SLOVENSKI STANDARD
oSIST prEN 40004-3:2026

01-november-2026

Zahteve za kibernetsko varnost za programirljiva logična vezja in integrirana vezja za določen namen z varnostno relevantnimi funkcijami

Cybersecurity requirements for Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities

Technische Sicherheitsstandards für anwendungsspezifische integrierte Schaltkreise (ASICs) und feldprogrammierbare Gate-Arrays (FPGAs) mit sicherheitsrelevanten Funktionalitäten

Sample Document

Normes techniques de sécurité pour les circuits intégrés spécifiques à une application (ASIC) et les circuits logiques programmables (FPGA) incluant des fonctionnalités de sécurité de données

Get full document from standards.iteh.ai

Ta slovenski standard je istoveten z: **prEN 40004-3:2026**

ICS:

31.200	Integrirana vezja, mikroelektronika	Integrated circuits. Microelectronics
35.030	Informacijska varnost	IT Security

oSIST prEN 40004-3:2026 **en**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

Sample Document

get full document from standards.iteh.ai

oSIST prEN 40004-3:2026

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 40004-3

September 2026

ICS 31.200; 35.030

-

English Version

Cybersecurity requirements for Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities

Normes techniques de sécurité pour les circuits intégrés spécifiques à une application (ASIC) et les circuits logiques programmables (FPGA) incluant des fonctionnalités de sécurité de données

Technische Sicherheitsstandards für anwendungsspezifische integrierte Schaltkreise (ASICs) und feldprogrammierbare Gate-Arrays (FPGAs) mit sicherheitsrelevanten Funktionalitäten

This draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2026-11-20.

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.

Sample Document

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.

get full document from standards.iteh.ai

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

© 2026 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Project: 82281 Ref. No. prEN 40004-3:2026 E

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

Contents

Page

European foreword 5
Introduction 6
1 Scope 8
2 Normative references 8
3 Terms and definitions 8
4 Product context 11
4.1 Product functions 11
4.2 Product architecture 12
4.3 Operational environment 12
4.3.1 General 12
4.3.2 Adversary environment types 12
4.3.3 Device environment components 13
4.4 Distribution of security functions 14
4.5 Users 15
4.6 Use cases 15
5 Technical requirements for products 22
5.1 General 22
5.1.1 General 22
5.1.2 Requirement 22
5.1.3 Applicability 22
5.2 Technical requirements related to platform implementation 23
5.2.1 TR-IMP Implementation best practices 23
5.2.2 TR-EXP No known exploitable vulnerabilities 23
5.2.3 TR_CFG Secure configuration of platform 24
5.3 Technical requirements related to platform functionalities 25
5.3.1 TR-PID Identification of platform 25
5.3.2 TR-PAU Authentication of platform 25
5.3.3 TR-INI Secure initialisation support 27
5.3.4 TR-SUP Secure update of platform 27
5.3.5 TR-HDC Secure handling of dependent components 29
5.3.6 TR-ERA Secure erasure of data 29
5.3.7 TR-ISO Isolation mechanisms 30
5.3.8 TR-ACC Access control to security functionalities 31
5.3.9 TR-STO Secure storage 32
5.3.10 TR-COM Secure communications 34
5.3.11 TR-CRY Secure cryptographic features 36
5.3.12 TR-REP Reporting of security events 36
5.3.13 TR-AVS Advanced availability support of basic and essential functions 37
5.3.14 TR-RST Reset of platform to initial state 38
5.3.15 TR-RES Tamper-resistance of platform 39
6 Assessment criteria for compliance with technical requirements 41
6.1 Introduction to the assessment and compliance criteria 41
6.1.1 General 41
6.1.2 Assessment objective 41
6.1.3 Assessment preparation 41
6.1.4 Assessment activities 42
6.1.5 Assessment verdict 42
6.1.6 Assessment evidence 43
6.2 Technical requirements assessment 43
6.2.1 Assessment of TR-IMP 43
6.2.2 Assessment of TR-EXP 43
6.2.3 Assessment of TR-CFG 45
6.2.4 Assessment of TR-PID 46

iTeh Standards (https://standards.iteh.ai) Document Preview
This document is not an ASD-STE100 Simplified Technical English document.

