rri



PLATTFORM INDUSTRIE 4.0

Trustworthiness and Security

Challenges and Opportunities for Product Related Data in the Age of AI

Takeshi Kawabata (Toshiba)
Robot Revolution & Industrial IoT Initiative, Japan

Dr. Wolfgang Klasen
German Platform Industry 4.0, Germany

Background and Introduction

Plattform Industrie 4.0, Germany, and Robot Revolution & Industrial IoT Initiative (RRI), Japan, have been successfully collaborating since 2017 on topics concerning security of Industrial IoT (IIoT) and establishing trustworthy relationships between value chain stakeholders, regardless of their business histories or geographical locations.



(March 2025)



(March 2017)



(May 2018)



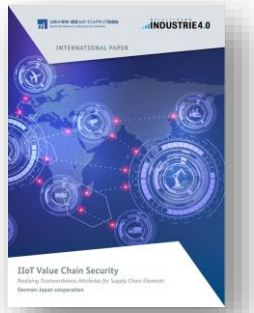
(April 2019)



(Sept. 2020)



(April 2022)



(April 2023)



(April 2024)

Available at Plattform Industrie 4.0 - Downloads & Aktuelles (plattform-i40.de)

Product-Related Data and the Digital Product Passport

PRD is information, the DPP provides structured access to selected PRD

Product Related Data (PRD)

Data associated with products that are generated and supplied within a supply chain and used throughout the value chain.

- Data on reusability and environmental impact
- Data on product composition, including the presence of hazardous substances
- Data generated or updated during product manufacturing or operation

Digital Product Passport (DPP)

A structured digital mechanism for providing access to selected product-related data throughout the product lifecycle.

- Links a physical product to its digital information
- Makes selected PRD accessible to relevant stakeholders

https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/2025-i40-trustworthiness-of-data.pdf?__blob=publicationFile&v=1

TRUSTWORTHINESS CONCEPT ENSURING TRUSTWORTHINESS OF PRODUCT RELATED DATA IN A VALUE CHAIN

Selected PRD is made accessible through the DPP

Outline

Part 1: Extending PRD Trustworthiness to AI Runtime Processing

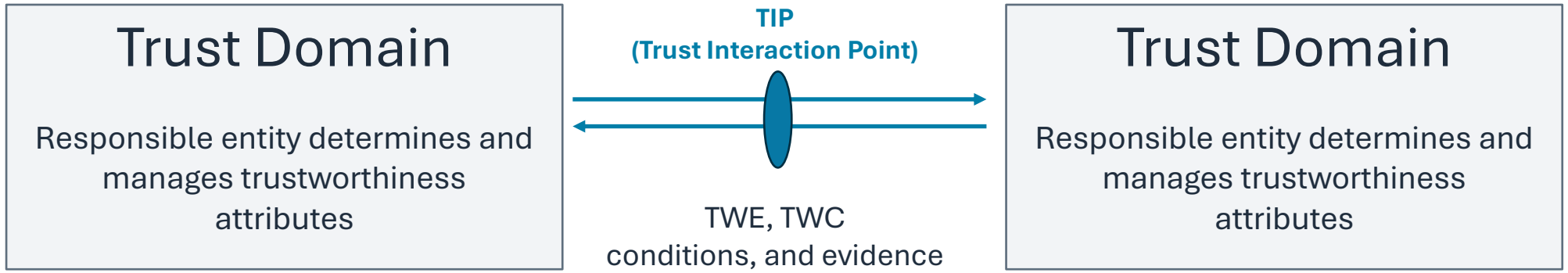
Runtime verification, controlled delegation, and accountability

Part 2: New European Standards for Secure and Trustworthy DPP Data

EN 18239 and EN 18246

Previous Discussion:
Verification of PRD Trustworthiness Across Trust Domains

Review of the Existing Framework Based on ISO 22373



Product-Related Data (PRD)
Trustworthiness must be verified when PRD is exchanged between stakeholders

Assumption

Key expectations and capabilities are established before or at the start of the interaction.

Runtime data may change within the agreed governance scope.

ISO 22373:2025
Security and resilience — Authenticity, integrity and trust for products and documents — Framework for establishing trustworthy supply and value chains

Use Case:
From Manufacturing PRD to In-Service PRD

AI-Based Predictive Maintenance for Industrial Batteries

Previous Focus

PRD at manufacturing and shipment
- Manufacturing-related CO_2 emissions
- Material and manufacturing info.

