



## Cybersecurity (CYBER); Cyber Resilience Act (CRA); Cybersecurity requirements for Virtual Private Networks

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](mailto: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 304 620 Virtual Private Networks Part 1 - 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](mailto: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**

&lt; DEN/CYBER-EUS-005 &gt;

---

**Keywords**

&lt; CRA &gt;

**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 .....	8
3	Foreword.....	8
4	Modal verbs terminology .....	9
5	Executive summary .....	9
6	Introduction .....	9
7	1 Scope.....	10
8	2 References .....	10
9	2.1 Normative references.....	10
10	2.2 Informative references .....	10
11	3 Definition of terms, symbols and abbreviations.....	11
12	3.1 Terms .....	11
13	3.2 Symbols .....	13
14	3.3 Abbreviations.....	13
15	4 Product context.....	13
16	4.0 Introduction.....	13
17	4.1 Product Functions .....	13
18	4.3 Product architecture .....	14
19	4.3.1 Product overview .....	14
20	4.3.2 VPN client.....	15
21	4.3.3 VPN server, VPN gateway.....	15
22	4.4 Operational Environment.....	15
23	4.X.X General description .....	15
24	4.4.1 Physical/Hardware environment .....	15
25	4.4.2 Logical/Software environment.....	16
26	4.4.4 Connectivity aspects.....	16
27	4.5 Distribution of Security Functions.....	16
28	4.5.1 Cybersecurity function distribution overview .....	16
29	4.5.2 Cybersecurity Functionalities Offered to Integrated Components .....	17
30	4.5.3 Cybersecurity functions required from the environment.....	17
31	4.6 Users .....	17
32	4.7 Use cases.....	17
33	5 Technical requirements for the Products.....	19
34	5.1 Notes on the structure of requirements .....	19
35	5.2 Technical cybersecurity requirements specifications.....	19
36	5.2.1 General .....	19
37	5.2.2 TR-NKEV: No known exploitable vulnerabilities at first use.....	19
38	5.2.2.1 Requirement .....	19
39	5.2.2.2 MI-KEVD: Documentation for secure update before or during first use .....	20
40	5.2.2.3 MI-KEVA: Automatic secure update before or during first use.....	20
41	5.2.2.3a MI-KEVE: Automatic secure update via administrator action before or during first use.....	20
42	5.2.2.5 MI-KEVT: Testing for known exploitable vulnerabilities .....	21
43	5.2.3 TR-SSDD: Secure software design and development.....	21
44	5.2.3.1 Requirement .....	21
45	5.2.3.2 MI-SSCA: Static source code analysis for memory errors.....	22
46	5.2.3.3 MI-FZ95: Runtime code coverage checking with memory access error detection.....	22
47	5.2.3.4 MI-IMSL: Implement in a memory-safe language.....	23
48	5.2.3.5 MI-BTIN: Boundary testing of inputs that may cause memory errors .....	23
49	5.2.3.6 MI-SCFS: Secure compilation flags.....	23
50	5.2.4 TR-SCUD: Secure updates.....	24
51	5.2.4.1 Requirement .....	24
52	5.2.4.2 MI-SUDC: Documentation of secure update.....	24

53	5.2.4.3	MI-SUVP: Secure update via product .....	24
54	5.2.4.4	MI-SUAP: Automatic secure update via product .....	24
55	5.2.4.5	MI-SUOE: Secure update provided by operational environment .....	25
56	5.2.4.6	MI-SUAO: Automatic secure update provided by operational environment .....	25
57	5.2.4.7	MI-SUCS: Updates are signed and verified before installation .....	25
58	5.2.4.8	MI-SUAU: Only authorized software updates .....	26
59	5.2.4.9	MI-SUVH: Secure update has validly signed hash.....	26
60	5.2.4.10	MI-SURP: Invalidated update is rejected .....	26
61	5.2.4.11	MI-SURC: Signing keys have strictly scoped usage .....	27
62	5.2.4.12	MI-SUSR: Signing keys have not been revoked or otherwise marked untrusted.....	27
63	5.2.4.13	MI-SUMV: Reject update to current or previous version.....	28
64	5.2.4.14	MI-SUED: Updates not applied from expired sources .....	28
65	5.2.5	TR-ROUT: VPN traffic routed only through VPN connection during VPN connection .....	29
66	5.2.5.1	Requirement .....	29
67	5.2.5.2	MI-ROUT-1 VPN routing stays in effect until VPN connection deactivated.....	29
68	5.2.5.3	MI-ROUT-2 VPN routing stays in effect during network-level tunnel failure.....	29
69	5.2.5.4	MI-ROUT-3 Tunnel all traffic by default.....	29
70	5.2.6	TR-CONF: VPN client preserves system configuration .....	30
71	5.2.6.1	Requirement .....	30
72	5.2.6.2	MI-CONF-1 VPN client restores any system configuration it changes to its previous state after the VPN connection ends .....	30
73			
74	5.2.6.3	MI-CONF-2 VPN client provides a method to restore any system configuration it changes to its previous state .....	30
75			
76	5.2.6.4	MI-CONF-3 VPN client does not degrade system security.....	31
77	5.2.6.5	MI-CONF-4 VPN client shall not require unnecessary permissions .....	31
78	5.2.6.6	MI-CONF-5: User interfaces shall prevent unintentional disabling of cybersecurity features.....	32
79	5.2.7	TR-NUTI: No untrusted traffic in the VPN connection .....	32
80	5.2.7.1	Requirement .....	32
81	5.2.7.2	MI-NUTI-1 Policy-driven traffic exclusion .....	32
82	5.2.7.3	MI-NUTI-2 Protocol validity checks.....	32
83	5.2.8	TR-AUTH: Authentication of nodes .....	33
84	5.2.8.1	Requirement .....	33
85	5.2.8.2	MI-AUTH-1 Authentication of cybersecurity-relevant nodes.....	33
86	5.2.8.3	MI-AUTH-2 Transmitted credentials must be encrypted .....	33
87	5.2.8.4	MI-AUTH-3 Authentication timeout.....	34
88	5.2.8.5	MI-AUTH-4 Cloned credentials detection .....	34
89	5.2.8.6	MI-AUTH-5 Forced revocation of authorization of endpoints.....	34
90	5.2.8.7	MI-AUTH-6 Brute force protection .....	34
91	5.2.9	TR-DNSL: DNS leak prevention .....	35
92	5.2.9.1	Requirement .....	35
93	5.2.9.2	MI-DNSL-1 Inform user of visibility of DNS queries .....	35
94	5.2.9.3	MI-DNSL-2 Configurable exclusive DNS routing.....	36
95	5.2.9.4	MI-DNSL-3 Exclusive DNS routing by default .....	36
96	5.2.9.6	MI-DNSL-5 Monitoring of DNS configuration .....	36
97	5.2.9.7	MI-DNSL-6 Secure DNS protocols.....	37
98	5.2.9.8	MI-DNSL-7 No DNS leaks during network-level tunnel failure .....	37
99	5.2.10	TR-EISO: Endpoint isolation.....	37
100	5.2.10.1	Requirement .....	37
101	5.2.10.2	MI-EISO: No route between different endpoints.....	37
102	5.2.11	TR-TRAF: No traffic through the node unless explicitly approved.....	38
103	5.2.11.1	Requirement .....	38
104	5.2.11.2	MI-TRAF-1: No capability to route traffic from other sources .....	38
105	5.2.11.3	MI-TRAF-2: Route traffic from other sources disabled by default .....	38
106	5.2.11.4	MI-TRAF-3: Notify user if routing traffic from other sources.....	38
107	5.2.11.5	MI-TRAF-4: No routing traffic from other sources if not necessary for services .....	39
108	5.2.12	TR-DMIN: Data minimization .....	39
109	5.2.12.1	Requirement .....	39
110	5.2.12.2	MI-NPER-1: No Personal Data collected without authorization.....	39
111	5.2.12.3	MI-NPER-2: No Personal Data sent outside endpoint .....	39
112	5.2.12.4	MI-NPER-3: Minimize Personal Data required for use, service provisioning and payment.....	39
113	5.2.12.5	MI-NPER-4: No Personal Data stored on remote data processing systems .....	40
114	5.2.13	TR-IPV6: Secure IPv6 Handling.....	40

