EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 18216

June 2025

ICS 35.240.63

English version

Digital product passport - Data exchange protocols

Digitaler Produktpass - Protokolle zum Datenaustausch

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/CLC/JTC 24.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents

Page

European foreword

This document (prEN 18216:2025) has been prepared by Technical Committee CEN/CENELEC JTC 24 "Digital Product Passport - Framework and System", the secretariat of which is held by DIN.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a standardization request addressed to CEN by the European Commission. The Standing Committee of the EFTA States subsequently approves these requests for its Member States.

For the relationship with EU Legislation, see informative Annex ZA, which is an integral part of this document.

Introduction

This proposal is in response to the Standardization Request from the European Comission for the digital product passport, as seen in "Commision Implementing Decision of 31.7.2024 on a standardization 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" (C(2024) 5423 final). As specified in the Annex I, module 5, requesting a standard on "data processing, data exchange protocols and data formats".

A digital product passport (DPP) is a dynamic digital record that contains information about a product throughout its life cycle. For DPPs to be effective and universally accessible, standardized data exchange protocols and frameworks need to be in place. Standardization and harmonisation of these protocols ensure that all actors of the DPP - such as manufacturers, suppliers, retailers, consumers, repairers, waste treatments facilities, and regulatory authorities - can access, extract, utilise, and update the shared product passport information seamlessly. The subsequent sections of this document outline the standardization for data exchange protocols.

1 Scope

This document defines a standard for secure and efficient data exchange protocols and data formats to be used for the digital product passport. Data exchange protocols establish the rules and procedures that systems follow when communicating and exchanging information. Data formats define the structure and presentation of that information so it can be understood and processed correctly by the involved systems. Together, protocols and formats ensure that data can be exchanged in a manner that is secure, reliable, and compatible across various platforms and sectors.

This will guarantee that data is machine-readable, structured, searchable, and transferable through an open, interoperable network without vendor lock-in.

a) Secure communication:

this standard defines protocols that ensure secure and authenticated data exchange between systems, ensuring that data is protected against unauthorised access and that only authorised entities can access the information.

b) Interoperability for data exchange:

The protocols and data formats defined in this standard allow for easy integration with existing data exchange systems, ensure compatibility of protocols and formats across various sectors and supporting a wide range of applications and use cases.

c) Ease of use and integration:

Ensure that the identified protocols and formats can be implemented easily, especially for mobile devices, and are user-friendly in order to facilitate widespread adoption.

d) Data integrity:

The protocols and data formats defined in this document ensure the integrity of information linked to physical objects and electronic data throughout the entire value chain, extending to the product's or asset's end-of-life end-of-life.

e) Documentation and Discoverability:

The protocols and formats are available to individuals without specialised knowledge, enabling broader adoption across sectors

In order to promote interoperability, reduce costs for businesses, and align with existing European regulations and initiatives, this document considers the data exchange protocols and data formats already in use in other legislations. Relevant existing standards are integrated into the development process to ensure consistency and coherence with industry practices and regulatory frameworks.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

a) ISO Online browsing platform: available at http://www.iso.org/obp

b) IEC Electropedia: available at http://www.electropedia.org/

3.1
identifier
digital identifier
sequence of characters associated with digital, non-digital, or abstract entities, such as books, images, reports, metadata records or events

[SOURCE: [1], 3.2.1]

3.2
data exchange
storing, accessing, transferring, and archiving of data

[SOURCE: [2], 3.1.5]

3.3
identification
process of recognizing an object in a particular domain as distinct from other objects

[SOURCE: [3], 3.2.1]

3.4
authentication
verification that a claimed identity is correct

[SOURCE: [4], 3.2]

3.5
data integrity
property that data has not been altered or destroyed in an unauthorized manner

Note 1 to entry: In the context of secure communication, data integrity ensures that data transmitted between parties remains unaltered and intact from the moment it leaves the sender to the moment it reaches the receiver. This means that the data has not been tampered with, modified, or corrupted during transmission – whether accidentally or through malicious actions.

[SOURCE: [5]]

3.6
secure communication
mechanism of transmitting data between systems in a way that ensures its confidentiality, intergrity and authenticity

4 Data exchange protocols

The data exchange protocols listed below shall be used.

a) RESTful APIs are built upon the HTTP (Hypertext Transfer Protocol) standard. While REST (Representational State Transfer) itself is an architectural style rather than a formal standard, it leverages the existing standards and capabilities of HTTP to perform operations on web resources.

b) HTTP over TLS (HTTPS)

Protocol: HTTPS (HyperText Transfer Protocol Secure) is the secure version of HTTP, used for secure communication over a computer network.