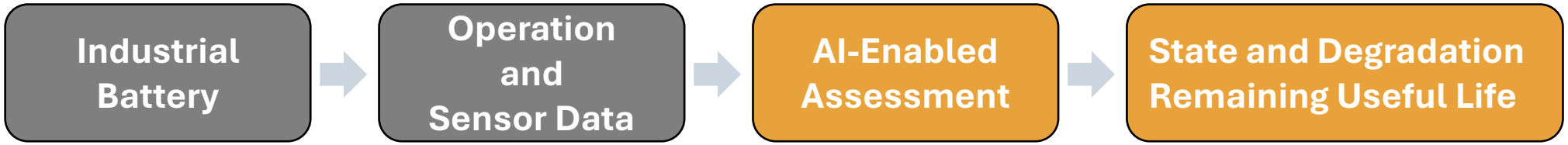
Relatively fixed generation process

Focus of This Presentation

PRD updated during operation
- State and degradation level
- Remaining useful life

Process determined and changed at runtime

"How much longer can this battery be used safely?"



Focus: AI **generates and updates new PRD** during the post-shipment operational phase

What Changes When AI Handles PRD?

The key change is not the use of AI itself, but runtime selection and adaptation.

Predefined and Agreed Process

- Data sources are determined in advance
- Assessment logic is determined in advance
- Processing path is known
- Providers and accountability are clear
- Conditions can be agreed in advance

Dynamic Process Involving AI Agents

- Available data may change
- A model may be selected at runtime
- External tools may be used
- Tasks may be delegated
- The actual process is determined during execution

The challenge is not simply the use of AI, but that **the actual process may be determined or changed at runtime.**

The Gap:
Agreed Conditions vs. the Actual Process

The central question is whether the actual execution remains within the agreed scope.

Agreed Operational Scope

- Supported battery types
- Required data and sensor quality
- Permitted diagnostic purposes
- Conditions for using models and tools
- Criteria requiring human approval
- Evidence requirements



Compare actual execution with agreed conditions

Actual Runtime Process

- Data actually available
- Model actually selected
- Tools actually used
- Actual delegation path
- Result and uncertainty

How can we verify that the actual execution remains within the agreed conditions?

Runtime Verification Against Pre-Agreed Conditions

PLATTFORM INDUSTRIE 4.0

1

Agreement

Define the operational scope

- Purpose
- Conditions
- Limits
- Required evidence

Onboarding

2

Observation

Record actual execution

- Data
- Model and tools
- Delegation
- Result and uncertainty

Runtime

3

Verification and Decision

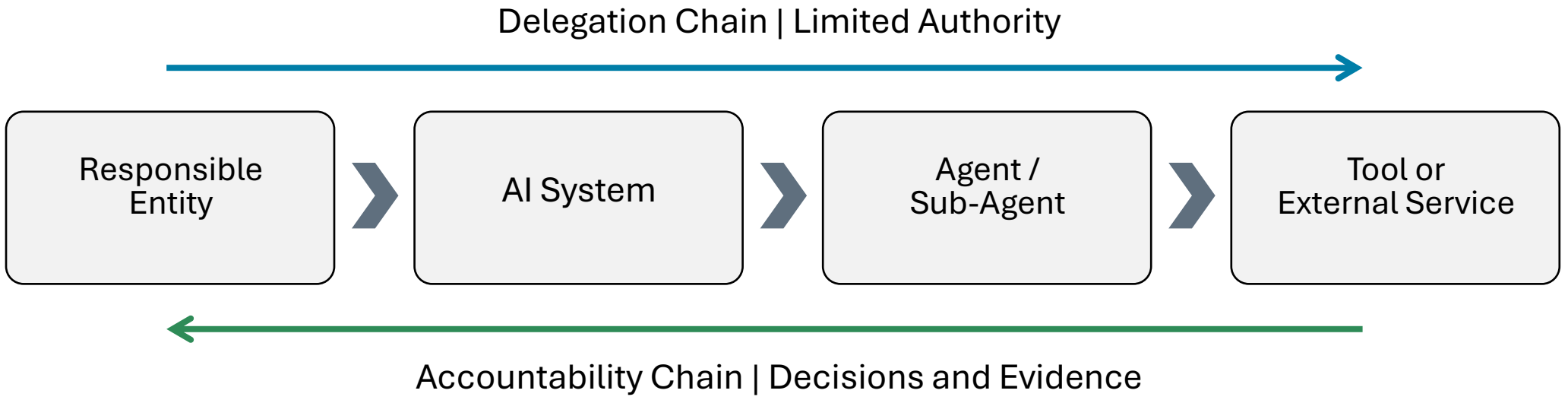
Compare and decide

- Continue
- Constrain
- Request approval
- Stop

Runtime

Establish the baseline during onboarding and verify execution at runtime

Delegating Tasks While Maintaining Accountability



Authority

assigned task, permitted data, permitted models and tools, limits on re-delegation

Evidence

actual data, models and tools, delegation path, results, uncertainty, and escalation

Task execution may be delegated, but accountability must remain traceable to the responsible entity.

