



SLOVENSKI STANDARD

SIST EN 18246:2026

01-november-2026

Digitalni potni list izdelka - Preverjanje pristnosti, zanesljivost in celovitost podatkov

Digital product passport - Data authentication, reliability and integrity

Digitaler Produktpass - Datenauthentifizierung, Zuverlässigkeit und Integrität

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

Ta slovenski standard je istoveten z: EN 18246:2026

ICS:

13.020.20	Okoljska ekonomija. Trajnostnost	Environmental economics. Sustainability
35.240.63	Uporabniške rešitve IT v trgovini	IT applications in trade

SIST EN 18246:2026

en,fr,de

Sample Document

get full document from standards.iteh.ai

EUROPEAN STANDARD

EN 18246

NORME EUROPÉENNE

EUROPÄISCHE NORM

September 2026

ICS 35.240.63

English version

Digital product passport - Data authentication, reliability and integrity

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

Digitaler Produktpass - Datenauthentifizierung,
Zuverlässigkeit und Integrität

This European Standard was approved by CEN on 17 August 2026.

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. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists 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.



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

Contents

Page

European foreword	4
Introduction	5
1 Scope.....	7
2 Normative references.....	7
3 Terms and definitions.....	7
4 General security assumptions for DPP.....	10
4.1 General.....	10
4.2 Actors of the system.....	10
4.3 Access to public DPP data	10
4.4 Communication	10
4.5 Product identifier as stored in data carrier	11
4.6 Data carrier authenticity.....	11
4.7 DPP authenticity and data integrity.....	11
5 Types of risk and requirements for unique product identifiers, data carriers and DPP data	12
5.1 Risk on data security and privacy.....	12
5.1.1 General.....	12
5.1.2 Protection of personal data.....	12
5.1.3 Security of personal data	12
5.1.4 Security of organizational data.....	12
5.1.5 Prevention of profiling.....	13
5.1.6 Ensuring safe user access.....	13
5.1.7 Protection against phishing, quishing, and malicious code	13
5.1.8 Safeguarding against mass data scraping	13
5.2 Risk and requirements on identification	14
5.2.1 General.....	14
5.2.2 Authentication and traceability of responsible actors.....	14
5.3 Risk to products.....	14
5.3.1 Protecting against counterfeiting	14
5.3.2 Risks related to DPP data integrity	14
5.4 Risk and requirements to prevent exclusion	14
5.4.1 General.....	14
5.4.2 Accessibility to a DPP with any consumer device	15
5.4.3 Accessibility for persons with disabilities.....	15
Annex A (normative) Electronically signed data constructs (ESDCs)	16
A.1 General.....	16
A.2 Introduction.....	16
A.3 Key characteristics.....	16
Annex B (informative) Examples of electronically signed data constructs (ESDCs).....	18
B.1 General.....	18
B.2 Electronic attestation of attributes	18

B.3	Visible digital seal (VDS - ISO 22376).....	19
B.4	AIDC digital signature verifiable data structure (DigSig - ISO/IEC 20248)	20
B.5	W3C Verifiable Credentials	21
B.6	Digital signatures and electronic seals	22
Annex C (informative)	Risk and considerations related to fair competition	23
C.1	General	23
C.2	Avoiding market restrictions by vendor-specific software.....	23
C.3	Disproportionate resource demand for SMEs.....	23
Annex ZA (informative)	Relationship between this European Standard and the requirements of Regulation (EU) 2024/1781 aimed to be covered	24
Bibliography		25

Sample Document

get full document from standards.iteh.ai

EN 18246:2026 (E)**European foreword**

This document (EN 18246:2026) has been prepared by the Joint Technical Committee CEN-CENELEC/JTC 24 “Digital Product Passport - Framework and System”, the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by March 2027, and conflicting national standards shall be withdrawn at the latest by March 2027.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a standardization request addressed to CEN-CENELEC 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.

Any feedback and questions on this document should be directed to the users’ national standards body/national committee. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organisations of the following countries are bound to implement this European Standard: 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 the United Kingdom.

Introduction

0.1 Background

A digital product passport (DPP) is a key enabling mechanism to make product information traceable and accessible across value chains – supporting economic operators, manufacturers, distributors, repairers, recyclers and consumers to make informed decisions and to support a circular economy. The implementation of DPPs will be carried out progressively. Sector-specific initiatives will determine the precise DPP content and requirements for individual product groups.

To support the implementation of DPPs, 8 standards have been developed:

- EN 18219:2026 – Digital product passport – Unique identifiers
- EN 18220:2026 – Digital product passport – Data carriers
- EN 18216:2026 – Digital product passport – Data exchange protocols
- EN 18222:2026 – Digital product passport – Application Programming Interfaces (APIs) for the product passport lifecycle management and searchability
- EN 18223:2026 – Digital product passport – System interoperability
- EN 18221:2026 – Digital product passport – Data storage, archiving, and data persistence
- EN 18239:2026 – Digital product passport – Access rights management, information system security, and business confidentiality
- EN 18246:2026 – Digital product passport – Data authentication, reliability and integrity (this document)

0.2 Overview

Trust is key to any transaction whether physical or digital. Data and information collected during the whole life cycle of the product is to be protected from both accidental and malicious compromise and misuse.

Reasonable security expectation is likely to address the following elements of the DPP deployment:

- management and verification of identifiers;
- relationship between the unique identifiers and possible authentication elements related to them;
- questions that deal with the identification of the verifier and any authorized access to privileged product-related information;
- authentication solutions;
- artefact metrics (technical measurements used to support verification or trust in physical objects), where relevant;
- information processing and communication that protects integrity along the supply chain of physical and related electronic documents, products, software and services life cycle to mitigate the risk of product fraud and counterfeit goods, by using object identification techniques; and
- electronically signed data constructs (ESDCs) or equivalent functions.