Standards:

— TLS (Transport Layer Security): Defined by RFC 8446 for TLS 1.3. and future versions.

— HTTP/1.1, HTTP/2 and HTTP/3: Defined by RFC 7230-7235, RFC 7540 and RFC9114, respectively

Other data exchange protcols are allowed upon bilateral agreement.

5 Data formats

The data format listed below shall be used.

a) JSON (JavaScript Object Notation): It is a human and machine readable data-interchange format used to transmit data between a server and a client.

Besides the abovementioned, the message format may be used:

b) XML (Extensive Markup Language) is a markup language and file format for storing, transmitting and reconstructing arbitrary data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable

c) JSON-LD (JavaScript Object Notation for Linked Data) is a human-readable data format that provides context and links data, enhancing interoperability and integration between different data sources. Its representation shall be processible by a regular JSON parser, allowing the possibility of including linked data context for advanced semantic processing.

For human readable representation the following shall be provided:

The DPP shall be provided according to W3C HTML standards, and should be tested across a range of browser technologies and platforms.

d) HTML (Hypertext Markup Language): is the standard markup language for documents designed to be displayed in a web browser. It defines the content and structure of web content and is often assisted by technologies such as Cascading Style Sheets (CSS) and JavaScript.ext

The digital product passport does not have to be stored in HTML, but will be rendered in HTML.

6 Data exchange protocol requirements

6.1 General introduction to data exchange protocols

A data exchange protocol is a set of rules and standards that govern how data is transmitted, received, and interpreted between different systems or organizations. In the context of digital product passports (DPPs), these protocols are essential for enabling seamless communication and interoperability among various stakeholders, such as manufacturers, suppliers, retailers, consumers, and regulatory authorities.

Data exchange protocols ensure that the information contained within a digital product passport – such as product specifications, origin, materials, compliance certifications, and sustainability metrics – is consistently formatted and securely transmitted. This consistency allows different software applications, platforms, and systems to understand and utilize the data effectively, regardless of the underlying technologies they employ.

6.2 Secure data exchange

All data exchanges between the server and client shall use TLS.

NOTE This requirement applies to situations where an individual uses a mobile app, desktop software or embedded system integration to access a product's DPP. The application connects to the DPP service to retrieve detailed information about the product. This allows the user to make informed decisions or gain insights about

the product directly through the app. It is assumed that the data exchange is between Business to Customer (B2C) and therefore the relevant standards are proposed.

Additional relevant standards:

a) [6]: Network Security Protocols.

b) [7]: Information Security Management System (ISMS).

6.3 Data confidentiality and integrity for data exchange

The data exchange protocol shall maintain confidentiality and integrity of DPP data.

DPP data shall be encrypted during transmission.

NOTE When transferring DPP data from one organization to another organization:

Specific considerations also exist when one organization transfers the digital product passport to another organization. This typically occurs within a supply chain, such as when a manufacturer sends product information to a distributor or retailer. In an instance like this it could involve both the physical transfer of data between two locations as well as the standard access to data. This also assumes that the data exchange/data transfer occurs between Business to Business (B2B) or Business to Government (B2G).

DPP controlled data shall be encrypted during transmission.

When authorities or other organizations are requesting confidential access to a digital product passport based on their specified access rights, there exist specific requirements for when sensitive DPP data is accessed or transferred between organisations, often in regulatory or compliance contexts (B2B/B2G).

6.4 Secure data transmission

Requirement: Secure data exchange protocols shall be used for DPP data exchange.

6.5 Non-repudiation

Entities involved in the DPP data request shall not be able to deny sending or receiving the DPP.