115	5.2.13.1	Requirement .....	40
116	5.2.13.2	MI-IPV6-1 Block IPv6 if Unsupported .....	40
117	5.2.13.3	MI-IPV6-2 Full Support if Claimed .....	41
118	5.2.14	TR-CRYPT: Use strong, VPN specific cryptography .....	41
119	5.2.14.1	Requirement .....	41
120	5.2.14.3	MI-CRYPT-1: Use conformant cryptography .....	41
121	5.2.15	TR-LOGG: Logging and monitoring .....	41
122	5.2.15.1	Requirement .....	41
123	5.2.15.2	MI-LOGG-1: Logging .....	41
124	5.2.15.3	MI-LOGG-2: Remote Logging .....	42
125	5.2.15.4	MI LOGG 3: No-Logs Policy and Traffic Anonymization .....	43
126	5.2.15.5	MI LOGG 3: No data persistence or storage enabled on exit nodes .....	43
127	5.2.16	TR-SCDL: Secure deletion .....	44
128	5.2.16.1	Requirement .....	44
129	5.2.16.2	MI-RSET: Secure deletion via reset .....	44
130	5.2.16.3	MI-INST: Secure deletion via reinstallation .....	44
131	5.2.16.4	MI-DELE: Secure deletion via secure deletion function .....	44
132	5.2.17	TR-SDTR: Secure data read and transfer .....	45
133	5.2.17.1	Requirement .....	45
134	5.2.17.2	MI-SDRF: Secure data read from product .....	45
135	5.2.17.3	MI-SDTR: Secure data transfer to another product .....	45
136	5.2.18	Intentionally left blank .....	46
137	5.2.19	TR-AVAI: Availability .....	46
138	5.2.19.1	Requirement .....	46
139	5.2.19.2	MI-FDRP: Fast packet drop .....	46
140	5.2.19.3	MI-LMEM: Limit memory usage .....	46
141	5.2.19.5	MI-DOST: Document risk transfer to operational environment for denial of service .....	47
142	5.2.19.6	MI-DOST: Rate limit unauthenticated traffic .....	47
143	5.2.19.7	MI-DOST: Automatic traffic handling during denial-of-service attack .....	47
144	5.2.20	TR-CDST: Confidentiality of data stored on the product .....	48
145	5.2.20.1	Requirement .....	48
146	5.2.20.2	MI-CDST: Protect confidentiality of data stored on the product .....	48
147	5.3	Risk mitigation sets .....	48
148	5.3.1	General .....	48
149	5.3.2	SP-1 Individual consumer required mitigations .....	48
150	5.3.3	SP-2 Privacy conscious household required mitigations .....	49
151	5.3.4	SP-3 Journalist or activist required mitigations .....	50
152	5.3.5	SP-4 Small organization required mitigations .....	52
153	5.3.5	SP-5 Large enterprise required mitigations .....	53
154	5.3.6	SP-6 Enterprise independent client mitigations .....	55
155	5.3.X	SP-7 Mesh VPN required mitigations .....	56
156	6	Assessment criteria for compliance with technical requirements .....	57
157	6.1	Introduction to the assessment and compliance criteria .....	58
158	6.2	No known exploitable vulnerabilities .....	59
159	6.3	Secure by design .....	59
160	6.4	Secure Updates .....	59
161	6.5	Authentication and Access Control .....	59
162	6.6	Confidentiality .....	60
163	6.7	Integrity .....	60
164	6.8	Data Minimisation .....	60
165	6.9	Availability Protection .....	60
166	6.10	Impact Minimisation .....	60
167	6.11	Minimisation of Attack Surfaces .....	60
168	6.12	Exploitation Mitigation Mechanisms .....	60
169	6.13	Logging and Monitoring .....	60
170	6.14	Data Removal and Transparency .....	60
171	6.15	Vulnerability Handling .....	60
172	Annex A (informative): Relationship between the present document and the requirements of EU		
173	Regulation (EU) 2024/2847 - the Cyber Resilience Act .....		61
174	Annex C (informative): Cybersecurity threat landscape, risk identification and assessment methodology .....		63

175	C.1	Assets.....	63
176	C.1.1	Data 63	
177	C.1.2	Product functions .....	63
178	C.2	Risk factors .....	63
179	C.2.1	General63	
180	C.2.2	RF-CFG: End-point configuration .....	64
181	C.2.3	RF-AUT: Account management and authentication of endpoints .....	64
182	C.2.5	RF-FUN: Sensitivity of functions .....	64
183	C.2.6	RF-ADM: Availability of administration.....	64
184	C.2.7	RF-RDP: Manufacturer infrastructure isolation.....	64
185	C.2.8	RF-DNC: Difficulty of network configuration .....	65
186	C.2.9	RF-COM: Complexity of feature set.....	65
187	C.2.10	RF-CON: Connectivity offered.....	65
188	C.2.11	RF-PER: Consequences of Protected Data compromise.....	65
189	C.3	Assumptions .....	65
190	C.3.1	Platform.....	65
191	C.3.2	Proper administrator.....	66
192	C.3.3	Attacker has limited physical access to product.....	66
193	C.3.4	Attacker has limited resources .....	66
194	C.4	Threats and security analysis .....	66
195	C.4.1	General66	
196	C.4.2	Security analysis methodology .....	66
197	C.4.3	TH-UEVU: Unknown exploitable vulnerabilities.....	66
198	C.4.4	TH-KEVU: Known exploitable vulnerabilities.....	67
199	C.4.5	TH-UEAC: Unauthorised endpoint access.....	67
200	C.4.6	TH-RDOS: Denial of service on remote data processing.....	68
201	C.4.7	TH-MITM: Machine-in-the-middle .....	68
202	C.4.8	TH-LEAK: Sensitive data leaks.....	69
203	C.4.9	TH-PLNS: Transmitting sensitive data in the clear in a single endpoint VPN .....	69
204	C.4.10	TH-PLNM: Transmitting sensitive data in the clear in multi-endpoint VPN.....	70
205	C.4.11	TH-UNAA: Unauthorised authentication .....	70
206	C.4.12	TH-LDEL: Attacker removes evidence of compromise.....	71
207	C.4.13	TH-CNFS: Access to assets via configuration errors in single endpoint VPN .....	71
208	C.4.14	TH-CNFM: Access to assets via configuration errors in a multi-endpoint VPN .....	72
209	C.4.15	TH-META: Compromise of Personal Data due to metadata and traffic analysis .....	72
210	C.4.16	TH-RCOM: RDPS compromise and isolation .....	73
211	C.4.17	TH-USED: Access to data via access to used product.....	73
212	C.4.18	TH-CPER: Compromise of Personal Data stored or transmitted by the product.....	74
213	C.5	Mapping of use cases to risk factors and security profiles.....	75
214	C.6	Security profiles.....	75
215	C.6.1	General75	
216	C.6.2	Mapping of security profiles to risk factors .....	75
217	Annex D (informative):	Risk evaluation guidance.....	76
218	D.1	Explanation of Risk Modelling Approach .....	76
219	D.2	Mapping of risks to requirements .....	77
220	D.3	Risk acceptance criteria .....	77
221	D.4	Risks not treated by the requirements .....	77
222	Annex G:	Guidelines on the implementation of the present document (informative):.....	78
223	Annex K:	Cryptography (Normative).....	79
224	K.1.1	Requirement.....	79
225	K.2	Crypto agility .....	79
226	K.2.1	Requirement.....	79
227	Annex R:	Remote Data Processing Solutions (Normative).....	81
228	Annex S:	Secure Updates (Normative) .....	82
229	Annex X:	Product specific state of the art cryptography (Normative).....	83
230	X.1	State of the Art Cryptography (CRY-SOTA-unlisted) .....	83
231	X.2	Symmetric atomic primitives.....	83

