



Cybersecurity (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for web browsers (release 5)

Exercising one of the **Principles of International Standardization – Openness** – and taking them to a different level, ETSI CYBER-EUSR has conducted open consultations on the vertical standards in support of the Cyber-Resilience Act, at a much earlier stage than it is usual in the standardization world. In this context, please keep in mind that the present document is an INTERIM draft, which expectably will be subject to substantial changes before their target publication date in the second semester of 2026.

ETSI CRA vertical standards v1.1.1 are being finalized and undergoing Public Enquiry via the National Standardization Organizations (NSO). Therefore, starting from 16 April 2026, ETSI CYBER-EUSR may only be able to address your comments in a future revision of the standard. **To enable ETSI CYBER-EUSR to address your comments before the first publication of the standards, you should cumulatively submit to your NSO any comments submitted here from 16 April 2026 onwards.** If you don't know how to do this, email us at cybersupport@etsi.org and we will guide you in the process.

Disclaimer: The INTERIM DRAFTS available for download in this page are provided for information and are for future development work within the ETSI Technical Committee CYBER EUSR Working Group (CYBER-EUSR) only. ETSI and its Members accept no liability for any further use/implementation of these specifications. Approved and published specifications and reports shall be obtained exclusively via the ETSI Documentation Service at <http://www.etsi.org/standards-search>

Commenting guidelines: Your comments to improve this early draft are very welcomed. To ensure the effectiveness of your contribution, please make sure to include the following elements in your comment:

1. Clear identification of the section of the draft your comment is referring to.
2. Objective proposal to delete content, add content or substitute content.
3. Concrete contribution (exact content you suggest including in the draft as an addition to, or in substitution of, existing content).
4. Brief rationale to justify the proposal (e.g. why the suggested content should be added an/or the existing content should be deleted or substituted).

Please note that comments without concrete contributions will be noted but not acted upon by ETSI CYBER-EUSR. We trust and value your expertise and therefore expect you to take this opportunity to proactively contribute to solving the issues you find while analysing this early draft.

Use of Artificial Intelligence (AI): Please do not use large language models to generate your comments. Inclusion of language generated by “AI” creates a potential for intellectual property conflicts and liability for ETSI, which is not acceptable.

How to comment: To comment or provide feedback on the present interim draft please visit: [STAN4CRA / EN 304 631 Smart home assistants · GitLab](#) and submit your comments as “issues” following the guidelines provided on this site. Alternatively, you may also send your comments to: cybersupport@etsi.org using the “[ETSI Commenting Format for Open Consultation.xlsx](#)” available in <https://docbox.etsi.org/CYBER/EUSR/Open>

Feedback on your comments: The resolutions made in **Consensus** by ETSI CYBER-EUSR members, on each comment received through these Open Consultations will be published at the ETSI Open Area and ETSI Lab, assuring full **Transparency**.

Reference

< WI-0000 >

Keywords

< CRA >

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.

0

1 **Contents**

2	Intellectual Property Rights	5
3	Foreword.....	5
4	Modal verbs terminology	6
5	Executive summary	6
6	Introduction	6
7	1 Scope	7
8	2 References	7
9	2.1 Normative references	7
10	2.2 Informative references	8
11	3 Definition of terms, symbols and abbreviations.....	8
12	3.1 Terms	8
13	3.2 Symbols	8
14	3.3 Abbreviations.....	9
15	4. Product context.....	9
16	4.0 Introduction.....	10
17	4.1 Product Functions	10
18	4.2 Product Architecture.....	10
19	4.3 Operational Environment.....	10
20	4.3.1 General description	10
21	4.3.2 Physical/Hardware environment	11
22	4.3.3 Logical/Software environment.....	11
23	4.3.4 Connectivity aspects.....	11
24	4.4 Distribution of Security Functions.....	11
25	4.4.1 Security functions provided outside the product.....	11
26	4.4.2 Security functions provided to other components	11
27	4.5 Users	11
28	4.6.1 Standalone browser use cases.....	12
29	4.6.2 Embedded browser use cases	12
30	5.1 Introduction - Applicability of the requirements	13
31	5.2 No known exploitable vulnerabilities	13
32	5.3 Secure by default configuration	13
33	5.4 Secure Updates	13
34	5.5 Authentication and access control	13
35	5.6 Confidentiality	14
36	5.7 Integrity	14
37	5.8 Data Minimisation	14
38	5.9 Availability Protection	14
39	5.10 Impact Minimisation.....	14
40	5.11 Minimisation of Attack Surfaces	15
41	5.12 Exploitation Mitigation Mechanisms.....	15
42	5.13 Logging and Monitoring.....	15
43	5.14 Data Removal and Transparency	15
44	5.15 Vulnerability Handling	15
45	6. Assessment criteria for compliance with technical requirements.....	15
46	6.1 Introduction to the assessment and compliance criteria.....	16
47	6.2 No known exploitable vulnerabilities	17
48	6.3 Secure by design.....	17
49	6.4 Secure Updates	17
50	6.5 Authentication and Access Control.....	17
51	6.6 Confidentiality	18
52	6.7 Integrity	18

53	6.8	Data Minimisation	18
54	6.9	Availability Protection	18
55	6.10	Impact Minimisation	18
56	6.11	Minimisation of Attack Surfaces	18
57	6.12	Exploitation Mitigation Mechanisms	18
58	6.13	Logging and Monitoring	18
59	6.14	Data Removal and Transparency	18
60	6.15	Vulnerability Handling	18
61	Annex A (informative): Relationship between the present document and the requirements of EU		
62	Regulation (EU) 2024/2847 - the Cyber Resilience Act		19
63	Annex B (informative): Cybersecurity threat landscape, risk identification and assessment methodology		25
64	Annex C (informative): Relationship between the present document and any related ETSI standards (if		
65	any, e.g. EN 303 645)		26
66	C.1	First clause of the annex	26
67	C.1.1	First subdivided clause of the annex	26
68	Annex <D...J> (informative):		26
69	Annex G: Guidelines on the implementation of the present document (informative):		27
70	Annex K (normative): Generic requirements and assessment criteria for the use of state of the art		
71	cryptography V 0.51 (2025-02-16)		28
72	K.1	State of the Art Cryptography (SOTA)	28
73	K.1.1	Requirement	28
74	K.1.2	Assessment criteria	28
75	K.1.2.1	Assessment objective:	28
76	K.1.2.2	Assessment preparation:	28
77	K.1.2.3	Assessment activities:	28
78	K.1.2.4	Supporting Evidence:	28
79	K.1.2.5	Assignment of verdict:	28
80	K.1.2.2	Additional conditional assessment:	29
81	K1.2.2.1	Assessment objective	29
82	K.1.2.2.2	Assessment preparation:	29
83	K.1.2.2.3	Assessment activities:	29
84	K.1.2.4	Supporting Evidence:	29
85	K.1.2.5	Assignment of verdict:	29
86	K.2	Requirement ("crypto agility")	29
87	K.2.1	Assessment criteria	30
88	K.2.1.1	Assessment objective:	30
89	K.2.1.2	Assessment preparation:	30
90	K.2.1.3	Assessment activities:	30
91	K.2.1.4	Supporting Evidence:	30
92	K.2.1.5	Assignment of verdict:	30
93	Annex O (informative): Products not handled by this document		31
94	O.1:	Products which are not web browsers	31
95	O.2:	Products with unhandled risks	31
96	Annex V (informative): Guide for derivative web browsers		32
97	V.1	General	32
98	V.2	Applying Voluntary Security Attestations	32
99	V.3	Applying vulnerability handling requirements	32
100	History		33
101			
102			

