



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

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-007

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	14
Foreword.....	15
Modal verbs terminology.....	15
Introduction	15
1 Scope	17
2 References	18
2.1 Normative references	18
2.2 Informative references.....	18
3 Definition of terms, symbols and abbreviations.....	20
3.1 Terms.....	20
3.2 Symbols.....	22
3.3 Abbreviations	22
4 Product context.....	23
4.1 Product Functions.....	23
4.2 Product Architecture.....	24
4.3 Operational Environment	26
4.3.1 General description.....	26
4.3.2 Hardware environment	26
4.3.3 Software environment.....	26
4.3.4 Connectivity aspects	27
4.4 Distribution of Security Functions	27
4.5 Users.....	28
4.6 Use Cases	28
4.6.1 UC-1: Local Password Manager.....	28
4.6.2 UC-2: Password Manager Application with Remote-Based Resources	29
4.6.3 UC-3: Hybrid Local and Remote-Based	30
4.6.4 UC-4: Browser Extension Password Manager.....	30
4.6.5 UC-5: Enterprise Password Manager.....	31
4.6.6 UC-6: Hardware-Based Password Manager	32
5 Technical requirements for Products.....	33
5.1 Introduction - Applicability of the requirements	33
5.2 Appropriate level of cybersecurity	37
5.2.0 Introduction.....	37
5.2.1 Normal Risk.....	38
5.2.1.0 Applicability: All UC.....	38
5.2.2 High Risk	38
5.2.3 Critical Risk	38
5.3 No known exploitable vulnerabilities.....	38
5.3.0 Introduction.....	38
5.3.1 Normal Risk.....	38
5.4 Secure by default configuration.....	38
5.4.0 Introduction.....	38
5.4.1 Normal Risk.....	38
5.5 Security updates	39
5.5.0 Introduction.....	39
5.5.1 Normal Risk.....	39
5.5.2 High Risk (none).....	40
5.5.3 Critical Risk	40
5.6 Authentication and Access Control	40
5.6.0 Introduction.....	40
5.6.1 Normal Risk.....	40
5.6.2 High Risk	40
5.6.3 Critical Risk.....	40

5.7	Confidentiality Protection	41
5.7.0	Introduction.....	41
5.7.1	Normal Risk.....	41
5.7.2	High Risk.....	41
5.7.3	Critical Risk.....	41
5.8	Integrity Protection.....	42
5.8.0	Introduction.....	42
5.8.1	Normal Risk.....	42
5.9	Data Minimisation.....	42
5.9.0	Introduction.....	42
5.9.1	Normal Risk.....	42
5.10	Availability Protection	42
5.10.0	Introduction.....	42
5.10.1	Normal Risk.....	42
5.11	Non-interference.....	42
5.11.0	Introduction.....	42
5.11.1	Normal Risk.....	42
5.12	Attack Surface Minimisation.....	43
5.12.0	Introduction.....	43
5.12.1	Normal Risk.....	43
5.12.2	High Risk (none).....	43
5.12.3	Critical Risk.....	43
5.13	Exploit Mitigation	43
5.13.0	Introduction.....	43
5.13.1	Normal Risk.....	43
5.14	Monitoring.....	43
5.14.0	Introduction.....	43
5.14.1	Normal Risk.....	43
5.14.2	High Risk (none).....	43
5.14.3	Critical Risk.....	43
5.15	Factory Reset and Data Portability.....	44
5.15.0	Introduction.....	44
5.15.1	Normal Risk.....	44
5.15.2	High Risk.....	44
5.15.3	Critical Risk.....	44
6	Assessment criteria for compliance with technical requirements	44
6.1	Introduction to the assessment and compliance criteria	44
6.2	Appropriate level of cybersecurity	46
6.2.1	Normal Risk.....	46
6.2.1.1	ACC-SD-NORM-1	46
6.2.1.1.1	Reference.....	46
6.2.1.1.2	Objective	46
6.2.1.1.3	Preparation.....	46
6.2.1.1.4	Activities	46
6.2.1.1.5	Verdict.....	46
6.2.1.1.6	Evidence	46
6.2.1.2	ACC-SD-NORM-2	46
6.2.1.2.1	Reference.....	46
6.2.1.2.2	Objective	47
6.2.1.2.3	Preparation.....	47
6.2.1.2.4	Activities	47
6.2.1.2.5	Verdict.....	47
6.2.1.2.6	Evidence	47
6.2.1.3	ACC-SD-NORM-3	47
6.2.1.3.1	Reference.....	47
6.2.1.3.2	Objective	47
6.2.1.3.3	Preparation.....	47
6.2.1.3.4	Activities	48
6.2.1.3.5	Verdict.....	48
6.2.1.3.6	Evidence	48
6.2.2	High Risk.....	48

