E DIN EN 18330:2026-03 (E)

Erscheinungsdatum: 2026-01-30

Smartcards, similar devices and Secure Elements - Criteria to achieve conformity with essential requirements of Regulation (EU) 2024/2847; English version prEN 18330:2026

Inhalt

Seite

European foreword 5

Introduction 6

1 Scope 7

2 Normative references 7

3 Terms and definitions 7
3.1 Terms and definitions 7
3.2 Symbols and abbreviated terms 8

4 Product context 9
4.1 Intended purpose and foreseeable use 9
4.2 Product functions 10
4.3 Product architecture 10
4.3.1 General notes on product architecture 10
4.3.2 Secure element 10
4.3.3 Smart card 11
4.3.4 Similar devices 11
4.4 Operational environment 12
4.5 Distribution of security functions 12
4.6 Users 12
4.7 Use cases 12

5 Security requirements 14
5.1 General notes on security requirements 14
5.2 Product security 14
5.2.1 Security by design 14
5.2.2 No known exploitable vulnerabilities 15
5.2.3 Secure-by-default configuration 15
5.2.4 Enable secure update 16
5.2.5 Prevent unauthorized access 17
5.2.6 Ensure data confidentiality 17
5.2.7 Preserve integrity 18
5.2.8 Data minimization 19
5.2.9 Essential and basic functions 19
5.2.10 Minimize service disruption 19
5.2.11 Limit attack exposure 20
5.2.12 Mitigate incident impact 21
5.2.13 Monitor security activity 21
5.2.14 Ensure secure erasure 22
5.3 Essential vulnerability handling requirements 23
5.4 General notes 23
5.4.1 Identify components and vulnerabilities 23
5.4.2 Address and remediate vulnerabilities 23
5.4.3 Regular testing 24
5.4.4 Public disclosure obligation 24
5.4.5 Public disclosure policy 25

5.4.6 Support third party reporting 25
5.4.7 Secure (automated) distribution of updates 25
5.4.8 Dissemination of updates 26
5.5 Additional security requirements 26
5.5.1 Requirements on RDPS 26
5.5.2 Manufacturer Environment Security 26

6 Conformity assessment 27
6.1 Assessment of product security 27
6.1.1 Security by Design assessment 27
6.1.2 No Known Exploitable Vulnerabilities assessment 27
6.1.3 Secure-by-Default Configuration assessment 27
6.1.4 Enable Secure Update assessment 28
6.1.5 Prevent unauthorized access assessment 29
6.1.6 Ensure data confidentiality assessment 30
6.1.7 Preserve data integrity assessment 30
6.1.8 Data minimization assessment 31
6.1.9 Essential and basic functions assessment 31
6.1.10 Service disruption minimization assessment 31
6.1.11 Limit attack exposure assessment 31
6.1.12 Mitigate incident impact assessment 32
6.1.13 Monitor security activity assessment 32
6.1.14 Ensure secure erasure assessment 32
6.2 Assessment of essential vulnerability handling 33
6.2.1 Identify components and vulnerabilities (SBOM) assessment 33
6.2.2 Address and remediate vulnerabilities assessment 33
6.2.3 Regular testing assessment 34
6.2.4 Public disclosure obligation assessment 34
6.2.5 Public disclosure policy assessment 34
6.2.6 Third party reporting support assessment 34
6.2.7 Secure (automated) distribution of updates assessment 34
6.2.8 Dissemination of updates assessment 35
6.3 Additional security requirements 35
6.3.1 RDPS security assessment 35
6.3.2 Manufacturer environment security assessment 35

Annex A (normative) Extended SARs and SFRs 36
A.1 Overview 36
A.2 Extended SARs 36
A.2.1 ADV_ARC.2 security architecture with default security configuration (extended) 36
A.2.2 ADV_PDM.1: processed data minimization 40
A.2.3 ALC_SBM: Software bill of materials 42
A.2.4 ALC_FLR.4: Flaw remediation with distinction between security and functional flaws 44
A.2.5 ALC_PSR.1: Periodic security review and testing 45

Annex B (informative) Risk acceptance criteria and risk management methodology 48
B.1 Risk acceptance + risk management methodology 48
B.2 Risk Assessment 48
B.2.1 Threat modelling 48
B.2.2 Severity assessment 48
B.2.3 Risk profile 49
B.2.4 Relation between risk profiles and use cases 49

Annex C (informative) Governmental use cases 50
C.1 Overview 50
C.2 Specifications and Protection Profiles 50

Annex D (informative) UICC and eUICC use cases 52
D.1 Overview 52
D.2 Applicable Protection Profiles 52

Annex ZA (informative) Relationship between this European Standard and the essential requirements of Regulation (EU) 2024/2847 aimed to be covered **53**

Bibliography **55**

Figures

Figure 1 Example of relations between an intended purpose of a Product and functions within use cases **10**

Figure 2 — Simplified architecture of a secure element **10**

Figure 3 — Representation of the ICCs and their division to the smart cards that are comprising the Secure Element and other that may have different types of integrated circuit. **11**

Figure 4 — Some examples of similar devices that may contain SE. **11**

Figure A.1 — component levelling of ADV_ARC family **36**

Figure A.2 — Component levelling of ADV_PDM family **40**

Figure A.3 — component levelling for ALC_SBM family **42**

Figure A.4 — component levelling of ALC_FLR family (extended) **44**

Figure A.5 — component levelling of ALC_PSR assurance family **46**

Tables

Table 1 — Terms and abbreviations **8**

Table 2 — Use cases in relation to appropriate vulnerability analysis level **13**

Table B.1 — Product threat categories **48**

Table B.2 — Product severity threats categories **48**

Table B.3 — resulting risk profiles (RP) **49**

Table C.1 — Overview of governmental use case for a Product **50**

Table ZA.1 — Correspondence between this European Standard and essential requirements from the CRA regulation. **53**