103 Intellectual Property Rights

104 Essential patents

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

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

114 Trademarks

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

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

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

127 Foreword

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

131 The present document has been prepared under the Commission's standardisation request C(2025)618 [i.3] to provide
 132 one voluntary means of conforming to the requirements of Regulation (EU) 2024/2847 [i.1] of the European Parliament
 133 and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and
 134 amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828, known as the Cyber
 135 Resilience Act (CRA).

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

140 *Transposition table*

141 *The Harmonised Standard shall have appropriate transposition periods specified. A Harmonised Standard confers*
 142 *presumption of conformity when it has been published in the Official Journal of the European Union (OJEU) and*
 143 *transposed by a member state.*

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

144

145 Modal verbs terminology

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

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

150 Executive summary

151 *"Executive summary" clause should be deleted if not necessary.*

152 Introduction

153 *"Introduction" clause should introduce the structure of the document and explain how the standard should be used.*

154 *More text to be added here.*

155

1 Scope

The present document specifies technical requirements and corresponding assessment criteria for web browsers related to cybersecurity. The products with digital elements in scope, thereafter "the products" are specified within the "technical description" of the "category of product" number "2". by the 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.2], which is as follows:

Software products with digital elements that enable end users to access, render, and interact with web content and services hosted on servers that are connected to networks such as the Internet. They typically include a browser engine for interpreting and displaying content written in markup language (e.g. HTML), support for web protocols (e.g. HTTP, HTTPS), the ability to execute scripts and manage user inputs as well as storage of temporary or persistent data from websites (cookies).

This category includes but is not limited to standalone applications that fulfil the functions of browsers, embedded browsers intended for integration into another system or application as well as browsers with AI agent integration.

The products are only covered within the product context described in clause 4. The present document specifies technical characteristics and methods of assessment for:

- **Standalone web browsers:** standalone applications that fulfill the functions of web browsers
- **Embedded web browsers:** reusable software components which act as a web browser integrated into a larger application

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

2 References

2.1 Normative references

Editor's Note: **In Harmonised Standards these references shall be specific** (identified by date of publication and/or edition number or version number) **publicly available and in English**, except in exceptional circumstances making sure that impacts have been evaluated and explanations have been given on how any negative implications should be avoided**. See clauses 2.10.1 and 8.4 of the [EDRs](#).

Editor's Note: **Legal acts can never be used as 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: "[European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms](#) - version 2 - April 2025
- [2] prEN 40000-1-3: "Cybersecurity requirements for products with digital elements - Vulnerability Handling" [Version and date to be added upon its publication by CEN CENELEC]

Editor's Note: The EC has confirmed that the horizontal standard on vulnerability handling should be the **ONLY** horizontal standard to be referenced normatively in verticals.

201 [3] <Standard Organization acronym> <document number> (<version number>): "<Title>".

202 2.2 Informative references

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

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

208 The following referenced documents are not necessary for the application of the present document but they assist the
 209 user with regard to a particular subject area.

210 [i.1] [Regulation \(EU\) 2024/2847](#) of the European Parliament and of the Council of 23 October 2024 on
 211 horizontal cybersecurity requirements for products with digital elements and amending
 212 Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber
 213 Resilience Act).

214 [i.2] [Commission Implementing Regulation \(EU\) 2025/2392](#) of 28 November 2025 on the technical
 215 description of the categories of important and critical products with digital elements pursuant to
 216 Regulation (EU) 2024/2847 of the European Parliament and of the Council.

217 [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025
 218 on a standardisation request to the European Committee for Standardisation (CEN), the European
 219 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications
 220 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)
 221 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal
 222 cybersecurity requirements for products with digital elements and amending Regulations (EU) No
 223 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".

224 [i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary"
 225 [Version and date to be added upon its publication by CEN CENELEC]

226 [i.5] [Web Platform Design Principles](#), World Wide Web Consortium Group Note, 27 January 2026

227 [i.6] [RFC 5246: TLS 1.2](#), IETF, August 2008

228 [i.7] [RFC 8446: TLS 1.3](#), IETF, August 2018

229 [i.8] [RFC 6979: HSTS](#), IETF, November 2012

230 [i.9] [Mixed Content \(W3C Candidate Recommendation Draft\)](#), W3C, 23 February 2023

231 [i.n] <Standard Organization acronym> <document number> (<version number>): "<Title>".

232 Editor's Note: The EC advises that the references between verticals should be informative.

233 3 Definition of terms, symbols and abbreviations

234 3.1 Terms

235 For the purposes of the present document, the terms given in Regulation (EU) 2024/2847 [i.1], CEN/CLC
 236 JT013095:2026 (CEN/CLC prEN 4000011) [i.4] and the following apply:

237 Editor's Note: A definition of term should be such that it can replace the term in context. Any additional information
 238 shall be given only in the form of examples or notes. (see ETSI Directives (see section EDRs, clause 2.11.1)).