6.2.2.1	ACC-SD-HIGH-1	48
6.2.2.1.1	Reference.....	48
6.2.2.1.2	Objective	48
6.2.2.1.3	Preparation.....	48
6.2.2.1.4	Activities	48
6.2.2.1.5	Verdict.....	48
6.2.2.1.6	Evidence.....	49
6.2.3	Critical Risk.....	49
6.2.3.1	ACC-SD-CRIT-1	49
6.2.3.1.1	Reference.....	49
6.2.3.1.2	Objective	49
6.2.3.1.3	Preparation.....	49
6.2.3.1.4	Activities	49
6.2.3.1.5	Verdict.....	49
6.2.3.1.6	Evidence	49
6.3	No known exploitable vulnerabilities.....	50
6.3.1	Normal Risk.....	50
6.3.1.1	ACC-KEV-NORM-1	50
6.3.1.1.1	Reference.....	50
6.3.1.1.2	Objective	50
6.3.1.1.3	Preparation.....	50
6.3.1.1.4	Activities	50
6.3.1.1.5	Verdict.....	50
6.3.1.1.6	Evidence	51
6.4	Secure by default configuration.....	51
6.4.1	Normal Risk.....	51
6.4.1.0	Introduction.....	51
6.4.1.1	ACC-SD-NORM-1	51
6.4.1.1.1	Reference.....	51
6.4.1.1.2	Objective	51
6.4.1.1.3	Preparation:	51
6.4.1.1.4	Activities	51
6.4.1.1.5	Verdict.....	51
6.4.1.1.6	Evidence:.....	52
6.4.1.2	ACC-SD-NORM-2	52
6.4.1.2.1	Reference: REQ-SD-NORM-2.....	52
6.4.1.2.2	Objective	52
6.4.1.2.3	Preparation.....	52
6.4.1.2.4	Activities	52
6.4.1.2.5	Verdict.....	52
6.4.1.2.6	Evidence	52
6.5	Security updates	52
6.5.1	Normal Risk.....	52
6.5.1.1	ACC-SU-NORM-1	52
6.5.1.1.1	Reference.....	52
6.5.1.1.2	Objective	52
6.5.1.1.3	Preparation.....	53
6.5.1.1.4	Activities	53
6.5.1.1.5	Verdict.....	53
6.5.1.1.6	Evidence	53
6.5.1.2	ACC-SU-NORM-2	53
6.5.1.2.1	Reference.....	53
6.5.1.2.2	Objective	53
6.5.1.2.3	Preparation.....	53
6.5.1.2.4	Activities	54
6.5.1.2.5	Verdict.....	54
6.5.1.2.6	Evidence	54
6.5.1.3	ACC-SU-NORM-3	54
6.5.1.3.1	Reference.....	54
6.5.1.3.2	Objective	54
6.5.1.3.3	Preparation.....	54
6.5.1.3.4	Activities	54

