SLOVENSKI STANDARD
oSIST prEN 18330:2026

01-marec-2026

Zahteve za kibernetsko varnost pametnih kartic ali podobnih naprav, vključno z varnostnimi elementi - Aplikacijska plast

Cybersecurity requirements for smartcards or similar devices, including secure elements - Application layer

Smartcards, ähnliche Komponenten und Secure Elements - Kriterien zur Erfüllung der wesentlichen Anforderungen der Verordnung (EU) 2024/2847

Ta slovenski standard je istoveten z: **prEN 18330**

ICS:

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

oSIST prEN 18330:2026 **en,fr,de**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 18330

January 2026

ICS 35.030; 35.240.15

English Version

Cybersecurity requirements for smartcards or similar devices, including secure elements - Application layer

Smartcards, ähnliche Komponenten und Secure Elements - Kriterien zur Erfüllung der wesentlichen Anforderungen der Verordnung (EU) 2024/2847

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 18330:2026 E

Contents

Page

European foreword 3
Introduction 4
1 Scope 5
2 Normative references 5
3 Terms, definitions, symbols and abbreviated terms 5
3.1 Terms and definitions 5
3.2 Symbols and abbreviated terms 7
4 Product context 8
4.1 Intended purpose and foreseeable use 8
4.2 Product functions 8
4.3 Product architecture 9
4.4 Operational environment 11
4.5 Distribution of security functions 12
4.6 Users 12
4.7 Use cases 12
5 Security requirements 14
5.1 General notes on security requirements 14
5.2 Product security 14
5.3 Essential vulnerability handling requirements 23
5.4 Additional security requirements 26
6 Conformity assessment 26
6.1 Assessment of product security 26
6.2 Assessment of essential vulnerability handling 33
6.3 Additional security requirements 35
Annex A (normative) Extended SARs and SFRs 36
Annex B (informative) Risk acceptance criteria and risk management methodology 51
Annex C (informative) Governmental use cases 54
Annex D (informative) UICC and eUICC use cases 56
Annex ZA (informative) Relationship between this European Standard and the essential requirements of Regulation (EU) 2024/2847 aimed to be covered 57
Bibliography 59

European foreword

This document (prEN 18330:2026) has been prepared by CEN/TC 224 Personal identification and related personal devices with secure elements, systems, operations and privacy in a multi sectorial environment.

This document is currently submitted to the CEN Enquiry.

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.

Introduction

The growing dependence on secure elements—consisting of a secure integrated circuit or platform and applications that perform secure operations—requires ongoing diligence and comprehensive cyber resilience planning by manufacturers and developers. This is essential to design systems capable of withstanding the threats outlined in [2], as well as other use case-specific risks.

Secure elements are extensively implemented in smart cards, key fobs, SIM cards, and similar devices, and are increasingly integrated into mobile phones, connected consumer products, and IoT systems. Within these environments, the application operating on the secure platform serves as a vital component of trusted functionality; therefore, any deficiencies in its design or implementation can potentially expose both the device and its ecosystem to significant security threats from malicious entities.

The security requirements outlined in this standard are designed to reinforce the robustness of applications running on secure elements and safeguard their security assets. These measures aim to enhance the application's resilience against prevalent cybersecurity risks, including attacks leveraging publicly known vulnerabilities, and to support the overall assurance of devices and systems that rely on secure computation, protected communication channels, and effective safeguarding of sensitive information.

1 Scope

This document defines cyber security requirements for products with digital elements belonging to product category “application on the Smart Cards, Secure Elements, and similar devices” (hereinafter called “Product”). It extends the prEN 50764:2026, which defines the cyber security requirements for the platform underneath the application.

All products with digital elements having the form of a Smart Card or any similar device, where application is not installed on a platform defined by prEN 50764:2026 are excluded from the scope of this document.

More details about the product context in scope is given with Clause 4.

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.

EN ISO/IEC 15408-2:2023, *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components (ISO/IEC 15408-2:2022)*

EN ISO/IEC 15408-3:2023, *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components (ISO/IEC 15408-3:2022)*

EN ISO/IEC 18045:2023, *Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation (ISO/IEC 18045:2022)*

prEN 40000-1-3:2026, *Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability Handling*

prEN 50764:2026, *Secure IC CRA standard – full reference to be available after publishing*

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 standardization at the following addresses:

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

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

3.1.1
application
software that provides service(s) to the user of the final product

3.1.2
application environment
firmware and/or software that provides functionalities to store and execute applications