



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for boot managers**

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-008

KeywordsCRA, cybersecurity

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	12
Foreword.....	12
Modal verbs terminology.....	13
Introduction	13
1 Scope	14
1.1 General	14
2 References	14
2.1 Normative references	14
2.2 Informative references.....	15
3 Definition of terms, symbols and abbreviations.....	16
3.1 Terms.....	16
3.2 Symbols.....	19
3.3 Abbreviations	19
4 Product context.....	20
4.1 Product Functions.....	20
4.1.1 Intended purpose.....	20
4.1.2 Reasonably foreseeable use	21
4.1.3 Reasonably foreseeable misuse.....	21
4.1.4 General functions.....	21
4.2 Product Architecture.....	22
4.2.1 Boot architecture.....	22
4.2.1.1 Unverified boot	22
4.2.1.2 Verified boot	22
4.2.1.3 Measured boot.....	23
4.2.2 Functional extensions	24
4.2.3 Product capabilities.....	24
4.2.3.1 Introduction.....	24
4.2.3.2 Update capability	24
4.2.3.3 Boot source	25
4.2.3.4 Configuration management	25
4.2.3.5 Hardware security	26
4.2.3.6 Recovery capability.....	26
4.2.3.7 Logging capability	26
4.2.3.8 Authentication capability	26
4.2.3.9 Debug interface	27
4.2.3.10 Key provisioning.....	27
4.2.4 Resource constraints	27
4.3 Operational environment.....	28
4.3.1 Introduction.....	28
4.3.2 Physical security context	28
4.3.3 Network exposure.....	28
4.3.4 Data sensitivity and value	28
4.3.5 System criticality	28
4.3.6 Lifecycle expectations	29
4.3.7 Administrative control.....	29
4.3.8 Availability requirements	29
4.3.9 Additional environmental characteristics.....	29
4.3.9.1 Environmental stress.....	29
4.3.9.2 Update frequency expectations	30
4.3.9.3 Interfaces	30
4.4 Distribution of security functions.....	30
4.4.1 Introduction.....	30
4.4.2 Security functions provided by the boot manager.....	30
4.4.3 Security functions required from the platform.....	31

4.4.4	Security functions delegated to boot target.....	31
4.4.5	Trust boundaries	31
4.5	Users.....	32
4.5.1	Introduction.....	32
4.5.2	User categories.....	32
4.5.3	User interaction patterns	32
4.6	Use cases	33
4.6.1	Purpose	33
4.6.2	Capabilities as risk exposures	33
4.6.3	Use case definitions	33
4.6.3.0	Use cases and security profiles.....	33
4.6.3.1	UC-IMM: Immutable	34
4.6.3.2	UC-VER: Verified and updateable	34
4.6.3.3	UC-HW: Hardware-assisted security	34
4.6.4	Functional capabilities and additional requirements.....	34
4.6.5	Use case selection	35
5	Technical requirements for products	35
5.1	Introduction: Applicability of the requirements	35
5.1.1	General.....	35
5.1.2	Use case declaration.....	36
5.1.2.0	Introduction.....	36
5.1.2.1	[UC-IMM].....	36
5.1.2.2	[UC-VER]	36
5.1.2.3	[UC-HW]	36
5.1.3	Not applicable verdict.....	36
5.2	Appropriate level of cybersecurity	37
5.2.0	Introduction appropriate level of cybersecurity requirements	37
5.2.1	[REQ-BM-RRM-001].....	37
5.2.2	[REQ-BM-RRM-002].....	37
5.2.3	[REQ-BM-RRM-003].....	37
5.2.4	[REQ-BM-RRM-004].....	37
5.2.5	[REQ-BM-RRM-005].....	37
5.3	No known exploitable vulnerabilities.....	38
5.3.0	Introduction to no known exploitable vulnerabilities requirements.....	38
5.3.1	[REQ-BM-KEV-001]	38
5.3.2	[REQ-BM-KEV-002]	38
5.3.3	[REQ-BM-KEV-003]	38
5.4	Secure by default configuration.....	38
5.4.0	Introduction to secure by default configuration requirements	38
5.4.1	[REQ-BM-SBD-001].....	38
5.4.2	[REQ-BM-SBD-002].....	39
5.4.3	[REQ-BM-SBD-003].....	39
5.4.4	[REQ-BM-SBD-004].....	39
5.4.5	[REQ-BM-SBD-005].....	39
5.4.6	[REQ-BM-SBD-006].....	39
5.5	Secure updates	40
5.5.0	Introduction to secure updates requirements	40
5.5.1	[REQ-BM-SU-001]	40
5.5.2	[REQ-BM-SU-002]	40
5.5.3	[REQ-BM-SU-003]	41
5.5.4	[REQ-BM-SU-004]	41
5.5.5	[REQ-BM-SU-005]	41
5.5.6	[REQ-BM-SU-006]	41
5.5.7	[REQ-BM-SU-007]	41
5.6	Authentication and access control	41
5.6.0	Introduction to authentication and access control requirements	41
5.6.1	[REQ-BM-AC-001]	41
5.6.2	[REQ-BM-AC-002]	42
5.6.3	[REQ-BM-AC-003]	42
5.6.4	[REQ-BM-AC-004]	42
5.6.5	[REQ-BM-AC-005]	42

