



# SLOVENSKI STANDARD

## oSIST prEN 50766:2026

01-marec-2026

---

**Zahteve za kibernetško varnost za mikroprocesorje in mikrokrmilnike, odporne proti nedovoljenim posegom**

Cybersecurity requirements for tamper-resistant microprocessors and microcontrollers

Cybersicherheitsanforderungen für sichere Mikroprozessoren und Mikrocontroller mit oder ohne Anwendungsumgebung oder Betriebssystem

Exigences de cybersécurité pour les microprocesseurs et microcontrôleurs sécurisés avec ou sans environnement d'application ou système d'exploitation

**Ta slovenski standard je istoveten z: prEN 50766:2026**

---

<https://standards.iteh.ai/catalog/standards/sist/661b4421-8e20-4628-939a-994a09514475/osist-pren-50766-2026>

**ICS:**

|        |                          |                        |
|--------|--------------------------|------------------------|
| 35.030 | Informacijska varnost    | IT Security            |
| 35.160 | Mikroprocesorski sistemi | Microprocessor systems |

**oSIST prEN 50766:2026**

**en**



EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**DRAFT**  
**prEN 50766**

January 2026

ICS 35.030; 35.160

English Version

## Cybersecurity requirements for tamper-resistant microprocessors and microcontrollers

Exigences de cybersécurité pour les microprocesseurs et microcontrôleurs sécurisés avec ou sans environnement d'application ou système d'exploitation

Cybersicherheitsanforderungen für sichere Mikroprozessoren und Mikrocontroller mit oder ohne Anwendungsumgebung oder Betriebssystem

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

|    |                                                                                                |    |
|----|------------------------------------------------------------------------------------------------|----|
| 17 | European foreword.....                                                                         | 5  |
| 18 | 1 Scope .....                                                                                  | 6  |
| 19 | 2 Normative references .....                                                                   | 6  |
| 20 | 3 Terms and definitions .....                                                                  | 6  |
| 21 | 4 Symbols and abbreviated terms .....                                                          | 8  |
| 22 | 5 Application of this document .....                                                           | 9  |
| 23 | 5.1 General.....                                                                               | 9  |
| 24 | 5.2 Technical requirement structure and common application instructions .....                  | 9  |
| 25 | 5.2.1 Requirement.....                                                                         | 9  |
| 26 | 5.2.2 Implementation options .....                                                             | 9  |
| 27 | 5.2.3 Applicability.....                                                                       | 9  |
| 28 | 5.2.4 Assessment.....                                                                          | 9  |
| 29 | 5.2.5 Assessment verdict.....                                                                  | 10 |
| 30 | 5.2.6 Assessment evidence .....                                                                | 11 |
| 31 | 6 Product context .....                                                                        | 11 |
| 32 | 6.1 Product's intended and reasonably foreseeable use .....                                    | 11 |
| 33 | 6.2 Product's functions .....                                                                  | 12 |
| 34 | 6.3 Product's operational environment of use .....                                             | 12 |
| 35 | 6.4 Product's system overview .....                                                            | 12 |
| 36 | 6.5 Product's user.....                                                                        | 13 |
| 37 | 6.6 Product's reasonably foreseeable misuse.....                                               | 13 |
| 38 | 7 Vulnerability handling activities and outcomes — TR_VUL Vulnerability handling process ..... | 13 |
| 39 | 7.1 Requirement.....                                                                           | 13 |
| 40 | 7.2 Applicability.....                                                                         | 14 |
| 41 | 7.3 Assessment.....                                                                            | 14 |
| 42 | 8 Product technical requirements.....                                                          | 14 |
| 43 | 8.1 General.....                                                                               | 14 |
| 44 | 8.2 Technical requirements related to platform implementation .....                            | 14 |
| 45 | 8.2.1 TR_IMP Implementation best practices.....                                                | 14 |
| 46 | 8.2.2 TR_EXP No known exploitable vulnerabilities .....                                        | 16 |
| 47 | 8.2.3 TR_CFG Secure configuration of platform .....                                            | 17 |
| 48 | 8.3 Technical requirements related to platform functionalities .....                           | 18 |
| 49 | 8.3.1 TR_PID Identification of platform.....                                                   | 18 |
| 50 | 8.3.2 TR_PAU Authentication of platform .....                                                  | 21 |
| 51 | 8.3.3 TR_INI Secure initialisation support.....                                                | 23 |
| 52 | 8.3.4 TR_SUP Secure update of platform .....                                                   | 27 |
| 53 | 8.3.5 TR_SUD Secure update of dependent components .....                                       | 31 |
| 54 | 8.3.6 TR_ERA Secure erasure of data .....                                                      | 33 |
| 55 | 8.3.7 TR_ISO Isolation mechanisms .....                                                        | 35 |
| 56 | 8.3.8 TR_ACC Access control to security functionalities .....                                  | 38 |
| 57 | 8.3.9 TR_STO Secure storage.....                                                               | 40 |
| 58 | 8.3.10 TR_COM Secure communications .....                                                      | 45 |
| 59 | 8.3.11 TR_CRY Secure cryptographic features .....                                              | 49 |
| 60 | 8.3.12 TR_REP Reporting of security events .....                                               | 50 |
| 61 | 8.3.13 TR_AVS Advanced availability support of basic and essential functions .....             | 53 |
| 62 | 8.3.14 SRD_RST Reset of platform to initial state .....                                        | 55 |
| 63 | 8.3.15 TR_RES Tamper-resistance of platform.....                                               | 57 |
| 64 | 8.4 Technical requirements related to platform operation .....                                 | 61 |
| 65 | 8.4.1 TR_SEG Application of platform security guidance .....                                   | 61 |
| 66 | Annex A (informative) Security analysis.....                                                   | 63 |