NOTE When transferring DPP data from one organisation to another organisation:

Specific considerations also exist when one organisation transfers the digital product passport to another organisation. This typically occurs within a supply chain, such as when a manufacturer sends product information to a distributor or retailer. In such cases it could involve both the physical transfer of data between two locations as well as the standard access to data. This also assumes that the data exchange/data transfer occurs between Business to Business (B2B) or Business to Government (B2G). Similarly, sensitive DPP data could be accessed or transferred between organisations inregulatory or compliance scenarios (B2B/B2G)

6.6 Data transfer protocols

Data exchange protocols shall at a minimum conform to Clause 5 (b), 7.2 and 7.5

NOTE When transferring DPP data from one organization to another organization:

Specific considerations also exist when one organization transfers the digital product passport to another organization. This typically occurs within a supply chain, such as when a manufacturer sends product information to a distributor or retailer. In such cases it could involve both the physical transfer of data between two locations as well as the standard access to data. This also assumes that the data exchange/data transfer occurs between Business to Business (B2B) or Business to Government (B2G). Similarly, sensitive DPP data could be accessed or transferred between organizations inregulatory or compliance scenarios (B2B/B2G).

7 Data exchange

7.1 Security and access control

The data exchange protocols like the ones mentioned in Clause 5, should fundamentally enable secure communication between systems over the internet. These protocols should impose requirements to ensure data security, encryption, and overall integrity during data communication.

7.2 Ease of use and integration

Implementation of identified protocols for use in a straightforward manner, particularly also in the case of mobile devices.

Selecting the right data exchange standards is not just about technical specifications; it is also about how these standards fit into the organisations' workflow and how easily they can be adopted by different users and between actors. This section provides an overview of the data exchange standards, focusing on their ease of use and integration for consumers, small and medium-sized enterprises (SMEs), and larger businesses. Table 1 summarises the key points for each standard, highlighting how they impact and how they can be utilised by different user groups.

Table 1 — Overview of ease of use and implementation of data exchange protocols

Standard	Consumers	SMEs	Large Businesses/ Organisations
HTTPS (HTTP over TLS)	**Ease of use:** Consumers interact with HTTPS daily when browsing websites or using online services, often without realizing it. Modern web browsers automatically handle HTTPS connections.	**Ease of use:** Setting up HTTPS for a website or application is made easy by services like Let's Encrypt, which provide free SSL/TLS certificates.	**Ease of use:** Larger businesses typically have IT departments or IT vendors familiar with HTTPS implementation.
	Integration: Not Applicable	**Integration:** SMEs can integrate HTTPS by installing certificates on their web servers.	**Integration:** can integrate HTTPS by installing certificates on their web servers.
Restful APIs	**Ease of Use:** Consumers use applications that rely on RESTful APIs without needing technical knowledge**.**	**Ease of use:** Developer-friendly. Several frameworks and tools that simplify creating and consuming RESTful APIs are available.	**Ease of use:** Developer-friendly. Several frameworks and tools that simplify creating and consuming RESTful APIs are available.
	Integration: Not applicable	**Integration:** SMEs can easily integrate RESTful APIs into their products and services, enabling them to communicate with other applications and services over the internet.	**Integration:** Larger business and organisations already have knowledge and experience with APIs and probably already offer services based on APIs

7.3 Data integrity

7.3.1 General

The protocols shall support integrity of information linked with physical objects and electronic data throughout the value chain down to the final end of life of the product/asset

Data integrity refers to the accuracy, consistency, and trustworthiness of data throughout its entire lifecycle. In the context of secure communication, it ensures that data transmitted between parties remains unaltered and intact from the moment it leaves the sender to the moment it reaches the receiver.

This means that the data has not been tampered with, modified, or corrupted during transmission—whether accidentally or through malicious actions. This section provides a description of how data integrity is maintained when using the data exchange protocols:

— HTTPS Over TLS

— Restful APIs

The following clauses define how the various data exchange protocols preserve data integrity.

7.3.2 HTTP over TLS

a) Message Authentication Codes (MACs):

1) Integrity checks: HTTPS uses the Transport Layer Security (TLS) protocol, which incorporates MACs to ensure data integrity. MACs are cryptographic hash functions applied to the message data and a shared secret key.

2) Verification: When data is received, the MAC is recalculated and compared with the transmitted MAC. If they match, the data is considered intact.

b) TLS handshake and cipher suites:

1) Secure negotiation: during the TLS handshake, the client and server agree on a Cipher Suite that includes a specific hash function (e.g. SHA-256) for integrity checks.

2) Sequence numbers: TLS uses sequence numbers to prevent replay attacks and ensure that messages are processed in the correct order.

c) Certificate validation:

1) Trusted authorities: certificates issued by trusted certificate authorities (CAs) help ensure that the entities involved are legitimate, preventing man-in-the-middle attacks that could compromise data integrity.