5.6.6	[REQ-BM-AC-006]	42
5.6.7	[REQ-BM-AC-007]	43
5.6.8	[REQ-BM-AC-008]	43
5.6.9	[REQ-BM-AC-009]	43
5.6.10	[REQ-BM-AC-010]	43
5.6.11	[REQ-BM-AC-011]	43
5.7	Confidentiality protection	43
5.7.0	Introduction to confidentiality protection requirements	43
5.7.1	[REQ-BM-CP-001]	44
5.7.2	[REQ-BM-CP-002]	44
5.7.3	[REQ-BM-CP-003]	44
5.7.4	[REQ-BM-CP-004]	44
5.7.5	[REQ-BM-CP-005]	44
5.7.6	[REQ-BM-CP-006]	45
5.7.7	[REQ-BM-CP-007]	45
5.7.8	[REQ-BM-CP-008]	45
5.7.9	[REQ-BM-CP-009]	45
5.7.10	[REQ-BM-CP-010]	45
5.8	Integrity protection	45
5.8.0	Introduction to integrity protection requirements	45
5.8.1	[REQ-BM-INT-001]	46
5.8.2	[REQ-BM-INT-002]	46
5.8.3	[REQ-BM-INT-003]	46
5.8.4	[REQ-BM-INT-004]	46
5.8.5	[REQ-BM-INT-005]	47
5.8.6	[REQ-BM-INT-006]	47
5.8.7	[REQ-BM-INT-007]	47
5.8.8	[REQ-BM-INT-008]	47
5.8.9	[REQ-BM-INT-009]	47
5.8.10	[REQ-BM-INT-010]	47
5.8.11	[REQ-BM-INT-011]	47
5.8.12	[REQ-BM-INT-012]	48
5.8.13	[REQ-BM-INT-013]	48
5.8.14	[REQ-BM-INT-014]	48
5.8.15	[REQ-BM-INT-015]	48
5.8.16	[REQ-BM-INT-016]	48
5.8.17	[REQ-BM-INT-017]	48
5.8.18	[REQ-BM-INT-018]	49
5.8.19	[REQ-BM-INT-019]	49
5.8.20	[REQ-BM-INT-020]	49
5.8.21	[REQ-BM-INT-021]	49
5.8.22	[REQ-BM-INT-022]	50
5.8.23	[REQ-BM-INT-023]	50
5.8.24	[REQ-BM-INT-024]	50
5.9	Data minimisation	50
5.9.0	Introduction to data minimisation requirements	50
5.9.1	[REQ-BM-DM-001]	50
5.9.2	[REQ-BM-DM-002]	50
5.10	Availability protection	51
5.10.0	Introduction to availability protection requirements	51
5.10.1	[REQ-BM-AP-001]	51
5.10.2	[REQ-BM-AP-002]	51
5.10.3	[REQ-BM-AP-003]	51
5.10.4	[REQ-BM-AP-004]	51
5.10.5	[REQ-BM-AP-005]	51
5.10.6	[REQ-BM-AP-006]	52
5.10.7	[REQ-BM-AP-007]	52
5.10.8	[REQ-BM-AP-008]	52
5.10.9	[REQ-BM-AP-009]	52
5.10.10	[REQ-BM-AP-010]	53
5.10.11	[REQ-BM-AP-011]	53
5.10.12	[REQ-BM-AP-012]	53