|     |                              |                                                                                        |           |
|-----|------------------------------|----------------------------------------------------------------------------------------|-----------|
| 68  | <b>A.1</b>                   | <b>General .....</b>                                                                   | <b>63</b> |
| 69  | <b>A.2</b>                   | <b>Assets .....</b>                                                                    | <b>64</b> |
| 70  | <b>A.3</b>                   | <b>Security incidents.....</b>                                                         | <b>65</b> |
| 71  | <b>A.3.1</b>                 | <b>General .....</b>                                                                   | <b>65</b> |
| 72  | <b>A.3.2</b>                 | <b>PI_DUD Disclosure of user data .....</b>                                            | <b>65</b> |
| 73  | <b>A.3.3</b>                 | <b>PI_MUD Manipulation of user data .....</b>                                          | <b>65</b> |
| 74  | <b>A.3.4</b>                 | <b>PI_MBD Modification of the behaviour of the device .....</b>                        | <b>65</b> |
| 75  | <b>A.3.5</b>                 | <b>PI_MCD Malicious control of the device .....</b>                                    | <b>65</b> |
| 76  | <b>A.3.6</b>                 | <b>PI_UEB Unavailability of essential and basic functions of the device .....</b>      | <b>65</b> |
| 77  | <b>A.3.7</b>                 | <b>PI_MDO Malicious use of the device against other devices or networks .....</b>      | <b>65</b> |
| 78  | <b>A.3.8</b>                 | <b>Completeness of incidents identification .....</b>                                  | <b>65</b> |
| 79  | <b>A.4</b>                   | <b>Security problem definition .....</b>                                               | <b>66</b> |
| 80  | <b>A.4.1</b>                 | <b>General .....</b>                                                                   | <b>66</b> |
| 81  | <b>A.4.2</b>                 | <b>Threats.....</b>                                                                    | <b>66</b> |
| 82  | <b>A.4.3</b>                 | <b>Organizational security policies .....</b>                                          | <b>67</b> |
| 83  | <b>A.4.4</b>                 | <b>Security assumptions .....</b>                                                      | <b>67</b> |
| 84  | <b>A.4.5</b>                 | <b>Risks analysis coverage.....</b>                                                    | <b>68</b> |
| 85  | <b>A.5</b>                   | <b>Security objectives.....</b>                                                        | <b>68</b> |
| 86  | <b>A.5.1</b>                 | <b>General .....</b>                                                                   | <b>68</b> |
| 87  | <b>A.5.2</b>                 | <b>Security objectives for the platform .....</b>                                      | <b>68</b> |
| 88  | <b>A.5.3</b>                 | <b>Security objectives for the environment.....</b>                                    | <b>69</b> |
| 89  | <b>A.5.4</b>                 | <b>Security problem definition coverage.....</b>                                       | <b>69</b> |
| 90  | <b>A.5.5</b>                 | <b>Security objectives coverage.....</b>                                               | <b>70</b> |
| 91  | <b>A.6</b>                   | <b>Risk environments .....</b>                                                         | <b>72</b> |
| 92  | <b>A.6.1</b>                 | <b>General .....</b>                                                                   | <b>72</b> |
| 93  | <b>A.6.2</b>                 | <b>Example of platform risk environment (attack potential) information reuse .....</b> | <b>72</b> |
| 94  | <b>Annex B (informative)</b> | <b>Platform categories and applicability overview .....</b>                            | <b>74</b> |
| 95  | <b>Annex C (informative)</b> | <b>Support of European security evaluation methodologies .....</b>                     | <b>77</b> |
| 96  | <b>C.1</b>                   | <b>General .....</b>                                                                   | <b>77</b> |
| 97  | <b>C.2</b>                   | <b>Compliance demonstration support.....</b>                                           | <b>77</b> |
| 98  | <b>C.2.1</b>                 | <b>Assessment of applicability .....</b>                                               | <b>77</b> |
| 99  | <b>C.2.2</b>                 | <b>TR_IMP Implementation best practices .....</b>                                      | <b>77</b> |
| 100 | <b>C.2.3</b>                 | <b>TR_EXP No known exploitable vulnerabilities .....</b>                               | <b>77</b> |
| 101 | <b>C.2.4</b>                 | <b>TR_CFG Secure configuration of platform .....</b>                                   | <b>78</b> |
| 102 | <b>C.2.5</b>                 | <b>TR_PID Identification of platform .....</b>                                         | <b>78</b> |
| 103 | <b>C.2.6</b>                 | <b>TR_PAU Authenticity of platform .....</b>                                           | <b>79</b> |
| 104 | <b>C.2.7</b>                 | <b>TR_INI Secure initialisation support.....</b>                                       | <b>79</b> |
| 105 | <b>C.2.8</b>                 | <b>TR_SUP Secure update of platform.....</b>                                           | <b>80</b> |
| 106 | <b>C.2.9</b>                 | <b>TR_SUD Secure update of dependent component .....</b>                               | <b>82</b> |