6.5.1.3.5	Verdict	54
6.5.1.3.6	Evidence	55
6.5.1.4	ACC-SU-NORM-3	55
6.5.1.4.1	Reference	55
6.5.1.4.2	Objective	55
6.5.1.4.3	Preparation	55
6.5.1.4.4	Activities	55
6.5.1.4.5	Verdict	55
6.5.1.4.6	Evidence	55
6.5.1.5	ACC-SU-NORM-4	56
6.5.1.5.1	Reference	56
6.5.1.5.2	Objective	56
6.5.1.5.3	Preparation	56
6.5.1.5.4	Activities	56
6.5.1.5.5	Verdict	56
6.5.1.5.6	Evidence	56
6.5.2	High Risk (none)	56
6.5.3	Critical Risk	56
6.5.3.1	ACC-SU-CRIT-1	56
6.5.3.1.1	Reference	56
6.5.3.1.2	Objective	57
6.5.3.1.3	Preparation	57
6.5.3.1.4	Activities	57
6.5.3.1.5	Verdict	57
6.5.3.1.6	Evidence	57
6.5.3.2	ACC-SU-CRIT-2	57
6.5.3.2.1	Reference	57
6.5.3.2.2	Objective	57
6.5.3.2.3	Preparation	57
6.5.3.2.4	Activities	58
6.5.3.2.5	Verdict	58
6.5.3.2.6	Evidence	58
6.6	Authentication and access control	58
6.6.1	Normal Risk	58
6.6.1.1	ACC-AC-NORM-1	58
6.6.1.1.1	Reference	58
6.6.1.1.2	Objective	58
6.6.1.1.3	Preparation	58
6.6.1.1.4	Activities	59
6.6.1.1.5	Verdict	59
6.6.1.1.6	Evidence	59
6.6.1.2	ACC-AC-NORM-2	59
6.6.1.2.1	Reference	59
6.6.1.2.2	Objective	59
6.6.1.2.3	Preparation	59
6.6.1.2.4	Activities	60
6.6.1.2.5	Verdict	60
6.6.1.2.6	Evidence	60
6.6.1.3	ACC-AC-NORM-3	60
6.6.1.3.1	Reference	60
6.6.1.3.2	Objective	60
6.6.1.3.3	Preparation	60
6.6.1.3.4	Activities	60
6.6.1.3.5	Verdict	61
6.6.1.3.6	Evidence	61
6.6.1.4	ACC-AC-NORM-4	61
6.6.1.4.1	Reference	61
6.6.1.4.2	Objective	61
6.6.1.4.3	Preparation	61
6.6.1.4.4	Activities	61
6.6.1.4.5	Verdict	62
6.6.1.4.6	Evidence	62

6.6.2	High Risk	62
6.6.2.1	ACC-AC-HIGH-1	62
6.6.2.1.1	Reference.....	62
6.6.2.1.2	Objective	62
6.6.2.1.3	Preparation.....	62
6.6.2.1.4	Activities	62
6.6.2.1.5	Verdict	63
6.6.2.1.6	Evidence	63
6.6.2.2	Assessment AC-HIGH-2.....	63
6.6.2.2.1	Reference.....	63
6.6.2.2.2	Objective	63
6.6.2.2.3	Preparation.....	63
6.6.2.2.4	Activities	63
6.6.2.2.5	Verdict	64
6.6.2.2.6	Evidence	64
6.6.3	Critical Risks	64
6.6.3.1	Assessment ACC-AC-CRIT-1	64
6.6.3.1.1	Reference.....	64
6.6.3.1.2	Objective	64
6.6.3.1.3	Preparation.....	64
6.6.3.1.4	Activities	65
6.6.3.1.5	Verdict	65
6.6.3.1.6	Evidence	65
6.6.3.2	Assessment ACC-AC-CRIT-2	65
6.6.3.2.1	Reference.....	65
6.6.3.2.2	Objective	65
6.6.3.2.3	Preparation.....	65
6.6.3.2.4	Activities	65
6.6.3.2.5	Verdict	66
6.6.3.2.6	Evidence	66
6.6.3.3	ACC-AC-CRIT-3.....	66
6.6.3.3.1	Reference.....	66
6.6.3.3.2	Objective	66
6.6.3.3.3	Preparation.....	66
6.6.3.3.4	Activities	66
6.6.3.3.5	Verdict	67
6.6.3.3.6	Evidence	67
6.6.3.4	ACC-AC-CRIT-4.....	67
6.6.3.4.1	Reference.....	67
6.6.3.4.2	Objective	67
6.6.3.4.3	Preparation.....	67
6.6.3.4.4	Activities	67
6.6.3.4.5	Verdict	68
6.6.3.4.6	Evidence	68
6.6.3.5	ACC-AC-CRIT-5.....	68
6.6.3.5.1	Reference.....	68
6.6.3.5.2	Objective	68
6.6.3.5.3	Preparation.....	68
6.6.3.5.4	Activities	68
6.6.3.5.5	Verdict	69
6.6.3.5.6	Evidence	69
6.6.3.6	ACC-AC-CRIT-6.....	69
6.6.3.6.1	Reference.....	69
6.6.3.6.2	Objective	69
6.6.3.6.3	Preparation.....	69
6.6.3.6.4	Activities	69
6.6.3.6.5	Verdict	70
6.6.3.6.6	Evidence	70
6.7	Confidentiality protection.....	70
6.7.1	Normal Risk.....	70
6.7.1.1	ACC-CON-NORM-1	70
6.7.1.1.1	Reference.....	70

