



Brussels, 31.7.2024
C(2024) 5423 final

ANNEXES 1 to 2

ANNEXES

to the

COMMISSION IMPLEMENTING DECISION

on a standardisation request to the European Committee for Standardisation, the European Committee for Electrotechnical Standardisation, and the European Telecommunications Standards Institute as regards digital product passports in support of Union policy on ecodesign requirements for sustainable products and on batteries and waste batteries

ANNEX I
List of European standards to be drafted and deadlines for their adoption as referred to in Article 1

Reference information		Deadline for the adoption by the ESOs
1.	European standard(s) on unique identifiers	31 December 2025
2.	European standard(s) on data carriers and links between physical product and digital representation	31 December 2025
3.	European standard(s) on access rights management, information, system security, and business confidentiality	31 December 2025
4.	European standard(s) on interoperability (technical, semantic, organisation)	31 December 2025
5.	European standard(s) on data processing, data exchange protocols and data formats	31 December 2025
6.	European standard(s) on data storage, archiving, and data persistence	31 December 2025
7.	European standard(s) on data authentication, reliability, integrity	31 December 2025
8.	European standards on Application Programming Interfaces (APIs) for the product passport lifecycle management and searchability	31 December 2025

ANNEX II
Requirements for the standards referred to in Article 1

PART A. GENERAL REQUIREMENTS FOR STANDARDS LISTED IN ANNEX I

1. Definitions and general technical requirements to be supported by the standards
- 1.1. For the purpose of this Annex, the following definitions apply:
 - (1) ‘Product’ means any physical good that is placed on the market or put into service.
 - (2) ‘Model’ means a version of a product of which all units share the same technical characteristics and the same model identifier.
 - (3) ‘Batch’ means a subset of a specific model composed of all products produced in a specific manufacturing plant at a specific moment in time.
 - (4) ‘Item’ means a single unit of a model.
 - (5) ‘Manufacturer’ means any natural or legal person who manufactures a product or who has such a product designed or manufactured and markets that product under its name or trademark or, in the absence of such person, any natural or legal person who places on the market or puts into service a product.
 - (6) ‘Upgrading’ means enhancing the functionality, performance, capacity, or aesthetics of a product.
 - (7) ‘Refurbishment’ means preparing or modifying an object that is waste or a product to restore its performance or functionality within the intended use, range of performance and maintenance originally conceived at the design stage, or to meet applicable technical standards or regulatory requirements, with the result of making a fully functional product.
 - (8) ‘Maintenance’ means an action carried out to keep a product in a condition where it is able to function as required.
 - (9) ‘Repair’ means returning a defective product or waste to a condition where it fulfils its intended use.
 - (10) ‘Data carrier’ means a linear bar code symbol, a two-dimensional symbol or other automatic identification data capture medium that can be read by a device.
 - (11) ‘Unique product identifier’ means a unique string of characters for the identification of products that also enables a web link to the product passport.
 - (12) ‘Unique operator identifier’ means a unique string of characters for the identification of actors involved in the value chain of products.
 - (13) ‘Unique facility identifier’ means a unique string of characters for the identification of locations or buildings involved in the value chain of a product or used by actors involved in the value chain of a product.

- (14) ‘Processing’ means processing as defined in Article 3, point (2), of Regulation (EU) 2018/1807 of the European Parliament and of the Council¹.
 - (15) ‘DPP-system’ means the set of IT standards and protocols required to ensure the full interoperability of product passports and compliance with the requirements referred to in point 2.1.
 - (16) ‘DPP-data’ means the information included in a product passport and accessible to different users based on their own respective access rights.
 - (17) ‘Decentralised identifier’ means a globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically.
- 1.2. The standards to be developed shall reflect the generally acknowledged state of art and be technology-neutral and take into account to the extent possible the energy use and energy efficiency of the DPP-system.
 - 1.3. The standards shall be rooted in existing mature international standards while at the same time taking into consideration new and innovative approaches, provided that a full cross-sectoral interoperability can be guaranteed. In particular, ISO/IEC standards shall be considered first and if necessary, complemented by existing European standards, national standards and fora standards (in this order). A landscape analysis of existing standards to be used for product passport has already been carried out and the results are available at: <https://www.standict.eu/landscape-analysis-report/landscape-digital-product-passport-standards>.
2. Legal requirements
 - 2.1. The standards shall support the application of the following requirements:
 - (a) The product passport shall be connected through a data carrier to a persistent unique product identifier;
 - (b) all information included in the product passport shall be based on open standards, developed with an inter-operable format and shall be, as appropriate, machine-readable, structured, and searchable, and transferrable through an open interoperable data exchange network without vendor lock-in;
 - (c) product passports shall be fully interoperable with other digital product passports required by Union law in relation to the technical, semantic and organisational aspects of end-to-end communication and data transfer;
 - (d) the access to information included in the product passport shall take place in accordance with the specific access rights at product group level identified in applicable Union law;
 - (e) customers, end-users, manufacturers, importers and distributors, dealers, professional repairers, refurbishers, remanufacturers, recyclers, market surveillance authorities and customs authorities, civil society organisations, trade unions consumers, economic operators and other relevant actors shall have free of charge and easy access to the product passport based on their respective access rights set out in applicable Union law;