5.10.13	[REQ-BM-AP-013]	53
5.10.14	[REQ-BM-AP-014]	53
5.10.15	[REQ-BM-AP-015]	53
5.10.16	[REQ-BM-AP-016]	53
5.11	Non-interference.....	54
5.11.0	Introduction to impact minimisation requirements	54
5.11.1	[REQ-BM-IM-001].....	54
5.12	Attack surface minimisation.....	54
5.12.0	Introduction to attack surfaces minimisation requirements	54
5.12.1	[REQ-BM-AMS-001]	54
5.12.2	[REQ-BM-AMS-002].....	54
5.12.3	[REQ-BM-AMS-003].....	55
5.12.4	[REQ-BM-AMS-004].....	55
5.12.5	[REQ-BM-AMS-005].....	55
5.12.6	[REQ-BM-AMS-006].....	55
5.12.7	[REQ-BM-AMS-007].....	56
5.13	Exploit mitigation.....	56
5.13.0	Introduction to exploit mitigation requirements	56
5.13.1	[REQ-BM-EM-001].....	56
5.14	Monitoring.....	56
5.14.0	Introduction to monitoring requirements	56
5.14.1	[REQ-BM-MON-001]	56
5.14.2	[REQ-BM-MON-002]	56
5.14.3	[REQ-BM-MON-003]	57
5.14.4	[REQ-BM-MON-004]	57
5.14.5	[REQ-BM-MON-005]	57
5.15	Factory reset and data portability	57
5.15.0	Introduction.....	57
5.15.1	[REQ-BM-FRDP-001].....	58
6	Assessment criteria for compliance with technical requirement.....	58
6.1	Introduction to the assessment and compliance criteria	58
6.1.0	Assessment criteria general structure.....	58
6.1.1	Boot manager assessment considerations	60
6.1.2	Scope of assessment.....	60
6.1.3	Assessment report requirements	60
6.2	Appropriate level of cybersecurity	61
6.2.0	Overview of requirements addressed in clause 6.2.....	61
6.2.1	[ACC-BM-RRM-001]	61
6.2.2	[ACC-BM-RRM-002]	61
6.2.3	[ACC-BM-RRM-003]	62
6.2.4	[ACC-BM-RRM-004]	63
6.2.5	[ACC-BM-RRM-005]	63
6.3	No known exploitable vulnerabilities.....	64
6.3.0	Overview of requirements addressed in clause 6.3.....	64
6.3.1	[ACC-BM-KEV-001]	64
6.3.2	[ACC-BM-KEV-002]	65
6.3.3	[ACC-BM-KEV-003]	66
6.4	Secure by default configuration.....	67
6.4.0	Overview of requirements addressed in clause 6.4.....	67
6.4.1	[ACC-BM-SBD-001].....	67
6.4.2	[ACC-BM-SBD-002].....	67
6.4.3	[ACC-BM-SBD-003].....	68
6.4.4	[ACC-BM-SBD-004].....	69
6.4.5	[ACC-BM-SBD-005].....	70
6.4.6	[ACC-BM-SBD-006].....	70
6.5	Secure updates.....	71
6.5.0	Overview of requirements addressed in clause 6.5.....	71
6.5.1	[ACC-BM-SU-001]	71
6.5.2	[ACC-BM-SU-002]	72
6.5.3	[ACC-BM-SU-003]	73
6.5.4	[ACC-BM-SU-004]	73