7.3.3 RESTful APIs

Underlying HTTPS protocol: inherited security: RESTful APIs often operate over HTTPS, leveraging TLS's data integrity mechanisms like message authentication codes.

a) Message validation:

1) Input validation: servers validate incoming data to ensure it meets expected formats and values, preventing malformed or malicious data from causing unintended effects.

2) Response validation: clients can validate responses using checksums or hash comparisons when provided.

b) Digital signatures and tokens:

1) JSON web tokens (JWT): Tokens may include signatures (using HMAC (hash-based message authentiation) or RSA (Rivest–Shamir–Adleman) algorithms) to verify the integrity of the token data.

2) OAuth 2.0 and OpenID Connect: tokens used for authentication and authorization can be validated to ensure they haven't been tampered with.

3) Idempotent operations:

i) HTTP methods: use of safe and idempotent HTTPs methods (like GET, PUT) helps maintain integrity by ensuring consistent outcomes.

8 Secure communication

8.1 General

Secure communication defines the mechanism of transmitting data between systems in a way that ensures its confidentiality, integrity and authenticity. This means that the data exchanged is protected from unauthorised access, tampering, or interception by malicious actors. Therefore, this subclause will outline how the data exchange protocols meet the requirements for secure communication. Therefore, this section outlines the secure communication requirements of the following technologies:

— HTTPS over TLS

— Restful APIs

8.2 How HTTPS and RESTful APIs satisfy secure communication

8.2.1 HTTPS (using TLS 1.2 or 1.3)

HTTPS ensures secure, encrypted communication between the user's mobile app, desktop software, or embedded system and the DPP service. This prevents man-in-the-middle attacks or eavesdropping during data transmission. The TLS protocol secures communication by using asymmetric public key infrastructure. This type of security system uses two different keys to encrypt communication between parties:

a) The private key – this key is controlled by the owner of a website and kept private. This key resides on a web server and is used to decrypt information encrypted by the public key.

b) The public key – this key is available to everyone to securely interact with the server. Information encrypted by the public key can only be decrypted using the private key.

8.2.2 RESTful APIs

RESTful APIs use the underlying HTTPS protocol to enable secure, stateless data exchange between the client and server. The security of RESTful APIs primarily relies on the HTTPS protocol, which ensures encryption and secure data transmission. RESTful APIs ensure secure communication by:

a) Statelessness: Each request to the server is independent and includes all the information needed for processing. This ensures that sensitive data, such as authentication tokens, is always transmitted over HTTPS, maintaining encryption during transfer.

b) Security: RESTful APIs shall implement appropriate measures to ensure confidentiality integrity, availability and authenticity.

c) Rate Limiting: To prevent abuse, REST APIs should implement: rate limiting per client, provide rate limit notification, Support rate limit exemptions for authorized services, and log rate limit events.

d) DDoS Protection: REST APIs should implement appropriate traffic filtering, support traffic rate limiting, provide attack protection, implement mitigation measures, and maintain service availability

e) Error Handling and Status Codes: RESTful APIs use HTTP status codes to communicate the outcome of a request to the client, ensuring transparency in how the API operate. Errors related to authentication (e.g. 401 unauthorised) or authorization (e.g. 403 Forbidden) help indicate failed security checks, protecting against unauthorised access.

8.3 Identification, authentication, and authorization

In addition to data exchange protocols, authentication and authorization play crucial roles in ensuring secure communication and controlled access to data. This digital product passport may contain

Commented [PL1]: Regarding rate limiting per client: Add an informative reference to https://datatracker.ietf.org/doc/html/draft-ietf-httpapi-ratelimit-headers as a relevant method for providing machine-readable info about rate limiting.

Commented [PL2]: DDoS is not only a problem for REST APIs. It's the classic attack to websites. Therefore, same requirement should be included in the HTTPS section of 8.2.1.
Proposed change:Add the same requirement for DDoS protection in section 8.2.1 on HTTPS

information available to the public as well as data restricted to specific groups with vested interests. For example, an electric vehicle battery could include the chain of ownership as public information accessible to everyone. However, it might also contain specialised information – such as manuals for battery cell pack production – that should only be accessed by authorized parties like battery recyclers or repair technicians.