¹ Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (OJ L 303, 28.11.2018, p. 59, ELI: <http://data.europa.eu/eli/reg/2018/1807/oj>).

- (f) the data included in the product passports shall be stored by the economic operator responsible for its creation or by operators authorised to act on their behalf;
 - (g) if the data included in the product passports is stored or otherwise processed by operators authorised to act on behalf of the economic operator responsible for the creation of the passport, operators shall not be allowed to sell, re-use or process such data, in whole or in part, beyond what is necessary for the provision of the relevant storing or processing services, unless specifically agreed with the economic operator placing the product on the market or putting it into service;
 - (h) the product passport shall remain available including after an insolvency, a liquidation or a cessation of activity in the Union of the economic operator that created the product passport;
 - (i) the rights to access, introduce, modify or update information in the battery passport shall be restricted based on the access rights specified in applicable Union law;
 - (j) data authentication, reliability and integrity shall be ensured;
 - (k) product passports shall be designed and operated so that a high level of security and privacy is ensured and fraud is avoided.
- 2.2. The requirements referred to in point 2.1 shall be taken into account from the beginning and throughout the entire process of developing the standards.
- 2.3. The standards shall not support any other legal requirements than the requirements referred to in point 2.1.
- 2.4. The structure of the standards shall be such that a clear distinction can be made between those clauses and sub-clauses of the standards which are necessary to be applied in order to support the requirements referred to in point 2.1 and those which are not. Clauses or sub-clauses which are not necessary shall not compromise or endanger conformity with the requirements referred to in 2.1.
- 2.5. The standards shall follow the principles laid down in the Union legal framework in the area of cybersecurity, processing of personal data and protection of privacy or networks. Coherence among mechanisms established in that Union legislation shall be ensured. Where applicable cybersecurity certification schemes under Regulation (EU) 2019/881 of the European Parliament and of the Council² are adopted, the standards shall be developed in a manner coherent with the relevant content of those schemes.
- 2.6. The standards shall rely, as relevant, on existing similar or equivalent approaches already used in Union legislation.
- 2.7. Each standard developed on the basis of the request referred to in Article 1 shall refer to this Decision.

² Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15, ELI: <http://data.europa.eu/eli/reg/2019/881/oj>).

- 2.8. A standard shall not make conformity with that standard dependent on requirements of administrative or organisational nature like management system requirements for organisations, competence requirement for natural persons or through normative references to management system standards of any kind.
- 2.9. To reduce dependencies between the elements in the set of standards listed in Annex I (the ‘modules’), the standardisation work shall be organized in a modular way to ensure interoperability, reduce lock-in effects, and enable parallel standardisation work. The standards shall be written as formalised avoiding different interpretations.
- 2.10. The interfaces between the eight modules shall be presented in a meta-structure to ensure the possibility that different standards fulfilling the same function can be used and that the change of a standard within one module does not make it necessary to lead change other modules.