6.5.5	[ACC-BM-SU-005]	74
6.5.6	[ACC-BM-SU-006]	75
6.5.7	[ACC-BM-SU-007]	76
6.6	Authentication and access control	76
6.6.0	Overview of requirements addressed in clause 6.6	76
6.6.1	[ACC-BM-AC-001]	77
6.6.2	[ACC-BM-AC-002]	78
6.6.3	[ACC-BM-AC-003]	78
6.6.4	[ACC-BM-AC-004]	79
6.6.5	[ACC-BM-AC-005]	80
6.6.6	[ACC-BM-AC-006]	80
6.6.7	[ACC-BM-AC-007]	81
6.6.8	[ACC-BM-AC-008]	82
6.6.9	[ACC-BM-AC-009]	83
6.6.10	[ACC-BM-AC-010]	83
6.6.11	[ACC-BM-AC-011]	84
6.7	Confidentiality protection	85
6.7.0	Overview of requirements addressed in clause 6.7	85
6.7.1	[ACC-BM-CP-001]	85
6.7.2	[ACC-BM-CP-002]	86
6.7.3	[ACC-BM-CP-003]	87
6.7.4	[ACC-BM-CP-004]	87
6.7.5	[ACC-BM-CP-005]	88
6.7.6	[ACC-BM-CP-006]	89
6.7.7	[ACC-BM-CP-007]	90
6.7.8	[ACC-BM-CP-008]	90
6.7.9	[ACC-BM-CP-009]	91
6.7.10	[ACC-BM-CP-010]	92
6.8	Integrity protection	93
6.8.0	Overview of requirements addressed in clause 6.8	93
6.8.1	[ACC-BM-INT-001]	93
6.8.2	[ACC-BM-INT-002]	94
6.8.3	[ACC-BM-INT-003]	95
6.8.4	[ACC-BM-INT-004]	95
6.8.5	[ACC-BM-INT-005]	96
6.8.6	[ACC-BM-INT-006]	97
6.8.7	[ACC-BM-INT-007]	97
6.8.8	[ACC-BM-INT-008]	98
6.8.9	[ACC-BM-INT-009]	99
6.8.10	[ACC-BM-INT-010]	99
6.8.11	[ACC-BM-INT-011]	100
6.8.12	[ACC-BM-INT-012]	101
6.8.13	[ACC-BM-INT-013]	101
6.8.14	[ACC-BM-INT-014]	102
6.8.15	[ACC-BM-INT-015]	103
6.8.16	[ACC-BM-INT-016]	103
6.8.17	[ACC-BM-INT-017]	104
6.8.18	[ACC-BM-INT-018]	105
6.8.19	[ACC-BM-INT-019]	106
6.8.20	[ACC-BM-INT-020]	106
6.8.21	[ACC-BM-INT-021]	107
6.8.22	[ACC-BM-INT-022]	108
6.8.23	[ACC-BM-INT-023]	109
6.8.24	[ACC-BM-INT-024]	109
6.9	Data minimisation	110
6.9.0	Overview of requirements addressed in clause 6.9	110
6.9.1	[ACC-BM-DM-001]	110
6.9.2	[ACC-BM-DM-002]	111
6.10	Availability protection	112
6.10.0	Overview of requirements addressed in clause 6.10	112
6.10.1	[ACC-BM-AP-001]	112
6.10.2	[ACC-BM-AP-002]	113

6.10.3	[ACC-BM-AP-003]	114
6.10.4	[ACC-BM-AP-004]	114
6.10.5	[ACC-BM-AP-005]	115
6.10.6	[ACC-BM-AP-006]	116
6.10.7	[ACC-BM-AP-007]	116
6.10.8	[ACC-BM-AP-008]	117
6.10.9	[ACC-BM-AP-009]	118
6.10.10	[ACC-BM-AP-010]	118
6.10.11	[ACC-BM-AP-011]	119
6.10.12	[ACC-BM-AP-012]	120
6.10.13	[ACC-BM-AP-013]	120
6.10.14	[ACC-BM-AP-014]	121
6.10.15	[ACC-BM-AP-015]	122
6.10.16	[ACC-BM-AP-016]	123
6.11	Non-interference	123
6.11.0	Overview of requirements addressed in clause 6.11	123
6.11.1	[ACC-BM-IM-001]	123
6.12	Attack surface minimisation	124
6.12.0	Overview of requirements addressed in clause 6.12	124
6.12.1	[ACC-BM-AMS-001]	124
6.12.2	[ACC-BM-AMS-002]	125
6.12.3	[ACC-BM-AMS-003]	126
6.12.4	[ACC-BM-AMS-004]	126
6.12.5	[ACC-BM-AMS-005]	127
6.12.6	[ACC-BM-AMS-006]	128
6.12.7	[ACC-BM-AMS-007]	128
6.13	Exploit mitigation	129
6.13.0	Overview of requirements addressed in clause 6.13	129
6.13.1	[ACC-BM-EM-001]	130
6.14	Monitoring	131
6.14.0	Overview of requirements addressed in clause 6.14	131
6.14.1	[ACC-BM-MON-001]	131
6.14.2	[ACC-BM-MON-002]	132
6.14.3	[ACC-BM-MON-003]	133
6.14.4	[ACC-BM-MON-004]	134
6.14.5	[ACC-BM-MON-005]	134
6.15	Factory reset and data portability	135
6.15.0	Overview of requirements addressed in clause 6.15	135
6.15.1	[ACC-BM-FRDP-001]	135

