Brussels, XXX
[…](2023) XXX draft

COMMISSION IMPLEMENTING DECISION

of XXX

on a standardisation request to [the European standardisation organisations]/[the European Committee for Standardisation] [the European Committee for Electrotechnical Standardisation] [the European Telecommunications Standards Institute] as regards [products(s)]/[service(s)] in support of […] […]

on a standardisation request to the European Committee for Standardisation, the European Committee for Electrotechnical Standardisation, the European Telecommunications Standards Institute as regards digital product passports in support of the COM(2022) 142 final proposal for a Regulation of the European Parliament and Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC

(Only the English, French and German texts are authentic)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council,[1] and in particular Article 10(1) thereof,

Whereas:

(1) The Commission proposal for a Regulation of the European Parliament and of the Council establishing a framework for setting ecodesign requirements for sustainable products[2] ('the ESPR proposal') lays down rules to improve the environmental sustainability of products and to ensure free movement in the internal market by setting ecodesign requirements that products shall fulfil to be placed on the market or put into service.

(2) Regulation (EU) 2023/1542 of the European Parliament and of the Council[3] establishes requirements on sustainability, safety, labelling, marking and information to allow the placing on the market or putting into service of batteries, as well as requirements for the collection, treatment, and recycling of waste batteries.

(3) Article 8 of the ESPR proposal requires that products may only be placed on the market or put into service if a digital product passport ('product passport') is available in accordance with delegated acts to be adopted under the future Regulation. Articles 9 and 10 of the proposal specify the general requirements and the essential requirements to be met by any product passport in order to comply with the future Regulation.

[1] COM(2022) 142 final. OJ L 316, 14.11.2012, p. 12.

[2] COM(2022) 142 final establishing a framework for setting ecodesign requirements for sustainable products and repealing Directive 2009/125/EC, COM(2022) 142 final

[3] Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC

(4) Article 77 of Regulation (EU) 2023/1542 requires that certain categories of batteries may only be placed on the market or put into service if they have an electronic battery passport in accordance with that Article. Article 78 of that Regulation specifies the essential requirements for the technical design and operation of the battery passport to be met by any such passport.

(5) The product passport is an important tool to foster the sustainability of products and the transition to sustainable business models by making information available to actors along the entire value chain. The availability of a product passport should significantly enhance end-to-end traceability of a product throughout its value chain, help consumers make informed choices by providing access to product information relevant to them, allow economic operators and other value chain actors such as repairers or recyclers to access relevant information, and enable competent national authorities to perform their duties.

(6) The product passports should be as uniform as possible across products, industry sectors and relevant EU legislations, and the way they are used as consistent as possible. This can help avoid confusion and misunderstandings arising when organisations or industries use different semantic or technical standards. In order to practically promote this uniformity, for products composed of other products, the Digital Product Passport should allow the inclusion of DPP information concerning other integrated product components, where relevant.

(7) The product passports should be easily shared and used across different systems and platforms. This should enable information exchange between various stakeholders, such as manufacturers, suppliers, consumers, and regulators.

(8) The implementation of product passports should rely on harmonised standards to provide clear and consistent requirements. This should facilitate interoperability reducing the time and resources required to implement and maintain the system as well as stimulate innovation and competition of market players offering product passports (services).

(9) To optimise access to the resulting information, the product passport should be designed and implemented to allow differentiated access to the information included in the product passport depending on the type of information and the type of stakeholders.

(10) To avoid costs to companies and to the public that are disproportionate compared to the wider benefits, the product passport should be defined at the item, batch or product model, depending on specific needs and complexity of the value chain, the size, nature or impacts of the products considered.

(11) All economic operators along the value chain must be given the possibility to create a DPP based on harmonised, open, and interoperable standards, without depending on any commercial technology and service provider.

(12) Unique identification of products is a fundamental element to enable traceability across the entire supply chain. Therefore, the product passport should be linked to a persistent unique product identifier. In addition, where appropriate, the passport should allow for the tracing of the economic operators and facilities involved in the entire supply chain. Based on the identifier, the DPP-system should include mechanisms to ensure the authenticity, integrity, and reliability of the data included in the DPP.