239 Editor's Note: Proposal to put together a common term sheet for all verticals developed in CYBER-EUSR.

240 3.2 Symbols

241 For the purposes of the present document, the [following] symbols [given in ... and the following] apply:

242 3.3 Abbreviations

243 For the purposes of the present document, the [following] abbreviations [given in ... and the following] apply:

244 **Editor's Note: The following is a list of abbreviations used in some of the CRA vertical standards. It is not complete yet.**

245 **Editor's Note: Please only keep the abbreviations that are used in the present document and avoid using the same**
 246 **abbreviation with different meaning in the CRA vertical standards.**

247	ACM	ENISA Agreed Cryptographic Methods
248	APT	Advanced persistent threats
249	C2	Command and Control
250	CC	Common Criteria
251	CPU	Central Processing Unit
252	CRA	Cyber Resilience Act
253	CVE	Common Vulnerabilities and Exposures
254	DB	Database
255	EDR	Endpoint Detection and Response
256	DHCP	Dynamic Host Configuration Protocol
257	GDPR	General Data Protection Regulation
258	GUI	Graphical User Interface
259	HSM	Hardware Security Module
260	HSTS	HTTP Strict Transport Security
261	HTTP	Hypertext Transport Protocol
262	IAM	Identity and Access Management
263	ICMP	Internet Control Message Protocol
264	ICT	Information and Communication Technology
265	IoT	Internet of Things
266	ISO	International Organization for Standardization
267	MITM	Man-In-The-Middle
268	MP	Main Product
269	MTTD	Mean Time to Detect
270	MTTR	Mean Time to Respond
271	NIST	National Institute of Standards and Technology
272	OS	Operating System
273	OT	Operational Technology
274	PC	Personal Computer
275	PIA	Privacy Impact Assessments
276	PII	Personally Identifiable Information
277	PoLP	Principle of Least Privilege
278	RDPS	Remote Data Processing Solution
279	RTO	Recovery Time Objective
280	SBOM	Software Bill of Materials
281	SCC	Security Category Classes
282	SDK	Software Development Kit
283	SIEM	Security Information and Event Management
284	SIF	Social Interactive Function
285	SOAR	Security Orchestration Automation and Response
286	TLS	Transport Layer Security
287	TUF	The Update Framework
288	UC	Use Case
289	UI	User Interface
290	XDR	Extended Detection and Response

291 4. Product context

292 **Editor's Note: This clause is not normative.**

293 4.0 Introduction

294 4.1 Product Functions

295 The intended purpose of standalone and embedded web browsers is to access and interact with the shared World Wide
296 Web. This access includes everything from reading the news and online encyclopedias to accessing critical systems
297 related to finance, government, healthcare, etc.

298 Browsers are general purpose software: When presented with a web browser, including an embedded one, user
299 expectations are generally that they can trust it as their "user agent" to do any internet-related task which they can
300 access – which, via links and other navigation mechanisms, expands to the whole web.

301 The breadth of reasonably foreseeable uses for all web browsers implies that there are many risks in common across use
302 cases.

303 4.2 Product Architecture

304 To access websites and make them available to users, web browsers need components to handle the following:

- 305 • Networking (including HTTPS and TLS)
- 306 • HTML interpretation and rendering
- 307 • CSS layout
- 308 • JavaScript and WebAssembly code execution

309 NOTE: Java™ is the trade name of a programming language developed by Oracle Corporation.

- 310 • Image decoding
- 311 • SVG, MathML rendering
- 312 • GPU use, both to support rendering of HTML+CSS and for WebGPU
- 313 • Multimedia and video conferencing
- 314 • Camera, microphone and geolocation

315 TODO: Describe how these are put together, typical process architectures, include a diagram, etc.

316 4.3 Operational Environment

317 4.3.1 General description

318 A web browser may be used on any device which supports a user interface and sufficient resources to run the browser.
319 This includes desktop and laptop computers, mobile phones, smart televisions, certain embedded devices, etc.

320 Different contexts where web browsers are used may have different risk profiles, for example:

- 321 • Use of a browser embedded within a social media application, for external links
- 322 • Consumer use on a personal computer or smartphone
- 323 • "Enterprise" desktop/laptop computers within the context of an undertaking (including critical infrastructure)

324 4.3.2 Physical/Hardware environment

325 4.3.3 Logical/Software environment

326 4.3.4 Connectivity aspects

327 4.4 Distribution of Security Functions

328 This clause should address supply chain and integration issues - when a product contains another or is combined with
329 another. The clause should explain in an informative manner how the security functions are distributed across the
330 components included in the product. However, how to address this issue is still not consistent across draft verticals.

331 - Formulation of requirements (see C IoT verticals)??

332 - Assumptions about the integration environment??

333 - What recommendation we make for due diligence on integrated components?

334 4.4.1 Security functions provided outside the product

335 Across browsers and operating systems, different choices are made in different contexts about what is provided by the
336 browser and what is implemented in the surrounding operating system and system libraries, with security functions
337 performed at those other levels. For example:

- 338 • Some standalone browsers (e.g., on mobile platforms) are implemented with the use of a platform-provided
339 embedded browser, subsuming most security functions
- 340 • Networking, including certificate validation and management, selection of algorithms, TLS broadly, etc.
- 341 • Image decoding, text rendering and Unicode handling (no inherent security function, but a historical source of
342 exploitable vulnerabilities)
- 343 • Integrated password manager (may also be provided via an extension)
- 344 • Handling links which may be interpreted as references to native applications, whether via OS-registered
345 origins or custom schemes
- 346 • Scoping permission to access camera, microphone, geolocation or other sensitive information
- 347 • etc. (This is list is not exhaustive.)

348 In such cases, when functionality is implemented outside of the browser in such system libraries or operating systems,
349 the responsibility for handling the risk is transferred to this library, following a risk assessment by the browser which
350 integrates the OS/library that this is reasonable.

351 4.4.2 Security functions provided to other components

352 Web browsers provide a secure, trustworthy environment to render websites, which may be used as part of other
353 products.

354 The web platform maintains a surface area such that "It should be safe to visit a web page" [i.5]. Going to a website
355 does not grant that website risky capabilities over the user's computer. By contrast, other platforms presenting a direct
356 user interface typically involve either a platform curation step, or some risk being taken on by the user. Many
357 mitigations in Clause 5 relate to ensuring that web browsers meet this guarantee.