PART B. SPECIFIC REQUIREMENTS FOR THE STANDARDS LISTED IN ANNEX I

1. Standard(s) on unique identifiers
 - 1.1. The standard(s) shall define requirements related to the following areas:
 - (1) uniqueness of each identifier (i.e., the same identifier shall not be assigned to different products, different economic operators or different facilities);
 - (2) syntax-related requirements;
 - (3) semantic-related requirements.
 - 1.2. The standards shall consider the diversity of identifiers currently used by economic operators and accommodate them as much as possible.
 - 1.3. The standard(s) shall allow the possibility to use both ‘centralised’ and ‘decentralised’ identifiers, including the definition of conformance criteria if different methods to produce an identifier are allowed.
 - 1.4. The unique product identifier shall always allow the possibility to include the three different granularity levels, i.e. model, batch, or item. This is needed because product passports of products sold online will only be available at model level, while product passports may need to be available at batch level with the possibility for economic operators to serialise their product passports having a product passport at item level. The move from batch to item level will also be necessary for product groups for which updates of product passports will be expected, for example due to repair activities. In addition, in some cases, for instance batteries covered by Regulation (EU) 2023/1542, the granularity level for the product passport is at item level.
 - 1.5. The standard(s) developed shall adequately take into account typology of identifiers already used in other Union legislations and initiatives.
 - 1.6. Existing relevant standards shall be duly considered when drafting the new European standard(s). A non-exhaustive list is provided below:
 - ISO/IEC 15459: Automatic identification and data capture techniques – Unique identification
 - ISO/IEC 61406: Identification Link
 - ISO/IEC 29161: Information technology - Data structure - Unique identification for the Internet of Things

- ISO/IEC 15418: Information technology - Automatic identification and data capture techniques - GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance
- ISO/IEC 9834-8:2004: (and RFC 4122): Procedures for generation and registration of Universally Unique Identifiers (UUIDs)
- ISO 17442: Financial services - Legal Entity Identifier (LEI)
- ISO/TR 23249: Blockchain and distributed ledger technologies - Overview of existing DLT systems for identity manage
- ISO/TR 6039: Blockchain and distributed ledger technologies - Identifiers of subjects and objects for the design of blockchain systems
- ISO 22383: Guidelines for selection and performance evaluation of authentication solutions for material goods
- ISO 22385: Guidelines for establishing a Framework for Trust and Interoperability
- ISO 22387: Confirmation procedures for the application of artefact metrics
- ISO 22376: Electronic Storage Specifications for use of Visible Digital Seal (VDS) for the authentication, verification and acquisition of data carried by a document or object
- ISO 22372: Framework for establishing trustworthy supply chains
- ISO/IEC 19762: Information technology - Automatic identification and data capture (AIDC) techniques - Harmonized vocabulary
- ITU-T X.1403: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY – Secure applications and services (2) – Distributed ledger technology security
- W3C on DIDs (available at: <https://www.w3.org/TR/did-core/>)
- W3C on verifiable credentials (available at: <https://www.w3.org/TR/vc-data-model/>)
- EN IEC 63365: Digital Nameplate – Digital Product Marking
- ISO/IEC 20248: Information technology - Automatic identification and data capture techniques – Digital signature data structure schema
- ISO/IEC 19845:2015 : Universal Business Language (UBL) v2.1
- EN 16931-1, -3-2, -3-3 : Electronic invoicing – Part 1 Semantic model of core elements, Part 2-3 UBL profile, Part 3-3 CII profile
- ISO 22378: Guidelines for establishing interoperability among independently functioning product identification and related authentication systems
- ISO 22381: Guidelines for establishing interoperability of object identification and authentication systems
- CEFACT Cross Industry Invoice (available at: https://unece.org/fileadmin/DAM/cefact/cf_plenary/2018_plenary/ECE_TRAD E_C_CEFACT_2018_12E.pdf)

2. Standard(s) on data carriers and links between physical product and digital representation
 - 2.1. The standard(s) shall define common rules for how to construct the Automatic Identification and Data Capture (AIDC) media to be used as data carrier linked to the product passport.
 - 2.2. The requirements shall concern, as applicable:
 - (a) symbology characteristics;
 - (b) data character encoding methods;
 - (c) symbol formats;
 - (d) dimensional characteristics;
 - (e) error correction rules;
 - (f) reference decoding algorithm;
 - (g) printing quality requirements;
 - (h) production quality requirements;
 - (i) user-selectable application parameters (if relevant);
 - (j) durability requirements.
 - 2.3. The data carrier shall contain links to the product passport. The data carrier shall act as a reference to both the public and the restricted DPP-data (i.e., the information included in each product passport, to be identified at product group level).
 - 2.4. The data carrier may also include control data elements. These elements shall enable the verification of the following:
 - (a) the authenticity of the data carrier;
 - (b) the product itself.
 - 2.5. In addition, the data carrier may also include cross-sectoral basic data elements, i.e. data that can be consulted offline. These elements shall make it possible to consult data from the data carrier even when the online information cannot be accessed, for example, when:
 - (a) the subject reading the data carrier is offline;
 - (b) a link present in the data carrier is broken;
 - (c) a link does not lead to a valid page on a website;
 - (d) the server hosting the product passport is down for maintenance or is overloaded.
 - 2.6. The cross-sectoral basic data elements may include the following six pieces of information:
 - (2) the product passport owner (the economic operator who created the product passport);
 - (3) unique operator identifier (the main manufacturer, if different from the product passport owner);
 - (4) the facility identifier (the location where the main manufacturing stage took place);