(13) The unique identifier and the corresponding identification system of the DPP shall allow to be made interoperable with existing legacy identification system. The passport system should allow a suitable assignment of data carriers to the product which has to be assessed without additional software which needs to be downloaded. Moreover, all identifiers shall be portable and transferable through an open interoperable data exchange network without vendor lock-in, including their portability across resolver services or systems.

(14) The data carrier and the unique identifiers should be created to ensure that the information contained in the product passport can be accessed, recorded and transmitted by all economic operators, depending on their access rights, as well as to guarantee the compatibility of the data carriers and unique identifier with external components such as scanning devices.

(15) To ensure that the product passport is flexible, agile and market-driven and evolving in line with business models, markets and innovation, it should be based on a decentralised data system, set up and maintained by economic operators. However, for enforcement and monitoring purposes, it may be necessary that competent national authorities and the Commission have direct access to all decentralised data systems and thus to all data carriers and unique identifiers linked to products placed on the market or put in service.

(16) The DPP system should allow economic operators for an interoperable extendibility of DPP based on regulatory requirements. Technical solution should enable extendibility of DPP in case of need in a later stage. Extendibility of DPP should cover at least: (1) additional type of data/properties/attributes and (2) additional records.

(17) In accordance with Article 34 of the ESPR proposal, product passports which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with corresponding ecodesign requirements set out in delegated acts adopted pursuant to Article 4 of that Regulation, to the extent that those requirements are covered by such harmonised standards or parts thereof.

(18) In accordance with Article 15 of Regulation (EU) 2023/1542 battery passports which are in conformity with harmonised standards or parts thereof the references of which have been published in the *Official Journal of the European Union* shall be presumed to be in conformity with corresponding requirements for the technical design and operation of the battery passport set out in Article 78 of that Regulation, to the extent that those requirements are covered by such harmonised standards or parts thereof.

(19) Harmonised standards are technology neutral and performance-based; they also contribute to ensuring equal conditions of competition among relevant economic operators, in particular small and medium-sized enterprises. Indirectly those standards also contribute to lower production costs benefitting consumers, and to ensure technical interoperability.

(20) The European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI) have indicated that the work covered by the standardisation request falls within their area of competence.

(21) It is therefore appropriate to request that CEN, CENELEC and ETSI draft new European standards in support of Articles 9 and 10 of COM(2022) 142 final and harmonised standards in support of Article 78 of Regulation (EU) 2023/1542. In case the ESPR proposal is subject to substantial modifications during the ordinary legislative procedure, this standardisation request may have to be amended accordingly.

(22) Requested standards should be coherent with the principles laid down in the European legal framework relating to cybersecurity or processing of personal data or protection of privacy or networks or fraud and with technical mechanisms established thereof, in particular, by: Regulation (EU) 2016/679 of the European Parliament and of the Council[4] and Directive 2002/58/EC of the European Parliament and of the Council[5] which regulate the processing of personal data and protection of privacy; Directive (EU) 2016/1148 of the European Parliament and of the Council[6] which lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market; Regulation (EU) 910/2014 of the European Parliament and of the Council[7] (eIDAS Regulation) which aims at ensuring that people and businesses can use their national electronic identification schemes (eIDs) in one Member State to access public services available online in other Member States and establishes an European internal market for Trust Services; Regulation (EU) 2019/881 of the European Parliament and of the Council[8] which lays down objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity) and a framework for the establishment of European cybersecurity certification schemes; Commission Delegated Regulation 2022/30[9] supplementing Directive 2014/53/EU of the European Parliament and of the Council which imposes cybersecurity requirements on certain categories of radio equipment as regards its placing on the EU market. The Commission and the European standardisation organisations CEN, CENELEC and ETSI should cooperate in view of finding solutions in cases where the need to ensure such coherence might raise practical issues for the development of the harmonised standards under the present standardisation request.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJEU L 119, 4 May 2016

[5] Directive (EU) 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJEU L 201, 31 July 2002

[6] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJEU L 194, 19 July 2016

[7] Regulation (EU) 910/201 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJEU L 257, 28 August 2014

[8] 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, OJEU L 151, 7 June 2019

[9] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive, OJEU L 7, 12 January 2022

(23) As cybersecurity threats evolve at a fast pace, CEN, CENELEC and ETSI should monitor constantly the generally acknowledged state of the art and report to the Commission promptly where an evolution has been observed, together with a plan to adapt existing harmonised standards.