358 This property makes the web an ideal low-risk way to deliver application user interfaces.

359 4.5 Users

360 Almost all computer users interact with web browsers at some point. This includes:

- 361 • General public

- 362 • Children, students
- 363 • Vulnerable adults
- 364 • Users of the web with respect to sensitive data
- 365 • Professionals in all fields of work
- 366 • Workers in critical infrastructure
- 367 • Users with accessibility needs ## 4.6 Use Cases

368 4.6.1 Standalone browser use cases

369 **UC-CONS:** Standalone web browser for individual consumers

- 370 • Used for accessing the whole web, including sensitive/critical applications.
- 371 • Users are, in general, not educated or aware of cybersecurity issues.
- 372 • Installed on mobile phones, desktop and laptop computers, televisions, larger embedded devices, etc.
- 373 • Includes flexible settings, including high-risk features like developer mode, etc.

374 **UC-INST:** Standalone web browser for institutional or enterprise use, including critical infrastructure

- 375 • Central IT administration may set "enterprise policy" to configure security-related policies.
- 376 • Used in environments which are often taking other sorts of precautions, e.g., at the network/VPN level,
377 physical access, etc.
- 378 • May be used to access "internal" websites which may have been developed with more or less attention to
379 security, or which have special authentication needs.

380 4.6.2 Embedded browser use cases

381 **UC-ETAB:** Browser-like tab component for embedding in a larger application

- 382 • Used by embedding applications to enable linking to outside content while encouraging the user to return to
383 the parent application
- 384 • Intended to facilitate access to just one website, omitting any UI to enter URLs or searches
- 385 • Grants access via links to the rest of the World Wide Web; users may "forget" that they are inside another
386 application
- 387 • Typically no settings UI, and no integration into enterprise policy.
- 388 • Could share the state with the user's default browser # 5. Technical requirements for the Products

389 Editor's Note: This is the normative clause of the standard, defining the technical requirements to implement the
390 Essential Security Requirements of the CRA regulation. The text of the regulation shall never be copied or interpreted
391 in the standard.

392 Editor's Note: The requirements shall be indexed, to facilitate their referencing, preferably using a common indexing
393 structure throughout all standards.

394 *Proposed structure for indexing the requirements:*

395 *REQ - PP - ESR - NNN*

396 *REQ: Used to identify requirement in the text*

397 *PP : Product short name added only if relevant when the product category may be divided in sub categories*

398 *ESR :Proposed abbreviations referring to the different essential requirements of the regulation*

399 *NNNNN - Incremental and unique sequence of numbers and letters*

400 Scheme used here: Use functional areas of the browser in place of PP, if there is any relevant functional area for the
401 requirement.

402 **Editor's Note: It is strongly recommended to follow the sequence of the CRA Annex I requirements when defining the**
403 **subclauses in Clause 5. However, where this structure would result in unnecessary duplication/overlap, subclauses and**
404 **requirements may be organized in a more suitable way, provided that clear traceability to the relevant CRA Annex I**
405 **requirements is maintained.**

406 5.1 Introduction - Applicability of the requirements

407 The technical requirements of the present document apply under the product context described in Clause 4, which shall
408 be in accordance with its intended use. The equipment shall comply with all applicable technical requirements of the
409 present document at all times when operating in such product context.

410 The applicability of the requirements to the Use Cases / Security Profiles are defined below:

411 **Editor's Note: If there is a matrix mapping the use cases to the technical requirements of the standard, it should be**
412 **inserted in this clause. Alternatively, there can be such a matrix/mapping in each subclause below.**

413 5.2 No known exploitable vulnerabilities

414 Proposed ESR code: KEV

415 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (a).

416 **NOTE:** It is proposed that a cross-vertical task force could work on the technical requirements to be included in
417 this clause.

418 5.3 Secure by default configuration

419 Proposed ESR code SBD

420 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (b).

421 **[REQ-TLS-SBD-1]:** The web browser shall be configured by default to reject TLS protocol versions, ciphers and
422 configurations which present high risk to exploitation.

423 **Editor's note: Consider whether "high risk to exploitation" is an appropriate phrase, and whether this requirement should**
424 **say "reject or warn" instead of "reject". See also REQ-TLS-CON-3.**

425 **Editor's note: This requirement might be implied by Annex K. TODO: Research this interpretation and delete if**
426 **redundant.**

427 **[REQ-TLS-SBD-2]:** The web browser shall be configured by default with an appropriate trusted root store based on the
428 manufacturer's risk assessment and documented policy.

429 Applicability: Web browsers which maintain their own root store, rather than using the OS's root store.

430 5.4 Secure Updates

431 Proposed ESR code: SU

432 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (c).

433 **[REQ-TLS-UPD-1]:** The web browser's root store shall be kept up to date appropriately, based on the manufacturer's
434 risk assessment and documented policy.

435 Applicability: Web browsers which maintain their own root store, rather than using the OS's root store.

436 5.5 Authentication and access control

437 Proposed ESR code: AAC

438 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (d).

439 5.6 Confidentiality

440 Proposed ESR code: CON

441 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (e).

442 In this clause, reference can be made to the Annex K (normative), specifying State Of The Art Cryptography

443 **[REQ-TLS-CON-1]**: The web browser shall support TLS versions and configurations indicated as "recommended" (R)
444 of the ENISA Agreed Cryptographic Methods [1], and it may support TLS versions and configurations indicated as
445 "legacy" (L).

446 Note: These algorithms are listed on page 37-38 of [1](#). TLS 1.3 [i.7] is R, and TLS 1.2 [i.6] is L. The L[2025] algorithms
447 (with CBC) are not considered state of the art, and should be ignored.

448 **Editor's note: This requirement might be implied by Annex K. TODO: Research this interpretation and delete if**
449 **redundant.**

450 **[REQ-TLS-CON-2]**: The web browser shall check the full validity of certificate chain through to the root, including
451 for expiration and revocation.

452 **[REQ-TLS-CON-3]**: The web browser shall warn or obstruct the user from interacting with with content served over
453 insecure connections, including expired certificates and insecure TLS configurations.

454 Example: When presenting content served with cryptographic methods with a certain risk of exploitation, a web
455 browser presents a user with a user interface element representing a broken lock, or an interstitial requiring user
456 interaction to proceed.

457 **[REQ-TLS-CON-4]**: The web browser shall implement appropriate technologies to promote or require the use of
458 HTTPS rather than HTTP.

459 Example: Implementation of HSTS [i.8], active mixed content blocking [i.9], and HTTPS-First loading strategies.

460 5.7 Integrity

461 Proposed ESR code: INT

462 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (f).