6.7.1.1.2	Objective	70
6.7.1.1.3	Preparation.....	70
6.7.1.1.4	Activities	70
6.7.1.1.5	Verdict.....	71
6.7.1.1.6	Evidence	71
6.7.2	High Risk.....	71
6.7.2.1	ACC-CON-HIGH-1	71
6.7.2.1.1	Reference.....	71
6.7.2.1.2	Objective	71
6.7.2.1.3	Preparation.....	71
6.7.2.1.4	Activities	71
6.7.2.1.5	Verdict.....	72
6.7.2.1.6	Evidence	72
6.7.2.2	ACC-CON-HIGH-2	72
6.7.2.2.1	Reference.....	72
6.7.2.2.2	Objective	72
6.7.2.2.3	Preparation.....	72
6.7.2.2.4	Activities	72
6.7.2.2.5	Verdict.....	72
6.7.2.2.6	Evidence	73
6.7.2.3	ACC-CON-HIGH-3	73
6.7.2.3.1	Reference.....	73
6.7.2.3.2	Objective	73
6.7.2.3.3	Preparation.....	73
6.7.2.3.4	Activities	73
6.7.2.3.5	Verdict.....	73
6.7.2.3.6	Evidence	73
6.7.3	Critical Risk.....	74
6.7.3.1	ACC-CON-CRIT-1	74
6.7.3.1.1	Reference.....	74
6.7.3.1.2	Objective	74
6.7.3.1.3	Preparation.....	74
6.7.3.1.4	Activities	74
6.7.3.1.5	Verdict.....	74
6.7.3.1.6	Evidence	74
6.8	Integrity protection.....	75
6.8.1	Normal Risk.....	75
6.8.1.1	ACC-INT-HIGH-1.....	75
6.8.1.1.1	Reference.....	75
6.8.1.1.2	Objective	75
6.8.1.1.3	Preparation.....	75
6.8.1.1.4	Activities	75
6.8.1.1.5	Verdict.....	75
6.8.1.1.6	Evidence	75
6.9	Data Minimisation.....	76
6.9.1	Normal Risk.....	76
6.9.1.1	ACC-DM-NORM-1	76
6.9.1.1.1	Reference.....	76
6.9.1.1.2	Objective	76
6.9.1.1.3	Preparation.....	76
6.9.1.1.4	Activities	76
6.9.1.1.5	Verdict.....	76
6.9.1.1.6	Evidence	76
6.10	Availability protection.....	77
6.10.1	Normal Risk.....	77
6.10.1.1	ACC-AP-NORM-1	77
6.10.1.1.1	Reference.....	77
6.10.1.1.2	Objective	77
6.10.1.1.3	Preparation.....	77
6.10.1.1.4	Activities	77
6.10.1.1.5	Verdict.....	77
6.10.1.1.6	Evidence	77

