E DIN EN 40000-10:2026-06 (E)

Erscheinungsdatum: 2026-05-22

Essential cybersecurity requirements for products - Part 10: Products with digital elements used in identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers; English version prEN 40000-10:2026

Contents

Page

European foreword 6

Introduction 7

1 Scope 8

2 Normative references 11

3 Terms, definitions, symbols and abbreviated terms 12
3.1 Terms and definitions 12
3.2 Symbols and abbreviated terms 17

4 Product context 18
4.1 Product functions 18
4.2 Product architecture 18
4.3 Operational environment 19
4.3.1 Introduction 19
4.3.2 General Description 19
4.3.3 Connectivity Aspects 19
4.4 Distribution of Security Functions 20
4.5 Users 20
4.6 Use Cases and security profiles 20

5 Requirements on Products 24
5.1 Introduction – Technical Guidance and Security Analysis 24
5.1.1 General 24
5.1.2 Requirement [REQ-TGSA-001] 24
5.1.3 Requirement [REQ-TGSA-002] 24
5.1.4 Requirement [REQ-TGSA-003] 24
5.1.5 Requirement [REQ-TGSA-004] 25
5.1.6 Requirement [REQ-TGSA-005] 25
5.1.7 Requirement [REQ-TGSA-006] 27
5.2 No known exploitable vulnerabilities 27
5.2.1 Requirement [REQ-KEV-001] 27
5.2.2 Requirement [REQ-KEV-002] 28
5.2.3 Requirement [REQ-KEV-003] 28
5.2.4 Requirement [REQ-KEV-004] 28
5.2.5 Requirement [REQ-KEV-005] 28
5.2.6 Requirement [REQ-KEV-006] 29
5.2.7 Requirement [REQ-KEV-007] 29
5.2.8 Requirement for the basic security profiles [REQ-KEV-008] 29
5.2.9 Additional requirement for the substantial security profiles [REQ-KEV-009] 29
5.2.10 Additional requirement for the high security profiles [REQ-KEV-010] 29
5.2.11 Additional requirement for the high security profiles [REQ-KEV-011] 30
5.3 Secure by design 30
5.3.1 Requirement [REQ-SBD-001] 30
5.3.2 Requirement [REQ-SBD-002] 30
5.3.3 Requirement [REQ-SBD-003] 30

5.3.4 Requirement [REQ-SBD-004] 31
5.3.5 Requirement [REQ-SBD-005] 31
5.4 Secure updates - Requirement [REQ-SU-001] 31
5.5 Authentication and access control 31
5.5.1 Requirement [REQ-AC-001] 31
5.5.2 Requirement [REQ-AC-002] 31
5.6 Integrity and Confidentiality 32
5.6.1 Requirement [REQ-CON-001] 32
5.6.2 Requirement [REQ-CON-002] 32
5.6.3 Requirement [REQ-CON-003] 32
5.7 Data minimisation 32
5.7.1 Requirement [REQ-DM-001] 32
5.7.2 Requirement [REQ-DM-002] 33
5.7.3 Requirement [REQ-DM-003] 33
5.8 Availability protection 33
5.8.1 Requirement [REQ-AP-001] 33
5.8.2 Requirement [REQ-AP-002] 33
5.8.3 Requirement [REQ-AP-003] 33
5.9 Impact minimisation 34
5.9.1 Requirement [REQ-IM-001] 34
5.9.2 Requirement [REQ-IM-002] 34
5.10 Minimisation of attack surfaces 34
5.10.1 Requirement [REQ-MAS-001] 34
5.10.2 Requirement [REQ-MAS-002] 34
5.10.3 Requirement [REQ-MAS-003] 35
5.10.4 Requirement [REQ-MAS-004] 35
5.10.5 Requirement [REQ-MAS-005] 35
5.11 Exploitation mitigation mechanisms 35
5.11.1 Requirement [REQ-EMM-001] 35
5.11.2 Requirement [REQ-EMM-002] 35
5.12 Logging and monitoring 36
5.12.1 Requirement [REQ-LOG-001] 36
5.12.2 Requirement [REQ-LOG-002] 36
5.13 Data removal and transparency 36
5.13.1 Requirement [REQ-DRT-001] 36
5.13.2 Requirement [REQ-DRT-002] 36
5.13.3 Requirement [REQ-DRT-003] 37
5.13.4 Requirement [REQ-DRT-004] 37
5.14 Vulnerability handling 37
5.14.1 Requirement [REQ-VH-001] 37
5.14.2 Requirement [REQ-VH-002] 37
5.14.3 Requirement [REQ-VH-003] 38
5.14.4 Requirement [REQ-VH-004] 38
5.14.5 Requirement [REQ-VH-005] 38
5.14.6 Requirement [REQ-VH-006] 38
5.14.7 Requirement [REQ-VH-007] 38