463 Note: TLS-related clauses contribute to integrity.

464 5.8 Data Minimisation

465 Proposed ESR code: DM

466 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (g).

467 Note: TLS-related clauses contribute to data minimization.

468 5.9 Availability Protection

469 Proposed ESR code: AP

470 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (h).

471 5.10 Impact Minimisation

472 Proposed ESR code: IM

473 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (i).

474 5.11 Minimisation of Attack Surfaces

475 Proposed ESR code: MAS

476 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (j).

477 5.12 Exploitation Mitigation Mechanisms

478 Proposed ESR code: EMM

479 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (k).

480 5.13 Logging and Monitoring

481 Proposed ESR code: LOG

482 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (l).

483 **[REQ-TLS-LOG-1]**: The web browser shall present a user interface giving visibility into the security properties of the
484 connection, including the origin.

485 5.14 Data Removal and Transparency

486 Proposed ESR code: DRT

487 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 1 (2) (m).

488 **[REQ-TLS-DRT-1]**: The web browser shall make available functionality to reset TLS-related functionality to the
489 initial safe settings, including selection of algorithms and protocol versions, root certificates, and any other relevant
490 properties.

491 Applicability: Web browsers which allow changing TLS-related settings.

492 5.15 Vulnerability Handling

493 This clause addresses the requirements in the CRA [i.1] Annex 1 Part 2.

494 The requirements specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [2] shall be fulfilled for the
495 product.

496 6. Assessment criteria for compliance with technical 497 requirements

498 *It has been agreed across vertical standards to define each assessment criteria following the common structure:*

- 499 • *Requirement reference*
- 500 • *Objective*
- 501 • *Preparation*
- 502 • *Activities*
- 503 • *Verdict*
- 504 • *Evidence*

505 *The assessment criteria clause shall be structured by requirement defined in clause 5.*

506 6.1 Introduction to the assessment and compliance criteria

507 This clause provides objective and reproducible assessment criteria to determine whether a product complies with the
508 technical security requirements of clause 5, based on the UC and/or the Security Profile it may belong towards its
509 placement in the EU market.

510 For each cybersecurity requirements defined in Clause 5, the following clauses specify assessment criteria to determine
511 if the technical requirement is met.

512 Please ensure that there is an easy, clear and unambiguous mapping of the requirements in clause 5 to the relevant
513 assessment criteria in clause 6.

514 The assessment criteria for each security requirements are described in a structured manner, as follows:

- 515 • **Assessment Objective:** Defines the security property or capability that shall be verified, ensuring that the
516 assessment remains focused on the intent of the requirement. It includes the reference index of the
517 requirement(s) it aims to assess.
- 518 • **Assessment Preparation:** Describes the environment, setup, and preconditions required before executing the
519 test. It includes the following elements as applicable:
 - 520 ○ Test environment: Describe the hardware, software, and network setup used for the assessment,
521 including versions, topology, and any relevant dependencies.
 - 522 ○ Preconditions: Specify any configurations, credentials, or operational states that should be established
523 before the test (e.g. product initialized, certificates loaded, user roles created).
 - 524 ○ Required tools: Identify the tools or software necessary to perform the assessment (e.g. vulnerability
525 scanners, protocol fuzzers, traffic analyzers, static code analyzers, cryptographic test suites).
 - 526 ○ Required information/documentation for the assessment: Specify all information that is necessary to
527 perform the assessment
 - 528 ○ Reference any vendor-provided setup guides, configuration instructions, or operational manuals, as
529 well as any relevant standards or technical notes, that define how the product shall be configured or
530 operated for the assessment.
- 531 • **Assessment Activities:** Provides execution steps to be performed. Assessment activities may include, as
532 applicable:
 - 533 ○ Review information/documentation for the assessment to confirm that the described implementation
534 matches the requirement (e.g. verify that the security architecture document specifies TLS 1.2 or
535 higher for all external interfaces, or that the password policy aligns with the defined threshold).
 - 536 ○ Perform security functional tests to verify the completeness and correctness of the
537 information/documentation for the assessment
 - 538 ○ Perform security functional or penetration tests to verify that implemented controls are correctly
539 implemented e.g. to prevent unauthorized access or data modification (e.g. via attempting to log in
540 with invalid credentials to test lockout enforcement or trying to modify protected configuration files
541 without administrative privileges).
 - 542 ○ Analyse code or binaries to identify potential security weaknesses or misconfigurations (e.g. perform
543 static analysis to detect hardcoded credentials or use dynamic analysis tools to identify buffer
544 overflow or injection vulnerabilities).
 - 545 ○ Inspect configurations to ensure that required security parameters are correctly applied (e.g. check
546 that weak cipher suites are disabled, two-factor authentication is enabled, and least-privilege access
547 controls are configured in the system).
 - 548 ○ Observe runtime behaviour to confirm that protections such as encryption, authentication, and
549 integrity verification operate as intended (e.g. monitor network traffic to ensure data in transit is
550 encrypted or observe system logs to verify successful validation of digital signatures during startup).
- 551 • **Assignment of Verdict:** Defines the pass/fail criteria.

- 552 ○ **Pass:** The assessment is considered passed if the product demonstrably fulfils the requirement and
553 meets the defined security thresholds. Examples of such thresholds include:
- 554 ▪ Minimum cryptographic strength (e.g. AES-128 or higher);
- 555 ▪ Password policy limits (e.g. minimum of 12 characters);
- 556 ▪ Login protection mechanisms (e.g. account lockout after five consecutive failed attempts);
- 557 ▪ Resistance to a specified attack potential (e.g. equivalent to CSA High/AVA_VAN.3 or
558 higher).
- 559 ○ **Fail:** The assessment is considered failed if the requirement is not fulfilled, or if the defined security
560 thresholds are not achieved (e.g. insufficient key length, missing authentication enforcement, or
561 inadequate resistance to the required attack potential).
- 562 • **Supporting Evidence :** Defines the artefacts and documentation collected to demonstrate that the requirement
563 has been assessed and fulfilled. The evidence shall be sufficient to enable independent verification of the
564 assessment results and to demonstrate compliance with the relevant CRA essential requirements. The
565 supporting evidence include, where applicable:
- 566 ○ Test or assessment reports showing the steps performed and results obtained;
- 567 ○ Logs, configuration files, or audit traces demonstrating the implementation of the requirement;
- 568 ○ Screenshots, captures, or console outputs confirming the correct execution or protection behaviour;
- 569 ○ Relevant vendor or design documentation describing the applied security measures;
- 570 *It would be very useful to use a common structure for the assessment criteria definition clause 6. The following is a*
571 *proposal - to be discussed among rapporteurs.*
- 572 *The assessment criteria shall be indexed, to facilitate their referencing, preferably using a common indexing structure*
573 *throughout all standards and enabling an easy mapping with the requirements of Clause 5.*
- 574 *Proposed structure for indexing the assessment criteria:*
- 575 *ACC - PP - ESR - NNN*
- 576 *ACC: Used to identify assessment and compliance criteria in the text*
- 577 *PP : Product short name added only if relevant when the product category may be divided in sub categories*
- 578 *ESR :Proposed abbreviations referring to the different essential requirements of the regulation*
- 579 *NNNNN - Incremental and unique sequence of numbers and letters - could be the same as for the corresponding*
580 *requirement (if one-to-one match), otherwise a mapping would be needed*

