



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for browsers**

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-006

Keywordsbrowsers, CRA, 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 of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	15
Foreword.....	15
Modal verbs terminology.....	16
Introduction	16
1 Scope	17
2 References	17
2.1 Normative references	17
2.2 Informative references.....	17
3 Definition of terms, symbols, abbreviations and naming conventions.....	19
3.1 Terms.....	19
3.2 Symbols.....	21
3.3 Abbreviations	21
3.4 Naming conventions.....	22
4 Product context.....	22
4.1 Product Functions.....	22
4.2 Product Architecture.....	23
4.3 Operational Environment	26
4.3.1 General description.....	26
4.3.2 Physical/Hardware environment.....	27
4.3.3 Logical/Software environment.....	27
4.3.4 Connectivity aspects	27
4.4 Distribution of Security Functions	27
4.4.1 Security Functions	27
4.4.2 Decision tree	28
4.4.3 Security functions provided outside of the product's context	28
4.5 Users.....	29
4.6 Use Cases	29
5 Technical requirements for products.....	30
5.1 Introduction - Applicability of the requirements	30
5.2 Appropriate level of cybersecurity	31
5.2.0 Introduction.....	31
5.2.1 REQ-ALC-1.....	31
5.2.2 REQ-ALC-2.....	31
5.3 No known exploitable vulnerabilities.....	31
5.3.0 Introduction.....	31
5.3.1 REQ-KEV-1	31
5.3.2 REQ-MEM-KEV-1.....	32
5.3.3 REQ-MEM-KEV-2.....	32
5.3.4 REQ-MEM-KEV-3.....	32
5.4 Secure by default configuration.....	32
5.4.0 Introduction.....	32
5.4.1 REQ-TLS-SBD-1	32
5.4.2 REQ-TLS-SBD-2	33
5.4.3 REQ-EXT-SBD-1.....	33
5.4.4 REQ-EXT-SBD-2.....	33
5.4.5 REQ-PWR-SBD-1	33
5.4.6 REQ-PWR-SBD-2.....	33
5.5 Security updates	33
5.5.0 Introduction.....	33
5.5.1 REQ-SU-1.....	33
5.5.2 REQ-TLS-SU-1	34
5.5.3 REQ-EXT-SU-1	34
5.5.4 REQ-EXT-SU-2	34

5.5.5	REQ-STORE-SU-1.....	34
5.5.6	REQ-STORE-SU-2.....	34
5.6	Authentication and access control	34
5.6.0	Introduction.....	34
5.6.1	REQ-STORE-AAC-1	34
5.6.2	REQ-STORE-AAC-2	34
5.6.3	REQ-PRIV-AAC-1.....	34
5.6.4	REQ-PRIV-CON-1.....	35
5.6.5	REQ-PRIV-CON-2.....	35
5.6.6	REQ-EXT-AAC-1	35
5.6.7	REQ-EXT-AAC-2	35
5.6.8	REQ-EXT-AAC-3	35
5.6.9	REQ-EXT-AAC-4	35
5.6.10	REQ-EXT-AAC-5	35
5.6.11	REQ-SOP-AAC-2.....	36
5.6.12	REQ-PWR-AAC-1	36
5.7	Confidentiality protection.....	36
5.7.0	Introduction.....	36
5.7.1	REQ-TLS-CON-1.....	36
5.7.2	REQ-TLS-CON-2.....	36
5.7.3	REQ-TLS-CON-3.....	36
5.7.4	REQ-TLS-CON-4.....	36
5.7.5	REQ-TLS-CON-5.....	36
5.7.6	REQ-STORE-CON-1	37
5.7.7	REQ-STORE-CON-2	37
5.7.8	REQ-STORE-CON-3	37
5.7.9	REQ-SOP-CON-1.....	37
5.7.10	REQ-SOP-CON-2.....	37
5.8	Integrity protection	37
5.8.0	Introduction.....	37
5.8.1	REQ-EXT-INT-1	37
5.8.2	REQ-PWR-INT-1	38
5.8.3	REQ-PWR-INT-2	38
5.8.4	REQ-ISL-MAS-1.....	38
5.9	Data minimisation	38
5.9.0	Introduction.....	38
5.9.1	REQ-PWR-DM-1	38
5.9.2	REQ-PWR-DM-2	38
5.10	Availability protection.....	38
5.10.0	Introduction.....	38
5.10.1	REQ-EXT-AP-1	38
5.10.2	REQ-STORE-AP-1.....	39
5.11	Non-interference.....	39
5.11.0	Introduction.....	39
5.11.1	REQ-EXT-IM-1.....	39
5.11.2	REQ-EXT-IM-2.....	39
5.11.3	REQ-PWR-IM-1.....	39
5.11.4	REQ-ISL-IM-1	39
5.12	Attack surface minimisation.....	39
5.12.0	Introduction.....	39
5.12.1	REQ-MEM-MAS-1	39
5.12.2	REQ-EXT-MAS-1	40
5.12.3	REQ-EXT-MAS-2.....	40
5.12.4	REQ-EXT-MAS-3.....	40
5.12.5	REQ-SOP-MAS-1	40
5.13	Exploit mitigation.....	40
5.13.0	Introduction.....	40
5.13.1	REQ-EXT-EMM-1	40
5.13.2	REQ-EXT-EMM-2	40
5.13.3	REQ-ISL-EMM-1.....	41
5.13.4	REQ-ISL-EMM-2.....	41
5.13.5	REQ-MEM-EMM-1	41

