SLOVENSKI STANDARD
oSIST prEN 40000-11:2026

01-julij-2026

Bistvene zahteve kibernetske varnosti za izdelke - 11. del: Strojne naprave z varnostnimi škatlami, ki vključujejo strojno fizično ovojnico in so zasnovane za zagotavljanje varnostnih funkcij, kot so varno shranjevanje in kriptografske operacije v odprtem okolju

Essential cybersecurity requirements for products - Part 11: Hardware Devices with Security Boxes incorporating a hardware physical envelope and designed to provide security functions such as secure storage and cryptographic operations in an open environment

Grundlegende Cybersicherheitsanforderungen gemäß CRA für Hardware-Geräte mit Sicherheitsboxen, die eine physische Hardware-Umhüllung enthalten und für die Bereitstellung von Sicherheitsfunktionen wie sichere Speicherung und kryptografische Operationen in einer offenen Umgebung ausgelegt sind

Exigences essentielles de cybersécurité pour les produits - Partie 11: Dispositifs matériels avec coffrets de sécurité intégrant une enveloppe physique et conçus pour fournir des fonctions de sécurité telles que le stockage sécurisé et des opérations cryptographiques dans un environnement ouvert

Ta slovenski standard je istoveten z: **prEN 40000-11**

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN 40000-11:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 40000-11

May 2026

ICS 35.030

English Version

Essential cybersecurity requirements for products - Part 11: Hardware Devices with Security Boxes incorporating a hardware physical envelope and designed to provide security functions such as secure storage and cryptographic operations in an open environment

Grundlegende Cybersicherheitsanforderungen gemäß CRA für Hardware-Geräte mit Sicherheitsboxen, die eine physische Hardware-Umhüllung enthalten und für die Bereitstellung von Sicherheitsfunktionen wie sichere Speicherung und kryptografische Operationen in einer offenen Umgebung ausgelegt sind

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 40000-11:2026 E

Contents

Page

European foreword

This document (prEN 40000-11:2026) 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 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

The present document defines cybersecurity requirements applicable to Hardware Devices in Security Boxes. It applies to products with digital elements designed to provide cryptographic services and secure storage as well as protection against physical attacks.

It supports the implementation of Regulation (EU) 2024/2847, the Cyber Resilience Act, specifically addressing the essential cybersecurity requirements defined in Annex I, Parts I and II.

Application of this document

In order to establish presumption of conformity using this standard, the following steps must be followed:

— **Step 1:** Decide on the pathway ('template' or 'rule-based') from Annex A to identify a suitable security profile for the HWSB based on its IPRFU.

  The security profile will define what security requirements are applicable based on selection of requirements modules from Clause 5 alongside an 'assurance profile' that is used with conformity assessment activities in Clause 6.

— **Step 2:** Develop an HWSB compliant with applicable security requirement using examples where appropriate.

— **Step 3:** Develop evidence required to complete conformity assessment activities listed in Clause 6 based on applicable security requirements and required test and evidence checks overlayed with the selected assurance profile.

— **Step 4:** Perform the conformity assessment including:

  o evidence review,

  o independent functional testing (if using assurance profile high), and

  o vulnerability testing.

Presumption of conformity as an HWSB is achieved if all checks and testing meet the listed pass criteria.

1 Scope

This document defines cyber security requirements for products with digital elements belonging to product category “Hardware Device with Security Boxes” (hereinafter called “Product” or “HWSB product”).

The technical description of “Hardware Devices with Security Boxes” can be found in Annex II of [CRA].

The Hardware Devices with Security Boxes in scope are designed for deployment in a range of environments and where the threat landscape includes attackers with various attack potential.

HWSB are hardware-based systems intended to provide secure storage, processing and use of sensitive data, including cryptographic assets, within a protected hardware boundary (envelope).

This document applies to the HWSB part of the product. The applicability of this document to specific products is determined based on their intended purpose, use case and risk assessment.