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

6.2.5 Assessment of TR-PAU 47
6.2.6 Assessment of TR-INI 48
6.2.7 Assessment of TR-SUP 49
6.2.8 Assessment of TR-HDC 51
6.2.9 Assessment of TR-ERA 52
6.2.10 Assessment of TR-ISO 53
6.2.11 Assessment of TR-ACC 54
6.2.12 Assessment of TR-STO 55
6.2.13 Assessment of TR-COM 57
6.2.14 Assessment of TR-CRY 59
6.2.15 Assessment of TR-REP 59
6.2.16 Assessment of TR-AVS 61
6.2.17 Assessment of TR-RST 61
6.2.18 Assessment of TR-RES 62
Annex A (informative) Security analysis 70
A.1 General 70
A.2 Assets 70
A.3 Threats 71
A.3.1 General 71
A.3.2 T_UDD Unauthorized disclosure of platform data 71
A.3.3 T_UMD Unauthorized modification of platform data 71
A.3.4 T_URD Unauthorized replacement of platform data 71
A.3.5 T_UAD Unauthorized addition of platform data 71
A.3.6 T_UED Unauthorized erasure of platform data 71
A.3.7 T_UMC Unauthorized modification of platform code 71
A.3.8 T_URC Unauthorized replacement of platform code 71
A.3.9 T_UAC Unauthorized addition of platform code 71
A.3.10 T_UEC Unauthorized erasure of platform code 72
A.3.11 T_CCF Compromise of a cryptographic security functionality 72
A.3.12 T_UAF Unauthorized access to the security functionalities of the platform 72
A.3.13 T_DBF Disruption of essential and basic functions of the platform 72
A.3.14 T_PER Impersonation of the platform 72
A.4 Assets coverage 72
A.5 Threats coverage 73
Annex B (informative) Platform requirements and implementation options 76
Annex C (informative) Support of European security evaluation methodologies 79
C.1 General 79
C.2 Mapping to external assessment methodologies 79
C.3 Mapping of external security profiles 83
Annex K (normative) Cryptographic algorithms 88
K.1 General 88
K.2 Cryptography 88
K.2.1 Requirement 88
K.2.2 Assessment of platform cryptographic mechanisms 91

Sample Document
get full document from standards.iteh.ai

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

K.3 Crypto agility 95
K.3.1 Requirement 95
K.3.2 Assessment of crypto-agility 96
K.4 ACM-extended cryptographic mechanisms 97
K.4.1 Requirement 97
K.4.2 List of ACM-extended cryptographic mechanisms 97
K.4.3 Assessment 138
K.5 Interoperability-based cryptographic mechanisms 138
K.5.1 Requirement 138
K.5.2 List of interoperability-based cryptographic mechanisms 138
K.5.3 Assessment 153
Annex ZZ (informative) Relationship between this European Standard and the essential cybersecurity requirements of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) aimed to be covered 154
Bibliography 157

Sample Document

get full document from standards.iteh.ai

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

European foreword

This document (prEN 40004-3:2026) has been prepared by CLC TC47X “semiconductors and trusted chips implementation”.

This document is currently submitted to the Enquiry

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)

This document has been prepared under a standardization request addressed to 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 ZZ, which is an integral part of this document.

Sample Document

get full document from standards.iteh.ai

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

Introduction

This standard specifies the technical requirements to be fulfilled by Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities, as defined in the Regulation (EU) 2025/2392 [21], to cover the Essential Cybersecurity Requirements set out in Annex I of the Regulation 2024/2847 (Cyber Resilience Act), and defines how compliance with those requirements is to be demonstrated.

Clause 4 does not contain technical requirements; it describes the product context that is considered for the application of this standard. Clause 4 also defines use cases that represent the main deployment scenarios reflecting the intended purpose and reasonably foreseeable use of the product, which serve as the basis for identifying relevant cybersecurity risks.