5.13.6	REQ-MEM-EMM-2	41
5.13.7	REQ-MEM-EMM-3	41
5.14	Monitoring.....	41
5.14.0	Introduction.....	41
5.14.1	REQ-TLS-LOG-1	41
5.14.2	REQ-EXT-LOG-1	42
5.14.3	REQ-STORE-LOG-1.....	42
5.14.4	REQ-PRIV-LOG-1	42
5.15	Factory reset and data portability	42
5.15.0	Introduction.....	42
5.15.1	REQ-PWR-DRT-1	42
5.15.2	REQ-TLS-DRT-1	42
5.15.3	REQ-EXT-DRT-1.....	42
5.15.4	REQ-STORE-DRT-1.....	43
5.15.5	REQ-STORE-DRT-2.....	43
5.15.6	REQ-STORE-DRT-3.....	43
6	Assessment criteria for compliance with technical requirements	43
6.1	Introduction to the assessment and compliance criteria	43
6.2	Appropriate level of cybersecurity	45
6.2.1	ACC-ALC-1	45
6.2.1.1	Reference	45
6.2.1.2	Objective	45
6.2.1.3	Preparation	45
6.2.1.4	Activities	45
6.2.1.5	Verdict.....	45
6.2.1.6	Evidence.....	45
6.2.2	ACC-ALC-2	46
6.2.2.1	Reference	46
6.2.2.2	Objective	46
6.2.2.3	Preparation	46
6.2.2.4	Activities	46
6.2.2.5	Verdict.....	46
6.2.2.6	Evidence.....	46
6.3	No known exploitable vulnerabilities.....	47
6.3.1	ACC-KEV -1	47
6.3.1.1	Reference	47
6.3.1.2	Objective	47
6.3.1.3	Preparation	47
6.3.1.4	Activities	48
6.3.1.5	Verdict.....	48
6.3.1.6	Evidence.....	48
6.3.2	ACC-MEM-KEV-1	49
6.3.2.1	Reference	49
6.3.2.2	Objective	49
6.3.2.3	Preparation	49
6.3.2.4	Activities	49
6.3.2.5	Verdict.....	49
6.3.2.6	Evidence.....	50
6.3.3	ACC-MEM-KEV-2	50
6.3.3.1	Reference	50
6.3.3.2	Objective	50
6.3.3.3	Preparation	50
6.3.3.4	Activities	50
6.3.3.5	Verdict.....	50
6.3.3.6	Evidence.....	51
6.3.4	ACC-MEM-KEV-3	51
6.3.4.1	Reference	51
6.3.4.2	Objective	51
6.3.4.3	Preparation	51
6.3.4.4	Activities	51
6.3.4.5	Verdict.....	51