Recap so far:
Extending PRD Trustworthiness to Runtime

The existing framework (ISO 22373) remains essential, with runtime verification and traceability added.

What Remains Essential

- TWE and TWC
- Agreed purposes and conditions
- Responsible entity
- Required evidence

What the Runtime Extension Must Address

- Actual data, models, and tools
- Actual delegation path
- Comparison with agreed conditions
- Traceability to the responsible entity

Establish the trustworthiness baseline during onboarding, then compare and verify actual AI processing against it at runtime.

Outline

Part 1: Extending PRD Trustworthiness to AI Runtime Processing

Runtime verification, controlled delegation, and accountability

Part 2: New European Standards for Secure and Trustworthy DPP Data

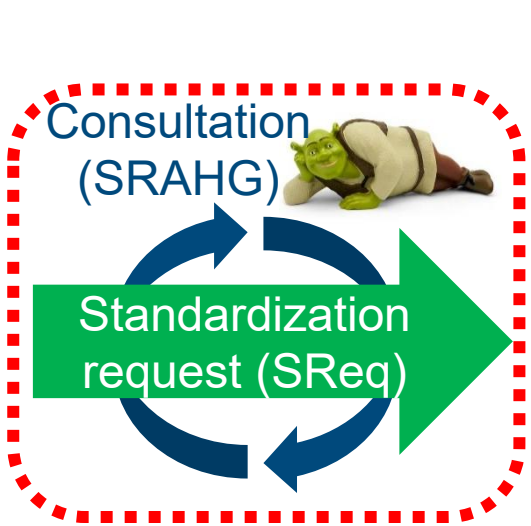
EN 18239 and EN 18246

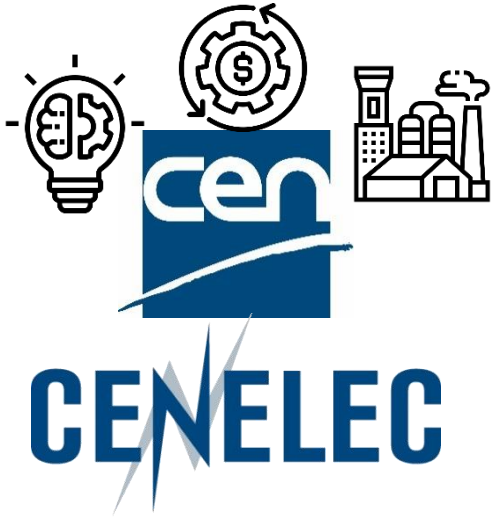
The „Digital Product Passport“
DPP Standardisation is a Public Private Partnership in Europe

PLATTFORM INDUSTRIE4.0



ESPR





ESPR = Ecodesign for Sustainable Products Regulation 2024/1781



Presumption of conformity

Harmonized standard



European Standard (EN)

The 8 DPP standards modular and interlinked

PLATTFORM INDUSTRIE 4.0

CEN CENELEC

EN 18239 Access rights mgt, information, system security, and business confidentiality

EN 18219 Unique identifiers

01234

Access Rights

Key Reference

EN 18222 API for the DPP lifecycle management and searchability

EN 18216 Data processing, data exchange protocols and data formats

EN 18246 Data authentication, reliability, integrity

EN 18220 Data carriers and links between physical product and digital representation

NFC

EN 18221 Data storage, archiving, and data persistence

Pre-requisite for data exchange and processes over internet

Data Carrier security

DPP System Terminology, Core Data model

EN 18223 Interoperability

The standards on DPP Security published by CEN/CENELEC JTC 24

PLATTFORM INDUSTRIE 4.0

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

Digital Product Passport - Access rights management, information system security, and business confidentiality

Passeport numérique des produits - Gestion des droits d'accès, sécurité du système d'information et confidentialité des affaires

Digitaler Produktpass - Management der Benutzerrechte, IT-Sicherheit und Geschäftsgeheimnisse