232	X.2.1 Block ciphers .....	83
233	X.2.2 Stream ciphers.....	83
234	X.2.3 Hash Functions .....	83
235	X.3 Symmetric constructions.....	83
236	X.3.1 Confidentiality modes of operation: encryption/decryption modes .....	83
237	X.3.2 Specific confidentiality modes: disk encryption .....	83
238	X.3.3 Integrity modes: message authentication codes .....	83
239	X.3.4 Symmetric entity authentication schemes.....	83
240	X.3.5 Authenticated encryption.....	84
241	X.3.6 Key protection.....	84
242	X.3.7 Key derivation functions.....	84
243	X.3.8 Password protection/password hashing mechanisms.....	84
244	X.3.9 Key combiners.....	84
245	X.4 Asymmetric atomic primitives.....	84
246	X.4.1 RSA/Integer factorization .....	84
247	X.4.2 Discrete logarithm in finite fields .....	84
248	X.4.3 Discrete logarithm in elliptic curves .....	84
249	X.4.4 Learning with errors in (structured) lattices.....	85
250	X.4.5 Hash function preimage resistance .....	85
251	X.4.6 Other intractable problems.....	85
252	X.5 Asymmetric constructions .....	85
253	X.5.1 Asymmetric encryption scheme.....	85
254	X.5.2 Digital signature.....	85
255	X.5.3 Asymmetric entity authentication schemes.....	85
256	X.5.4 Key establishment and key encapsulation.....	85
257	X.6 Cryptographic Industry Standards .....	85
258	History .....	86
259		
260		

## 261 Intellectual Property Rights

### 262 Essential patents

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

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

### 272 Trademarks

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

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

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

## 285 Foreword

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

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

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

### 298 *Transposition table*

299 *The Harmonised Standard shall have appropriate transposition periods specified. A Harmonised Standard confers*  
 300 *presumption of conformity when it has been published in the Official Journal of the European Union (OJEU) and*  
 301 *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

302

---

## 303 Modal verbs terminology

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

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

---

## 308 Executive summary

309 The purpose of this document is to provide essential cybersecurity requirements of a Virtual Private Network product  
310 intending to be placed on the European Union market.

---

## 311 Introduction

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

313 *More text to be added here. See ec02599f87e61677115439eb485b03619e9ffcad for some aggressive deletions.*

314

# 1 Scope

The present document specifies vulnerability handling activities, technical requirements and corresponding assessment criteria for Virtual Private Networks 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 "NN". 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]; and
- are only covered within the product context described in clause 4.

The present document specifies technical characteristics and methods of assessment for:

1. Software that operates as a VPN end-point
2. Software that operates as a node within a mesh VPN network
3. Remote data processing and associated software used for such VPN products

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](#).

## 2 References

### 2.1 Normative references

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

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

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

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

- |     |     |   |
|-----|-----|---|
| 340 | [1] | ENISA Report 1747792503: " <a href="#">European Cybersecurity Certification Group Sub-group on Cryptography Agreed Cryptographic Mechanisms</a> - version 2 - April 2025    |
| 342 | [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] |

### 2.2 Informative references

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

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

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

- |     |       |   |
|-----|-------|---|
| 352 | [i.1] | Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) <a href="https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng">https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng</a> |
|-----|-------|---|

- 356 [i.2] Commission Implementing Regulation (EU) 2025/2392 of 28 November 2025 on the technical  
357 description of the categories of important and critical products with digital elements pursuant to  
358 Regulation (EU) 2024/2847 of the European Parliament and of the Council. [https://eur-  
359 lex.europa.eu/eli/reg\\_impl/2025/2392/oj](https://eur-lex.europa.eu/eli/reg_impl/2025/2392/oj)
- 360 [i.3] [Standardisation request M/606 - C\(2025\)618](#): "Commission Implementing decision of 3.2.2025  
361 on a standardisation request to the European Committee for Standardisation (CEN), the European  
362 Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications  
363 Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU)  
364 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal  
365 cybersecurity requirements for products with digital elements and amending Regulations (EU) No  
366 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".
- 367 [i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary"  
368 (Version and date to be added upon its publication by CEN CENELEC)
- 369 [i.5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on  
370 ENISA (the European Union Agency for Cybersecurity) and on information and communications  
371 technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity  
372 Act). <https://eur-lex.europa.eu/eli/reg/2019/881>
- 373 [i.6] ETSI EN 303 645 (v3.1.3 2024-09): "Cyber Security for Consumer Internet of Things: Baseline  
374 Requirements".  
375 [https://www.etsi.org/deliver/etsi\\_en/303600\\_303699/303645/03.01.03\\_60/en\\_303645v030103p.pdf](https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf)  
376 [f](#)
- 377 [i.7] ETSI TC 103 701 (v2.1.1 2025-05) "Cyber Security for Consumer Internet of Things:  
378 Conformance Assessment of Baseline Requirements".  
379 [https://www.etsi.org/deliver/etsi\\_ts/103700\\_103799/103701/02.01.01\\_60/ts\\_103701v020101p.pdf](https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/02.01.01_60/ts_103701v020101p.pdf)
- 380 [i.8] CEN-CENELEC 18031 series (2024): "Common security requirements for radio equipment".
- 381 [i.9] IEEE-ITSO 6100 (1.0.0): "Uptane Standard for Design and Implementation".  
382 <https://uptane.org/papers/ieee-isto-6100.1.0.0.uptane-standard.html>
- 383 [i.10] ITU-T x.509: "Public-key and attribute certificate frameworks". [https://www.itu.int/rec/T-REC-  
384 X.509/en](https://www.itu.int/rec/T-REC-X.509/en)
- 385 [i.11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the  
386 protection of natural persons with regard to the processing of personal data and on the free  
387 movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)  
388 [https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng#art\\_4](https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng#art_4)
- 389 [i.12] ETSI TS 104 103: "Cyber Security (CYBER); Encrypted Traffic Integration (ETI); Problem  
390 Statement review and requirements definition".  
391 [https://www.etsi.org/deliver/etsi\\_ts/104100\\_104199/104103/01.01.01\\_60/ts\\_104103v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/104100_104199/104103/01.01.01_60/ts_104103v010101p.pdf)

---

## 3 Definition of terms, symbols and abbreviations

### 3.1 Terms

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

#### 396 **cloud**

397 data centre or collection of data centres operated entirely by a third party which rents out space and time on their  
398 equipment, as well as providing services for managing infrastructure from outside networks

#### 399 **consumer**

400 natural person who acts for purposes which are outside that person's trade, business, craft or profession