6.3.4.6	Evidence.....	52
6.4	Secure by default configuration.....	52
6.4.1	ACC-TLS-SBD-1	52
6.4.1.1	Reference	52
6.4.1.2	Objective	52
6.4.1.3	Preparation	52
6.4.1.4	Activities	52
6.4.1.5	Verdict.....	52
6.4.1.6	Evidence.....	52
6.4.2	ACC-TLS-SBD-2	52
6.4.2.1	Reference	52
6.4.2.2	Objective	53
6.4.2.3	Preparation	53
6.4.2.4	Activities	53
6.4.2.5	Verdict.....	53
6.4.2.6	Evidence.....	53
6.4.3	ACC-EXT-SBD-1.....	53
6.4.3.1	Reference	53
6.4.3.2	Objective	54
6.4.3.3	Preparation	54
6.4.3.4	Activities	54
6.4.3.5	Verdict.....	54
6.4.3.6	Evidence.....	54
6.4.4	ACC-EXT-SBD-2.....	54
6.4.4.1	Reference	54
6.4.4.2	Objective	54
6.4.4.3	Preparation	54
6.4.4.4	Activities	55
6.4.4.5	Verdict.....	55
6.4.4.6	Evidence.....	55
6.4.5	ACC-PWR-SBD-1.....	55
6.4.5.1	Reference	55
6.4.5.2	Objective	55
6.4.5.3	Preparation	55
6.4.5.4	Activities	55
6.4.5.5	Verdict.....	56
6.4.5.6	Evidence.....	56
6.4.6	ACC-PWR-SBD-2.....	56
6.4.6.1	Reference	56
6.4.6.2	Objective	56
6.4.6.3	Preparation	56
6.4.6.4	Activities	56
6.4.6.5	Verdict.....	57
6.4.6.6	Evidence.....	57
6.5	Security updates	57
6.5.1	ACC-SU-1	57
6.5.1.1	Reference	57
6.5.1.2	Objective	57
6.5.1.3	Preparation	57
6.5.1.4	Activities	57
6.5.1.5	Verdict.....	58
6.5.1.6	Evidence.....	58
6.5.2	ACC-TLS-SU-1	58
6.5.2.1	Reference	58
6.5.2.2	Objective	58
6.5.2.3	Preparation	58
6.5.2.4	Activities	58
6.5.2.5	Verdict.....	58
6.5.2.6	Evidence.....	59
6.5.3	ACC-EXT-SU-1	59
6.5.3.1	Reference	59
6.5.3.2	Objective	59

6.5.3.3	Preparation	59
6.5.3.4	Activities	59
6.5.3.5	Verdict.....	59
6.5.3.6	Evidence.....	60
6.5.4	ACC-EXT-SU-2	60
6.5.4.1	Reference	60
6.5.4.2	Objective	60
6.5.4.3	Preparation	60
6.5.4.4	Activities	60
6.5.4.5	Verdict.....	60
6.5.4.6	Evidence.....	60
6.5.5	ACC-STORE-SU-1	61
6.5.5.1	Reference	61
6.5.5.2	Objective	61
6.5.5.3	Preparation	61
6.5.5.4	Activities	61
6.5.5.5	Verdict.....	61
6.5.5.6	Evidence.....	61
6.5.6	ACC-STORE-SU-2	61
6.5.6.1	Reference	61
6.5.6.2	Objective	61
6.5.6.3	Preparation	62
6.5.6.4	Activities	62
6.5.6.5	Verdict.....	62
6.5.6.6	Evidence.....	62
6.6	Authentication and access control	62
6.6.1	ACC-STORE-AAC-1	62
6.6.1.1	Reference	62
6.6.1.2	Objective	63
6.6.1.3	Preparation	63
6.6.1.4	Activities	63
6.6.1.5	Verdict.....	63
6.6.1.6	Evidence.....	63
6.6.2	ACC-STORE-AAC-2	63
6.6.2.1	Reference	63
6.6.2.2	Objective	64
6.6.2.3	Preparation	64
6.6.2.4	Activities	64
6.6.2.5	Verdict.....	64
6.6.2.6	Evidence.....	64
6.6.3	ACC-PRIV-AAC-1.....	64
6.6.3.1	Reference	64
6.6.3.2	Objective	64
6.6.3.3	Preparation	64
6.6.3.4	Activities	65
6.6.3.5	Verdict.....	65
6.6.3.6	Evidence.....	65
6.6.4	ACC-PRIV-CON-1.....	65
6.6.4.1	Reference	65
6.6.4.2	Objective	65
6.6.4.3	Preparation	65
6.6.4.4	Activities	66
6.6.4.5	Verdict.....	66
6.6.4.6	Evidence.....	66
6.6.5	ACC-PRIV-CON-2.....	66
6.6.5.1	Reference	66
6.6.5.2	Objective	67
6.6.5.3	Preparation	67
6.6.5.4	Activities	67
6.6.5.5	Verdict.....	67
6.6.5.6	Evidence.....	67
6.6.6	ACC-EXT-AAC-1	67