Digital product passport - Data authentication, reliability and integrity

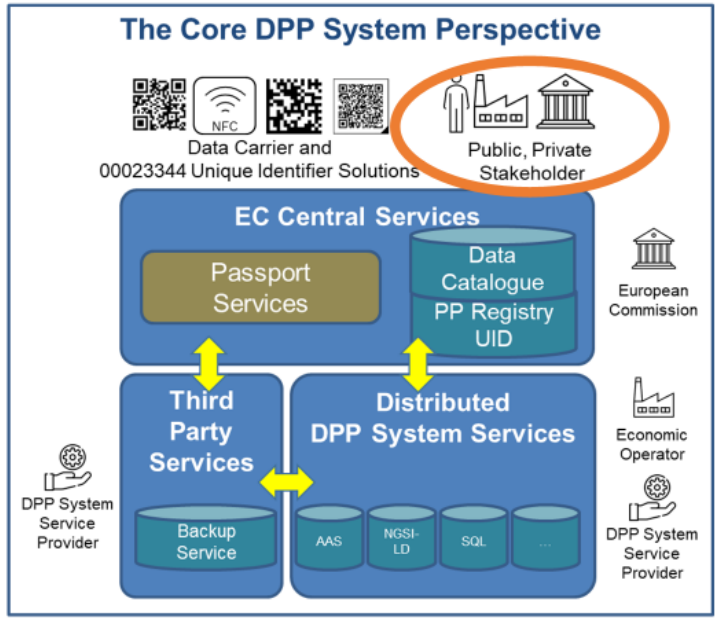
Passeport numérique des produits - Authentification, fiabilité et intégrité des données

Digitaler Produktpass - Datenauthentifizierung, Zuverlässigkeit und Integrität

General remarks on EN 18239:2026 and EN 18246:2026

- Both standards support the requirements of the European **Ecodesign for Sustainable Products Regulation 2024/1781, the so-called ESPR**. The basic terms and definitions are aligned with the other EU DPP standards
- An important basic principle of the Digital Product Passport is the **distinction between public and controlled data**
- **Public data should be freely accessible to consumers. Controlled data, on the other hand, may only be viewed by authorized actors**
- At the same time, **access to public information must not be made unnecessarily difficult** by security mechanisms. Consumers should be able to access freely available information as easily as possible.
- Central role is played by the so-called **Economic Operator (EO).** This includes manufacturers, importers, dealers, authorized representatives and other authorized actors. The Economic Operator provides the DPP data for the products for which it is responsible.

EN 18239 Access Rights Management



- Introduction into the Business transactions and responsibilities relevant for DPP
- Based on product lifecycle and business roles, requirements for DPP access rights management, information system security and business confidentiality are defined.
- Requirements on system and service resilience (e.g. Access revoking policy or Recovery capability)
- Globally unique operator identifier shall be used for authentication and access control to "controlled data".

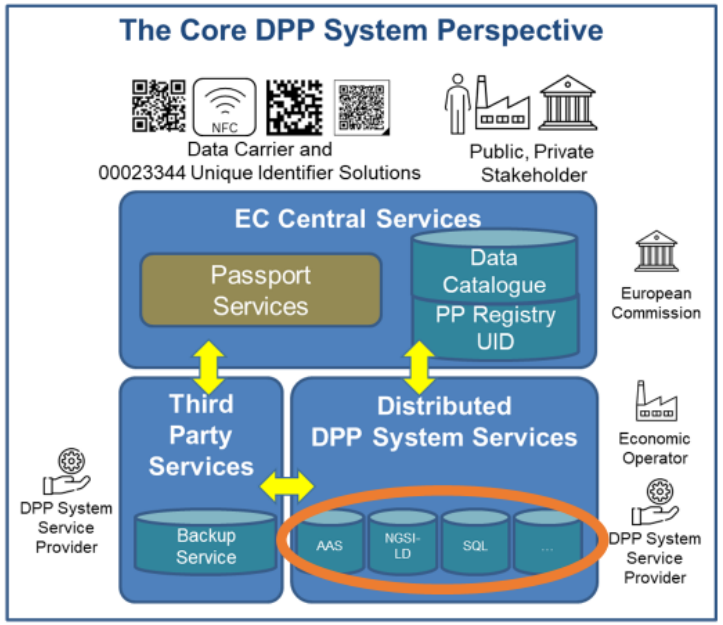
© CEN-CENELEC 2026

EN 18239:2026 Digital Product Passport

— access rights management, information system security, and business confidentiality