- 401 **cybersecurity**
- 402 cybersecurity as defined in Article 2, point (1), of Regulation (EU) 2019/881 [i.5]
- 403 **end-point**
- 404 device that is connected to a virtual private network and serves as an entry point for packets destined for that network
- 405 **exit node**
- 406 VPN server software and associated hardware which routes packets to and from their intended destination
- 407 **hardware**
- 408 physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data
- 409 **indirect connection**
- 410 connection to a device or network, which does not take place directly but rather as part of a larger system that is directly
- 411 connectable to such a device or network
- 412 **intended purpose**
- 413 "use for which a product with digital elements is intended by the manufacturer, including the specific context and
- 414 conditions of use, as specified in the information supplied by the manufacturer in the instructions for use, promotional
- 415 or sales materials and statements, as well as in the technical documentation;"
- 416 NOTE: An intended purposes is what is specified in the information supplied by the manufacturer in the
- 417 instructions for use, promotional or sales materials and statements, as well as in the technical
- 418 documentation.
- 419 **logical connection**
- 420 virtual representation of a data connection implemented through a software interface
- 421 **physical connection**
- 422 connection between electronic information systems or components implemented using physical means, including
- 423 through electrical, optical or mechanical interfaces, wires or radio waves
- 424 **Personal Data**
- 425 personal data as defined by (EU) 2016/679 General Data Protection Regulation [i.11]
- 426 **product with digital elements**
- 427 software or hardware product and its remote data processing solutions (including software or hardware components
- 428 being placed on the market separately)
- 429 **remote data processing**
- 430 "data processing at a distance for which the software is designed and developed by the manufacturer, or under the
- 431 responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from
- 432 performing one of its functions."
- 433 **software**
- 434 part of an electronic information system which consists of computer code
- 435 **software bill of materials**
- 436 formal record containing details and supply chain relationships of components included in the software elements of a
- 437 product with digital elements
- 438 **system configuration**
- 439 set of settings that a VPN client may modify to establish, maintain, or terminate a VPN connection

440 NOTE: A complete system configuration can include, but is not limited to, routing tables, DNS configuration,  
441 firewall rules, network interfaces, NAT settings and proxy settings.

#### 442 **virtual private network**

443 "Products with digital elements that establish an encrypted logical tunnel that is constructed from the system resources  
444 of a physical or virtual network."

445 NOTE: This includes cases where that product provides access from a restricted-use logical computer network to  
446 the public internet.

## 447 **3.2 Symbols**

448 There are no symbols requiring definition used in the present document.

## 449 **3.3 Abbreviations**

450 For the purposes of the present document, the following abbreviations apply:

451	CRA	Cyber Resilience Act
452	DNS	Domain Name Server
453	EDR	Endpoint Detection and Response
454	IAM	Identity and Access Management
455	MITM	Machine-In-The-Middle
456	OS	Operating System
457	OT	Operational Technology
458	RDPS	Remote Data Processing Solution
459	TLS	Transport Layer Security
460	TUF	The Update Framework
461	UC	Use Case
462	UI	User Interface
463	VPN	Virtual Private Network

---

## 464 **4 Product context**

### 465 **4.0 Introduction**

#### 466 **4.1 Product Functions**

467 The VPN product is a collection of software running on different devices, contextually referred to as nodes. Each  
468 software element may have a different set of functionality and may be more or less trusted than other elements. How the  
469 functionality and trust are distributed vary according to the architecture and use case of the VPN. For example, a VPN  
470 intended to protect the user of an endpoint node from surveillance would prefer an architecture that did not trust any  
471 node not controlled by the end user.

472 Potential functions include:

- 473 • Authenticating client connections
- 474 • Hide the contents of traffic sent through the tunnel
- 475 • Determining to which exit nodes a clients may direct traffic towards
- 476 • Establishing a tunnel between devices and exit nodes
- 477 • Obfuscating the source or destination address of traffic sent through the tunnel
- 478 • Routing restricted-use network traffic in or out of specific nodes

479 Roles of nodes in VPNs (a node can have some or all):

- 480 • Authorisation: grant nodes access to the restricted use network

- 481 • Encryption: encrypt traffic within the confines of the restricted use network
- 482 • Edge: uses a public network to communicate with the restricted use network
- 483 • Gateway: provides link between public network and restricted use network
- 484 • Router: forward traffic between nodes in the restricted use network
- 485 • Filter: select which traffic may transit this node in the restricted use network
- 486 • Relays: assist nodes in connecting to the restricted use network

487 During reasonably foreseeable use, VPN nodes may:

- 488 • Authorise other nodes to use the restricted use network
- 489 • Request authorisation to use the restricted network
- 490 • Serve configuration information
- 491 • Update their configuration information
- 492 • Assist nodes in connecting to the restricted use network
- 493 • Send traffic between nodes on the restricted use network
- 494 • Send traffic from the restricted use network to the public network
- 495 • Send traffic from the public network to the restricted use network
- 496 • Filter traffic transiting a node according to complex rules
- 497 • Leave the restricted network
- 498 • Revoke the access of a node to the restricted use network
- 499 • Validate the payload prior to its encryption in VPN [i.12]

## 500 4.3 Product architecture

### 501 4.3.1 Product overview

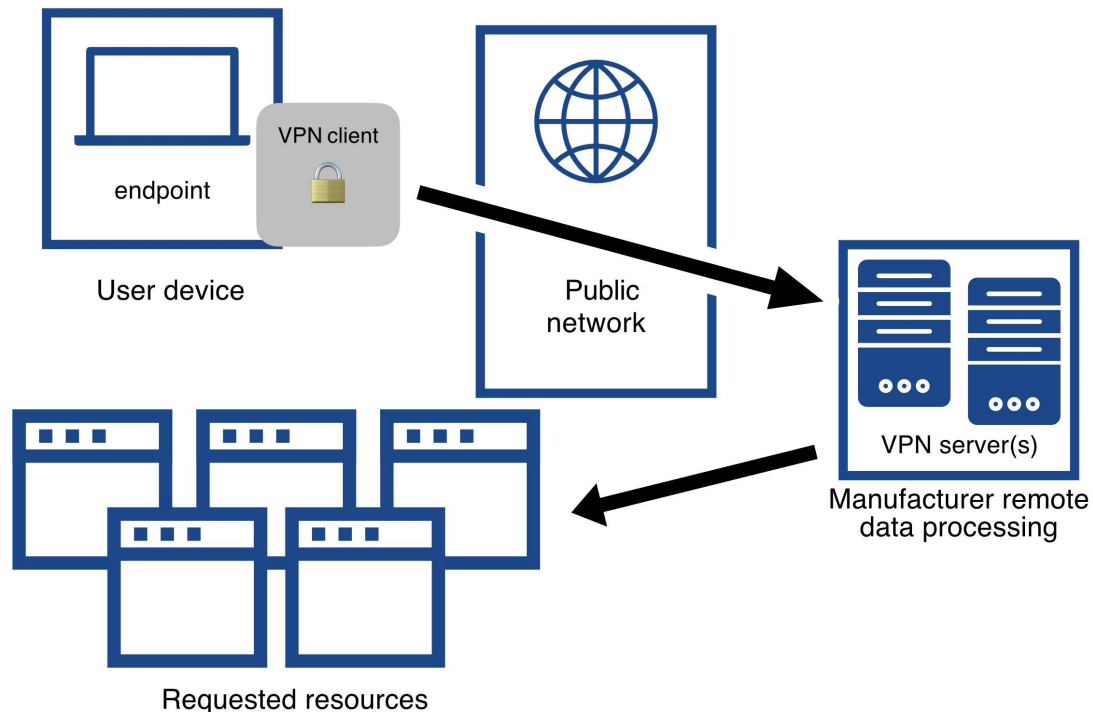
502 As a complete product, a Virtual Private Network includes, at minimum, VPN software capable of establishing a secure  
503 encrypted tunnel between two or more devices.