8.3.1 9.2.1 OAuth 2.0

[8]OAuth 2.0 is a widely used framework for authorization, allowing third-party applications to securely access a server's resources without exposing user credentials. It ensures secure communication through token-based access control. OAuth 2.0 works to secure communication as follows:

a) Authorization via Access Tokens: OAuth 2.0 operates by issuing access tokens to a client (application) after the user grants permission. These tokens represent the user's authorization to access specific resources and are passed along with API requests. Because tokens are sent over HTTPS, they are encrypted and secured from interception.

b) Access Token Expiry and Refresh: Tokens have an expiration period, e.g. even if a token is compromised, its usage is limited. To maintain access, refresh tokens can be issued, allowing the client to request a new access token without re-authentication. This reduces the risk associated with long-lived credentials.

c) Token Scopes: OAuth 2.0 allows for scoping, which limits the actions permitted by the access token. For example, a token might allow only read only access to a user's profile but not write access. This principle of least privilege minimises risk by restricting unauthorised actions

8.3.2 OpenID Connect (OIDC)

is an identity layer built on top of [9]OAuth 2.0, primarily used for authentication (verifying a user's identity). It ensures secure communication in the authentication process as follows:

a) ID Token: When a user logs in, OpenID Connect issues an ID token along with the OAuth access token. This ID token contains information about the authenticated user (e.g. their identity) in a digitaly signed JSON Web Token (JWT) format to ensure its authenticity.

b) JWT (JSON Web Token) Signing and Encryption: The ID token is typically signed using asymmetric cryptography (RSA) or HMAC (for symmetric encryption). The signature can be verified by the client to ensure the token hasn't been tampered with and is issued by a trusted provider.

c) User Authentication Flow: OpenID Connect allows for single sign-on (SSO) across multiple applications using a centralised identity provider (e.g., Google, Microsoft). This ensures that users only authenticate once and securely reuse the ID token to access multiple services, without repeatedly entering credentials.

d) HTTPS for Token Transmission: As with OAuth 2.0, all token exchanges in OpenID Connect are encrypted using HTTPS, ensuring secure transmission of the user's identity, and preventing man-in-the-middle attacks

8.3.3 CEF eID

The Connecting Europe Facility (CEF) [10] eID is a framework that enables secure cross-border electronic identification, allowing users to authenticate themselves when accessing public and private services across the EU. It ensures secure and verified access to resources based on authentication mechanisms and standardised security features. This includes:

a) Secure Access to Resources: As a robust authentication method, CEF eID ensures that users accessing digital resources – such as government portals or cloud-based services – are securely identified. This allows service providers to trust the user's identity.

b) XML Signatures for Security: CEF eID is built on security technologies, including the use of XML signatures, which ensure the integrity and authenticity of transmitted data. These digital signatures verify that the communication or document has not been altered and that the origin of the data is trusted.

8.3.4 Decentralised identifiers (DIDs)

Decentralised identifiers (DIDs) [11] is a framework for self-sovereign identity (SSI), allowing individuals to create, control, and manage their digital identities without relying on centralised authorities. DIDs provide secure and privacy-enhancing identity management as follows:

a) Self-Sovereign Identity Control: DIDs allow users to generate their own identifiers without relying on a central authority. These identifiers are stored on decentralised systems, such as blockchain, enabling users to maintain full control over their digital identities.

b) Verifiable Credentials: DIDs are often paired with verifiable credentials, cryptographically signed pieces of information about a person or entity. These credentials can be presented to third parties as proof of identity or other claims without revealing excessive personal information, ensuring privacy and security.

c) Public-Key Infrastructure and Cryptographic Security: DIDs leverage public-key cryptography to ensure the authenticity and integrity of identity data. The holder of a DID controls the corresponding private key, allowing them to sign and verify identity-related transactions securely.

d) Secure Data Transmission: Like other secure identity frameworks, DIDs rely on encrypted channels (e.g. HTTPS) to transmit sensitive identity-related information, ensuring protection from eavesdropping or tampering.

Annex A
(informative)

Systems compatible with data exchange protocols

The requirements on data exchange protocols can be compatible with the following systems.

This list is non-exhaustive. Other solutions are possible.

a) AS4 Profile of ebMS 3.0. The OASIS ebMS 3.0 Standard combined multiple Web Service standards to create a single comprehensive specification for defining the secure and reliable exchange of documents using Web Services. (AS4 Profile of ebMS 3.0 Version 1.0 (oasis-open.org))

b) Asset Administration Shell: The Asset Administration Shell (AAS) is the digital representation of an asset. The AAS consists of a number of submodels in which all the information and functionalities of a given asset – including its features, characteristics, properties, statuses, parameters, measurement data and capabilities – can be described. It allows for the use of different communication channels and applications and serves as the link between objects and the connected, digital and distributed world. The AAS is designed to be flexible and interoperable allowing it to operate over various data exchange protocols suitable for industrial environments.

c) EDI (Electronic Data Interchange): It is the computer-to-computer exchange of business documents in a standardised electronic format between trading partners. EDI replies on various data transfer protocols to transmit documents.