6.11	Non-interference.....	78
6.11.1	Normal Risk.....	78
6.11.1.1	Assessment REQ-IM-NORM-1	78
6.11.1.1.1	Reference.....	78
6.11.1.1.2	Objective	78
6.11.1.1.3	Preparation.....	78
6.11.1.1.4	Activities	78
6.11.1.1.5	Verdict.....	78
6.11.1.1.6	Evidence	78
6.11.1.2	ACC-IM-NORM-2.....	79
6.11.1.2.1	Reference.....	79
6.11.1.2.2	Objective	79
6.11.1.2.3	Preparation.....	79
6.11.1.2.4	Activities	79
6.11.1.2.5	Verdict.....	79
6.11.1.2.6	Evidence	79
6.12	Attack surface minimisation.....	80
6.12.1	Normal Risk.....	80
6.12.1.1	ACC-MAS-NORM-1	80
6.12.1.1.1	Reference.....	80
6.12.1.1.2	Objective	80
6.12.1.1.3	Preparation.....	80
6.12.1.1.4	Activities	80
6.12.1.1.5	Verdict.....	80
6.12.1.1.6	Evidence	80
6.12.2	High Risk (none).....	81
6.12.3	Critical Risk.....	81
6.12.3.1	ACC-MAS-CRIT-1.....	81
6.12.3.1.1	Reference.....	81
6.12.3.1.2	Objective	81
6.12.3.1.3	Preparation.....	81
6.12.3.1.4	Activities	81
6.12.3.1.5	Verdict.....	81
6.12.3.1.6	Evidence	81
6.13	Exploitation Mitigation	81
6.13.1	Normal Risk.....	81
6.13.1.1	ACC-EMM-NORM-1	81
6.13.1.1.1	Reference.....	81
6.13.1.1.2	Objective	82
6.13.1.1.3	Preparation.....	82
6.13.1.1.4	Activities	82
6.13.1.1.5	Verdict.....	82
6.13.1.1.6	Evidence	82
6.14	Monitoring.....	82
6.14.1	Normal Risk.....	82
6.14.1.1	ACC-LOG-NORM-1	82
6.14.1.1.1	Reference.....	82
6.14.1.1.2	Objective	82
6.14.1.1.3	Preparation.....	83
6.14.1.1.4	Activities	83
6.14.1.1.5	Verdict.....	83
6.14.1.1.6	Evidence	83
6.14.2	High Risk (none).....	83
6.14.3	Critical Risk.....	83
6.14.3.1	ACC-LOG-CRIT-1	83
6.14.3.1.1	Reference.....	83
6.14.3.1.2	Objective	83
6.14.3.1.3	Preparation.....	83
6.14.3.1.4	Activities	84
6.14.3.1.5	Verdict.....	84
6.14.3.1.6	Evidence	84
6.14.3.2	ACC-LOG-CRIT-2	84

6.14.3.2.1	Reference.....	84
6.14.3.2.2	Objective	84
6.14.3.2.3	Preparation.....	84
6.14.3.2.4	Activities	85
6.14.3.2.5	Verdict	85
6.14.3.2.6	Evidence	85
6.15	Factory reset and data portability	85
6.15.1	Normal Risk.....	85
6.15.1.1	REQ-DRT-NORM-1.....	85
6.15.1.1.1	Reference.....	85
6.15.1.1.2	Objective	85
6.15.1.1.3	Preparation.....	85
6.15.1.1.4	Activities	85
6.15.1.1.5	Verdict	86
6.15.1.1.6	Evidence	86
6.15.2	High Risk.....	86
6.15.2.1	ACC-DRT-HIGH-1.....	86
6.15.2.1.1	Reference.....	86
6.15.2.1.2	Objective	86
6.15.2.1.3	Preparation.....	86
6.15.2.1.4	Activities	86
6.15.2.1.5	Verdict	87
6.15.2.1.6	Evidence	87
6.15.3	Critical Risk.....	87
6.15.3.1	REQ-DRT-CRIT-1 (ex IEF-REQ-5).....	87
6.15.3.1.1	Reference.....	87
6.15.3.1.2	Objective	87
6.15.3.1.3	Preparation.....	87
6.15.3.1.4	Activities	87
6.15.3.1.5	Verdict	88
6.15.3.1.6	Evidence	88

Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847 - the Cyber Resilience Act.....	89
-------------------------------	---	-----------

Annex B (informative):	Security analysis.....	92
-------------------------------	-------------------------------	-----------