504 In consumer deployments, the most common state of the art implementation is a product that provides a secure tunnel to  
505 one or more servers—usually managed by the manufacturer as "exit nodes"—which then route traffic to its originally  
506 intended destination, typically on a public network like the Internet.

507 In enterprise wide area deployments, a common state of the art implementation is a product with digital elements that  
508 provides a secure overlay network to one or more servers that enable routing of traffic between remote restricted-use  
509 enterprise networks.

510 The product consists of any client software installed on a user device as well as any remote data processing on  
511 manufacturer infrastructure required for the product to function as expected.

512 Some VPN products also provide management capabilities to network administrators: user and group management,  
513 access control, logging and monitoring.



514

515 **Figure 4.3.1-1: A diagram illustrating an offsite device using a VPN client to encrypt traffic and send it**  
 516 **through a public network, to a VPN server which decrypts the traffic**

### 517 4.3.2 VPN client

518 For the purpose of the current document, a VPN client is a software application responsible for connecting a single  
 519 end-point (such as a computing device or home router) to servers operating as exit nodes. A VPN client typically uses  
 520 authentication credentials provided by the manufacturer or administrator and input by the user to establish secure  
 521 tunnel(s) to an aforementioned exit node running VPN server software.

522 After establishing a tunnel, the VPN client changes configuration of the host device operating system to facilitate  
 523 connections to the private network—this can include changes to DNS configuration, firewall rules, routing table, etc.  
 524 This configuration is tailored to the end-user, and may be based on a combination of local user or administrator  
 525 preferences and policies configured by the VPN manufacturer. A VPN client could have an option to perform traffic  
 526 validation prior to sending the data through the established secure tunnel [i.12].

### 527 4.3.3 VPN server, VPN gateway

528 A VPN server is responsible for maintaining tunnels between VPN clients and the traffic destinations they are  
 529 requesting.

## 530 4.4 Operational Environment

### 531 4.X.X General description

#### 532 4.4.1 Physical/Hardware environment

533 The physical hardware the VPN product is using may be:

- 534 • In a secure professionally managed environment
- 535 • In a private home

- 536
- In a public area

## 537 4.4.2 Logical/Software environment

538 VPNs can be expected to operate in a network environment alongside other Important products such as Identity and  
539 Access Management Systems, Network Interfaces, Routers, Firewalls, and SIEM systems. Manufacturers are expected  
540 to harden VPN attack surfaces against potential attack vectors from compromised PwDEs, but in particular those  
541 considered Important and Critical. See clause 4.5 for further information about the relationship between VPNs and  
542 related software.

543 A VPN requires an existing physical or virtual network whose resources it can use. The underlying network provides  
544 the functions necessary to connect to at least one node of the VPN.

545 Functions the underlying network provides:

- 546
- Physical equipment capable of transmitting network traffic
- 547
- Routing/forwarding of network traffic

548 A VPN product runs on a node in the context of an operating system, as an application, a library, a service, a driver, a  
549 kernel service, or a combination thereof. The operating system may provide:

- 550
- Network stack
- 551
- Virtual or physical network interfaces
- 552
- Network configuration
- 553
- DNS and other network services
- 554
- Certificate authority services
- 555
- Encryption
- 556
- Application support
- 557
- Packet filtering
- 558
- Denial of service protection
- 559
- Software installation and update
- 560
- Payload traffic validation [i.12]

561 VPN products often include or are used in concert with:

- 562
- Network management systems
- 563
- Security information and event monitoring
- 564
- Distributed log collection and monitoring
- 565
- Firewalls

## 566 4.4.4 Connectivity aspects

## 567 4.5 Distribution of Security Functions

### 568 4.5.1 Cybersecurity function distribution overview

569 This clause describes the two-way relationship where the VPN product both delegates risks and provides cybersecurity  
570 functionalities to other components in its ecosystem.

571 The cybersecurity of a VPN product is dependent on a chain of trust that spans across multiple components in its  
 572 operational environment. Consequently, the VPN product delegates certain risks to other components while offering  
 573 cybersecurity functionalities that mitigate different risks for those same components.

## 574 4.5.2 Cybersecurity Functionalities Offered to Integrated Components

575 The VPN product offers the following cybersecurity functionalities to other components in its operational environment:

- 576 • **Secure Data Transport:** The primary function of a VPN is to create a secure, encrypted tunnel over an  
 577 untrusted network. This functionality protects all network traffic originating from the client device or network  
 578 from eavesdropping and other network-based attacks.
- 579 • **Controlled Network Access:** The VPN client acts as a cybersecurity gatekeeper for the remote network. This  
 580 functionality protects the remote network by only allowing authenticated and authorized traffic to pass  
 581 through.

## 582 4.5.3 Cybersecurity functions required from the environment

583 The following risks are delegated by the VPN product to other components within its operational environment:

- 584 • **Operating System stability and Runtime Environment robustness:** A VPN product relies on a secure and  
 585 stable underlying operating system (OS) to function. The risks associated with OS vulnerabilities or a  
 586 compromised runtime environment are delegated to the OS.
- 587 • **Hardware Integrity:** The VPN product depends on the integrity of the physical hardware for the  
 588 confidentiality of cryptographic keys and data processing. Risks of physical tampering or hardware-based  
 589 attacks are delegated to the hardware manufacturer.
- 590 • **Identity and Authentication:** The VPN product delegates the risks associated with user credential  
 591 management to a trusted Identity and Access Management (IAM) system. It relies on this external component  
 592 for secure authentication and authorisation of users.

## 593 4.6 Users

- 594 • general public
- 595 • children
- 596 • journalists
- 597 • small business workers
- 598 • gamers
- 599 • students
- 600 • remote enterprise workers
- 601 • enterprise network and IT professionals

## 602 4.7 Use cases

603 This list of use cases is an informative resource to the manufacturer to simplify choosing a set of cybersecurity  
 604 requirements. It is not an exhaustive list, and deployments may cross over more than one use.

605 See [i.3] for formal definitions of micro, small, and medium-sized enterprises.

- 606 • **UC-1 Individual consumer**
  - 607 ○ Client installed on personal devices like mobile phone, portable or desktop computer
  - 608 ○ Client communicates with exit nodes managed by manufacturer
  - 609 ○ Securing traffic on untrusted access networks