Clause 5 specifies technical cybersecurity requirements for the product to mitigate the identified risks, including their applicability conditions.

Clause 6 specifies the assessment criteria and compliance verification procedures with the requirements of Clause 5.

Annex A informs about the methodology used to assess the security risks of the products in their context.

Annex B provides a synthetic mapping of the technical requirements with appropriate implementation options.

Annex C provides an analysis of the coverage of technical requirements evaluation by external methodologies.

Annex K supports the definition of the cryptographic requirements and assessment criteria used by the present document.

Annex ZZ maps the technical requirements of the present document with the essential requirements of the Regulation 2024/2847 Annex I Part I.

For each technical requirement, this standard specifies a set of valid implementation options and the assessment activities to be performed in order to demonstrate compliance with those requirements.

The applicability of the technical requirements depends on the risks associated with the intended use of the Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities. This standard defines use cases and associates each of them with a corresponding set of applicable technical requirements, as determined through threat analysis.

The use case of a Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities is determined consistently with the cybersecurity risk assessment performed by the manufacturer, as required under Article 13 of the Cyber Resilience Act.

This standard is defined at a level of granularity that is generic across different Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities. Consequently, for a specific product, the manufacturer's risk assessment can conclude that certain technical requirements associated with a given use case are not applicable without affecting the compliance of the platform with this standard. This standard provides guidance on common technical reasons for such non-applicability; however, the determination and justification of exclusions fall outside the scope of this standard and remain under the manufacturer's risk assessment obligation.

Platforms commonly include mechanisms beyond those necessary to fulfil technical requirements. Even if such mechanisms are listed in this document as potential implementation options (e.g. storage, communication, availability), those fall outside the scope of this document as they do not actively mitigate identified threats.

A platform can be deployed in environments exposing it to threats beyond those addressed by its defined use case, thereby implying a redefinition of the use case of the integrating product, provided that any additional required protections are implemented by the platform user. All such considerations are however outside the scope of this standard.

In summary, the application of this standard by Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities manufacturers follows the steps below:

— identification of the use case from Clause 4.6, based on the manufacturer's risk assessment;

Sample Document

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

- identification of the associated technical requirements from Table 1 and Table 2 of Clause 4.6;
- identification the final set of technical requirements to be implemented, taking into account the identified use case and any justified exclusions resulting from the manufacturer's specific risk assessment;
- implementation of the identified technical requirements in accordance with the implementation options specified in Clause 5.
- assessment of the platform implementation of each technical requirement in accordance in accordance with Clause 6.

Users of Field Programmable Gate Arrays and Application Specific Integrated Circuits with security-related functionalities can use this standard to identify the use case corresponding to their own intended use and select the appropriate Field Programmable Gate Arrays or Application Specific Integrated Circuits.

Sample Document

get full document from standards.iteh.ai

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

1 Scope

This document specifies the technical requirements for general-purpose Application Specific Integrated Circuits (ASICs) and Field Programmable Gate Arrays (FPGAs) with security features, related to cybersecurity. The products with digital elements in scope, thereafter “platforms”:

— are specified within the “technical description” of the “category of product” number “NN” by the Commission Implementing Regulation (EU) 2025/2392 [16] as:

- “Application specific integrated circuits (ASIC) with security-related functionalities are products with digital elements that are integrated circuits, fully or partially custom-designed to perform a specific function or implement a specific application, and which additionally provide security-related functionalities that aim to secure other products, networks or services beyond the ASIC itself, such as trusted execution environments or secure communication interfaces.”

- “Field-programmable gate arrays (FPGA) with security-related functionalities are products with digital elements that are integrated circuits characterized by a matrix of configurable logic blocks designed to be reprogrammable after manufacturing to perform a specific function or implement a specific application, and which additionally provide security-related functionalities that aim to secure other products, networks or services beyond the FPGA itself, such as trusted execution environments or secure communication interfaces.”

— are only covered within the product context described in Clause 4.