- (5) the unique product identifier (identifier of the product registered in the product passport registry);
 - (6) an additional product identifier (an optional additional identifier associated to the product);
 - (7) the product group (information about the type of product).
- 2.7. The selection of existing standards or the development of a new standard to meet the requirements in point(s) 2.2 to 2.4 shall be based on an assessment of the benefits and drawbacks of including each of the three kinds of data (DPP data, control data elements and cross-sectoral basic data elements) as part of the common rules for how to create a data carrier.
- 2.8. In case of a visual data carrier, the possibility of setting a product passport visual identity (i.e., by specifying the colours of the data carrier, including specific text, logo or image into the data carrier, or accompanying the data carrier by a specific text, logo or image, etc.) shall be duly considered.
- 2.9. The links to the product passport shall include both the link to the public DPP-data and to the restricted DPP-data.
- 2.10. The control data elements could be a link about how to identify counterfeiting and a hash of the product passport registered in the product passport registry.
- 2.11. The standard(s) shall also specify how the link between the data carrier and the product passport shall be established, including aspects such as look-up mechanisms. Rules and requirements guaranteeing the persistency of the links shall be integrated, including the links' portability across resolver services or systems.
- 2.12. Existing relevant standards shall be duly considered when drafting the new European standard(s). A non-exhaustive list is provided below:
- EN IEC 61406-1: Identification Link
 - EN IEC 63365: Digital Nameplate - Digital Product Marking
 - CLC/TR 50489: Smart tracker chips - Feasibility study on the inclusion of RFID in Electrical and Electronic Equipment for WEEE management
 - ISO/IEC 24458: Information technology – Automatic identification and data capture techniques – Bar code printer and bar code reader performance testing specification
 - ISO/IEC 22603-1: Information technology - Digital representation of product information - Part 1: General requirements
 - ISO/IEC 21471: Information technology - Automatic identification and data capture techniques – Extended rectangular data matrix (DMRE) bar code symbology specification
 - ISO/IEC 18004: Information technology - Automatic identification and data capture techniques - QR Code bar code symbology specification
 - ISO/IEC 16022: Information technology - Automatic identification and data capture techniques – Data Matrix bar code symbology specification
 - ISO/IEC 15426-2: Information technology - Automatic identification and data capture techniques - Bar code verifier conformance specification - Part 2: Two-dimensional symbols

- ISO/IEC 15424: Information technology - Automatic identification and data capture techniques – Data Carrier Identifiers (including Symbology Identifiers)
 - ISO/IEC 15415: Information technology - Automatic identification and data capture techniques - Bar code symbol print quality test specification - Two-dimensional symbols
 - ISO/IEC 15418: Information technology - Automatic identification and data capture techniques - GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance
 - ISO 23354: Business requirements for end-to-end visibility of logistics flow
 - ISO 15000-2:2021 : AS4 profile of ebXML Messaging v3
 - PEPPOL eDelivery (available at [eDelivery Documentation - OpenPeppol](#))
 - GS1 DataMatrix Guideline (available at : <https://www.gs1.org/standards/gs1-datamatrix-guideline/25>)
 - ISO/IEC NP 18975: Encoding and resolving identifiers over HTTP
 - GS1 Digital Link (available at: <https://www.gs1.org/standards/gs1-digital-link>)
 - DIDs (available at: <https://www.w3.org/TR/did-core/>)
 - DID Resolution (available at: <https://w3c-ccg.github.io/did-resolution/>)
 - DID Registration (available at: <https://identity.foundation/did-registration/>)
 - Digital Object Identifier (available at: <https://www.iso.org/standard/81599.html>)
 - Uniform Resource Names (available at: <https://www.rfc-editor.org/rfc/rfc8141>)
 - PEPPOL Service Metadata Locator (available at: <https://docs.peppol.eu/edelivery/>)
3. Standards on access rights management, information system security and business confidentiality
- 3.1. Identity management ensures that organisations, individuals, machines, and services are provided with acknowledged identities. The standard(s) shall define clear rules and requirements related to access control measures to regulate the access to restricted product passport information.
- 3.2. When developing the European standard(s), the following elements shall be adequately considered:
- (a) access rights management shall be attribute-based;
 - (b) the economic operators placing the products on the internal market shall be responsible for managing the corresponding product passport access rights (or a service provider contracted by the economic operator);