- 610
  - User may lack advanced security knowledge
- 611
  - Does not connect endpoints with other endpoints directly
- 612
  - **UC-2** Privacy conscious household
- 613
  - All VPN infrastructure owned, rented, or managed by the user
- 614
  - Client installed on router or other network level
- 615
  - Obfuscating traffic and IP to avoid tracking by ISPs, data brokers
- 616
  - Does not connect endpoints with other endpoints directly
- 617
  - **UC-3** Journalist, activist, legal professionals
- 618
  - At high risk of surveillance
- 619
  - Actively circumventing observation from competitors, hackers, opponents, and unsanctioned state
- 620
  - actors
- 621
  - Does not connect endpoints with other endpoints directly
- 622
  - **UC-4** Small enterprise, small not-for-profit organisation
- 623
  - Limited or no full-time IT/network administration
- 624
  - Seeking secure connections primarily to SaaS products
- 625
  - Requires managed service for configuration and maintenance
- 626
  - May connect endpoints with other endpoints directly
- 627
  - Not critical for core business operations
- 628
  - **UC-5** Large enterprise
- 629
  - Full-time IT/network administration
- 630
  - Connects many endpoints to private network with many hosts
- 631
  - Requires managed service for configuration and maintenance
- 632
  - Connects endpoints with other endpoints directly
- 633
  - Critical for business operations
- 634
  - Needs to inspect traffic extensively for security
- 635
  - **UC-6** Enterprise with independent VPN infrastructure
- 636
  - All enterprise users with limited technical knowledge
- 637
  - Desires partial or full time remote access to enterprise network
- 638
  - Accesses one or some remote networks via enterprise gateway
- 639
  - Configuration managed by administrators, pushed via gateway and/or third party solution
- 640
  - Device managed by administrators, including VPN client lifecycle (install, update, etc....), via
- 641
  - dedicated tools
- 642
  - Most of security is managed by other components (gateway for network, local EDR for endpoint
- 643
  - security, ....)
- 644
  - Does not see VPN as critical for core business operations
- 645
  - **UC-7** Mesh Network

- 646 ○ Client installed on various devices, such as mobile phones, laptops, desktop computers, servers or
- 647 network devices
- 648 ○ Connecting multiple endpoint traffic over untrusted access networks
- 649 ○ Administrating user possesses some security knowledge
- 650 ○ Does connect endpoints with other endpoints directly

---

## 651 5 Technical requirements for the Products

### 652 5.1 Notes on the structure of requirements

653 **IMPORTANT:** Not all requirements are necessary for all products. The mapping tables at the end of each requirement  
 654 shows which risk factors and use cases determine which requirements are necessary for the product.

655 **See Annex C for more information.**

656 The most important quality of a cybersecurity requirement is that it should ideally be objectively testable on an instance  
 657 of the product. If it can't be tested on the product itself, it is a documentation requirement, in which the manufacturer  
 658 documents the steps they took to implement the requirement (such as configuration files or written policies used by  
 659 employees).

660 The present document makes the following assumptions regarding requirements and enforcement:

- 661 • Manufacturers are already required to provide the ability to enable testing and collect output on the product as  
 662 placed on the market, and will supply instructions for enabling and collecting test data.
- 663 • The MSA can and will request source code if desired.

664 Mitigations are how a cybersecurity requirement can be satisfied. Mitigations should be tailored to the use case and take  
 665 into account the user's sophistication and the operational environment.

666 Some risks may be transferred partially or fully to other components of the system or the user of the product. When that  
 667 is the case, mitigations that transfer the risk will be included as an option to fulfill a cybersecurity requirement,  
 668 depending on the use case and risk factors.

### 669 5.2 Technical cybersecurity requirements specifications

#### 670 5.2.1 General

671 This clause is a list of cybersecurity requirements necessary to satisfy essential cybersecurity requirements as described  
 672 in Annex I Part I of the EU Cyber Resilience Act. Each cybersecurity requirement can be satisfied by one or more  
 673 potential mitigations. A control may or may not be required to mitigate risks of an individual use case. **NOT ALL**  
 674 **MITIGATIONS ARE NECESSARY FOR ALL USE CASES.** See clause 5.3 for the mappings of security profiles to  
 675 mitigations and Annex C for additional information.

#### 676 5.2.2 TR-NKEV: No known exploitable vulnerabilities at first use

##### 677 5.2.2.1 Requirement

678 Recognizing that there may be vulnerabilities discovered between the time that a product is placed on the market and  
 679 the time of that product's first use, and that the product should be free from known exploitable vulnerabilities both when  
 680 first made available and when first used by a consumer, the product shall be able to be updated at the time of first use to  
 681 address known exploitable vulnerabilities which were discovered after the product's placement on the market and before  
 682 first use.

683 **Guidance:** From a practical standpoint, a known exploitable vulnerability is a flaw that has the potential to be  
 684 effectively used by an adversary under practical operational conditions, particularly those for which there is reliable  
 685 evidence of active exploitation in the wild by malicious actors and/or is listed on trusted vulnerabilities databases, such  
 686 as the EUVD (<https://euvd.enisa.europa.eu/>).

### 687 5.2.2.2 MI-KEVD: Documentation for secure update before or during first use

688 The product shall be accompanied by documentation describing how the product can be securely updated, including  
689 how to update the product prior to, or as part of, first use.

- 690 • Reference: TR-NKEV
- 691 • Applicability: The product has software or firmware update capability
- 692 • Objective: Prevent exploitation of known exploitable vulnerabilities at first use
- 693 • Preparation: Examine public or private vulnerability information sources and select a fixed vulnerability for  
694 testing. Filter candidates to ensure they specifically affect the platform, architecture, or software components  
695 used by the product. Then, prioritize those candidates based on the existence of publicly available exploit code  
696 (e.g., Proof of Concept), evidence of active exploitation in the wild, the severity of the vulnerability, and the  
697 potential impact its exploitation would have on the product.
- 698 • Activities: On a new product, carry out the initial secure update, scan the product to see if a recently fixed  
699 vulnerability has been fixed on the product, and examine the documentation for the required info
- 700 • Verdict: The secure update completes successfully, the most recently fixed vulnerability is fixed, and the  
701 documentation includes all the required information => PASS, otherwise FAIL
- 702 • Evidence: Documentation of vulnerability handling, documentation of how to securely update the product, the  
703 report for the selected vulnerability, description of how to scan for the vulnerability, log of vulnerability scan  
704 results

### 705 5.2.2.3 MI-KEVA: Automatic secure update before or during first use

706 The product shall implement automatic secure update before or during first use.

- 707 • Reference: TR-NKEV
- 708 • Applicability: The product has software or firmware update capability
- 709 • Objective: Prevent exploitation of known exploitable vulnerabilities at first use
- 710 • Preparation: Examine public or private vulnerability information sources and select a recently fixed  
711 vulnerability. Filter candidates to ensure they specifically affect the platform, architecture, or software  
712 components used by the product. Then, prioritize those candidates based on the existence of publicly available  
713 exploit code (e.g., Proof of Concept), evidence of active exploitation in the wild, the severity of the  
714 vulnerability, and the potential impact its exploitation would have on the product.
- 715 • Activities: Follow the instructions to install and use the product for the first time, scan the product to see if a  
716 recently fixed vulnerability has been fixed on the product, and examine the documentation for the required info
- 717 • Verdict: The secure update completes successfully, the most recently fixed vulnerability is fixed, and the  
718 documentation includes all the required information => PASS, otherwise FAIL
- 719 • Evidence: Documentation of vulnerability handling, documentation of how to securely update the product, the  
720 report for the selected vulnerability, description of how to scan for the vulnerability, log of vulnerability scan  
721 results

### 722 5.2.2.3a MI-KEVE: Automatic secure update via administrator action before or during first 723 use

724 The product shall implement secure update by via administrator actions before or during first use.

- 725 • Reference: TR-NKEV
- 726 • Applicability: The product has software or firmware update capability and is administered by a professional  
727 network administrator.
- 728 • Objective: Prevent exploitation of known exploitable vulnerabilities at first use

- 729 • Preparation: Examine public or private vulnerability information sources and select a fixed vulnerability. Filter  
730 candidates to ensure they specifically affect the platform, architecture, or software components used by the  
731 product. Then, prioritize those candidates based on the existence of publicly available exploit code (e.g., Proof  
732 of Concept), evidence of active exploitation in the wild, the severity of the vulnerability, and the potential  
733 impact its exploitation would have on the product.
- 734 • Activities: Follow the instructions for the administrator to receive and install the latest release, use the product  
735 for the first time, scan the product to see if a recently fixed vulnerability has been fixed on the product, and  
736 examine the documentation for the required info
- 737 • Verdict: The secure update completes successfully, the most recently fixed vulnerability is fixed, and the  
738 documentation includes all the required information => PASS, otherwise FAIL
- 739 • Evidence: Documentation of vulnerability handling, documentation of how to securely update the product, the  
740 report for the selected vulnerability, description of how to scan for the vulnerability, log of vulnerability scan  
741 results

#### 742 5.2.2.5 MI-KEVT: Testing for known exploitable vulnerabilities

743 In accordance with the requirement to apply effective and regular tests to the security of the product, the product shall  
744 be tested to demonstrate the absence or mitigation of known exploitable vulnerabilities. Testing shall specifically target  
745 known exploitable vulnerabilities that impact the product's architecture, platform, and the specific software components  
746 identified in the product's Software Bill of Materials (SBOM).