(24) The requested standards should be adopted by CEN, CENELEC and ETSI by the deadlines set out in this Decision. Given the short timeline for the implementation of the European policies requiring the use of the product passport, it may not be possible to extend the deadlines set.

(25) The standards to be drafted should build mainly on existing standards and best industry practice at international level, avoiding the lock-in of proprietary solutions. Therefore, existing ISO and IEC standards should be looked at first, complemented (if necessary) by considering specifications from existing European standards, national standards and fora standards (in this order).

(26) Recalling that all relevant interested parties, including the Member States and the European stakeholder organisations receiving Union financing in accordance with Regulation (EU) No 1025/2012, may identify needs to develop additional standards, it may be necessary to consider adding new items to the list of standards set out in Annex I to this Decision. It may therefore be necessary to adjust the scope of this request accordingly.

(27) The European standardisation organisations (ESO) have agreed to follow the Guidelines for the execution of standardisation requests10. In addition, the Commission has provided different elements of guidance for the assessment of the deliverables. CEN, CENELEC and ETSI should verify that any deliverable is in line with the provided guidance.

(28) In order to ensure transparency and facilitate the execution of the requested standardisation activities CEN, CENELEC and ETSI should prepare a work programme and submit it to the Commission.

(29) In order to enable the Commission to better monitor the requested standardisation work, CEN, CENELEC and ETSI should provide the Commission with access to an overall project plan containing detailed information on the execution of the standardisation request.

(30) Information as to which essential requirements are covered by a harmonised standard is necessary when assessing, in accordance with Article 10(5) of Regulation (EU) 1025/2012, the compliance of the documents drafted by ESOs. Such information is also necessary before publication of references of harmonised standards in the Official Journal of the European Union in accordance with Article 10(6) of Regulation (EU) 1025/2012. In each harmonised standard CEN, CENELEC and ETSI should therefore describe the extent to which it aims to cover one or several essential requirements set out in Article 78 of Regulation (EU) 2023/1542.

(31) In accordance with Article 10(3) of Regulation (EU) No 1025/2012, each standardisation request is subject to acceptance by the relevant European standardisation organisation. It is therefore necessary to provide for the rules on validity of this request if it is not accepted by CEN, CENELEC, and ETSI.

[10] SWD(2015) 205 final of 27 October 2015

(32) In order to ensure legal certainty as to the validity of the request after its execution, it is appropriate to provide for a date of expiry of this Decision.

(33) The ESOs, the European stakeholders' organisations receiving Union financing, the Ecodesign Consultation Forum, and the Market Surveillance Committee established by Article 45 of Directive 2014/53/EU have been consulted.

(34) The measures provided for in this Decision are in accordance with the opinion of the Committee established by Article 22 of Regulation (EU) No 1025/2012.

HAS ADOPTED THIS DECISION:

Article 1
Requested standardisation activities

(1) The European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC) and the European Telecommunications Standards Institute (ETSI) are requested to draft the European and harmonised standards listed in Annex I to this Decision in support of the essential requirements set out in Article 9 and 10 of COM(2022) 142 final and Article 78 of Regulation (EU) 2023/1542

(2) The standards, referred to in paragraph 1 shall meet the requirements set out in Annex II to this Decision.

(3) CEN, CENELEC, and ETSI shall provide the Commission with the titles of the requested harmonised standards in all the official languages of the Union.

Article 2
Work programme

(1) CEN, CENELEC and ETSI shall prepare a work programme indicating all the standards referred to in Article 1, paragraph 1, the responsible technical bodies and a timetable for the execution of the requested standardisation activities in line with the deadlines set out in Annex.

(2) CEN, CENELEC and ETSI shall submit the draft work programme to the Commission by [2 months after notification] and provide it with access to an overall project plan.

(3) CEN, CENELEC and ETSI shall inform the Commission of any amendments to the work programme.