- (c) the access rights for each information included in the product passport shall be product group specific;
 - (d) the public data included in the product passport shall not require any access right management;
 - (e) the access rights shall include any mandatory and necessary licensing rules governing items related to data models, data exchange protocols, data processing, and interoperability.
- 3.3. The standard(s) shall also identify rules to guarantee IT-security, cybersecurity, and data protection.
- 3.4. The standard(s) shall also address the issue of how to transfer responsibilities, access-rights, and data from one economic operator to another, for example when a product passport needs to be updated to include information related to repair activities performed by a professional repairer.
- 3.5. Existing relevant standards shall be duly considered when drafting the new European standard(s). A non-exhaustive list is provided below:
- EN IEC 63278-3: Asset Administration Shell for Industrial Applications – Part 3: Security provisions for Asset Administration Shells.
 - ISO 22385: Guidelines for establishing a Framework for Trust and Interoperability
 - ISO/IEC 29146: Information technology - Security techniques - A framework for access management
 - ISO/IEC 24760: IT Security and Privacy - A framework for identity management
 - ISO/IEC 24761: Information technology - Security techniques - Authentication context for biometrics
 - ISO/IEC TS 29003: Information technology - Security techniques - Identity proofing
 - ISO/IEC 20248: Information technology - Automatic identification and data capture techniques – Digital signature data structure schema
 - ISO/IEC 30147: Information technology - Internet of things - Methodology for trustworthiness of IoT system/service
 - ISO/IEC AWI 30149: Internet of things (IoT) - Trustworthiness framework
 - ISO 15000-2:2021 : AS4 profile of ebXML Messaging v3
 - ISO/IEC 27040: Information technology - Security techniques - Storage security
 - ISO/TR 6039: Blockchain and distributed ledger technologies - Identifiers of subjects and objects for the design of blockchain systems
 - ISO 23257 Blockchain and distributed ledger technologies — Reference architecture
 - ISO/TS 23635 Blockchain and distributed ledger technologies — Guidelines for governance

- ISO/WD TR 23642 Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues
- ISO/IEC 27040: Information technology - Security techniques - Stage security
- IEC 62443 series
- IEC 63069
- IEC TR 63283-3 and series
- IEC 63278-3 and series
- IEC 61406 series
- ITU-T Rec X.1144 (XACML v3, available at : <https://www.itu.int/rec/T-REC-X.1144-201310-1>)
- Verifiable Credentials (available at : <https://www.w3.org/TR/vc-data-model/>)
- ODRL Model (available at : <https://www.w3.org/TR/odrl/>)
- ODRL Vocabulary (available at : <https://www.w3.org/TR/odrl-vocab/>)
- OAuth2 (available at: <https://oauth.net/2/>)
- IETF RFC7515 on JSON Web Signature (available at: <https://datatracker.ietf.org/doc/html/rfc7515>)
- Certificate Transparency (IETF RFCs 6962 and 9162 available at <https://datatracker.ietf.org/doc/rfc6962/> and <https://datatracker.ietf.org/doc/rfc9162/>)
- OCSP Stapling (IETF RFC 6066, among others, available at <https://datatracker.ietf.org/doc/html/rfc6066>)

4. Standards on interoperability (technical, semantic, and organisational)

4.1. The standard(s) shall define, inter alia, rules related to the following:

- (a) semantic description of a product, including but not limited to unambiguous meaning and consistent naming and, where relevant, a value list, a specific format and defined units of measure for all quantitative values;
- (b) a common information model allowing for the implementation of dictionary systems;
- (c) metadata models and formats to be used in exchange and representation. The standard(s) shall include rules on how to systematically use such metadata models when developing product group specific data models.