B.0	Cybersecurity threat landscape, risk identification and assessment methodology	92
B.1	Assets	92
B.1.1	Data	92
B.1.1.1	Vault data.....	92
B.1.1.2	Key material.....	93
B.1.1.3	Configuration data	93
B.1.1.4	Identity and device data	93
B.1.1.5	Operational data.....	94
B.1.1.6	Transient data.....	94
B.1.2	Product functions.....	94
B.1.2.1	Vault management essential functions.....	94
B.1.2.2	Autofill and credential delivery essential functions.....	95
B.1.2.3	Authentication and access control essential functions	95
B.1.2.4	Synchronisation functions.....	95
B.1.2.5	Browser extension functions.....	95
B.1.2.6	Enterprise administration functions	96
B.1.2.7	Backup and recovery functions.....	96
B.1.2.8	Update and maintenance functions	96
B.1.2.9	Hardware-specific functions	96
B.2	Use Cases	97
B.2.1	UC-1 Local Password Manager Risk Assessment.....	97
B.2.1.1	Threat Profile.....	97
B.2.1.2	Impact Analysis	97

B.2.2	UC-2 Password Manager Application with Remote-Based Resources Risk Assessment	98
B.2.2.1	Threat Profile	98
B.2.2.2	Impact Analysis	99
B.2.3	UC-3: Hybrid Local and Remote-Based Resources Risk Assessment	99
B.2.3.1	Threat Profile	99
B.2.3.2	Impact Analysis	100
B.2.4	UC-4: Browser Extension Risk Assessment	100
B.2.4.1	Threat Profile	100
B.2.4.2	Impact Analysis	101
B.2.5	UC-5: Enterprise Password Manager Risk Assessment	101
B.2.5.1	Threat Profile	101
B.2.5.2	Impact Assessment	102
B.2.6	UC-6: Hardware-Based Password Manager Risk Assessment	102
B.2.6.1	Threat Profile	102
B.2.6.2	Impact Analysis	103

Annexes C to J: Void.....104

Annex K (normative): Generic cryptographic requirements and assessment.....105

K.1	Cryptography	105
K.1.1	Requirement	105
K.1.2	Assessment of product cryptographic configuration	106
K.1.2.0	General	106
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms	106
K.1.2.1.1	Assessment objective	106
K.1.2.1.2	Assessment preparation	106
K.1.2.1.3	Assessment activities	106
K.1.2.1.4	Assessment evidence	106
K.1.2.1.5	Assessment verdict	107
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms	107
K.1.2.2.1	Assessment objective	107
K.1.2.2.2	Assessment preparation	107
K.1.2.2.3	Assessment activities	107
K.1.2.2.4	Assessment evidence	108
K.1.2.2.5	Assessment verdict	108
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms	108
K.1.2.3.1	Assessment objective	108
K.1.2.3.2	Assessment preparation	108
K.1.2.3.3	Assessment activities	108
K.1.2.3.4	Assessment evidence	109
K.1.2.3.5	Assessment verdict	109
K.2	Crypto agility	109
K.2.1	Requirement	109
K.2.2	Assessment of crypto-agility	110
K.2.2.1	Assessment objective	110
K.2.2.2	Assessment preparation	110
K.2.2.3	Assessment activities	110
K.2.2.4	Assessment evidence	111
K.2.2.5	Assessment verdict	111
K.3	ACM-extended cryptographic mechanisms	111
K.3.1	Requirement	111
K.3.2	List of ACM-extended cryptographic mechanisms	112
K.3.2.1	Symmetric atomic primitives	112
K.3.2.1.1	Stream ciphers	112
K.3.2.1.2	Hash Functions	112
K.3.2.2	Symmetric constructions	112
K.3.2.2.1	Integrity modes: message authentication codes	112
K.3.2.2.2	Authenticated encryption	113
K.3.2.2.3	Key derivation functions	113
K.3.2.2.4	Password protection/password hashing mechanisms	113
K.3.2.3	Asymmetric atomic primitives	114