Article 3
Reporting

(1) CEN, CENELEC and ETSI shall report annually to the Commission on the execution of the request referred to in Article 1, indicate, for the standards referred to in Article 1, paragraph 1, the progress made in implementation of the work programme

referenced to in Article 2 and provide information on any standards referred to Article 1, paragraph 2, that need to be prepared or reviewed.

(2) CEN, CENELEC and ETSI shall submit the first annual report to the Commission by 31 December 2024 and the final report by 31 December 2025.

(3) Without prejudice to the reporting obligations set out in paragraphs 1 to 3, CEN, CENELEC and ETSI shall promptly report to the Commission any major concerns relating to the scope of the request referred to in Article 1 and the deadlines set out in Annex I to this Decision.

Article 4
Validity of the standardisation request

(1) If CEN or CENELEC or ETSI do not accept the request referred to in Article 1 of this Decision, in accordance with Article 10(3) of Regulation (EU) No 1025/2012, the request may not constitute a basis for the standardisation activities referred to in Article 1 of this Decision.

(2) This Decision shall expire on 30 June 2026.

Article 5
Addressee

This Decision is addressed to the European Committee for Standardisation, the European Committee for Electrotechnical Standardisation and the European Telecommunications Standards Institute.

Done at Brussels,

For the Commission

ANNEX I

List of standards to be drafted as referred to in Article 1

Table 1: List of European and harmonised standards[1] to be drafted and deadlines for their adoption

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

[1] The requested standards are considered harmonised standards only under Directive (EU) 2023/1542

[2] 'Adoption' refers to the relevant European standardisation organisation making an adopted standard available to its members or the public.

ANNEX II

Requirements for the standards referred to in Article 1

Part A. General requirements for standards listed in Annex I

For the purpose of Annexes I and II, 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 or an importer, 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) ‘product passport’ means a set of data specific to a product that includes the information specified in the applicable delegated act adopted pursuant to Article 4 of COM(2022) 142 final or specified in Article 77 of Regulation (EU) 2023/1542, and that is accessible via electronic means through a data carrier.
(11) ‘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.
(12) ‘unique product identifier’ means a unique string of characters for the identification of products that also enables a web link to the product passport.
(13) ‘unique operator identifier’ means a unique string of characters for the identification of actors involved in the value chain of products.
(14) ‘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.
(15) ‘processing’ means processing as defined in Article 3, point (2), of Regulation (EU) 2018/1807.
(16) ‘DPP-system’ means the set of IT standards and protocols required to ensure the full interoperability of digital product passports (‘product passports’) and compliance with essential requirements defined in Articles 9 and 10 of COM(2022) 142 final or defined in Articles 77 and 78 of Regulation (EU) 2023/1542.
(17) ‘DPP-data’ means the information included in a product passport and accessible to different users based on their own respective access rights.

(18) ‘decentralised identifier’ means a globally unique persistent identifier that does not require a centralized registration authority and is often generated and/or registered cryptographically.

The standards to be developed shall reflect the generally acknowledged state of art and be technology-neutral.

As the reliability of the DPP-system is very important for policy implementation and enforceability, 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 should be looked at first, complemented (if necessary) 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.

1. Legal requirements to be supported by the harmonised standards

1.1 Each standard shall support the application of the:

(a) Essential requirements referred to in Articles 9 and 10 of COM(2022) 142 final, when that standard or those standards aim to cover that essential requirement.
(b) Essential requirements referred to in Articles 77 and 78 of Regulation (EU) 2023/1542, when that standard or those standards aim to cover that essential requirement.

1.2 The requirements referred to in point 1.1 of this Part of this Annex shall be taken into account from the beginning and throughout the entire process of developing the standards.

1.3 The standards shall not support any other legal requirements than those set out in Articles 9 and 10 of COM(2022) 142 final, and in Articles 77 and 78 of Regulation (EU) 2023/1542.

1.4 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 benefit from the presumption of conformity and those which are not. In the case where those clauses or sub-clauses, which are not necessary to be applied, are included they shall not compromise or endanger the conformity with any of the requirements.

1.5 Standards shall follow the principles laid down in the Union legal framework in the area of cybersecurity or processing of personal data or protection of privacy or networks. Coherence among mechanisms established in the aforementioned legislation shall be ensured.