4.2. Existing relevant standards shall be duly considered when drafting the new European standard(s). A non-exhaustive list is provided below:

- EN IEC 63278: Asset Administration Shell for Industrial Applications
- EN IEC 61360: Standard data element types with associated classification scheme - Part 1: Definitions - Principles and methods
- ISO/IEC 21823: Internet of things (IoT) - Interoperability for IoT systems

- Baseline protocol (available at: <https://github.com/eea-oasis/baseline-standard/blob/main/core/baseline-core-v1.0-psd01.md>)
 - ISO 11354-1:2011: Enterprise interoperability framework
5. Standard(s) on data processing, data exchange protocols and data formats
- 5.1. The standard(s) shall define, inter alia, rules related to the following:
- (a) data exchange protocols, including rules to exchange data between two or more parties;
 - (b) processes to introduce, modify, and update information in the product passport.
- 5.2. Existing relevant standards shall be duly considered when drafting the new European standard(s). A non-exhaustive list is provided below:
- ISO 9735: Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules
 - ISO 14533: Processes, data elements and documents in commerce, industry and administration – Long term signature profiles
 - ISO/IEC 19845: Universal Business Language (UBL) v2.1
 - ISO/IEC 20248: Information technology - Automatic identification and data capture techniques – Digital signature data structure schema
 - EN 16931: Electronic invoicing
 - ISO 23247: Automation systems and integration - Digital twin framework for manufacturing
 - ISO 10303 series: Industrial automation systems and integration - Product data representation and exchange
 - ISO 15000-2:2021 : AS4 profile of ebXML Messaging v3
 - ISO 23354: Business requirements for end-to-end visibility of logistics flow
 - ISO 15000-2:2021 : AS4 profile of ebXML Messaging v3
 - EN ISO 23386 Building information modelling and other digital processes used in construction - Methodology to describe, author and maintain properties in interconnected data dictionaries
 - EN ISO 12006-3 Building construction — Organization of information about construction works — Part 3: Framework for object-oriented information
 - EN 17549-2 Building information modelling – Information structure based on EN ISO 16739 1 to exchange data templates and data sheets for construction objects Part 2. Configurable construction objects and requirements
 - ISO 59040 Circular Economy – Product Circularity Data Sheet (under development)
 - ISO/CD TR 6277 Blockchain and distributed ledger technologies – Data flow model for blockchain and DLT

- ISO/AWI TS 23516 Blockchain and Distributed Ledger Technology — Interoperability Framework
- PEPPOL eDelivery (available at <http://peppol.eu/downloads/the-peppol-edelivery-network-specifications/>)
- ISO/ IEC 19987 - Information technology — EPC Information Services (EPCIS) Standard
- ISO/ IEC 19988 - Information technology - Core Business Vocabulary Standard
- EPCIS – Automotive Business Vocabulary, VDA 5530 - part 1
- IEC 62720 – Units of Measurement (available as a database standard at <https://cdd.iec.ch>)
- IEC 61360-4 DB - IEC Common Data Dictionary - IEC CDD) (available as a database standard at <https://cdd.iec.ch>)
- ECLASS
- W3C Web of Things (WoT) Architecture
- W3C WoT Thing Description (TD)
- SAREF Core Ontologie - ETSI TS 103 264
- UNECE-UN/CEFACT Cross Industry Invoice (available at: https://unece.org/fileadmin/DAM/cefact/cf_plenary/2018_plenary/ECE_TRADE_C_CEFAC_T_2018_12E.pdf)
- UNECE-UN/CEFACT Supply chain reference data model (available at: https://unece.org/fileadmin/DAM/uncefact/BRS/BRS_SCRDM_v1.0.0.2.pdf)
- UNCL (available at: <https://unece.org/sites/default/files/2022-06/CCL22A.zip>)
- UNCL (available at: <https://service.unece.org/trade/untdid/d22a/d22a.zip>)
- UNLOCODE (available at: https://unece.org/cefact/codesfortrade/codes_index.html)
- OpenIDConnect (available at: <https://openid.net/connect/>)
- OID4VC (available at: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html)
- OID4VP (available at: https://openid.net/specs/openid-connect-4-verifiable-presentations-1_0-07.html)
- VCs (available at: <https://www.w3.org/TR/vc-data-model/>)
- JSON-LD (available at: <https://www.w3.org/TR/json-ld11/>)
- VC-JSON (available at: [GitHub - w3c/vc-json-schema/](https://github.com/w3c/vc-json-schema/))
- Circular product data exchange use case (available at: <https://uncefact.unece.org/display/uncefactpublic/EXTENSION+TEXTILE+AND+LEATHER+BRS+PART+2%3A+Use+case+and+CCBDA+data+structure+supporting+product+circularity->

