SLOVENSKI STANDARD
oSIST prEN 40000-10:2026

01-julij-2026

Bistvene zahteve kibernetske varnosti za izdelke - 10. del: Izdelki z digitalnimi elementi, ki se uporabljajo v sistemih upravljanja identitete in programski ter strojni opremi za vodenje privilegiranega dostopa, vključno z bralniki za preverjanje pristnosti in nadzor dostopa, vključno z biometričnimi bralniki

Essential cybersecurity requirements for products - Part 10: Products with digital elements used in identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

Grundlegende Anforderungen an die Cybersicherheit für Produkte mit digitalen Elementen, die in Identitätsmanagementsystemen und Software und Hardware für die Verwaltung des privilegierten Zugangs verwendet werden, einschließlich Authentifizierungs- und Zugangskontrollleser, einschließlich biometrischer Leser

Ta slovenski standard je istoveten z: **prEN 40000-10**

ICS:

35.030	Informacijska varnost	IT Security
35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

oSIST prEN 40000-10:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 40000-10

May 2026

ICS 35.030; 35.240.15

English Version

Essential cybersecurity requirements for products - Part 10: Products with digital elements used in identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers

Grundlegende Anforderungen an die Cybersicherheit für Produkte mit digitalen Elementen, die in Identitätsmanagementsystemen und Software und Hardware für die Verwaltung des privilegierten Zugangs verwendet werden, einschließlich Authentifizierungs- und Zugangskontrollleser, einschließlich biometrischer Leser

This draft European Standard is submitted to CEN members for enquiry. It has been drawn up by the Technical Committee CEN/TC 224.

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

CEN members are the national standards bodies 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.

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.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

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

Ref. No. prEN 40000-10:2026 E

Contents

European foreword

This document (prEN 40000-10:2026) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

This document is currently submitted to the CEN Enquiry.

This document has been prepared under a standardisation 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 document has been prepared in response to a standardisation request issued by the European Commission in support of the implementation of Regulation (EU) 2024/2847 (Cyber Resilience Act, CRA).

The Cyber Resilience Act establishes horizontal cybersecurity requirements for products, including requirements for the design, development and production of such products, as well as obligations for economic operators throughout the lifecycle of those products. In particular, it lays down essential cybersecurity requirements and conformity assessment procedures to ensure a high level of cybersecurity within the Union.

This document specifies cybersecurity requirements and associated assessment provisions for identity management systems that qualify as products and are classified as important products (Class 1) in accordance with Commission Implementing Regulation (EU) 2025/2392.

The purpose of this document is to support manufacturers, conformity assessment bodies and other relevant stakeholders in demonstrating conformity with the essential cybersecurity requirements set out in Annex I of the Cyber Resilience Act for the category of products covered by its scope.

This document follows a risk-based approach, taking into account the specific characteristics, intended use, and threat landscape applicable to identity management systems, including authentication, authorisation, identity lifecycle management and access control functionalities. It defines relevant risk profiles and maps them to corresponding cybersecurity requirements and assessment methods.

1 Scope

This document specifies cybersecurity requirements and associated assessment requirements for identity management systems that qualify as products within the meaning of Regulation (EU) 2024/2847. Such products are classified as important products (class 1) according to the implementing regulation Commission Implementing Regulation (EU) 2025/2392.

Identity management systems are products that provide mechanisms for authentication or authorisation and that may also provide mechanisms for the lifecycle management of identity credentials of natural persons, legal persons, devices or systems, such as identity registration, provisioning, maintenance, deregistration.

These systems include access management systems that control access of natural persons, legal persons, devices or systems to digital resources or physical locations.

Privileged access management software is an access management system that controls and monitors access rights to IT or OT systems and sensitive information within an organisation, including systems enforcing differentiated access control policies for privileged users.

This category includes but is not limited to authentication and access control readers, biometric readers, single sign-on software, federated identity management software, one-time password software, hardware authentication devices such as transaction authentication number (TAN) generators, authentication software and multi-factor authentication software.

This document covers:

- general description of the product belonging to that category and the product and/or components such product with digital elements;
- description of their use case;
- security analysis;
- definition of applicable risk profiles to be considered for these product with digital elements;
- applicable cybersecurity requirements for each risk profile;
- applicable cybersecurity assessment and test requirements for each risk profile.

Products within the scope of this document:

The following non-exhaustive categories of products are within the scope of this document where their primary or supporting function relates to identity management, authentication, authorisation, or logical and physical access control to natural persons, legal persons, devices or systems.