Commented [PL3]: Annex A provides a limited list of standards that are incoherent mixing and matching different concepts:
AS/4 is a message exchange protocol based on SOAP API
EDI is not a technology but, essentially, is a process defining standards for data formats and leveraging, for the exchange, technologies like AS/4 and, then, it makes no sense to have the two technologies mentioned as alternative solutions.
AAS is, essentially, a master data infrastructure for assets
Verifiable Credentials concept is not mentioned at all.
From a practical implementation point of view Annex A does not contain valuable information. Being very limited and incomplete, it may result misleading

Solution: remove Annex A

Annex ZA
(informative)

Relationship between this European Standard and the ecodesign requirements of Commission Regulation (EU) No 2024/1781 aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2024) 5423 final of 31.07.2024 to provide one voluntary means of conforming to the ecodesign requirements of Commission Regulation (EU) No 2024/1781 of 28.06.2024 implementing Directive 2009/125/EC of the European Parliament and of the Council with regard to ecodesign requirements for digital product passports in support of Union policy on ecodesign requirements for sustainable products and on batteries and waste batteries

Once this standard is cited in the Official Journal of the European Union under that Regulation, compliance with the normative Clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding ecodesign requirements of that Regulation and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Commission Regulation (EU) No 2024/1781 of 28.06.2024 implementing Directive 2009/125/EC of the European Parliament and of the Council with regard to ecodesign requirements digital product passports in support of Union policy on ecodesign requirements for sustainable products and on batteries and waste batteries and Commission's standardization request C(2024) 5423 final of 31.07.2024

part 5: European standard(s) on data processing, data exchange protocols and data formats

[Essential]/ [interoperability]/[...] Requirements of [Directive]/[Regulation]/ [Decision] [...]	Clause(s)/sub-Clause(s) of this EN	Remarks/Notes
10.1.d	5, 5.a, 5.b	interoperable, open standards for data exchange protocols
10.1.d	6, 6.a, 6.d	open interoperable standards for machine readable data formats without vendor lock-in
11.a	6, 6.a, 6.d	open interoperable standards for machine readable data formats without vendor lock-in
11.a	8, 8.2, 8.3	fully interoperable standards for data exchange and data integrity
11.g	9.3, 7.4	handles identification, authentification and authorisation aspects
11.h	9.1, 9.2	ensures secure communication via HTTP over TLS and secure implementation of RESTful API
14	7.2, 7.6	ensures secure data exchange with non-repudiation
15.1	7.2, 7.3	ensures secure data exchange, data confindentiality and integrity
15.2	7.1, 7.2	provides full set of data exchange protocols for integration in customs applications and registry
15.4	7.1, 7.3, 7.5	non repudiable exchange of data via open confidential and secure exchange protocols

WARNING Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING Other Union legislation may be applicable to the falling within the scope of this standard

.

Bibliography

[1] ISO 24619:2011, *Language resource management — Persistent identification and sustainable access (PISA)*

[2] ISO 15531-43:2006, *Industrial automation systems and integration — Industrial manufacturing management data — Part 43: Manufacturing flow management data: Data model for flow monitoring and manufacturing data exchange*

[3] ISO/IEC 24760-1:2011, *Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts*

[4] ISO/IEC/IEEE 8802-1AR:2020, *Telecommunications and exchange between information technology systems — Requirements for local and metropolitan area networks — Part 1AR: Secure device identity*

[5] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[6] ISO/IEC 27033 series, *Information technology - Security techniques - Network security*

[7] ISO/IEC 27001, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[8] FC 6749 - The OAuth 2.0 Authorization Framework (ietf.org) https://datatracker.ietf.org/doc/html/rfc6749

[9] OpenID Connect Protocol (auth0.com) https://auth0.com/docs/authenticate/protocols/openid-connect-protocol

[10] eID (europa.eu) https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eID

[11] Decentralized Identifiers (DIDs) v1.0 (w3.org) https://www.w3.org/TR/did-core/