747 To demonstrate compliance, the manufacturer may rely on manual security testing (e.g., penetration testing), automated  
748 vulnerability scanners, or a combination of both, depending on what is most comprehensive and technically feasible for  
749 the product's technology stack.

750 The product shall be considered conformant with this requirement if it:

- 751 1. has no known exploitable vulnerabilities discovered during testing,
  - 752 2. has discoverable known exploitable vulnerabilities whose age is consistent with the specification of how long  
753 vulnerabilities may go unfixed after public disclosure, as described in the vulnerability handling procedure for  
754 the product, or
  - 755 3. for each detected vulnerability, has publicly available documentation explaining how the risk has been  
756 mitigated.
- 757 • Reference: TR-NKEV
  - 758 • Objective: Prevent exploitation of known exploitable vulnerabilities
  - 759 • Preparation: Using the product's SBOM and relevant publicly accessible vulnerability databases (e.g. [GCVE](#),  
760 [EUVD](#)), compile a list of target components and potential known exploitable vulnerabilities. Select the  
761 appropriate testing methodology (e.g., the most comprehensive automated scanners available, or a manual  
762 penetration test plan) to verify the mitigation of these vulnerabilities.
  - 763 • Activities: On a new product, carry out a security update, run the tests, and compare the results with the  
764 generated list of known exploitable vulnerabilities.
  - 765 • Verdict: No vulnerabilities found, or all reported vulnerabilities satisfy either the age or mitigation requirement  
766 => PASS, otherwise FAIL
  - 767 • Evidence: Documented vulnerability handling policy, product SBOM, list of testing tools used or manual test  
768 plan, test reports/scan results, correlation of discovered vulnerabilities with documentation of mitigation or age  
769 of vulnerability.

### 770 5.2.3 TR-SSDD: Secure software design and development

#### 771 5.2.3.1 Requirement

772 Software shall be designed and developed in a secure manner.

773 **Guidance:** In alignment with the Cyber Resilience Act Annex I Part I (1), this section addresses overarching risks and  
 774 mitigations regarding the secure design and development of the product that are not specifically treated by other  
 775 categorical essential requirements (such as confidentiality, access control, or secure updates). The requirements herein  
 776 ensure the final product itself embodies security by design.

777 NOTE: Security profiles (as described in Annex B) determine which of these controls can be utilised to mitigate  
 778 the threat. In particular, across all security profiles only one—at most—of the following three is called for  
 779 when applied to a single product: FZ95, BTIN, IMSL. See B.TK for more information.

### 780 5.2.3.2 MI-SSCA: Static source code analysis for memory errors

781 All cybersecurity-relevant parts of the product shall be checked for known code patterns that produce common memory  
 782 errors, such as:

- 783 • buffer overflow
- 784 • out-of-bounds
- 785 • use after free
- 786 • double free
- 787 • use of uninitialized variables
- 788 • dereference of invalid pointer

789 Any identified memory errors or suppression of warnings shall be documented with a rationale for why it does not  
 790 constitute an unacceptable risk.

- 791 • Reference: TR-SSDD
- 792 • Objective: Prevent unauthorized memory access
- 793 • Preparation: Determine the appropriate static source code analysis tool and the manner of running it to verify  
 794 the absence of the listed errors
- 795 • Activities: Review the source code for the product by running the selected source code analysis tool. Review  
 796 the documentation for any warnings or suppression of warnings.
- 797 • Verdict: The output of the source code analysis tool confirms the absence of the listed memory errors, or all  
 798 warnings and suppressions have convincing documentation for why they are an acceptable risk => PASS,  
 799 otherwise FAIL
- 800 • Evidence: The source code for the product, the output of the source code analysis tool, and the documentation  
 801 for any warnings or suppression of warnings.

### 802 5.2.3.3 MI-FZ95: Runtime code coverage checking with memory access error 803 detection

804 The product shall be checked for memory errors by running a tool that exercises the functions of the product in an  
 805 environment that permits measuring code coverage and detecting memory access errors. All memory errors detected  
 806 shall be documented with a rationale for why it does not constitute an unacceptable risk.

- 807 • Reference: TR-SSDD
- 808 • Objective: Prevent unauthorized memory access
- 809 • Preparation: None
- 810 • Activities: Run the tool while measuring code coverage and monitoring for memory access errors until 95%  
 811 code coverage has been reached
- 812 • Verdict: Code coverage was at least 95%, all reported memory errors are documented and justified => PASS,  
 813 otherwise FAIL

- 814       • Evidence: Logs of code coverage tool, memory error report, documentation of any memory errors

#### 815   5.2.3.4       MI-IMSL: Implement in a memory-safe language

816   The product shall be implemented in a memory-safe language. Any use of unsafe memory features shall be documented  
817   to explain why they are necessary and do not present a cybersecurity risk.

- 818       • Reference: TR-SSDD

- 819       • Objective: Prevent unauthorised memory access

- 820       • Preparation: None

- 821       • Activities: Review source code to determine its language and what exceptions to memory safety exist

- 822       • Verdict: Source code is in a memory-safe language and the documentation of all uses of unsafe memory  
823       features convincingly demonstrates that each one of them does not present a cybersecurity risk => PASS,  
824       otherwise FAIL

- 825       • Evidence: Source code, documentation of unsafe memory features

#### 826   5.2.3.5       MI-BTIN: Boundary testing of inputs that may cause memory errors

827   The input fields of the product that may produce memory errors shall be identified. The product shall be boundary  
828   tested for all such inputs while monitoring for memory errors. All memory errors detected shall be documented with a  
829   rationale for why it does not constitute an unacceptable risk.

- 830       • Reference: TR-SSDD

- 831       • Objective: Prevent unauthorized memory access

- 832       • Preparation: Identify input fields in the product that may produce memory errors

- 833       • Activities: Run a tool that tests the boundaries of the input values (minimum valid, maximum valid, minimum  
834       possible, maximum possible, off-by-one, etc.) while monitoring for memory errors

- 835       • Verdict: All boundary values tested and all memory errors detected are documented and justified => PASS,  
836       otherwise FAIL

- 837       • Evidence: Logs of boundary testing tool, memory error report, documentation of any memory errors

#### 838   5.2.3.6       MI-SCFS: Secure compilation flags

839   All cybersecurity-relevant software shall incorporate built-in exploit mitigation mechanisms appropriate to the target  
840   platform and language (e.g., Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP/NX), or  
841   Stack Canaries). Any exceptions to these mitigations shall be documented as to why they do not create an unacceptable  
842   risk.