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847 - The Cyber Resilience Act	137
-------------------------------	--	------------

Annex B (informative):	Security analysis	140
-------------------------------	--------------------------	------------

B.0	Introduction	140
B.1	Assets	140
B.1.1	A-CRYPT: Cryptographic keys and certificates	140
B.1.2	A-ROLLBACK: Rollback protection data	140
B.1.3	A-CONFIG: Configuration data	141
B.1.4	A-AUTH: Authentication credentials	141
B.1.5	A-MEASURE: Measurement and attestation data	141
B.1.6	A-AUDIT: Audit logs	141
B.1.7	A-RUNTIME: Runtime state data	142
B.1.8	A-CODE: Boot manager executable code	142
B.1.9	A-UPDATE: Update packages and delivery mechanisms	142
B.2	Risk Factors	142
B.2.1	General	142
B.2.2	RF-SURFACE: Capability-driven attack surface	142
B.2.3	RF-NET: Network reachability	143

B.2.4	RF-AVAIL: Operational continuity	143
B.2.5	RF-IMPACT: Compromise severity	143
B.3	Assumptions	144
B.3.1	General	144
B.3.2	Hardware platform assumptions	144
B.3.3	Process assumptions	144
B.3.4	Boot target assumptions	144
B.4	Threats	145
B.4.1	Security property impacts	145
B.4.1.1	General	145
B.4.1.2	Confidentiality	145
B.4.1.3	Integrity	145
B.4.1.4	Availability	146
B.4.1.5	Impact of other devices	146
B.4.2	Threat identification methodology	146
B.4.2.0	Introduction	146
B.4.2.1	Development approach	147
B.4.2.2	Threat sources	147
B.4.2.3	Categorisation rationale	147
B.4.2.4	Limitations	147
B.4.3	Threat catalogue	147
B.4.3.1	Introduction	147
B.4.3.2	T-INTEGRITY: Boot integrity attacks	147
B.4.3.2.0	Introduction	147
B.4.3.2.1	Code execution attacks	147
B.4.3.2.2	Configuration tampering	148
B.4.3.2.3	Cryptographic compromise	148
B.4.3.2.4	Parser and input validation attacks	149
B.4.3.2.5	Rollback attacks	149
B.4.3.3	T-PERSIST: Persistent firmware threats	149
B.4.3.4	T-PHYS: Physical attacks	150
B.4.3.5	T-SUPPLY: Supply chain attacks	151
B.4.3.6	T-NET: Network-based attacks	151
B.4.3.7	T-AVAIL: Availability and resilience threats	152
B.5	Mapping of risk factors to use cases	152
B.6	Mapping of risk factors to security profiles	153
B.6.1	General	153
B.6.2	UC-IMM: LOW	153
B.6.3	UC-VER: MEDIUM	153
B.6.4	UC-HW: HIGH	153
Annex C (informative):	Product documentation	154
C.1	Introduction	154
C.2	Security design documentation	154
C.3	Physical security documentation	155
C.4	Integrity mechanism documentation	155
C.5	Configuration security documentation	155
C.6	Vulnerability handling documentation	155
C.7	Security testing evidence	155
Annex D (informative):	Relation to physical attack resistance standards	157
D.1	Purpose	157
D.1.0	Introduction	157
D.1.1	Component standards: prEN 50765 and prEN 50766	157

