulation_en (accessed 2024-02)

[2] ISO/TC 292 Online, ISO 22373 Security and resilience – Authenticity, integrity and trust for products and documents – Framework for establishing trustworthy supply chains, https://www.isotc292online.org/projects/iso-22373/ (accessed 2024-02)

[3] VDE Verlag GmbH, DIN VDE V 0170-100 VDE V 0170-100:2021-02, Digital name plate, Part 100: Digital product marking, https://www.vde-verlag.de/standards/0100615/din-vde-v-0170-100-vde-v-0170-100-2021-02.html (accessed 2024-02)

[4] IEC TC65, Industrial-process measurement, control and automation, https://www.iec.ch/dyn/www/f?p=103:14:608079278865292::::FSP_ORG_ID:25623 (accessed 2024-02)

[5] ZVEI, DPP4.0 Big Picture, https://www.zvei.org/fileadmin/user_upload/Themen/Industrie/Fachverband_Automation/2023-09-15_IDTA_AAS_Tech_Days_DPP4.0_Wegener.pdf (accessed 2024-02)

[6] Toyota Motor Corporation, Sustainability Data Book, p.24, https://global.toyota/pages/global_toyota/sustainability/report/sdb/sdb23_en.pdf (accessed 2024-02)

[7] ISO/IEC 25019:2023(en), Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Quality-in-use model, https://www.iso.org/obp/ui/en/#iso:std:iso-iec:25019:ed-1:v1:en (accessed 2024-02)

[8] Plattform Industrie 4.0, Germany, and Robot Revolution & Industrial IoT Initiative (RRI), IIoT Value Chain Security – Realizing Trustworthiness Attributes for Supply Chain Elements, https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security3.html (accessed 2024-02)

[9] Plattform Industrie 4.0, Germany, and Robot Revolution & Industrial IoT Initiative (RRI), Japan, IIoT Value Chain Security – The Role of Trustworthiness, https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/IIoT_Value_Chain_Security.pdf?__blob=publicationFile&v=9 (accessed 2024-02)

LIST OF PARTICIPANTS

Atsushi Kitamura (Mitsubishi Electric Corporation) | Ayaji Furukawa (Toshiba Corporation) | Fumikado Anzai (Mitsubishi Heavy Industries, Ltd.) | Hirozumi Eki, Junya Fujita (Hitachi Ltd.) | Kumiko Mahara (Sony Semiconductor Solutions Corporation) | Nobuaki Suzuki (Toshiba Corporation) | Dr. Satoshi Kai (Hitachi Ltd.) | Dr. Takashi Ogura (Hitachi Ltd.) | Prof. Tsutomu Matsumoto (Yokohama National University) | Takeshi Kawabata (Toshiba Corporation) | Yoshitaka Kumagai (Robot Revolution & Industrial IoT Initiative) | Aliza Maftun (Siemens AG) | Björn Flubacher (BSI) | Dr. Christian Krug (VDI) | Dr. Detlef Houdeau (Infineon) | Detlef Tenhagen (HARTING) | Jan de Meer (HTW Berlin) | Prof. Kai Rannenberg (Goethe University Frankfurt) | Dr. Lutz Jänicke (Phoenix Contact) | Dr. Marvin Böll (DKE) | Michael Jochem (Bosch) | Thomas Walloschke (secon) | Vanessa Bellinghausen (BSI) | Dr. Wolfgang Klasen (Siemens AG)

A discussion paper by the Action Group “Industrial Security” of Robot Revolution & Industrial Initiative and the Working Group “Security of networked Systems” of the Plattform Industrie 4.0

www.plattform-i40.de