6.6.6.1	Reference	67
6.6.6.2	Objective	67
6.6.6.3	Preparation	67
6.6.6.4	Activities	68
6.6.6.5	Verdict.....	68
6.6.6.6	Evidence.....	68
6.6.7	ACC-EXT-AAC-2	68
6.6.7.1	Reference	68
6.6.7.2	Objective	68
6.6.7.3	Preparation	68
6.6.7.4	Activities	68
6.6.7.5	Verdict.....	69
6.6.7.6	Evidence.....	69
6.6.8	ACC-EXT-AAC-3	69
6.6.8.1	Reference	69
6.6.8.2	Objective	69
6.6.8.3	Preparation	69
6.6.8.4	Activities	69
6.6.8.5	Verdict.....	70
6.6.8.6	Evidence.....	70
6.6.9	ACC-EXT-AAC-4	70
6.6.9.1	Reference	70
6.6.9.2	Objective	70
6.6.9.3	Preparation	70
6.6.9.4	Activities	71
6.6.9.5	Verdict.....	71
6.6.9.6	Evidence.....	71
6.6.10	ACC-EXT-AAC-5	71
6.6.10.1	Reference	71
6.6.10.2	Objective	71
6.6.10.3	Preparation	71
6.6.10.4	Activities	72
6.6.10.5	Verdict.....	72
6.6.10.6	Evidence.....	72
6.6.11	ACC-SOP-ACC-2.....	72
6.6.11.1	Reference	72
6.6.11.2	Objective	72
6.6.11.3	Preparation	72
6.6.11.4	Activities	73
6.6.11.5	Verdict.....	73
6.6.11.6	Evidence.....	73
6.6.12	ACC-PWR-AAC-1	73
6.6.12.1	Reference	73
6.6.12.2	Objective	73
6.6.12.3	Preparation	74
6.6.12.4	Activities	74
6.6.12.5	Verdict.....	74
6.6.12.6	Evidence.....	74
6.7	Confidentiality protection.....	74
6.7.1	ACC-TLS-CON-1.....	74
6.7.1.1	Reference	74
6.7.1.2	Objective	74
6.7.1.3	Preparation	75
6.7.1.4	Activities	75
6.7.1.5	Verdict.....	75
6.7.1.6	Evidence.....	75
6.7.2	ACC-TLS-CON-2.....	75
6.7.2.1	Reference	75
6.7.2.2	Objective	75
6.7.2.3	Preparation	75
6.7.2.4	Activities	76
6.7.2.5	Verdict.....	76

6.7.2.6	Evidence.....	76
6.7.3	ACC-TLS-CON-3.....	76
6.7.3.1	Reference	76
6.7.3.2	Objective	76
6.7.3.3	Preparation	76
6.7.3.4	Activities	77
6.7.3.5	Verdict.....	77
6.7.3.6	Evidence.....	77
6.7.4	ACC-TLS-CON-4.....	77
6.7.4.1	Reference	77
6.7.4.2	Objective	77
6.7.4.3	Preparation	77
6.7.4.4	Activities	77
6.7.4.5	Verdict.....	77
6.7.4.6	Evidence.....	78
6.7.5	ACC-TLS-CON-5.....	78
6.7.5.1	Reference	78
6.7.5.2	Objective	78
6.7.5.3	Preparation	78
6.7.5.4	Activities	78
6.7.5.5	Verdict.....	78
6.7.5.6	Evidence.....	78
6.7.6	ACC-STORE-CON-1	78
6.7.6.1	Reference	78
6.7.6.2	Objective	79
6.7.6.3	Preparation	79
6.7.6.4	Activities	79
6.7.6.5	Verdict.....	79
6.7.6.6	Evidence.....	79
6.7.7	ACC-STORE-CON-2	80
6.7.7.1	Reference	80
6.7.7.2	Objective	80
6.7.7.3	Preparation	80
6.7.7.4	Activities	80
6.7.7.5	Verdict.....	80
6.7.7.6	Evidence.....	80
6.7.8	ACC-STORE-CON-3	80
6.7.8.1	Reference	80
6.7.8.2	Objective	81
6.7.8.3	Preparation	81
6.7.8.4	Activities	81
6.7.8.5	Verdict.....	81
6.7.8.6	Evidence.....	81
6.7.9	ACC-SOP-CON-1	82
6.7.9.1	Reference	82
6.7.9.2	Objective	82
6.7.9.3	Preparation	82
6.7.9.4	Activities	82
6.7.9.5	Verdict.....	82
6.7.9.6	Evidence.....	82
6.7.10	ACC-SOP-CON-2	83
6.7.10.1	Reference	83
6.7.10.2	Objective	83
6.7.10.3	Preparation	83
6.7.10.4	Activities	83
6.7.10.5	Verdict.....	83
6.7.10.6	Evidence.....	84
6.8	Integrity protection.....	84
6.8.1	ACC-EXT-INT-1.....	84
6.8.1.1	Reference	84
6.8.1.2	Objective	84
6.8.1.3	Preparation	84