- EN 18239:2026 deals with access control, confidentiality and protection of business-relevant information.
- This standards defines security **requirements for the handling of controlled DPP data**. The description is technology-agnostic. The standard therefore does not prescribe any specific procedures.
- The DPP system must ensure that organizations, people, machines, and digital services **have recognized identities**. This is the only way to reliably determine who is allowed to access certain data and who can make changes
- Anyone who accesses or manages protected data must be **clearly identifiable**. Actions must be attributable to a responsible party.
- **The standard demand mechanisms against the deniability of actions: anyone who has made a change to controlled DPP data must not be able to credibly deny this action later**.
- Actual roles and access rights are not defined by this standard. **They will be defined on product group basis, e.g., by additional regulatory requirements. EOs may assign additional authorizations to their data.**
- **Other aspects** of EN 18239 are: general IT/Cybersecurity, protection of trade secrets, the resilience of the DPP system, the availability of services, implementation of security-by-design and continuous improvement.
- For security and key management orientation to EN ISO/IEC 27001:2023 is required.

EN 18246 Data authentication, reliability and integrity



- General security assumptions for DPP Data carrier authenticity
- Types of risk and requirements for unique product identifiers, data carriers and DPP Data
- Specific approaches and standards that can be used to implement electronically signed data constructs (ESDC)
- Addresses Quishing topic (i.e.; QR-code Phishing)
- Security measures shall not prevent access to DPP public data without additional software

© CEN-CENELEC 2026

EN 18246:2026 Digital product passport - Data authentication, reliability and integrity

- EN 18246: 2026 deals with the question of **how trust in the data itself can be created**.
- The standard defines requirements and framework conditions for secure information processing and communication to ensure integrity, authenticity and reliability in the DPP data exchange.
- The concept of the **“Electronic Signed Data Construct” (ESDC)** is defined: it is a structured data set with components such as headers, user data, signature and optional additional information. ESDCs create a general foundation for trustworthy and verifiable digital product information suitable for environments with many participants and different domains.
- The standard also **analyzes various risk areas**, including personal data, the security of organizational data, the avoidance of profiling, the protection of user access and **protection against phishing, quishing, malware, and risks from mass data extraction**.
- Other **requirements concern the identification of responsible actors and their traceability**. Measures against product counterfeiting and manipulation of DPP data are also addressed.
- The use of public DPP data must be possible with common consumer devices and must not exclude people with disabilities. This takes into account not only security, but also digital participation.
- The appendix to 18246 describes various approaches to the implementation of ESDCs, including ISO 22376, ISO/IEC 20248, W3C Verifiable Credentials and various ETSI standards for digital signatures.

Concluding EN 18239:2026 and EN 18246:2026

- Together they form the **security-related foundation of the Digital Product Passport** and were developed to support the requirements of the European ESPR regulation and to create trust in digital product information.
- EN 18239:2026 focuses on access control, confidentiality, role and authorization management as well as organizational and technical security measures.
- EN 18246:2026 addresses integrity, authenticity, reliability and the trustworthy verification of DPP data.
- Both standards take a **deliberately technology-open approach**. They define requirements without prescribing specific algorithms or safety mechanisms. This allows to remain flexible for different industries and future technical developments.
- It is obvious, that **further specifications on security mechanisms, governance structures and interoperability will be necessary**. These are expected to be provided in supplementary documents or regulatory requirements.
- The two standards thus represent an **important milestone** on the way to a secure, trustworthy digital product passport.

Important open issues for Security and Trustworthiness of Product Related Data (PRD)

- **Asset binding** of PRD will be of increasing importance to prevent misuse of PRDs
- How can a common **globally accepted** (distributed?) **governance architecture** be established?
- High **Resilience** to ensure continuous availability of PRD across the value chain
- **Challenges imposed by AI:**
  What additional considerations are needed when AI becomes involved in value chains?
  - When value-chain stakeholders use AI systems and AI agents to generate, process, exchange, and verify PRD, **are conventional approaches to ensuring data trustworthiness still sufficient**?
  - How can Security & Trustworthiness handle the ultra rapid changes in capability and quality of AI?
  - Can **agentic AI** securely use globally accepted identities?
- .....

  We will continue this discussion toward Hannover Messe, April 2027



Thank you very much

Contact Information:

Mr. Takeshi Kawabata

Toshiba Corp.

takeshi.kawabata.x44@mail.toshiba

Dr. Wolfgang Klasen

Senior Advisor Security -
External service provider at Siemens AG

wolfgang.klasen.ext@siemens.com