The present document covers those products to demonstrate compliance with essential cybersecurity requirements in the Regulation (EU) 2024/2847 [16] Annex I Part I under the conditions identified in Annex ZZ.

ASICs and FPGAs additionally provide security-related functionalities, such as encryption, authentication, secure key storage, random number generation, trusted execution environment, or other hardware- based protection mechanisms, that aim to secure other products, networks or services beyond the ASIC or FPGA itself, such as secure boot chain, virtualization or secure communication interfaces

Sample Document
Get full document from standards.iteh.ai

Such ASICs and FPGAs are intended to be integrated in a larger system, complemented by application software, and optionally by additional hardware components by integrators to build a device corresponding to a given intent of use. The intent of use of the platform integrated into a device is likely be known to the manufacturer of the ASIC with security-related functionalities, while the intent of use of the platform integrated into a device might not be known to the manufacturer of the FPGA with security-related functionalities.

The ASICs and FPGAs in scope are designed for deployment in environments where the security features of the product integrating the platform are of importance, and where the threat landscape includes attackers with low/medium attack potential.

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.

FprEN 40000-1-1:2026, *Cybersecurity requirements for products with digital elements - Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in, FprEN 40000-1-1:2026 and the following 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/

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

3.1
access control
mechanism granting permission to a subject on an object

3.2
application
dependent component that provides a direct service to the end-user

3.3
asset
data, code or function that needs protection to prevent loss or disruption caused by a potential incident

3.4
best practices for cryptography
measures based on cryptographic techniques that have been shown to provide appropriate security for the corresponding use case

3.5
cryptographic mechanism
security-related procedure using cryptography

Note 1 to entry: The term “cryptographic mechanism” is used in this annex as an umbrella term covering the categories used in the ECCG Agreed Cryptographic Mechanisms v2.0 catalogue, including cryptographic algorithms, primitives, schemes, protocols, protocol profiles, cipher suites, modes of operation, constructions and parameter sets.

Note 2 to entry: The terms “cryptographic primitive”, “cryptographic construction”, “cryptographic scheme” and “cryptographic protocol” are used consistently with the ECCG Agreed Cryptographic Mechanisms v2.0 catalogue.

Note 3 to entry: A cryptographic mechanism can be specified at different levels of abstraction. For example, AES is a cryptographic primitive, AES-GCM is a mode of operation / authenticated encryption construction, TLS 1.3 is a protocol, a TLS 1.3 restricted cipher-suite profile is a protocol profile, and TLS_AES_128_GCM_SHA256 is a cipher suite.

Sample Document
get full document from standards.iteh.ai

3.6
cryptographic property
property provided or supported by a cryptographic mechanism

Note 1 to entry: Cryptographic properties include, for example, confidentiality, integrity, authenticity, entity authentication, message authentication, key establishment, key confirmation, replay protection, collision resistance, second-preimage resistance, pre-image resistance, signature unforgeability, non-repudiation, forward secrecy and password-verifier protection. Where relevant, a cryptographic property can be expressed using a formal cryptographic notion, for example IND-CPA, IND-CCA, IND-CCA2, EUF-CMA, SUF-CMA or authenticated key exchange security.

Note 2 to entry: A cryptographic property is distinct from a product-level technical requirement, although it can support such a requirement. For example, a secure communication requirement can rely on cryptographic properties such as confidentiality, integrity and authentication.

3.7
dependent component
software or hardware component using a functionality of a platform

EXAMPLE The dependent component can also refer to the integrator’s design (configuration/programming bitstream) mapped into the configurable hardware (FPGA logic).

3.8
device
composition of platform(s) and dependent component(s)

Note 1 to entry: When a platform is under assessment following this standard, other platforms and dependent components are out of scope.

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

3.9
end-user
user of the device

3.10
external entity
entity in interaction with the platform

EXAMPLE Application, other dependent components or devices in physical or logical interaction with the platform.