6.8.1.4	Activities	84
6.8.1.5	Verdict.....	84
6.8.1.6	Evidence.....	84
6.8.2	ACC-PWR-INT-1	85
6.8.2.1	Reference	85
6.8.2.2	Objective	85
6.8.2.3	Preparation	85
6.8.2.4	Activities	85
6.8.2.5	Verdict.....	85
6.8.2.6	Evidence.....	85
6.8.3	ACC-PWR-INT-2	85
6.8.3.1	Reference	85
6.8.3.2	Objective	86
6.8.3.3	Preparation	86
6.8.3.4	Activities	86
6.8.3.5	Verdict.....	86
6.8.3.6	Evidence.....	86
6.8.4	ACC-ISL-MAS-1	86
6.8.4.1	Reference	86
6.8.4.2	Objective	86
6.8.4.3	Preparation	86
6.8.4.4	Activities	87
6.8.4.5	Verdict.....	87
6.8.4.6	Evidence.....	87
6.9	Data minimisation	87
6.9.1	ACC-PWR-DM-1	87
6.9.1.1	Reference	87
6.9.1.2	Objective	87
6.9.1.3	Preparation	87
6.9.1.4	Activities	88
6.9.1.5	Verdict.....	88
6.9.1.6	Evidence.....	88
6.9.2	ACC-PWR-DM-2	88
6.9.2.1	Reference	88
6.9.2.2	Objective	88
6.9.2.3	Preparation	88
6.9.2.4	Activities	89
6.9.2.5	Verdict.....	89
6.9.2.6	Evidence.....	89
6.10	Availability protection.....	89
6.10.1	ACC-EXT-AP-1	89
6.10.1.1	Reference	89
6.10.1.2	Objective	89
6.10.1.3	Preparation	89
6.10.1.4	Activities	90
6.10.1.5	Verdict.....	90
6.10.1.6	Evidence.....	90
6.10.2	ACC-STORE-AP-1	90
6.10.2.1	Reference	90
6.10.2.2	Objective	90
6.10.2.3	Preparation	90
6.10.2.4	Activities	90
6.10.2.5	Verdict.....	91
6.10.2.6	Evidence.....	91
6.11	Non-interference.....	91
6.11.1	ACC-EXT-IM-1	91
6.11.1.1	Reference	91
6.11.1.2	Objective	91
6.11.1.3	Preparation	91
6.11.1.4	Activities	91
6.11.1.5	Verdict.....	91
6.11.1.6	Evidence.....	92