K.3.2.3.1	Discrete logarithm in elliptic curves	114
K.3.2.4	Asymmetric constructions	114
K.3.2.4.1	Asymmetric encryption scheme	114
K.3.2.4.2	Digital signature scheme	114
K.3.2.4.3	Key establishment and key encapsulation.....	114
K.3.2.5	Protocols	115
K.3.2.5.1	Password-authenticated key agreement.....	115
K.3.2.5.2	Transport and authenticated channels	115
K.3.2.6	List of cryptographic catalogues	115
K.3.3	Assessment	115
Annexes L to Q: Void		116
Annex R (normative): Remote Data Processing Solutions		117
R.1	Scope & Applicability	117
R.2	RDPS as a product-boundary extension.....	117
R.3	Threat Model	118
R.3.0	Introduction	118
R.3.1	Assets	118
R.3.2	Threat catalogue	119
R.3.3	Assets ↔ Threats mapping.....	120
R.4	Security Requirements	120
R.4.1	General and guidance for requirement-structure selection	120
R.4.2	Applicability of Annex R requirements.....	120
R.4.3	Local product side requirements	122
R.4.3.1	Data authenticity of interactions received from the RDPS side	122
R.4.3.2	Integrity of interactions received from the RDPS side	122
R.4.3.3	Confidentiality of data exchanged with the RDPS side	123
R.4.3.4	Availability	123
R.4.4	RDPS side requirements.....	124
R.4.4.1	Data authenticity of interactions received from the local product side	124
R.4.4.2	Integrity of interactions received from the local product side.....	125
R.4.4.3	Confidentiality of data exchanged with the local product side	125
R.4.4.4	Availability	126
R.4.5	Threats ↔ Requirements mapping.....	127
R.5	Conformity assessment.....	127
R.5.1	Introduction	127
R.5.1	Local product side requirements	127
R.5.1.1	Assessment case for REQ-RDPS-L-AUTH-NORM-001	127
R.5.1.2	Assessment case for REQ-RDPS-L-AUTH-HIGH-002	128
R.5.1.3	Assessment case for REQ-RDPS-L-AUTH-CRIT-003.....	129
R.5.1.4	Assessment case for REQ-RDPS-L-INTEG-NORM-001	130
R.5.1.5	Assessment case for REQ-RDPS-L-INTEG-HIGH-002	131
R.5.1.6	Assessment case for REQ-RDPS-L-INTEG-CRIT-002	131
R.5.1.7	Assessment case for REQ-RDPS-L-CONF-NORM-001.....	132
R.5.1.8	Assessment case for REQ-RDPS-L-CONF-HIGH-002.....	133
R.5.1.9	Assessment case for REQ-RDPS-L-CONF-CRIT-003	134
R.5.1.10	Assessment case for REQ-RDPS-L-AVAIL-NORM-001	135
R.5.1.11	Assessment case for REQ-RDPS-L-AVAIL-HIGH-002.....	136
R.5.1.12	Assessment case for REQ-RDPS-L-AVAIL-CRIT-003.....	136
R.5.2	RDPS side requirements.....	137
R.5.2.1	Assessment case for REQ-RDPS-R-AUTH-NORM-001	137
R.5.2.2	Assessment case for REQ-RDPS-R-AUTH-HIGH-002	138
R.5.2.3	Assessment case for REQ-RDPS-R-AUTH-CRIT-003.....	139
R.5.2.4	Assessment case for REQ-RDPS-R-INTEG-NORM-001	140
R.5.2.5	Assessment case for REQ-RDPS-R-INTEG-HIGH-002	141
R.5.2.6	Assessment case for REQ-RDPS-R-INTEG-CRIT-003	142
R.5.2.7	Assessment case for REQ-RDPS-R-CONF-NORM-001	143
R.5.2.8	Assessment case for REQ-RDPS-R-CONF-HIGH-002	143

R.5.2.9	Assessment case for REQ-RDPS-R-CONF-CRIT-003	144
R.5.2.10	Assessment case for REQ-RDPS-R-AVAIL-NORM-001.....	145
R.5.2.11	Assessment case for REQ-RDPS-R-AVAIL-HIGH-002.....	146
R.5.2.12	Assessment case for REQ-RDPS-R-AVAIL-CRIT-003.....	147
History		148

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 organisations 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 Organisational 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.

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 organisations 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 Organisational 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.

Bluetooth® is a trademark registered and owned by Bluetooth SIG, Inc.

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] to provide one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 [i.1] 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, known as the Cyber Resilience Act (CRA).

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 provides the technical cybersecurity requirements for the products in scope, following a risk-based approach in support of the Cyber Resilience Act (CRA) [i.1]. The technical cybersecurity requirements are thereby proportionate to the intended purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

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 (UCs) 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 maps the technical requirements of the present document with the essential requirements of the CRA [i.1] Regulation.

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