3.11
firmware
set of executable instructions which are optionally provided as a part of the platform and which can be immutable and/or mutable

3.12
isolation mechanism
security mechanism regulating the accesses to assets between the different parts in a system separated in parts

3.13
logical attack
attack requiring only logical vector to disturb the platform

3.14
physical attack
attack requiring the close presence of the attacker to the platform

Sample Document
get full document from standards.iteh.ai

3.15
platform
FPGA or ASIC optionally with firmware, and/or any type of software, and/or remote data processing solution

Note 1 to entry: Platforms may be application-specific (ASICs) or generic devices (FPGAs).

Note 2 to entry: Software does not include user software.

3.16
platform code
code that is part of the implementation of the platform functionality

Note 1 to entry: Platform code also includes the platform aspects of the bitstream for FPGAs

3.17
platform data
data handled by the platform i.e. user data, user code and platform manufacturer data

3.18
platform manufacturer data
data owned by the platform manufacturer handled by the platform

3.19
potential incident
specific event that could occur due to a threat exploiting a vulnerability

3.20
security functionality
functionality provided by the platform to the dependent components for the protection of assets

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

EXAMPLE Secure storage, cryptographic operations.

3.21
tamper-evidence
security property of a platform intended to ensure the detection of logical and/or physical attacks leading to achievement of threats identified in the risk assessment

3.22
tamper-resistance
security property of a platform intended to prevent the successful exploitation of vulnerabilities by logical and/or physical attacks leading to realization of threats identified in the risk assessment

3.23
tamper-response
security property of a platform intended to provide the ability to react to the detection of logical and/or physical attacks leading to realization of threats identified in the risk assessment

3.24
update package
bundle containing platform bitstream and/or firmware and/or software code and/or data, potentially associated with metadata

3.25
user
platform user
entity that will make use of the platform (including software component, intermediate user and end-user)

Sample Document

3.26
user code
code implementing the (software) dependent component executed on the platform

get full document from standards.iteh.ai

3.27
user data
data owned by (or associated to) the user handled by the platform

4 Product context

4.1 Product functions

In this document, products refer to platforms as defined in Clause 3 that are intended to be combined with other components, software and/or hardware, to form a complete device. Their essential function is to provide generic security functionalities to these associated components, referred to as dependent components, by means of their own hardware, optionally augmented by firmware and/or software. These platforms are intended to be used across a wide range of industries and applications, able to support multiple end functions.

ASICs and FPGAs are intended to be integrated in a larger system, complemented by application software, and initialization information optionally by additional hardware components by integrators to build a device corresponding to a given intent of use. The intent of use of the platform integrated into a device is likely be known to the manufacturer of the ASIC with security-related functionalities, while the intent of use of the platform integrated into a device may not be known to the manufacturer of the FPGA with security-related functionalities.

Additionally, the platforms covered in this document range from those offering limited security capabilities suitable for integration into devices that operate in environments where the threat landscape includes attackers with a low, negligible attack potential through to those platforms offering protection against attacks with a medium attack potential, whether through remote-only or physical access to the device.

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

4.2 Product architecture

Platforms in scope are composed of hardware, optionally augmented by firmware and/or any type of software. The platform can also optionally rely on a remote data processing solution involving a communication channel between the core of the platform and its remote part. All such platform components, including any remote part and the connecting communication link, are affected by the threats outlined in 4.4; they consequently need to implement the associated technical requirements.

Such platforms implement security functionalities that can be invoked by dependent component(s), which are outside of the scope of this standard. These security functionalities at minimum mitigate the risks associated with to the platform use case (see 4.6).

Additional security implementation that do not comply with the requirements of this standard may also be included, provided that they do not compromise the compliance of the security functionalities subject to this standard.

EXAMPLE A given functionality is supported by multiple cryptographic algorithms, including one(s) that comply with this standard and others that do not, (because they are not intended for the European market).

4.3 Operational environment

4.3.1 General

Platforms operate within varying operational environments which influence the risks to be countered. These environments can be categorized into two main types:

— Adversary environment, which refers to the external conditions and capabilities that shape the exposure of the platform itself to attacks and, consequently, determines the security features required for its self-protection.

— Device environment, which refers to the device assets and security functionalities and, consequently, determines the platform security features required to ensure or support the device own security.