581 6.2 No known exploitable vulnerabilities

582 Proposed ESR code: KEV

583 6.3 Secure by design

584 Proposed ESR code SBD

585 6.4 Secure Updates

586 Proposed ESR code: SU

587 6.5 Authentication and Access Control

588 Proposed ESR code: AAC

589 **6.6 Confidentiality**

590 Proposed ESR code: CON

591 In this clause, reference can be made to the Annex K (normative), specifying State Of The Art Cryptography
592 assessment criteria.

593 **6.7 Integrity**

594 Proposed ESR code: INT

595 **6.8 Data Minimisation**

596 Proposed ESR code: DM

597 **6.9 Availability Protection**

598 Proposed ESR code: AP

599 **6.10 Impact Minimisation**

600 Proposed ESR code: IM

601 **6.11 Minimisation of Attack Surfaces**

602 Proposed ESR code: MAS

603 **6.12 Exploitation Mitigation Mechanisms**

604 Proposed ESR code: EMM

605 **6.13 Logging and Monitoring**

606 Proposed ESR code: LOG

607 **6.14 Data Removal and Transparency**

608 Proposed ESR code: DRT

609 **6.15 Vulnerability Handling**

610 The assessment criteria specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [2] shall be met for the
611 product

612

613 **Annex A (informative):**
614 **Relationship between the present document and the**
615 **requirements of EU Regulation (EU) 2024/2847 - the**
616 **Cyber Resilience Act**

617 The present document has been prepared in response to the Commission's standardisation request C(2025)618 [i.3] to
618 provide, in additions to its other uses, one voluntary means of conforming to the essential requirements of Regulation
619 (EU) 2024/2847 [i.2] known as the Cyber Resilience Act (CRA).

620 Once the present document is cited in the Official Journal of the European Union under Regulation (EU) 2024/2847
621 [i.2], conformance with the normative clauses of the present document given in the tables in Annex A confers, to
622 products with digital elements in the scope of the present document, a presumption of conformity with the
623 corresponding essential requirements of that Regulation and associated EFTA regulations.

624
625

**Table A.1: Relationship between the present document and
the requirements of Regulation (EU) 2024/2847 - the Cyber Resilience Act**

No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
1	Annex I, Part 1, (1)	"Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks."	Clause 5	C	See mapping table on the applicability of the technical cybersecurity requirements in clause 5.1
2	Annex I, Part 1, (2)(a)	"Products with digital elements shall be made available on the market without known exploitable vulnerabilities."	Clause 5.2	U/C	
3	Annex I, Part 1, (2)(b)	"Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state."	Clause 5.3	U/C	
4	Annex I, Part 1, (2)(c)	"Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them"	Clause 5.4	U/C	
5	Annex I, Part 1, (2)(d)	"Products with digital elements shall ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access"	Clause 5.5	U/C	

No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
6	Annex I, Part 1, (2)(e)	"Products with digital elements shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by best practice mechanisms, and by using other technical means."	Clause 5.6	U/C	
7	Annex I, Part 1, (2)(f)	"Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions."	Clause 5.7	U/C	
8	Annex I, Part 1, (2)(g)	"Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation)."	Clause 5.8	U/C	
9	Annex I, Part 1, (2)(h)	"Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks."	Clause 5.9	U/C	
10	Annex I, Part 1, (2)(i)	"Products with digital elements shall minimise the negative impact by the products themselves or connected products on the availability of services provided by other products or networks."	Clause 5.10	U/C	
11	Annex I, Part 1, (2)(j)	"Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces."	Clause 5.11	U/C	

No	Description	Requirements of Regulation	Clause(s) of the present document	U/C	Condition
12	Annex I, Part 1, (2)(k)	"Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques."	Clause 5.12	U/C	
13	Annex I, Part 1, (2)(l)	"Products with digital elements shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user."	Clause 5.13	U/C	
14	Annex I, Part 1, (2)(m)	"Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner."	Clause 5.14	U/C	
15	Annex I, Part 2		Clause 5.15	U	

626
627

628 NOTE: The table cannot indicate direct relationship between the relevant legal requirement and *other* standards
629 or normative clauses contained in *other* standards.

630 NOTE: If the standard is developed according to the structure in the present skeleton document, then the number
631 of the clauses in the table below don't need to be changed.

632 NOTE: The last two columns shall be either filled with details and the reference of the table(s) mapping the
633 applicability of the technical cybersecurity requirements, or deleted all together.

634 **Key to columns:**

635 **Requirement:**

636 **No** A unique identifier for one row of the table which may be used to identify a requirement.

637 **Description** A textual reference to the requirement.

638 **Requirements of Regulation** Identification of article(s) defining the requirement in the Regulation.

639 **Clause(s) of the present document** Identification of clause(s) defining the requirement in the present document unless
640 another document is referenced explicitly.

641 **Requirement Conditionality:**

642 **U/C** Indicates whether the requirement is unconditionally applicable (U) or is conditional upon the manufacturer's
643 claimed functionality of the equipment (C).

644 **Condition** Explains the conditions when the requirement is or is not applicable for a requirement which is classified
645 "conditional".

646 Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list
647 published in the Official Journal of the European Union. Users of the present document should consult frequently the
648 latest list published in the Official Journal of the European Union.

