E DIN EN 40000-11:2026-06 (E)

Erscheinungsdatum: 2026-05-22

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; English version prEN 40000-11:2026

Inhalt

Seite

European foreword 6

Introduction 7

1 Scope 8

2 Normative references 8
2.1 General 8
2.2 Evaluation methodologies 8
2.3 EUCC, State of the Art documents and Guidelines 8
2.4 Horizontal standards 8

3 Terms and definitions and abbreviations 9

4 Product context 13
4.1 Product components and architecture 13
4.1.1 Overview 13
4.1.2 Secure envelope 14
4.1.3 Hardware components 16
4.1.4 Firmware 18
4.1.5 Security Functions 20
4.1.6 Interfaces and Connectivity 22
4.1.7 External Services and Supporting Systems 23
4.1.8 Architectural Variability 23
4.2 Operational Environment 24
4.2.1 Physical Environment 24
4.2.2 Logical and physical connectivity 25
4.3 Distribution of security functions 25
4.3.1 HWSB Integration 25
4.3.2 Objectives on the environment 25
4.4 Users 28
4.5 Example HWSB Use Case 28
4.5.1 General purpose HSM 28
4.5.2 Payment Terminal / Point of Interaction (POI) 29
4.5.3 Tachograph Systems 29
4.5.4 Embedded/OEM Systems 30
4.5.5 Other HWSB Use Cases 31

5 Requirements 31
5.1 Overview 31
5.2 Technical Requirements 32
5.2.1 User Authentication (REQ-USER-AUTH-XXX) 32
5.2.2 Event Authorization (REQ-AUTHORIZATION-XXX) 36
5.2.3 Device Authentication (REQ-DEVICE-AUTH-XXX) 38
5.2.4 Sensitive Data Import (REQ-SD-IMPORT-XXX) 41
5.2.5 Secure Communication (REQ-SEC-COM-XXX) 43
5.2.6 Secure Firmware Update (REQ-COP-SECUP-XXX) 46
5.2.7 Stored Data Integrity (REQ-SDI-XXX) 48

5.2.8 Stored Data Confidentiality (REQ-SDC-HWSB-XXX) 49
5.2.9 Code Execution Integrity (REQ-CEI-XXX) 50
5.2.10 Secure Audit (REQ-LOG -XXX) 55
5.2.11 Assured Cryptography (REQ-CRY-XXX) 58
5.2.12 Physical Protection (REQ-PHY-XXX) 65
5.2.13 Secure-by-default configuration (REQ-COP-SECDEF-XXX) 70
5.2.14 Secure Backup and Restore (REQ-BACKUP-XXX) 71
5.2.15 Processed Data Minimization (REQ-DATAMIN-XXX) 74
5.2.16 Residual Information Protection (REQ-DPR-XXX) 75
5.2.17 Attack Impact Minimization (REQ-AIM-XXX) 76
5.2.18 Attack Surface Minimization (REQ-AS-MINIMISE-XXX) 76
5.3 Assurance requirements 77
5.3.1 Vulnerability handling process (REQ-ASS-VUL-HAND) 77
5.3.2 Exploitable Vulnerabilities (REQ-ASS-VUL-EXP) 78
5.3.3 Software Bill of Materials (REQ-ASS-SBOM) 78
5.3.4 Selection Guidance 79

6 Conformity Assessment / Tests (normative) 79
6.1 Assessment methodology 79
6.2 Assessment format 79
6.2.1 Assessment Reference 79
6.2.2 Assessment Objective 79
6.2.3 Assessment Preparation 79
6.2.4 Assessment Activities 80
6.2.5 Assessment Verdict 80
6.2.6 Assessment evidence 80
6.3 Product requirements assessment 80
6.3.1 Assessment - Operator Authentication 80
6.3.2 Assessment - Event Authorization 82
6.3.3 Assessment - Device Authentication 83
6.3.4 Assessment - Sensitive Data Import 84
6.3.5 Assessment - Secure Communication 86
6.3.6 Assessment - Secure Firmware Update 87
6.3.7 Assessment - Stored Data Integrity 88
6.3.8 Assessment - Stored Data Confidentiality 90
6.3.9 Assessment - Code execution integrity 91
6.3.10 Assessment - Secure Audit 92
6.3.11 Assessment - Assured Cryptography 94
6.3.12 Assessment - Physical Protection 95
6.3.13 Assessment - Secure-by-default Configuration 97
6.3.14 Assessment - Secure Backup and Restore 98
6.3.15 Assessment - Processed Data Minimization 99
6.3.16 Assessment - Residual Information Protection 100
6.3.17 Assessment – Attack Impact Minimization 101
6.3.18 Assessment - Attack Surface Minimization 102