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*

AIS20/31, *A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI)*

NIST SP800-90A, *Recommendation for Random Number Generation using Deterministic Random Bit, National Institute of Science and Technology (NIST)*

NIST SP800-90B, *Recommendation for the entropy sources used for random bit generation, National Institute of Science and Technology (NIST)*

NIST SP800-90C, *Recommendations for Random Bit Generator (RBG) Constructions, National Institute of Science and Technology (NIST)*

ISO/IEC 18031:2025, *Information technology — Security techniques — Random bit generation*

3 Terms and definitions and abbreviations

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:

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

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

3.1
application
software that provides service(s) to the user of the final product

3.2
attack potential
measure of effort needed to exploit a vulnerability in a product

Note 1 to entry: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

[SOURCE: EN ISO/IEC 15408-1:2023, 3.8]

3.3
client application
application running external to the HWSB that consumes its services either over a local or remote interface

3.4
firmware
code that is embedded inside the HWSB

3.5
internal application
application running internal to the HWSB that consumes its services over an internal interface

3.6
local application
application running external to the HWSB that consumes its services over a local interface

3.7
multi-factor authentication
authentication of an operator using at least two independent authentication factors. All authentication data is verified by the cryptographic module

Note 1 to entry: An authentication factor is operator related information that resides outside the module, is used as proof of identity, and may include a method/process to produce varying or short-lived authentication data from the operator related information.

Note 2 to entry: Independent authentication factor categories for human operators include: something known, such as a secret password, something possessed, such as a physical key or token, and a physical property, such as a biometric.

[SOURCE: ISO/IEC 19790:2025, 3.86]

3.8
remote application
application running external to the HWSB that consumes its services over a remote interface

3.9
security attribute
property of subjects, users, objects, information, sessions or resources that is used in defining the security functions and whose values are used in enforcing the security functions

Note 1 to entry: Users can include external IT products.

[SOURCE: EN ISO/IEC 15408-1:2023, 3.77]

3.10
security profile
suite of assurance activities and requirements modules linked pre-defined levels of confidence that the HWSB implements its selected security requirements and mitigates threats relevant to its IPRFU

3.11
user
human or machine operator accessing and consuming services from the HWSB

3.12
user data
data stored and/or processed in the HWSB on behalf of the user

Abbreviations

ADV	(CC) Development (assurance class)
AES	Advanced Encryption Standard
AGD	(CC) Guidance Documents (assurance class)
ALC	(CC) Life-Cycle support (assurance class)
API	Application Programming Interface
ASE	(CC) Security Target Evaluation (assurance class)
ATE	(CC) Tests (assurance class)
ATM	Automated Teller Machine
AVA	(CC) Vulnerability Assessment (assurance class)
CA	Certificate Authority
CC	Common Criteria
CCMC	CEN-CENELEC Management Centre
CEN	European Committee for Standardization
CEN/TC	CEN Technical Committee
CIK	Crypto Ignition Key
CPLD	Complex Programmable Logic Device
CPU	Central Processing Unit
CRA	Cyber Resilience Act
DICE	Device Identifier Composition Engine
DNA	Deoxyribonucleic Acid.
DoS	Denial of Service
DRAM	Dynamic random-access memory
DRBG	Deterministic Random Bit Generator
DTBS	Data To Be Signed
DTMF	Distributed Management Task Force
ECC	Elliptic Curve Cryptography
EFP	Environmental Failure Protection
EN	European Norm (standard)
ENISA	European Union Agency for Cybersecurity
EU	European Union

EUCC	European Common Criteria–based Cybersecurity Certification Scheme
EFTA	European Free Trade Association
FIB	Focused Ion Beam
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standard
FPGA	Field-Programmable Gate Array
FRAM	Ferroelectric random-access memory (CC) Resource Utilization (functional class)
FW	FirmWare
GNSS	Global Navigation Satellite System
HBOM	Hardware Bill of Materials
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
HSS	Hierarchal Signature Scheme
HW	HardWare
HWSB	HardWare device with Security Box
I2C	Inter-Integrated Circuit
IC	Integrated Circuit
ID	Identifier
IEC	International Electrotechnical Commission
IPsec	Internet Protocol security
IPRFU	Intended Purpose and Reasonable Foreseeable Use
ISO	International Organization for Standardization
ISO/IEC	Joint ISO / IEC standard
IT	Information Technology
KLF	Key Loading Facility
LMS	Leighton-Micali Signature
MAC (net)	Media Access Control (address)
MAC (crypto)	Message Authentication Code
MACsec	Medium Access Control (layer) security
MCU	Microcontroller Unit
MFA	Multi-Factor Authentication
ML-DSA	Module-Lattice Digital Signature Algorithm.
MPU	Microprocessor Unit
OEM	Original Equipment Manufacturer
OTP	One Time Password
PAN	Primary Account Number
PCB	Printed Circuit Board
PCI (interface)	Peripheral Component Interconnect
PCI (other)	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PCIe	Peripheral Component Interconnect express
PIN	Personal Identification Number