Sample Document
get full document from standards.iteh.ai

The environment categories to be selected depend on the integrating product use case and its corresponding risk assessment.

4.3.2 Adversary environment types

4.3.2.1 Logical environment

The logical environment refers to software and hardware components outside the platform that can interact with it either directly through exposed interfaces, or indirectly via shared resources such as memory or buses. It is consequently capable of affecting the logical behaviour of the platform.

The logical environment of the platform falls into one of the two categories:

— Trusted logical environment (ENV-TRL): environment where the interacting components are not expected to intentionally compromise the platform (USR-TRC as defined in 4.5), or where no such components are present. In these environments, only attacks through the device external interfaces are applicable, excluding attacks from other components of the device.

EXAMPLE 1 Devices with single trusted application with no software loader.

— Untrusted logical environment (ENV-NTL): environment where the interacting components are considered potential vectors that could be compromised (USR-NTC as defined in 4.5). In these environments, isolation of the platform from external component is required to mitigate attacks applicable in the risk context defined in 4.3.2.3.

EXAMPLE 2 Open devices (loadable untrusted code), multi-application.

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026

oSIST prEN 40004-3:2026

4.3.2.2 Physical environment

The physical environment refers to users who have physical access to the platform.

The physical environment of the platform falls into one of the two categories:

— Trusted physical environment (ENV-TRP): environment where such users are not expected to intentionally attempt to compromise the platform (USR-TRI and USR-TRE as defined in 4.5). In these environments, attacks requiring physical access ~~to be exploited~~ are not applicable.

EXAMPLE 1 Private locations such as homes, secure server rooms within company premises, or private areas situated inside public buildings likes hospitals, libraries or shops.

— Untrusted physical environment (ENV-NTP): environment where such users are considered potential attackers or vectors of attacks (USR-NTE as defined in 4.5). In such environments, secure implementation of the platform and absence of vulnerabilities are expected to mitigate attacks requiring physical access to be exploited.

EXAMPLE 2 Public areas or easily accessible without control such as transportation hubs, public kiosks, urban infrastructure.

4.3.2.3 Risk context

In this standard, platforms are intended for integration into devices whose functionalities range from those which are associated with an existing but low likelihood of vulnerability exploitation and low adverse impact in terms of damage to users or other products, to those whose functionalities present a certain likelihood of vulnerability exploitation and medium adverse impact in terms of harm to users or other products, networks or services

To address this context platforms are expected to provide well-designed and effective security functionalities against attacks, physical and/or logical as determined by the logical and physical environment

The risk context falls into one of two categories

— Low risk environment (ENV_RKL);

— Medium risk environment (ENV_RKM).

Low risk context (ENV-RKL): in this case, platforms are intended for integration into devices where the cybersecurity risk remains limited, based on the intended use and deployment context. To address this context, platforms are required to provide well-designed and effective security functionalities with no vulnerability

Medium risk context (ENV-RKM): in this case, platforms are intended for integration into devices whose functionalities present a certain likelihood of vulnerability exploitation and medium adverse impact in terms of harm to users or other products, networks or services. To address this context, platforms are required to demonstrate the resistance of its security functionalities against attacks, physical and/or logical as determined by the logical and physical environment,

For High risk environment applications, it is expected that the platform integrator will conduct any necessary additional tests as determined by the final application

4.3.3 Device environment components

Platforms are integrated into devices intended to address various risks, resulting in distinct device environments components requiring dedicated platform security features to ensure the device ultimately achieves its intended security functionalities. The device environment components requiring appropriate platform security features are the following:

— Authenticated environment (DEV-AUT), in devices that depend on the platform to establish a trusted relationship with external entities based on verified authenticity, and/or that support the deployment of software in the field, where it is essential to verify the authenticity of the platform on which the software will run.

Sample Document
get full document from standards.iteh.ai

oSIST prEN 40004-3:2026 • https://standards.iteh.ai/catalog/standards/sist/25a0cecd-62b8-4d56-b013-18d883dd8014/osist-pren-40004-3-2026