6.11.2	ACC-EXT-IM-2	92
6.11.2.1	Reference	92
6.11.2.2	Objective	92
6.11.2.3	Preparation	92
6.11.2.4	Activities	92
6.11.2.5	Verdict.....	92
6.11.2.6	Evidence.....	92
6.11.3	ACC-PWR-IM-1.....	93
6.11.3.1	Reference	93
6.11.3.2	Objective	93
6.11.3.3	Preparation	93
6.11.3.4	Activities	93
6.11.3.5	Verdict.....	93
6.11.3.6	Evidence.....	93
6.11.4	ACC-ISL-IM-1	93
6.11.4.1	Assessment.....	93
6.11.4.2	Objective	94
6.11.4.3	Preparation	94
6.11.4.4	Activities	94
6.11.4.5	Verdict.....	94
6.11.4.6	Evidence.....	94
6.12	Attack surface minimisation.....	94
6.12.1	ACC-MEM-MAS-1	94
6.12.1.1	Reference	94
6.12.1.2	Objective	95
6.12.1.3	Preparation	95
6.12.1.4	Activities	95
6.12.1.5	Verdict.....	95
6.12.1.6	Evidence.....	95
6.12.2	ACC-EXT-MAS-1.....	96
6.12.2.1	Reference	96
6.12.2.2	Objective	96
6.12.2.3	Preparation	96
6.12.2.4	Activities	96
6.12.2.5	Verdict.....	96
6.12.2.6	Evidence.....	96
6.12.3	ACC-EXT-MAS-2.....	97
6.12.3.1	Reference	97
6.12.3.2	Objective	97
6.12.3.3	Preparation	97
6.12.3.4	Activities	97
6.12.3.5	Verdict.....	97
6.12.3.6	Evidence.....	97
6.12.4	ACC-EXT-MAS-3.....	98
6.12.4.1	Reference	98
6.12.4.2	Objective	98
6.12.4.3	Preparation	98
6.12.4.4	Activities	98
6.12.4.5	Verdict.....	98
6.12.4.6	Evidence.....	98
6.12.5	ACC-SOP-MAS-1	98
6.12.5.1	Assessment.....	98
6.12.5.2	Objective	99
6.12.5.3	Preparation	99
6.12.5.4	Activities	99
6.12.5.5	Verdict.....	99
6.12.5.6	Evidence.....	99
6.13	Exploit mitigation.....	99
6.13.1	ACC-EXT-EMM-1.....	99
6.13.1.1	Reference	99
6.13.1.2	Objective	100
6.13.1.3	Preparation	100

6.13.1.4	Activities	100
6.13.1.5	Verdict.....	100
6.13.1.6	Evidence.....	100
6.13.2	ACC-EXT-EMM-2.....	100
6.13.2.1	Reference	100
6.13.2.2	Objective	100
6.13.2.3	Preparation	100
6.13.2.4	Activities	101
6.13.2.5	Verdict.....	101
6.13.2.6	Evidence.....	101
6.13.3	ACC-ISL-EMM-1.....	101
6.13.3.1	Assessment.....	101
6.13.3.2	Objective	101
6.13.3.3	Preparation	101
6.13.3.4	Activities	102
6.13.3.5	Verdict.....	102
6.13.3.6	Evidence.....	102
6.13.4	ACC-ISL-EMM-2.....	102
6.13.4.1	Assessment.....	102
6.13.4.2	Objective	102
6.13.4.3	Preparation	102
6.13.4.4	Activities	102
6.13.4.5	Verdict.....	103
6.13.4.6	Evidence.....	103
6.13.5	ACC-MEM-EMM-1	103
6.13.5.1	Reference	103
6.13.5.2	Objective	103
6.13.5.3	Preparation	103
6.13.5.4	Activities	103
6.13.5.5	Verdict.....	103
6.13.5.6	Evidence.....	104
6.13.6	ACC-MEM-EMM-2	104
6.13.6.1	Reference	104
6.13.6.2	Objective	104
6.13.6.3	Preparation	104
6.13.6.4	Activities	104
6.13.6.5	Verdict.....	104
6.13.6.6	Evidence.....	104
6.13.7	ACC-MEM-EMM-3	105
6.13.7.1	Reference	105
6.13.7.2	Objective	105
6.13.7.3	Preparation	105
6.13.7.4	Activities	105
6.13.7.5	Verdict.....	105
6.13.7.6	Evidence.....	105
6.14	Monitoring.....	106
6.14.1	ACC-TLS-LOG-1	106
6.14.1.1	Reference	106
6.14.1.2	Objective	106
6.14.1.3	Preparation	106
6.14.1.4	Activities	106
6.14.1.5	Verdict.....	106
6.14.1.6	Evidence.....	106
6.14.2	ACC-EXT-LOG-1	106
6.14.2.1	Reference	106
6.14.2.2	Objective	106
6.14.2.3	Preparation	106
6.14.2.4	Activities	107
6.14.2.5	Verdict.....	107
6.14.2.6	Evidence.....	107
6.14.3	ACC-STORE-LOG-1	107
6.14.3.1	Reference	107