## prEN 50766:2026 (E)

|     |                                                                                             |            |
|-----|---------------------------------------------------------------------------------------------|------------|
| 107 | <b>C.2.10 TR_ERA Secure erasure of data .....</b>                                           | <b>83</b>  |
| 108 | <b>C.2.11 TR_ISO Isolation mechanisms .....</b>                                             | <b>84</b>  |
| 109 | <b>C.2.12 TR_ACC Access control to security functionalities .....</b>                       | <b>85</b>  |
| 110 | <b>C.2.13 TR_STO Secure storage.....</b>                                                    | <b>86</b>  |
| 111 | <b>C.2.14 TR_COM Secure communication .....</b>                                             | <b>88</b>  |
| 112 | <b>C.2.15 TR_CRY Secure cryptographic features .....</b>                                    | <b>89</b>  |
| 113 | <b>C.2.16 TR_REP Reporting of security events .....</b>                                     | <b>90</b>  |
| 114 | <b>C.2.17 TR_AVS Advanced availability support of basic and essential functions .....</b>   | <b>91</b>  |
| 115 | <b>C.2.18 TR_RST Reset of platform to initial state .....</b>                               | <b>92</b>  |
| 116 | <b>C.2.19 TR_RES Tamper resistance of platform.....</b>                                     | <b>93</b>  |
| 117 | <b>C.2.20 TR_SEG Application of platform security guidance .....</b>                        | <b>94</b>  |
| 118 | <b>C.3 SESIP profiles analysis of compliance support .....</b>                              | <b>94</b>  |
| 119 | <b>Annex ZZ (informative) Relationship between this European Standard and the essential</b> |            |
| 120 | <b>requirements of Regulation (EU) 2024/2847 aimed to be covered .....</b>                  | <b>99</b>  |
| 121 | <b>Bibliography .....</b>                                                                   | <b>102</b> |

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

[oSIST prEN 50766:2026](https://standards.iteh.ai/catalog/standards/sist/661b4421-8e20-4628-939a-994a09514475/osist-pren-50766-2026)

<https://standards.iteh.ai/catalog/standards/sist/661b4421-8e20-4628-939a-994a09514475/osist-pren-50766-2026>

## 122 European foreword

123 This document (prEN 50766:2026) has been prepared by CLC TC47X “semiconductors and trusted chips  
124 implementation”.

125 This document is currently submitted to the Enquiry

126 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)

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

130 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 50766:2026](https://standards.iteh.ai/catalog/standards/sist/661b4421-8e20-4628-939a-994a09514475/osist-pren-50766-2026)

<https://standards.iteh.ai/catalog/standards/sist/661b4421-8e20-4628-939a-994a09514475/osist-pren-50766-2026>