Annex A (normative) Security Profile 106
A.1 Introduction 106
A.2 Selecting Assurance Profile and Requirements Modules based on IPRFU 107
A.3 Assurance Profile 110
A.4 Requirements Modules 112

Annex B (informative) Security Analysis 118
B.1 Overview 118
B.2 IPRFU 118
B.2.1 Intended Purpose 118
B.2.2 Reasonably Foreseeable Use 119
B.2.3 Mapping IPRFU to HWSB during security analysis 119
B.3 Analysis 119

B.3.1 Security Objectives and Assets 119
B.3.2 Threats 120
B.3.3 Threat mapping to Objectives and Assets 121
B.3.4 Security control mapping to threats 123

Annex C (informative) Other verticals of interest 126

Annex K (normative) Cryptography 127
K.1 State of the Art Cryptography (CRY-SOTA) 127
K.1.1 Requirement 127
K.1.2 Assessment criteria 127
K.2 Crypto agility 130
K.2.1 Requirement 130
K.2.2 Assessment criteria 130

Annexe R (normative) Additional provisions for products relying on remote data processing solutions (RDPS) 132
R.1 Scope & Applicability 132
R.2 RDPS as a product-boundary extension 132
R.X Standard-specific identification of RDPS-dependent functions, RDPS interface(s), and RDPS 133
R.X.1 RDPS-dependent product functions 133
R.X.2 RDPS interface(s) 133
R.X.3 RDPS(s) 134
R.3 Threat Model 134
R.3.1 Assets 134
R.3.2 Threat catalogue 135
R.3.3 Assets ↔ Threats mapping 136
R.4 Security Requirements 136
R.4.1 General 136
R.4.2 Local product side requirements 137
R.4.3 RDPS side requirements 142
R.4.4 Threats ↔ Requirements mapping 147
R.4.5 Mapping of CRA Annex I to Annex R requirements 147
R.6 Security controls and mitigation guidance for RDPS requirements (informative) 150
R.6.1 Controls catalogue for REQ-RDPS-L-001 150
R.6.2 Controls catalogue for REQ-RDPS-L-002 150
R.7 Conformity assessment 151
R.7.1 General 151
R.7.2 Conformity assessment for REQ-RDPS-L-001 151
R.7.3 Conformity assessment for REQ-RDPS-R-001 152
R.7.x Conformity assessment for REQ-RDPS-R-004 154

Annex ZA (informative) Relationship between this European Standard and the essential cybersecurity requirements line 39: for Hardware Devices with Security Boxes 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 157

Bibliography 159

Figures

Figure 1 : HWSB product generic architecture 14

Figure 2 : Layered security envelope 15

Figure 3 : Distributed secure envelope with protection islands 15

Figure 1: RDPS as a product-boundary extension (Annex R scope: RDPS interface + RDPS)..... 133

Tables

Table A- 1: Rule Based Security Profile – Selection Options 108

Table A- 2: Rule Based Security Profile – Selection Options 109

Table A- 3: Template Based Security Profile – Selection Options 110

Table A- 4: Security Profile – Assurance Profiles..... 112

Table A- 5: Requirements Modules – Applicability Matrix..... 117

Table B- 2: Security Control to Threat Mapping..... 125

Table 1: Threats ↔ Assets mapping..... 136

Table 2: Threats ↔ Requirements mapping..... 147

Table ZA.1 — Correspondence between this European Standard and essential requirements from the CRA regulation..... 157