



SLOVENSKI STANDARD

oSIST prEN 50765:2026

01-marec-2026

Zahteve za kibernetsko varnost za mikroprocesorje in mikrokrmilnike z varnostnimi funkcijami

Cybersecurity requirements for microprocessors and microcontrollers with security-related functionalities

Cybersicherheitsanforderungen für Mikroprozessoren und Mikrocontroller mit sicherheitsrelevanten Funktionen

Exigences de cybersécurité pour les microprocesseurs et microcontrôleurs avec fonctions liées à la sécurité

Ta slovenski standard je istoveten z: **prEN 50765:2026**

[oSIST prEN 50765:2026](https://standards.iteh.ai/catalog/standards/sist/4219f352-12c5-4753-915a-534cc2669f76/osist-pr-en-50765-2026)

<https://standards.iteh.ai/catalog/standards/sist/4219f352-12c5-4753-915a-534cc2669f76/osist-pr-en-50765-2026>

ICS:

35.030	Informacijska varnost	IT Security
35.160	Mikroprocesorski sistemi	Microprocessor systems

oSIST prEN 50765:2026

en

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
prEN 50765

January 2026

ICS 35.030; 35.160

English Version

**Cybersecurity requirements for microprocessors and
microcontrollers with security-related functionalities**

Exigences de cybersécurité pour les microprocesseurs et
microcontrôleurs avec fonctions liées à la sécurité

Cybersicherheitsanforderungen für Mikroprozessoren und
Mikrocontroller mit sicherheitsrelevanten Funktionen

This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2026-04-10.

It has been drawn up by CLC/TC 47X.

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

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the 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 Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

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

Contents

Page

1	European foreword.....	5
2	1 Scope	6
3	2 Normative references	6
4	3 Terms and definitions	6
5	4 Symbols and abbreviated terms	8
6	5 Application of this document	9
7	5.1 General.....	9
8	5.2 Technical requirement structure and common application instructions	9
9	5.2.1 Requirement.....	9
10	5.2.2 Implementation options	9
11	5.2.3 Applicability.....	9
12	5.2.4 Assessment.....	9
13	5.2.5 Assessment verdict.....	10
14	5.2.6 Assessment evidence	11
15	6 Product context	11
16	6.1 Product's intended and reasonably foreseeable use	11
17	6.2 Product's functions	12
18	6.3 Product's operational environment of use	12
19	6.4 Product's system overview	12
20	6.5 Product's user.....	13
21	6.6 Product's reasonably foreseeable misuse.....	13
22	7 Vulnerability handling activities and outcomes — TR_VUL Vulnerability handling process	13
23	7.1 Requirement.....	13
24	7.2 Applicability.....	13
25	7.3 Assessment.....	14
26	8 Product technical requirements.....	14
27	8.1 General.....	14
28	8.2 Technical requirements related to platform implementation.....	14
29	8.2.1 TR_IMP Implementation best practices.....	14
30	8.2.2 TR_EXP No known exploitable vulnerabilities	16
31	8.2.3 TR_CFG Secure configuration of platform	17
32	8.3 Technical requirements related to platform functionalities	18
33	8.3.1 TR_PID Identification of platform.....	18
34	8.3.2 TR_PAU Authentication of platform	21
35	8.3.3 TR_INI Secure initialisation support.....	24
36	8.3.4 TR_SUP Secure update of platform	27
37	8.3.5 TR_SUD Secure update of dependent components	31
38	8.3.6 TR_ERA Secure erasure of data	33
39	8.3.7 TR_ISO Isolation mechanisms	35
40	8.3.8 TR_ACC Access control to security functionalities	38
41	8.3.9 TR_STO Secure storage.....	41
42	8.3.10 TR_COM Secure communications	45
43	8.3.11 TR_CRY Secure cryptographic features	49
44	8.3.12 TR_REP Reporting of security events	51
45	8.3.13 TR_AVS Advanced availability support of basic and essential functions	54
46	8.3.14 TR_RST Reset of platform to initial state.....	56
47	8.3.15 TR_RES Tamper-resistance of platform.....	58
48	8.4 Technical requirements related to platform operation	61