D.1.2	Assessment standards	157
D.2	Threat coverage in the wider landscape	157
D.3	Exploitation mitigation guidance	157
Annex E (informative): Relation to NIST SP 800-193		159
E.1	Purpose	159
E.2	Protection (NIST SP 800-193, Section 4.2)	159
E.2.1	Authenticated update mechanism (NIST SP 800-193, Section 4.2.1.1)	159
E.2.2	Integrity protection (NIST SP 800-193, Section 4.2.1.2)	159
E.2.3	Non-bypassability (NIST SP 800-193, Section 4.2.1.3)	160
E.2.4	Protection of critical data (Section 4.2.4)	160
E.3	Detection (NIST SP 800-193, Section 4.3)	160
E.3.1	Detection of corrupted code (NIST SP 800-193, Section 4.3.1)	160
E.3.2	Detection of corrupted critical data (NIST SP 800-193, Section 4.3.2)	160
E.3.3	Notification	161
E.4	Recovery (NIST SP 800-193, Section 4.4)	161
E.4.1	Recovery of mutable code (NIST SP 800-193, Section 4.4.1)	161
E.4.2	Recovery of critical data (NIST SP 800-193, Section 4.4.2)	161
E.5	Firmware categories (NIST SP 800-193)	161
Annexes F to J:Void		162
Annex K (normative): Generic cryptographic requirements and assessment		163
K.1	Cryptography	163
K.1.1	Requirement	163
K.1.2	Assessment of product cryptographic configuration	164
K.1.2.0	General	164
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms	164
K.1.2.1.1	Assessment objective	164
K.1.2.1.2	Assessment preparation	164
K.1.2.1.3	Assessment activities	164
K.1.2.1.4	Assessment evidence	165
K.1.2.1.5	Assessment verdict	165
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms	165
K.1.2.2.1	Assessment objective	165
K.1.2.2.2	Assessment preparation	165
K.1.2.2.3	Assessment activities	165
K.1.2.2.4	Assessment evidence	166
K.1.2.2.5	Assessment verdict	166
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms	166
K.1.2.3.1	Assessment objective	166
K.1.2.3.2	Assessment preparation	166
K.1.2.3.3	Assessment activities	166
K.1.2.3.4	Assessment evidence	167
K.1.2.3.5	Assessment verdict	167
K.2	Crypto agility	167
K.2.1	Requirement	167
K.2.2	Assessment of crypto-agility	168
K.2.2.1	Assessment objective	168
K.2.2.2	Assessment preparation	168
K.2.2.3	Assessment activities	169
K.2.2.4	Assessment evidence	169
K.2.2.5	Assessment verdict	169
K.3	ACM-extended cryptographic mechanisms	169
K.3.1	Requirement	169
K.3.2	List of ACM-extended cryptographic mechanisms	169

K.4	Interoperability-based cryptographic mechanisms	170
K.4.1	Requirement	170
K.4.2	List of interoperability-based cryptographic mechanisms	170
History		171

Sample Document

get full document from standards.iteh.ai

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This draft Harmonised European Standard (EN) has been produced by ETSI Technical Committee Cyber Security (CYBER), and is now submitted for the combined Public Enquiry and Vote phase of the ETSI Standardisation Request deliverable Approval Procedure (SRdAP).

The present document has been prepared under the Commission's standardisation request C(2025) 618 [i.3] final to provide one voluntary means of conforming to the 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) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (CRA) [i.1].

Once the present document is cited in the Official Journal of the European Union under that Regulation, compliance with the normative clauses of the present document given in Table A.1 confers, within the limits of the scope of the present document, a presumption of conformity with the corresponding requirements of that Regulation and associated EFTA regulations.

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document is a European harmonised standard that defines technical cybersecurity requirements for boot managers as products with digital elements according to Regulation (EU) 2024/2847 [i.1], the Cyber Resilience Act (CRA).

How to use the present document

Clause 4 describes the product context: architecture, capabilities, operational environment, and use cases. This clause is informative and contains no requirements.

Clause 4.6 defines three use cases for boot manager products (UC-IMM, UC-VER and UC-HW), each associated with a security profile (LOW, MEDIUM or HIGH).

The manufacturer declares the use case matching the product's capabilities as specified in Table 4.6.4-1.

Clause 5 contains the normative technical requirements. Requirements apply based on the declared security profile and on the functional capabilities the product implements. Clause 5.1 specifies the applicability rules.