649 Other Union legislation may be applicable to the product(s) falling within the scope of the present document.

650

651 **Annex B (informative):**
652 **Cybersecurity threat landscape, risk identification**
653 **and assessment methodology**

654 This Annex applies a "state of the art" risk assessment methodology to the Product in scope of the present document, to
655 identify threats, evaluate the risks and define security profiles applicable to the different use cases of the product
656 context.

657 Consider defining a common sub-structure.

658

659 Annex C (informative):
660 Relationship between the present document and any
661 related ETSI standards (if any, e.g. EN 303 645)

662 C.1 First clause of the annex

663 C.1.1 First subdivided clause of the annex

664 <Text>.

665 Annex <D...J> (informative):

666 <Publication> : "<Title>".<Edition>. <Year>, <Issue designation>, <Page location>.

667

668 **Annex G:**
669 **Guidelines on the implementation of the present**
670 **document (informative):**

671 *This Annex is optional and may be referred to from the Introduction of the document to provide more information on*
672 *how to implement the standard.*

673

674 **Annex K (normative):**
675 **Generic requirements and assessment criteria for the**
676 **use of state of the art cryptography V 0.51 (2025-02-**
677 **16)**

678 ETSI Drafting rules do not allow footnotes. All footnotes in this Annex will have to be deleted or replaced by relevant
679 references and notes before publication. Once the text of this Annex will be agreed, the definitions included in the notes
680 will be moved to Clause 3 of the present document.

681 NOTE: the text of this annex is currently being edited, not final.

682 K.1 State of the Art Cryptography (SOTA)

683 K.1.1 Requirement

684 The product shall, by default, use State-of-the-Art cryptography algorithms listed in (CRY-SOTA), to be used for the
685 supported security mechanism of the product where applicable.

686 NOTE: The use of *security mechanism e.g. authentication, access control, secure communication, secure storage*
687 *and secure update are described in the main text of this standard.*

688 NOTE: Cryptographic algorithm primitives (in short, algorithms e.g. public- and private-key encryption
689 algorithms, hash functions, authentication codes, digital signatures) are classified as CRY-SOTA if they
690 are listed in the [ACM]¹ document and are suitable for the implementation of supported security
691 mechanisms of the product.

692 NOTE: Supporting evidence options that an algorithm, which is not included in CRY-SOTA, is applicable and
693 suitable for the respective use case, are listed in the related assessment criteria (K.1.2.1) clause.

694 K.1.2 Assessment criteria

695 K.1.2.1 Assessment objective:

696 The purpose of this assessment case is (the conceptual assessment) whether the implemented algorithms are identified
697 as CRY-SOTA.

698 K.1.2.2 Assessment preparation:

- 699 • Preconditions for the test: If applicable, the product is in the default- configuration. Otherwise, the product is
700 in the delivery state, where it is available on the market in accordance with CRA Annex I part 1(2) (b).

701 K.1.2.3 Assessment activities:

- 702 • For every security mechanism the list of used algorithms, which are reachable over an external interface and
703 identified as CRY- SOTA shall be documented.

704 K.1.2.4 Supporting Evidence:

- 705 • description of the performed test
706 • all test records of the performed test

707 K.1.2.5 Assignment of verdict:

- 708 • The verdict PASS shall be assigned if evidence has been provided.

¹ defined in [ACM]

- 709 • The verdict FAIL shall be assigned otherwise

710 If the verdict in K.1.2.1 has been assigned FAIL, the following assessment has to be performed additionally:

711 K.1.2.2 Additional conditional assessment:

712 K1.2.2.1 Assessment objective

713 If for a certain security mechanism and use case no CRY-SOTA algorithm is applicable, evidence shall be provided in
714 the documentation that a suitable algorithm has been implemented for this evidence instead.

715 K.1.2.2.2 Assessment preparation:

716 Preconditions for the test: If applicable, the product is in the default configuration state. Otherwise, the product is in the
717 delivery state, where it is available on the market in accordance with CRA Annex I part 1(2) (b).

718 K.1.2.2.3 Assessment activities:

719 For every security mechanism and for every used algorithm, which is reachable over an interface of the product and
720 identified as not included in CRY- SOTA, the documentation shall provide evidence

- 721 • that this algorithm is applicable and suitable for the respective use case

722 K.1.2.4 Supporting Evidence:

723 1. Identification of the certain algorithm by reference in further publicly available applicable algorithm
724 catalogues as national cryptographic catalogues² or vertical use case specific cryptographic algorithm
725 catalogues³

726 2. No entry of known exploitable vulnerabilities provided in ENISA "European Vulnerability Database."⁴

727 3. Description of the performed test

728 4. all test records of the performed test

729 K.1.2.5 Assignment of verdict:

- 730 • The verdict PASS shall be assigned if respective evidence has been provided,

- 731 • The verdict FAIL shall be assigned otherwise.

732 NOTE: Functional correctness and completeness assessment criteria of the documentation are to be specified in
733 accordance with the capabilities set in the specific vertical Standards.

734 K.2 Requirement ("crypto agility")

735 Where applicable the product shall by default be prepared to update cryptographic algorithm used for the supported
736 security mechanism of the product to maintain when there are indications that the used cryptographic algorithm will not
737 stay SOTA anymore within the intended lifetime of the product.

738 NOTE: To maintain SOTA for cryptographic algorithm within the intended lifetime of the product concepts to
739 consider are crypto agility additional to the capability of updating cryptographic algorithms on the
740 product in accordance to Secure Update and Secure Communication mechanism.

² e.g. BSI – BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths , Vers. 2025-01, January 31, 2025

³ e.g. EPC342-08 /Version 15.0 /Guidelines on cryptographic algorithms usage and key management - PPSSG / 7 March 2025

⁴ European Vulnerability Database established pursuantto Article 12(2) of Directive (EU) 2022/2555, <https://euvd.enisa.europa.eu/ENISA>

741 NOTE: Formal verification can use mathematical proofs and /or rigorous methods to prove an algorithm's
 742 correctness, ensuring it meets its formal specification for all valid inputs, unlike testing which only
 743 samples cases. This process involves creating formal models, using techniques like [theorem proving](#) or
 744 [model checking](#), and is crucial for critical systems like [cryptography](#) finding hard-to-spot bugs and
 745 guaranteeing security/reliability.

746 NOTE: The [ACM] listing has two classes of SOTA algorithms; **Legacy mechanisms** with an expiry date as
 747 defined in ACM, and **Recommended mechanisms** with no set expiry date.