50	8.4.1	TR_SEG Application of platform security guidance	61
51		Annex A (informative) Security analysis.....	64
52	A.1	General	64
53	A.2	Assets	65
54	A.3	Security incidents.....	66
55	A.3.1	General	66
56	A.3.2	PI_DUD Disclosure of user data	66
57	A.3.3	PI_MUD Manipulation of user data	66
58	A.3.4	PI_MBD Modification of the behaviour of the device	66
59	A.3.5	PI_MCD Malicious control of the device	66
60	A.3.6	PI_UEB Unavailability of essential and basic functions of the device	66
61	A.3.7	PI_MDO Malicious use of the device against other devices or networks	66
62	A.3.8	Completeness of incidents identification	66
63	A.4	Security problem definition.....	67
64	A.4.1	General	67
65	A.4.2	Threats.....	67
66	A.4.3	Organizational security policies	68
67	A.4.4	Security assumptions	68
68	A.4.5	Risks analysis coverage.....	69
69	A.5	Security objectives.....	69
70	A.5.1	General	69
71	A.5.2	Security objectives for the platform	69
72	A.5.3	Security objectives for the environment.....	70
73	A.5.4	Security problem definition coverage.....	70
74	A.5.5	Security objectives coverage.....	71
75	A.6	Risk environments	73
76	A.6.1	General	73
77		Annex B (informative) Platform categories and applicability overview	74
78		Annex C (informative) Support of European security evaluation methodologies	77
79	C.1	General	77
80	C.2	Compliance demonstration support.....	77
81	C.2.1	Assessment of applicability	77
82	C.2.2	TR_IMP Implementation best practices	77
83	C.2.3	TR_EXP No known exploitable vulnerabilities	77
84	C.2.4	TR_CFG Secure configuration of platform	77
85	C.2.5	TR_PID Identification of platform	77
86	C.2.6	TR_PAU Authenticity of platform	78
87	C.2.7	TR_INI Secure initialisation support.....	79
88	C.2.8	TR_SUP Secure update of platform.....	80

prEN 50765:2026 (E)

89	C.2.9 TR_SUD Secure update of dependent component	81
90	C.2.10 TR_ERA Secure erasure of data	82
91	C.2.11 TR_ISO Isolation mechanisms	83
92	C.2.12 TR_ACC Access control to security functionalities	84
93	C.2.13 TR_STO Secure storage.....	85
94	C.2.14 TR_COM Secure communication	86
95	C.2.15 TR_CRY Secure cryptographic features	86
96	C.2.16 TR_REP Reporting of security events	87
97	C.2.17 TR_AVS Advanced availability support of basic and essential functions	88
98	C.2.18 TR_RST Reset of platform to initial state	89
99	C.2.19 TR_RES Tamper resistance of platform.....	90
100	C.2.20 TR_SEG Application of platform security guidance	90
101	Annex ZZ (normative) Relationship between this European Standard and the essential	
102	requirements of Regulation (EU) 2024/2847 aimed to be covered	92
103	Bibliography	95

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN 50765:2026](https://standards.iteh.ai/catalog/standards/sist/4219f552-12e5-4753-915a-534ec2669f7b/osist-pren-50765-2026)

<https://standards.iteh.ai/catalog/standards/sist/4219f552-12e5-4753-915a-534ec2669f7b/osist-pren-50765-2026>

104 **European foreword**

105 This document (prEN 50765:2026) has been prepared by CLC/TC 47X "Semiconductors and trusted chips
106 implementation"

107 This document is currently submitted to the Enquiry.

108 The following dates are proposed:

- latest date by which the existence of this document has to be announced at national level (doa) dav + 6 months
- latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) dav + 12 months
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) dav + 36 months (to be confirmed or modified when voting)

109 This document has been prepared under a standardization request addressed to CENELEC by the European
110 Commission. The Standing Committee of the EFTA States subsequently approves these requests for its
111 Member States.

112 For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[oSIST prEN 50765:2026](https://standards.iteh.ai/catalog/standards/sist/4219f552-12e5-4753-915a-534ec2669f7b/osist-pren-50765-2026)

<https://standards.iteh.ai/catalog/standards/sist/4219f552-12e5-4753-915a-534ec2669f7b/osist-pren-50765-2026>