Logical and Physical Identity lifecycle management

Products for:

- identity registration and enrolment;
- credential issuance, provisioning and activation;
- credential maintenance, suspension, revocation and deletion;
- identity wallets and digital credential containers;
- EUDI Wallet, EU Business Wallet;
- crypto asset Wallet;
- digital travel credential;
- middleware enabling the use, validation or verification of identity credentials;

- national or sectorial identity registries implemented as products;
- biometric databases;
- enrolment stations;
- digital transaction control components;
- mobile driving license;
- electronic identification products, including systems supporting digital product passport.

Logical and Physical Authentication

Products for:

- authentication software;
- multi-factor authentication (MFA) systems;
- two-factor authentication (2FA) systems;
- one-time password (OTP) software and hardware tokens;
- online authentication tokens;
- hardware authentication devices;
- single sign-on (SSO) systems;
- federated identity management systems;
- authentication and access control readers;
- biometric readers;
- presentation attack detection (PAD) software;
- identity attack detection (IAD) software;
- biometric matching software;
- automatic border control product;
- entry/exist product;
- ESTIA application.

Logical and Physical Biometric identity management

Products for:

- capture biometric data for enrolment purposes;
- perform biometric verification or identification;
- biometric matching;
- remote data processing system of biometric reference data;
- incorporate artificial intelligence components for biometric recognition, verification, identification or fraud detection.

Logical and Physical Access management

Products for:

- logical access control systems;

- physical access control systems;
- access control readers and local control units;
- access control supervision and monitoring software;
- access management supervision systems;
- anti-intrusion systems;
- CCTV;
- smart lock.

Logical and Physical Privileged access management

- control and monitor access rights of privileged users;
- enforce differentiated access control policies;
- manage privileged credentials;
- monitor, record and audit privileged sessions;
- protect access to critical IT or OT systems and sensitive information.

Product not in the scope of this document:

All other important and critical products that are covered by harmonised standards as per the standardisation request Mandate M/606 2025-02-03 such as:

- chip, Embedded OS, Applets;
- PKI products;
- cyber security products needed for securing IT infrastructures (VPN, SIEM….);
- all products that are classified as default such as the anti-fire detectors products.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

prEN 40000-1-3:2025, *Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling*

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

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

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

— ISO Online browsing platform: available at https://www.iso.org/obp/

— IEC Electropedia: available at https://www.electropedia.org/

3.1.1
asset
anything that has value to an individual, an organization or a government

[SOURCE: ISO/IEC 27035-3:2020, 3.1]

3.1.2
authenticity
property that an entity is what it claims to be

[SOURCE: EN ISO/IEC 27000:2020, 3.6]

3.1.3
availability
property of being accessible and usable on demand by an authorized entity

[SOURCE: EN ISO/IEC 27000:2020, 3.7]

3.1.4
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: EN ISO/IEC 27000:2020, 3.10]

3.1.5
integrity
property of accuracy and completeness

[SOURCE: EN ISO/IEC 27000:2020, 3.36]

3.1.6
likelihood
chance of something happening

Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. However, in English, “probability” is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, “likelihood” is used with the intent that it should have the same broad interpretation as the term “probability” has in many languages other than English.

[SOURCE: ISO 31000:2018, 3.7]

3.1.7
remediation
change made to a product or service to remove or mitigate a vulnerability

Note 1 to entry: A remediation typically takes the form of a binary file replacement, configuration change, or source code patch and recompile. Different terms used for “remediation” include patch, fix, update, hotfix, and upgrade. Mitigations are also called workarounds or countermeasures.

[SOURCE: EN ISO/IEC 29147:2020, 3.7]

3.1.8
residual risk
cybersecurity risk remaining after risk treatment

[SOURCE: EN ISO/IEC 27000:2020, 3.57]

3.1.9
product with digital elements
(hereinafter called “product”)
software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately

[SOURCE: CRA, Article 3(1)]

3.1.10
hardware
physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data

[SOURCE: CRA, Article 3(5)]

3.1.11
software
part of an electronic information system which consists of computer code

[SOURCE: CRA, Article 3(4)]

3.1.12
intended purpose
use for which a product with digital elements is intended by the manufacturer, including the specific context and conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation

[SOURCE: CRA, Article 3(23)]

3.1.13
embedded software
software product with digital elements loaded in a hardware Product with digital element, and in which it is executed

Note 1 to entry: an embedded software is a sub part of a hardware Product with digital elements

3.1.14
hardware product with digital elements
product with digital elements that have the shape of a hardware

Note 1 to entry: hardware Product with digital elements are tangible

Note 2 to entry: a hardware Product with digital element can be the environment on which a software Product with digital element is executed and optionally loaded.