PKCS	Public-Key Cryptography Standards
PKCS#11	Cryptoki API (PKCS #11)
PKI	Public Key Infrastructure
POI	Point of Interaction
PP	Protection Profile
RAM	Random Access Memory
RBAC	Role-Based Access Control
RDPS	Remote Data Processing Solution
REQ	Requirement
RNG	Random Number Generator
RATS	Remote Attestation Procedure
ROM	Read-Only Memory
RSA	Rivest-Shamir-Adelman (Asymmetric cryptographic algorithm)
RTC	Reat Time Clock
SAR	Security Assurance Requirement
SBOM	Software Bill Of Materials
SCA	Side-Channel Attack
SEMA	Simple EMissions Analysis
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SLH-DSA	Stateless Hash-Based Signature Algorithm
SPA	Simple Power Analysis
SPD	Security Problem Definition
SPDX	Software Package Data Exchange (SBOM format / identifier scheme)
SPDM	Security Protocol and Data Model
SPI	Serial Peripheral Interface
SRAM	Static Random-Access Memory
SSH	Secure SHell
ST	Security Target
SW	Software
TA	Timing Analysis
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform Module
TR	Technical Report
TRNG	True Random Number Generator
TS	Technical Specification
TSF	TOE Security Functions
TSP	Trust Service Provider
UART	Universal Asynchronous Receiver/Transmitter
UC	Use Case

URI	Uniform Resource Identifier
USB	Universal Serial Bus
VU	Vehicle Unit (tachograph context)

4 Product context

4.1 Product components and architecture

4.1.1 Overview

An HWSB product is composed of an HWSB and some applications. These applications use the HWSB as a provider of security services such as secure storage, cryptographic processing, authentication, integrity protection and controlled access to sensitive assets.

An HWSB comprises:

— a secure physical boundary (secure envelope),

— hardware components,

— firmware,

— security functions and services,

— interfaces for interaction with internal, local and remote applications, and

— functions that operate in a Remote Date Processing Solution (RDPS).

The HWSB product may include:

— internal applications, located within the secure boundary,

— local applications, operating in a controlled environment, and

— remote applications, operating through potentially uncontrolled networks or environments.

Figure 1 highlights the HWSB components (in green) and in scope and the additional applications (in blue) that may be part of the HWSB product and that are out of scope.