- Sustainable Development and Circular Economy Reference Data Model (available at: <https://uncefact.unece.org/display/uncefactpublic/Sustainable+Development+and+Circular+Economy+Reference+Data+Model>)
- Circular product data exchange structure (available at: <https://uncefact.unece.org/display/uncefactpublic/EXTENSION+TEXTILE+AND+LEATHER+BRS+PART+2%3A+Use+case+and+CCBDA+data+structure+supporting+product+circularity>)
- Product transparency data exchange structure (available at: <https://unece.org/trade/uncefact/mainstandards#:~:text=Product%20Transparency%20Message%C2%A0>)
- Product traceability data exchange structure (EPCIS) (available at: <https://uncefact.unece.org/display/uncefactpublic/JSON-LD+Web+Vocabulary>)
- Product transparency data exchange structure (available at: <https://uncefact.unece.org/display/uncefactpublic/JSON-LD+Web+Vocabulary>)
- Circular product data exchange structure (available at: <https://uncefact.unece.org/display/uncefactpublic/EXTENSION+TEXTILE+AND+LEATHER+BRS+PART+2%3A+Use+case+and+CCBDA+data+structure+supporting+product+circularity>)
- Sustainable Development and Circular Economy Reference Data Model (available at: <https://uncefact.unece.org/display/uncefactpublic/JSON-LD+Web+Vocabulary>)
- Product Circularity Data Sheet (available at: https://pcds.lu/wp-content/uploads/2020/11/20200214_Light_PCDS_v3.2s_FORM.pdf)
- GS1 Attribute Definitions for Business (available at: <https://www.gs1.org/standards/attribute-definitions-for-business>)
- GS1 Global Data Model Attribute Implementation Guide (available at: <https://www.gs1.org/standards/gs1-global-data-model-attribute-implementation-guideline/current-standard>)
- GS1 Digital Link Standard (available at: <https://www.gs1.org/standards/gs1-digital-link>)
- GS1 General Specifications (available at: <https://www.gs1.org/standards/barcodes-epcrfid-id-keys/gs1-general-specifications>)
- GS1 Digital Link Implementation Guideline ((available at: <https://www.gs1.org/standards/gs1-digital-link>)
- GS1 DataMatrix Guideline (available at: <https://www.gs1.org/standards/gs1-datamatrix-guideline/25>)
- Global Traceability Standard (available at: <https://www.gs1.org/standards/gs1-global-traceability-standard/current-standard>)

6. Standards on data storage, archiving and data persistence

- 6.1. The standard(s) shall define rules for decentralised data storage, archiving and data persistence. The archiving service securely stores historical passport data, preserving a comprehensive record of past information. This feature is particularly relevant for market surveillance purposes. Persistence is required to make sure that data included in the product passports remains available even when the economic operator creating the passport is no longer active.
- 6.2. Existing relevant standards shall be duly considered when drafting the new European standard(s). A non-exhaustive list is provided below:
- EN IEC 63278: Asset Administration Shell for Industrial Applications
 - Decentralized Web Node (available at: <https://identity.foundation/decentralized-web-node/spec/>)
 - Encrypted Data Vaults (available at: <https://identity.foundation/edv-spec/>)
 - Certificate Transparency (IETF RFCs 6962 and 9162 available at <https://datatracker.ietf.org/doc/rfc6962/> and <https://datatracker.ietf.org/doc/rfc9162/>)
7. Standards on data authentication, reliability and integrity
- 7.1. The standard(s) shall provide an open and interoperable method between automated identification services and data carriers to read data, verify data originality and data integrity in offline and online use cases. The standard(s) shall establish a framework for ensuring trust, interoperability and interoperation via secure and reliable electronically signed encoded data set (ESEDS) schemes for multi-actor applications in multi-sector environment.
- 7.2. When developing the standard(s), at least the following elements shall be addressed:
- (a) management and verification of identifiers;
 - (b) relationship between the unique identifiers and possible authentication elements related to them;
 - (c) questions that deal with the identification of the verifier and any authorised access to privileged product related information;
 - (d) verifier access history (logs);
 - (e) authentication solutions;
 - (f) artefact metrics, where relevant;
 - (g) information processing and communication that protects integrity along the supply chain of physical and related electronic documents, products, software and services life cycle to mitigate the risk of product fraud and counterfeit goods, by using object identification techniques;
 - (h) verifiable credentials.
- 7.3. Existing relevant standards shall be duly considered when drafting the new European standard(s). A non-exhaustive list is provided below:
- ISO/IEC 20248: Information technology - Automatic identification and data capture techniques – Digital signature data structure schema