748 NOTE: For products or components of products that cannot have their cryptographic algorithms updated for
 749 example if the implementation or part uses a hardware-based root of trust, it is important that the intended
 750 lifetime of the equipment does not exceed the recommended usage lifetime of the cryptographic
 751 algorithms used by the product. Thereby the implementation of an algorithm can include the specific
 752 implementation of their parameters

753 NOTE: If a component storing the algorithm or corresponding parameters of a main product is replaced by a new
 754 component, the product is considered as a new product according to the New Legislative Framework Blue
 755 Guide, if the replacement provides a substantial modification to the main product

756 K.2.1 Assessment criteria

757 K.2.1.1 Assessment objective:

758 The purpose of this assessment case is (the conceptual assessment) whether the product is prepared to update
 759 cryptographic algorithms for the supported security mechanism.

760 K.2.1.2 Assessment preparation:

- 761 • Preconditions for the test: If applicable, the product is in the default- configuration. Otherwise, the product is
 762 in the delivery state, where it is available on the market in accordance with CRA Annex I part I(2) (b).

763 K.2.1.3 Assessment activities:

- 764 • For every used SOTA algorithm, which is reachable over an interface, the life span of the algorithm is
 765 documented, as well its property, if the algorithm is considered as legacy or recommended algorithm.⁵
- 766 • If the life span of the product exceeds the life span of a legacy algorithm, the algorithm is marked as updatable
 767 by a recommended algorithm in the documentation.
- 768 • If an algorithm is identified as SOTA recommended, no further action is required.

769 K.2.1.4 Supporting Evidence:

- 770 • Description /documentation of the performed test.
- 771 • All test records of the performed test.

772 K.2.1.5 Assignment of verdict:

- 773 • The verdict PASS shall be assigned if respective evidence has been provided,
- 774 • The verdict FAIL shall be assigned otherwise.

775

776

⁵ defined in [ACM]

777 Annex O (informative): 778 Products not handled by this document

779 (NOTE: This section is informative and may be removed if the EC prefers. Inclusion or omission of use cases in this
780 standard does not affect manufacturers' legal requirement to perform a risk assessment.)

781 O.1: Products which are not web browsers

- 782 • Platforms providing for the use of web technology which only handle trusted content under the control of the
783 platform provider, such as:
 - 784 ○ Products that use web technologies are part of their internal UI
 - 785 ○ An embedded HTML renderer for use in an offline ebook reader
- 786 • Products which contain a web browser but whose primary purpose is not that of a web browser
 - 787 ○ e.g., a social media application which contains an in-app browser tab for following links
 - 788 ○ The embedded browser inside the social media app is definitely a browser (if it was distributed to the
789 supply chain as a product). But the overall social media application isn't, and might not be "important"
790 with respect to Annex III of the Cyber Resilience Act.
- 791 • Use of web technology without direct end users, e.g., to download websites to build an index to search the web
792 or for automated testing.

793 O.2: Products with unhandled risks

794 Certain products on the market as of the time of this writing, which may be considered to fit within the definition of
795 web browsers, are subject to certain risks for which this document does not contain a treatment.

- 796 • Embedded browsers which provide a mechanism for the integrator to give privileged handling of certain
797 first-party content
 - 798 ○ Untreated risks: validating the first party content; avoiding privilege escalation from third-party
799 content
- 800 • Embedded browsers which contain the capability for the integrator to add additional functionality to websites,
801 e.g., via bridges from script to native APIs
 - 802 ○ Untreated risks: ensuring isolation between native code and web content
- 803 • Applications of web technology which use a distribution mechanism for content other than navigation to
804 websites, e.g., app stores or mini-app platforms
 - 805 ○ Untreated risks: safe curation, distribution of applications; safety of any additional APIs provided to
806 applications which go beyond typical web browser APIs
 - 807 ○ Note: this case might be analyzed as out of scope of the definition of web browsers
- 808 • Web browsers with AI agent integration, to autonomously perform actions (e.g., navigations, form
809 submissions)
 - 810 ○ Untreated risks: information leaks to and across websites, actions may be taken which are not what
811 the user wanted
 - 812 ○ The harmonised standard is expected to deliver technical solutions within the generally acknowledged
813 state of the art and not in areas still rapidly evolving.

814

815 **Annex V (informative):**
816 **Guide for derivative web browsers**

817 **V.1 General**

818 A significant proportion of browsers placed on the market are derivative products based on open source browser
819 engines or substantially complete browser implementations. Requirements under the CRA for such "derivative web
820 browsers" are the same as for any other web browser. This section contains some relevant considerations for derivative
821 browsers.

822 **V.2 Applying Voluntary Security Attestations**

823 The conformity assessment for such derived browsers may make reference to "Security attestation of free and
824 open-source software", per Article 25 of the CRA [i.1]. As of the time of this writing, there is ongoing work at the
825 European Commission and in open-source efforts to define such attestations and how they may be applied.

826 The hope in the browser context is that such attestations may make it easier to apply this standard, if an "upstream"
827 attestation may be applied to demonstrate some of the requirements in this document.

828 **V.3 Applying vulnerability handling requirements**

829 Vulnerability handling requirements are defined in Annex I part II of [i.1], and explained further in [2]. This section
830 includes notes on how these sections may apply in practice.

831 Updates from upstream for derivative browsers come in two forms:

832 • **Rebases:**

- 833 ○ Updating a derivative browser to a newer version from upstream is referred to as a "rebase".
- 834 ○ Some upstream browsers have fast (e.g., monthly) major version release cycles, with a vulnerability
835 handling policy where upstream only ports fixes to a certain window of versions (e.g., a few months).
- 836 ○ If a derivative browser does not "rebase" to a version with such upstream backports, it risks not
837 getting all relevant fixes (if no one else developed the backport).
- 838 ○ The failure to rebase is where the highest security risk from derived browsers exists in practice as of
839 this publication.

840 • **Security hotfixes:**

- 841 ○ Upstream browsers sometimes release patches against current versions to address especially urgent
842 exploitable vulnerabilities. It is important to distribute these updates promptly, relative to risk.
- 843 ○ Note that, with frequent rebases, the window for such exploits is somewhat limited, as they will be
844 picked up in the rebase.

845

846 History

847 *The following table will automatically be filled in by the ETSI Secretariat.*

Document history		

848

849

850 *Last update on 2026-02-26*