1.6 Where applicable cybersecurity certification schemes under the Regulation (EU) 2019/881 are adopted, the standards shall be developed in a coherent manner with the relevant content of those specifications.

1.7 Standards should rely, as relevant, on existing similar/equivalent approaches already used in other European legislations.

Each standard developed on the basis of the request referred to in Article 1 of this Decision shall refer to this Decision.

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.

To reduce dependencies between elements in the eight standardisation areas (hereafter indicated as 'modules') included in this request, the standardisation work should 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.

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 the change of a standard within one module does not lead to the requirement of changes in other modules.

Part B. Specific requirements for the harmonised standards listed in Table 1 of Annex I

1. Requirements for specific harmonised standards

1.1 Standard(s) on unique identifiers

The standard(s) shall define requirements related to the following areas:

(a) uniqueness of each identifier (i.e., the same identifier shall not be assigned to different products, different economic operators, or different facilities),
(b) Syntax-related requirements,
(c) Semantic-related requirements,

The standards shall consider the diversity of identifiers currently used by economic operators and accommodate them as much as possible.

The standard(s) should allow both the possibility to use 'centralised' and 'decentralised' identifiers, including the definition of conformance criteria if different methods to produce an identifier are allowed.

The unique product identifier should always allow the possibility to include the three different granularity levels introduced in ESPR, i.e. model, batch, or item. This is needed because DPP of products sold online will only be available at model level, while the ESPR delegated acts may require the product specific DPP to be available at batch level with the possibility for economic operators to serialise their DPPs having a DPP at item level. The need to move from batch to item will also be needed for those product groups for which updated of passports will be relevant, for example those products for which repair activities can be expected. Moreover, in some cases like in Battery Regulation (EU) 2023/1542, the granularity level for the DPP passport is at item level.

The maximum length of the product unique identifier string should be maximum 70 characters. Any solution proposed should guarantee the uniqueness of the identifier string and

compliance with existing legal requirements with particular reference to Commission Implementing Regulation (EU) 2015/2447[3].

In order to promote interoperability, reduce costs for companies, and support coherency and consistency of digitalisation efforts, the standard(s) developed should adequately take into account typology of identifiers already used in other European legislations and initiatives.

Existing relevant standards should be duly considered when drafting the new harmonised 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
- Decentralised Identifiers (DIDs) v1.0 (available at: https://www.w3.org/TR/did-core/)
- W3C on verifiable credentials (available at: https://www.w3.org/TR/vc-data-model/)
- ISO 7603: Decentralized Identity standard for the identification of subjects and objects
- 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

[3] Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code (consolidated version on 15/03/2023). EUR-Lex - 02015R2447-20230315 - EN - EUR-Lex (europa.eu)

- 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_TRADE_C_CEFACT_2018_12E.pdf)

1.2 Standard(s) on data carriers and links between physical product and digital representation

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.

The requirements should 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

The data carrier shall contain links to the product passport. These elements shall act as a reference to both the public and the restricted DPP-data (i.e., the information included in each DPP, to be identified through specific Delegated Acts at product group level).

The data carrier should also include control data elements. These elements should enable the verification of:

(a) the authenticity of the data carrier.

(b) The product itself.

Finally, the data carrier may also include cross-sectoral basic data elements, i.e. data that can be consulted offline. These elements should make it possible to consult data from the data carrier even when the online information cannot be accessed. For example, when:

- the subject reading the data carrier is offline;
- a link present in the data carrier is broken;
- a link does not lead to a valid page on a website;
- the server hosting the DPP is down for maintenance or is overloaded.

The cross-sectoral basic data elements should include the following six information elements:

(1) DPP owner (the economic operator who created the DPP).
(2) Unique operator identifier (the main manufacturer, if different from the DPP owner)
(3) The facility identifier (the location where the main manufacturing stage took place)
(4) The unique product identifier (identifier of the product registered in the DPP registry)

(5) An additional product identifier (additional identifier associated to the product, optional)
(6) The product group (information about the type of product).

The selection of existing standards or the development of a new standard to meet the aforementioned objectives should be based on an assessment of the benefits and drawbacks of including each of the three kinds of data as part of the common rules for how to create a data carrier.