- ISO 22378: Guidelines for establishing interoperability among independently functioning product identification and related authentication systems
 - ISO 22383: Guidelines for selection and performance evaluation of authentication solutions for material goods
 - ISO 22385: Guidelines for establishing a Framework for Trust and Interoperability
 - ISO 22387: Confirmation procedures for the application of artefact metrics
 - ISO 8000 – Data Quality
 - Certificate Transparency (IETF RFCs 6962 and 9162 available at <https://datatracker.ietf.org/doc/rfc6962/> and <https://datatracker.ietf.org/doc/rfc9162/>)
8. Standards on Application Programming Interfaces (APIs) for the product passport lifecycle management and searchability
- 8.1. The standard(s) aim at harmonising the APIs for automating the management of the product passport throughout its lifecycle and serving remote queries coming from the product passport registry or applications from national authorities.
- 8.2. Custodians of product passports (either economic operators or service providers) shall make available APIs covering the following:
- (a) CRUD (Create, Read, Update, Delete) operations on products passports;
 - (b) remote queries on the products passports under their custodianship.
- 8.3. When developing the standard(s), at least the following aspects shall be adequately specified:
- (a) syntax and semantics of the API interfaces;
 - (b) security and access control to the APIs;
 - (c) performance and response time;
 - (d) considerations on versioning and backward compatibility of API interfaces;
 - (e) message exchange patterns, for instance synchronous, asynchronous, request-response, fire-and-forget, publish and subscribe;
 - (f) availability and scalability;
 - (g) mechanisms to ensure the authenticity, integrity and reliability of the data.
- 8.4. The Study: "APIs4DGov - Digital Government APIs. The Road to value-added Open-driven services" by the JRC (available at <https://data.jrc.ec.europa.eu/collection/id-0097>) shall be used in the design of the APIs. Furthermore, existing relevant standards shall be duly considered when drafting the new API standard(s). A non-exhaustive list is provided below:
- WS-* standards (available at <https://www.oasis-open.org/specs/index.php>)

- SOAP messaging framework (available at <https://www.w3.org/TR/soap12/>)
- REST (Representational state transfer) architectural style
- HTTP (available at <https://datatracker.ietf.org/doc/html/rfc9112>)
- ISO/IEC 21778:2017 - Information technology — The JSON data interchange syntax
- IETF RFC7515 on JSON Web Signature (available at: <https://datatracker.ietf.org/doc/html/rfc7515>)
- JSON-LD (available at: <https://www.w3.org/TR/json-ld11/>)
- eDelivery Building Blocks (available at <https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/eDelivery>)
- PEPPOL eDelivery (available at <http://peppol.eu/downloads/the-peppol-edelivery-network-specifications/>)
- ISO 15000-2:2021 : AS4 profile of ebXML Messaging v3
- ISO 22385: Guidelines for establishing a Framework for Trust and Interoperability
- ISO/IEC 24760: IT Security and Privacy - A framework for identity management
- ISO EN 301549:2015 Accessibility requirements suitable for public procurement of ICT products and services in Europe
- ISO/IEC 19845:2015 : Universal Business Language (UBL) v2.1
- ISO/IEC NP 18975: Encoding and resolving identifiers over HTTP
- OpenIDConnect (available at: <https://openid.net/connect/>)
- OpenID for Verifiable Credentials (available at: <https://openid.net/sg/openid4vc/>)
- OpenAPI Specification (available at: <https://spec.openapis.org/oas/v3.0.3>)
- JSON Web Token (available at: <https://www.rfc-editor.org/rfc/rfc7519>)