6.14.3.2	Objective	107
6.14.3.3	Preparation	107
6.14.3.4	Activities	108
6.14.3.5	Verdict.....	108
6.14.3.6	Evidence.....	108
6.14.4	ACC-PRIV-LOG-1	108
6.14.4.1	Reference	108
6.14.4.2	Objective	108
6.14.4.3	Preparation	108
6.14.4.4	Activities	108
6.14.4.5	Verdict.....	109
6.14.4.6	Evidence.....	109
6.15	Factory reset and data portability	109
6.15.1	ACC-PWR-DRT-1	109
6.15.1.1	Reference	109
6.15.1.2	Objective	109
6.15.1.3	Preparation	109
6.15.1.4	Activities	109
6.15.1.5	Verdict.....	109
6.15.1.6	Evidence.....	110
6.15.2	ACC-TLS-DRT-1	110
6.15.2.1	Reference	110
6.15.2.2	Objective	110
6.15.2.3	Preparation	110
6.15.2.4	Activities	110
6.15.2.5	Verdict.....	110
6.15.2.6	Evidence.....	110
6.15.3	ACC-EXT-DRT-1	111
6.15.3.1	Reference	111
6.15.3.2	Objective	111
6.15.3.3	Preparation	111
6.15.3.4	Activities	111
6.15.3.5	Verdict.....	111
6.15.3.6	Evidence.....	111
6.15.4	ACC-STORE-DRT-1.....	111
6.15.4.1	Reference	111
6.15.4.2	Objective	112
6.15.4.3	Preparation	112
6.15.4.4	Activities	112
6.15.4.5	Verdict.....	112
6.15.4.6	Evidence.....	112
6.15.5	ACC-STORE-DRT-2.....	113
6.15.5.1	Assessment.....	113
6.15.5.2	Objective	113
6.15.5.3	Preparation	113
6.15.5.4	Activities	113
6.15.5.5	Verdict.....	113
6.15.5.6	Evidence.....	113
6.15.6	ACC-STORE-DRT-3.....	113
6.15.6.1	Reference	113
6.15.6.2	Objective	114
6.15.6.3	Preparation	114
6.15.6.4	Activities	114
6.15.6.5	Verdict.....	114
6.15.6.6	Evidence.....	114
Annex A (informative):	Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847.....	115
Annex B (informative):	Security analysis.....	118
Annex C to F: Void		133

Annex G (informative):	Guidelines on the implementation of the present document.....	134
G.1	Applicability hooks	134
G.1.1	General	134
G.1.2	The applicability set	134
G.2	Guidance for derivative browsers.....	134
G.2.1	General	134
G.2.2	Inherited and modified security properties	135
G.2.3	Reuse of upstream evidence	135
G.2.4	Relationship to conformity assessment	135
Annexes H to J:	Void	136
Annex K (normative):	Generic cryptographic requirements and assessment.....	137
K.1	Cryptography.....	137
K.1.1	Requirement	137
K.1.2	Assessment of product cryptographic configuration	138
K.1.2.0	General.....	138
K.1.2.1	Assessment of ACM-listed cryptographic mechanisms.....	139
K.1.2.1.1	Assessment objective	139
K.1.2.1.2	Assessment preparation.....	139
K.1.2.1.3	Assessment activities	139
K.1.2.1.4	Assessment evidence.....	139
K.1.2.1.5	Assessment verdict.....	139
K.1.2.2	Assessment of ACM-extended cryptographic mechanisms	139
K.1.2.2.1	Assessment objective	139
K.1.2.2.2	Assessment preparation.....	140
K.1.2.2.3	Assessment activities	140
K.1.2.2.4	Assessment evidence.....	140
K.1.2.2.5	Assessment verdict.....	140
K.1.2.3	Assessment of interoperability-based cryptographic mechanisms.....	141
K.1.2.3.1	Void.....	141
K.1.2.4	Assessment of pilot cryptographic mechanisms	141
K.1.2.4.1	Assessment objective	141
K.1.2.4.2	Assessment preparation.....	141
K.1.2.4.3	Assessment activities	141
K.1.2.4.4	Assessment evidence.....	141
K.1.2.4.5	Assessment verdict.....	142
K.2	Crypto agility.....	142
K.2.1	Requirement	142
K.2.2	Assessment of crypto-agility	143
K.2.2.1	Assessment objective.....	143
K.2.2.2	Assessment preparation	143
K.2.2.3	Assessment activities	143
K.2.2.4	Assessment evidence	143
K.2.2.5	Assessment verdict	144
K.3	ACM-extended cryptographic mechanisms	144
K.3.1	Requirement	144
K.3.2	List of ACM-extended cryptographic mechanisms.....	144
K.3.3	Assessment.....	145
Annex L (informative):	Bibliography.....	146
Annex M (informative):	Change history	147
History		148

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) 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 final [i.3] 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) 168/2013 and (EU) 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