In case of a visual data carrier, the possibility of setting a DPP 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.) should be duly considered.

The links to the product passport should include both the link to the public DPP-data and to the restricted DPP-data.

The control data elements could be a link about how to identify counterfeiting and a hash of the DPP registered in the DPP registry.

The standard(s) shall also specify how the link between the data carrier and the DPP 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.

Existing relevant standards should be duly considered when drafting the new harmonised 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 http://peppol.eu/downloads/the-peppol-edelivery-network-specifications/)
- 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/)

1.3 Standards on access rights management, information system security, and business confidentiality

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. When developing the harmonised standard(s), the following elements should be adequately considered:

(a) Access rights management shall be attribute-based.
(b) It will be the economic operators placing the products on the EU market who will be responsible for managing the corresponding DPP access rights (or a service provider contracted by the economic operator).
(c) The access rights for each information included in the DPP will be product group specific. They will be included in the delegated acts adopted by the Commission pursuant to Article 4 of COM(2022) 142 final.
(d) The public data included in the DPP will not require any access right management.
(e) The access rights should include any mandatory and necessary licensing rules governing items related to data models, data exchange protocols, data processing, and interoperability.

The standard(s) shall also identify rules to guarantee IT-security, cybersecurity, and data protection.

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 DPP will need to be updated to include information related to repair activities performed by a professional repairer.

Existing relevant standards should be duly considered when drafting the new harmonised 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 - Strage 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-I)
- 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)

1.4 Standards on interoperability (technical, semantic, organisation)

The standard(s) shall define, inter alia, rules related to:

(a) Semantic description of a product, including but not limited to unambiguous meaning and consistent naming, 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. It should include rules on how to systematically use such metadata models when developing product group specific data models.

Existing relevant standards should be duly considered when drafting the new harmonised 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

1.5 Standard(s) on data processing, data exchange protocols and data formats

The standard(s) shall define, inter alia, rules related to:

(a) Data exchange protocols, including rules to exchange data between two or more parties,
(b) Processes to introduce, modify, and update information in the passport,

Existing relevant standards should be duly considered when drafting the new harmonised 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 23387 Data templates for construction objects used in the life cycle of built assets — Concepts and principles.
- 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_CEFACT_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)
- UNCCL (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: https://w3c-ccg.github.io/vc-json-schemas/)
- 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 traceability data exchange structure (EPCIS) (available at: https://service.unece.org/trade/uncefact/publication/Transport%20and%20Logistics/Textile-Leather_UNECE/Traceability%20Event%20Message%20D22A/XSD/Schema.zip)

- 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)

1.6 Standards on data storage, archiving, and data persistence

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 would remain available even when the economic operator creating the passport is no longer active.

Existing relevant standards should be duly considered when drafting the new harmonised 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/)

1.7 Standards on data authentication, reliability, integrity

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. It/They 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.

The following issues should be addressed (non-exhaustive list):

(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 product fraud and counterfeit goods, by using object identification techniques,
(h) verifiable credentials,

Existing relevant standards should be duly considered when drafting the new harmonised 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/)

1.8 Standards on APIs for the DPP lifecycle management and searchability

The standard(s) aim at harmonising the Application Programming Interfaces (APIs) for automating the management of the digital product passport throughout its lifecycle and serving remote queries coming from the Digital Product Passport registry or applications from national authorities.

Custodians of Digital Product Passports (either Economic Operators or Service Providers) shall make available APIs covering:

- CRUD operations (**C**reate, **R**ead, **U**pdate, **D**elete) on Digital Products Passports and
- remote **Q**ueries on the Digital Products Passports under their custodianship.

When developing the standard(s), the following aspects, inter alia, should be adequately specified:

1. Syntax and semantics of the API interfaces
2. Security and access control to the APIs
3. Performance and response time
4. Considerations on versioning and backward compatibility of API interfaces
5. Message exchange patterns, e.g. synchronous, asynchronous, request-response, fire-and-forget, publish and subscribe
6. Availability and scalability
7. Mechanisms to ensure the authenticity, integrity and reliability of the data

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) should be used in the design of the APIs. Furthermore, existing relevant standards should 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/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)