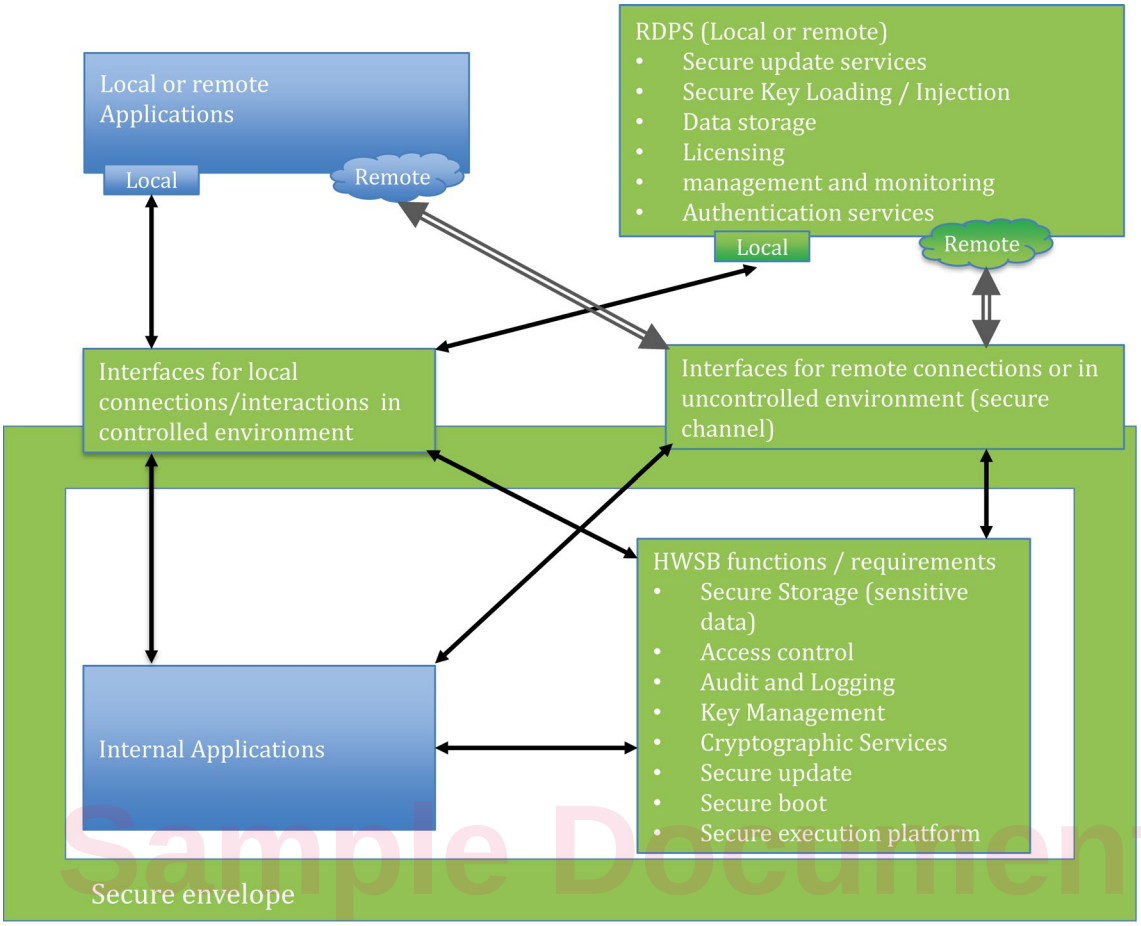

Figure 1 — HWSB product generic architecture

The following subclause provides more details on each component.

4.1.2 Secure envelope

The secure envelope defines the physical security boundary of the HWSB product.

It shall:

— enclose all components whose protection relies on the physical security of the device,

— provide a continuous protective boundary against unauthorized physical access,

— protect against tampering, probing, substitution and bypass,

— include tamper detection and, where applicable, tamper response mechanisms.

The secure envelope may include:

— tamper-resistant or tamper-evident enclosure elements,

— fasteners, seals and intrusion detection mechanisms,

— tamper sensors and associated circuitry,

— conductive or mechanical paths crossing the boundary.

Any interface traversing the secure envelope shall be protected at the point of penetration.

HWSB may include multiple layers to its secure envelope where different levels of security are provided by each layer. It is also possible that HWSB consist of multiple secure enclaves each containing their own secure envelope and with interfaces between each envelope being cryptographically secured.

Example layered or distributed secure envelope are provided in Figure 2 and Figure 3:

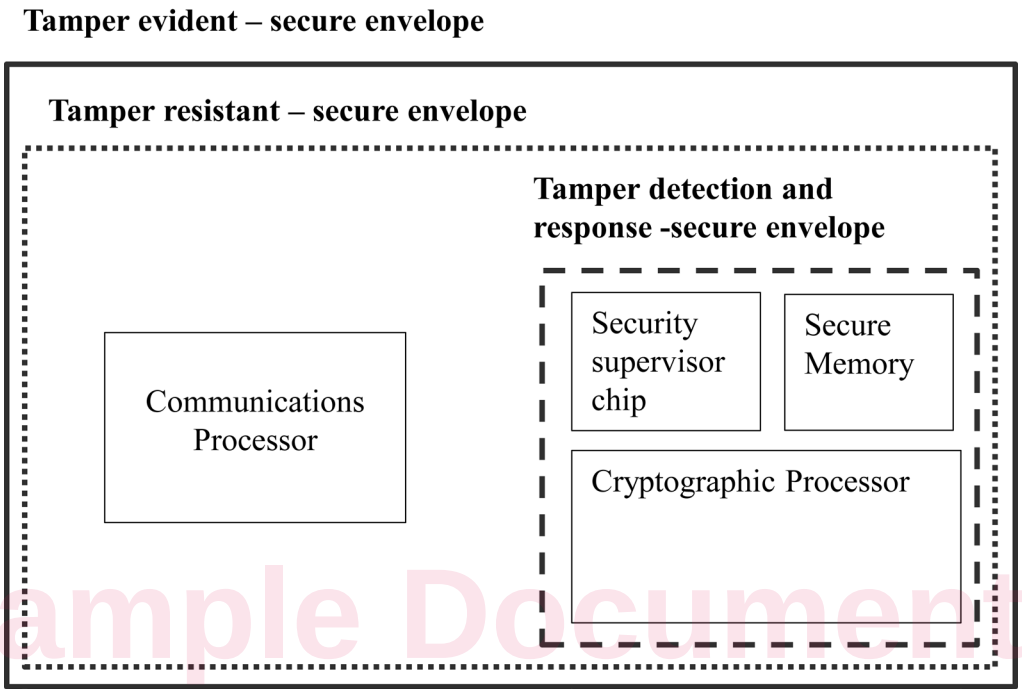

Figure 2 — Layered security envelope

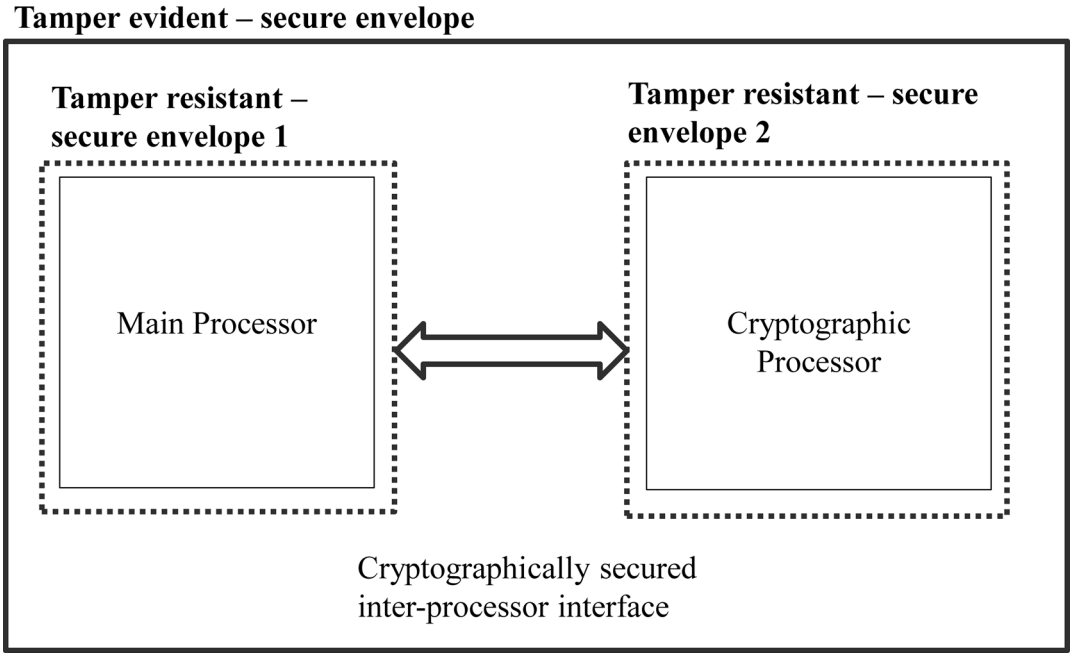

Figure 3 — Distributed secure envelope with protection islands