



# SLOVENSKI STANDARD

## oSIST prEN 18246:2025

01-oktober-2025

---

**Digitalni potni list za proizvode - 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: prEN 18246**

---

**ICS:**

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

**oSIST prEN 18246:2025**

**en,fr,de**



EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**DRAFT**  
**prEN 18246**

August 2025

ICS 13.020.20; 35.240.63

English version

**Digital product passport - Data authentication, reliability  
and integrity**

Digitaler Produktpass - Datenauthentifizierung,  
Zuverlässigkeit und Integrität

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**

<b>Contents</b>	<b>Page</b>
<b>European foreword .....</b>	<b>4</b>
<b>Introduction .....</b>	<b>5</b>
<b>1 Scope.....</b>	<b>6</b>
<b>2 Normative references.....</b>	<b>6</b>
<b>3 Terms and definitions .....</b>	<b>6</b>
<b>4 General security assumptions for DPP.....</b>	<b>7</b>
4.1 General.....	7
4.2 Actors of the system.....	7
4.3 Access to public DPP data .....	7
4.4 Communication .....	8
4.5 Product identifier as stored in data carrier .....	8
4.6 Data carrier authenticity.....	8
4.7 DPP data authentication.....	8
4.8 Electronically signed data constructs (ESDCs).....	9
4.8.1 Introduction to ESDCs .....	9
4.8.2 General services of ESDCs .....	9
4.8.3 General implementation principles of ESDCs.....	9
<b>5 Types of risk and requirements for unique product identifiers, data carriers and DPP Data .....</b>	<b>10</b>
5.1 Risk on data security and privacy.....	10
5.1.1 General.....	10
5.1.2 Protection of personal data.....	10
5.1.3 Security of personal data .....	10
5.1.4 Security of organizational data.....	11
5.1.5 Prevention of profiling.....	11
5.1.6 Ensuring safe user behaviour.....	11
5.1.7 Protection against phishing, quishing, and malicious code .....	11
5.1.8 Safeguarding against mass data scraping .....	11
5.2 Risk and requirements on identification .....	11
5.2.1 General.....	11
5.2.2 Authentication and traceability of responsible actors.....	12
5.2.3 Alignment between data providers and product manufacturers .....	12
5.3 Risk to products.....	12
5.3.1 Protecting against counterfeiting .....	12
5.3.2 Risks to DPP-related product fraud .....	12
5.4 Risk and requirements related to fair competition .....	12
5.4.1 General.....	12
5.4.2 Avoiding market restrictions by vendor specific software .....	12
5.4.3 Disproportionate resource demand for SMEs .....	13
5.5 Risk and requirements to prevent exclusion .....	13
5.5.1 General.....	13
5.5.2 Accessibility to a DPP with any consumer device .....	13
5.5.3 Accessibility for persons with disabilities .....	13
<b>Annex A (informative) Examples of electronically signed data constructs (ESDCs) .....</b>	<b>14</b>