6 Conformity assessment against the normative requirements 40
6.1 Introduction 40
6.2 Conformity assessment against the normative requirements 43
6.2.1 Technical Guidance Requirements (5.1) 43
6.2.2 Security Analysis and Security Profile Level Requirements (5.2) 52
6.2.3 Secure-by-Design Requirements (5.3) 56
6.2.4 Cybersecurity Analysis Requirements (5.4) 71

6.2.5 Vulnerability Management Requirements (5.5) 75
6.2.6 Security Profile Requirements (5.6) 81
Annex A (informative) Hardware products 84
Annex B (informative) Software products 87
Annex C (informative) Physical access control system 90
C.1 General architecture of a PACS 90
C.2 Detailed description of subsystems containing products 90
C.2.1 Opening and locking devices including on/off-line connected locks 90
C.2.2 Reading modules 90
C.2.3 Local processing unit 91
C.2.4 Door and I/O modules 91
C.2.5 Centralized access management 91
C.2.6 User interfaces 92
Annex D (informative) Identity management system 93
D.1 General architecture of an IDMS 93
D.2 Detailed description of subsystems containing Products 93
D.2.1 Identity repositories and directory services 93
D.2.2 Identity enrolment and provisioning components 93
D.2.3 Authentication services 94
D.2.4 Authorization and policy management services 94
D.2.5 Governance, audit, and compliance components 94
D.2.6 User interfaces and self-service tools 94
Annex E (normative) Threat levels and severity levels of the security analysis 95
Annex F (informative) Security problem definition 97
F.1 Synthesis 97
F.2 Rationale 97
F.3 Description of the technical operating environment 97
F.4 Assets to be protected 97
F.5 Threats 97
F.6 Security functions 97
F.7 Threats coverage 97
Annex G (normative) Product interfaces 98
Annex H (informative) Product communication protocols 101
Annex I (normative) Attacks rating methodology 102
Annex J (informative) Cryptographic specifications proposed document structure 105
J.1 General description of the product 105
J.2 Keys architecture 105
J.3 List of the cryptographic dependencies 105
J.4 Mapping between the security functions and the cryptographic mechanisms 105
J.5 Detail of the cryptographic mechanisms 105
Annex K (normative) Cryptography 106

K.1 State of the Art Cryptography (CRY-SOTA) 106
K.1.1 Requirement 106
K.1.2 Assessment criteria 106
K.2 Crypto agility 108
K.2.1 Requirement 108
K.2.2 Assessment criteria 109
Annex L (normative) Risk registry 111
Annex R (normative) Additional provisions for products relying on remote data processing solutions (RDPS) 124
R.1 Scope & Applicability 124
R.2 RDPS as a product-boundary extension 124
R.X Standard-specific identification of RDPS-dependent functions, RDPS interface(s), and RDPS 125
R.X.1 RDPS-dependent product functions 125
R.X.2 RDPS interface(s) 125
R.X.3 RDPS(s) 125
R.3 Threat Model 126
R.3.1 General 126
R.3.2 Assets 126
R.3.3 Threat catalogue 126
R.3.4 Assets ↔ Threats mapping 128
R.4 Security Requirements 128
R.4.1 General 128
R.4.2 Local product side requirements 129
R.4.3 RDPS side requirements 133
R.4.4 Threats ↔ Requirements mapping 137
R.4.5 Mapping of CRA Annex I to Annex R requirements 138
R.5 Security controls and mitigation guidance for RDPS requirements (informative) 141
R.5.1 General 141
R.5.2 Controls catalogue for REQ-RDPS-L-001 141
R.5.3 Controls catalogue for REQ-RDPS-L-002 141
R.6 Conformity assessment 141
R.6.1 General 142
R.6.2 Conformity assessment for REQ-RDPS-L-001 142
R.6.3 Conformity assessment for REQ-RDPS-R-001 143
R.6.4 Conformity assessment for REQ-RDPS-R-004 144
Annex ZA (informative) Relationship between this European Standard and the essential requirements of Regulation (EU) 2024/2847 (CRA) aimed to be covered 147
Bibliography 149