Clause 6 defines assessment criteria for each requirement.

Annex A maps requirements in the present document to CRA essential requirements.

Annex B documents the security analysis underlying the requirements.

Annex C contains information on the product documentation.

Annex D describes the relation to physical attack resistance.

Annex E provides an informative mapping to NIST SP 800-193 [i.10]

Annex K defines generic requirements and assessment criteria for the use of state-of-the-art cryptography. This Annex is normative.

1 Scope

1.1 General

The present document specifies technical cybersecurity product requirements and corresponding assessment criteria for boot managers. The products with digital elements in scope, there after "the products":

- are specified within the technical description of the category of product number 8 by the Commission Implementing Regulation (EU) 2025/2392 [i.2] as:
 - "Software products with digital elements that manage the process of initial system startup after power on/restart by initialising hardware, loading or transferring control to the operating system environment or system resources, and selecting boot options. This category includes but is not limited to UEFI firmware, single-stage and multi-stage boot loaders."
- are only covered within the product context described in clause 4.

The scope covers software and firmware components that manage the boot process from power-on through establishment of the chain of trust to handoff to the boot target. Products in scope include boot management software and firmware regardless of distribution model or integration level. These are:

- **System firmware** that performs hardware initialisation and boot management.
- **Bootloaders** that manage boot target selection, verification, and loading.
- **Embedded boot firmware** in IoT and embedded devices.
- **Network boot implementations** enabling remote boot capabilities.
- Boot managers that **integrate with hardware security components** for chain of trust establishment.

NOTE 1: Boot managers may be single-stage (direct loading) or multi-stage (staged verification).

NOTE 2: For microcontrollers (MCUs) and microprocessors (MPUs):

- **Silicon-integrated immutable firmware:** Mask ROM, fused code, or boot firmware integrated during chip manufacturing is assessed as part of MCU/MPU hardware under semiconductor standards.
- **Updateable boot managers:** Boot software in flash storage (including OTP programmed post-manufacture) is assessed using the present document when distinctly identifiable or independently updatable.

NOTE 3: Runtime services executing after boot target handoff (such as secure monitor mode handlers or attestation services) are in scope only if they provide verification or attestation services to the boot process itself, not to the boot target.

The present document covers those products to demonstrate compliance with essential cybersecurity requirements in the Regulation (EU) 2024/2847 [i.1], Annex I Part I under the conditions identified in Annex A.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the [ETSI docbox](#).

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are necessary for the application of the present document.

- [1] [ENISA Report 1747792503](#) (version 2 - April 2025): "European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding but are not required for conformance to the present document.

- [i.1] [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).
- [i.2] [Commission Implementing Regulation \(EU\) 2025/2392](#) of 28 November 2025 on the technical description of the categories of important and critical products with digital elements pursuant to Regulation (EU) 2024/2847 of the European Parliament and of the Council.
- [i.3] [Standardisation request M/606 - C\(2025\)618](#): Commission Implementing decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support 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).
- [i.4] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Part 1-3: Vulnerability handling" (produced by CEN CENELEC).

NOTE: Version and date to be added upon its publication by CEN CENELEC.

- [i.5] prEN 40000-1-2: "Cybersecurity requirements for products with digital elements - Part 1-2: Generic Security Framework" (produced by CEN CENELEC).

NOTE: Version and date to be added upon its publication by CEN CENELEC.

- [i.6] EN 17927:2023: "Security Evaluation Standard for IoT Platforms (SESIP)".
- [i.7] prEN 50765:2026: "Cybersecurity requirements for microprocessors and microcontrollers with security-related functionalities".
- [i.8] prEN 50766:2026: "Cybersecurity requirements for tamper-resistant microprocessors and microcontrollers".
- [i.9] ISO/IEC 15408: "Common Criteria for Information Technology Security Evaluation".
- [i.10] NIST SP 800-193: "Platform Firmware Resiliency Guidelines", National Institute of Standards and Technology.
- [i.11] CAPEC™: "Common Attack Pattern Enumeration and Classification", MITRE Corporation.
- [i.12] MITRE EMB3D™: "Embedded Device Security Threat Model", MITRE Corporation.
- [i.13] CWE™: "Common Weakness Enumeration", MITRE Corporation..