- 843       • Applicability: Product implemented in a compiled language

- 844       • Reference: TR-SSDD

- 845       • Objective: Secure software design and development

- 846       • Preparation: Document the exploit mitigations technically relevant to the architecture of the target platform.

- 847       • Activities: Inspect the compiled executable binaries to verify the presence of the required exploit mitigations,  
848       and review documentation for exceptions

- 849       • Verdict: Binaries actively implement the appropriate exploit mitigations, and all exceptions are documented  
850       and justified => PASS, otherwise FAIL

- 851       • Evidence: Output of binary analysis tools demonstrating the presence of exploit mitigations, and  
852       documentation of exceptions

## 853 5.2.4 TR-SCUD: Secure updates

### 854 5.2.4.1 Requirement

855 The product shall be securely updatable.

### 856 5.2.4.2 MI-SUDC: Documentation of secure update

857 The product shall be accompanied by documentation of the secure update methods for any software in the product.

- 858 • Reference: TR-SCUD
- 859 • Objective: Prevent exploitation of known vulnerabilities
- 860 • Activities: Assess the documentation for completeness
- 861 • Verdict: Documentation describes secure update methods sufficiently for a third party to implement them =>  
862 PASS, otherwise FAIL
- 863 • Evidence: Documentation and analysis of completeness

### 864 5.2.4.3 MI-SUVP: Secure update via product

865 The product shall provide a method of securely updating any software in the product via the product itself.

- 866 • Applicability: All products that include a software update mechanism.
- 867 • Reference: TR-SCUD
- 868 • Objective: Prevent exploitation of known vulnerabilities
- 869 • Preparation: Prepare an update for each part of the product that can be updated with a different version number  
870 from the currently installed product version
- 871 • Activities: Check the versions of all parts of the product that can be updated, install the new update, and check  
872 the versions again
- 873 • Verdict: The second versions read are that of the new product update => PASS, otherwise FAIL
- 874 • Evidence: New update version numbers, and log of querying the product parts' versions, installing the update,  
875 and querying the versions again

### 876 5.2.4.4 MI-SUAP: Automatic secure update via product

877 The product shall provide a method of automatically securely updating any software in the product via the product itself  
878 with an option for the user or administrator to disable or defer automatic updates.

- 879 • Reference: TR-SCUD
- 880 • Objective: Prevent exploitation of known vulnerabilities
- 881 • Preparation: Prepare an update for each part of the product that can be updated with a different version number  
882 from the currently installed product version
- 883 • Activities: Check the versions of all parts of the product that can be updated, create the conditions that allow  
884 automatic secure update to occur. Then execute the same setup for all the tests:
  - 885 1. install the update, record the version again
  - 886 2. defer the update, wait the deferral period, relaunch the product, observe any update popups, install the  
887 update, record the version again
  - 888 3. disabling automatic updates, record the product version
- 889 • Verdict: If all the following verdicts conclude => PASS, otherwise FAIL

- 890 1. For the first test, the second versions read are that of the new product update
- 891 2. For the second test, after deferral of the update, the product reads the same product version. After the  
892 deferral period, the update is prompted again. Once installed, versions read are that of the new  
893 product update
- 894 3. For the third test with automatic updates disabled, the versions read are the same as the first versions
- 895 • Evidence: New update version numbers, and log of querying the product parts' versions, installing the update,  
896 and querying the versions again

#### 897 5.2.4.5 MI-SUOE: Secure update provided by operational environment

898 The technical documentation provided with the product shall document that the operational environment shall provide a  
899 method of securely updating the product.

- 900 • Reference: TR-SCUD
- 901 • Objective: Prevent exploitation of known vulnerabilities
- 902 • Activities: Assess the documentation provided with the product
- 903 • Verdict: Documentation describes requirements for the secure updates provided by the operational  
904 environment => PASS, otherwise FAIL
- 905 • Evidence: Documentation and analysis of completeness

#### 906 5.2.4.6 MI-SUAO: Automatic secure update provided by operational environment

907 The technical documentation provided with the product shall document that the operational environment shall provide a  
908 method of automatically securely updating the product with an option for the product to be configured to disable  
909 automatic updates.

- 910 • Reference: TR-SCUD
- 911 • Objective: Prevent exploitation of known vulnerabilities
- 912 • Activities: Assess the documentation provided with the product
- 913 • Verdict: Documentation describes requirements for automatic secure updates provided by the operational  
914 environment => PASS, otherwise FAIL
- 915 • Evidence: Documentation and analysis of completeness

#### 916 5.2.4.7 MI-SUCS: Updates are signed and verified before installation

917 **Editor's note:** The following secure update requirements are generic to all Important Class I products, and are expected  
918 to be published along with similar shared cybersecurity requirements in a separate standard. They are placed directly in  
919 this standard for comment and review.

920 Updates for the product are cryptographically signed. The product shall verify the signature before installation in order  
921 to mitigate the installation of tampered and/or modified updates.

- 922 • Reference: TR-SCUD
- 923 • Objective: Prevent the installation of modified updates.
- 924 • Activities: For each part of the product that can be updated, attempt installation of:
- 925 ○ an update with missing signature
- 926 ○ an update with an invalid signature
- 927 • Verdict: The installation fails and warns the user about an invalid signature and possible tampering => PASS,  
928 otherwise FAIL

- 929       • Evidence: New update version numbers, and installation log containing mention of a signature mismatch.

#### 930 5.2.4.8 MI-SUAU: Only authorized software updates

931 The product shall reject an update that does not match the expected cryptographic hash.

- 932       • Reference: TR-SCUD
- 933       • Objective: Secure updates
- 934       • Preparation: Create an update with an invalid hash
- 935       • Activities: Attempt to install the update
- 936       • Verdict: Update is not installed => PASS, otherwise FAIL
- 937       • Evidence: Update and invalid hash, error message, before and after comparison of any data that would have  
938       been altered if it had been installed

#### 939 5.2.4.9 MI-SUVH: Secure update has validly signed hash

940 The product shall reject a hash that is not validly signed by an authorized signing authority.

941 **Guidance:** The product needs a method of knowing what specific updates are valid for installation. Because of the  
942 requirement MI-SURP (rollback protection), the product must have a method of knowing also which previously-valid  
943 updates are no longer valid. A simple way of doing this is by providing the device with a metadata file listing all  
944 updates that are valid along with each update's hash, size, and name. The device downloads this metadata file upon each  
945 update check, verifies that it is signed by a valid signing key, and performs other necessary checks (such as checking  
946 expiry or replacement).

- 947       • Reference: TR-SCUD
- 948       • Objective: Secure updates
- 949       • Preparation: Create updates with signature signed by an untrusted key
- 950       • Activities: For each part of the product that can be updated, attempt installation of an update signed by an  
951       untrusted key
- 952       • Verdict: All updates are not installed => PASS, otherwise FAIL
- 953       • Evidence: Updates and invalid hashes and file sizes, error message, before and after comparison of any data  
954       that would have been altered if it had been installed

#### 955 5.2.4.10 MI-SURP: Invalidated update is rejected

956 The product shall reject an update file that has been indicated to no longer be valid, even if that update file was valid at  
957 some point in the past.

958 **Guidance:** This requirement should not be interpreted to mean that update systems should always have exactly one  
959 valid version, and prevent rollbacks to anything but the most current version. However, it is important that products  
960 have a way of determining whether a particular update, that was issued at some point in the past and was trusted at the  
961 instant it was issued, should still be trusted.

962 The exact parameters and criteria by which software releases are considered to be trusted are defined by the  
963 manufacturer, determined by the product, its cybersecurity needs, and its intended and reasonably foreseeable uses.  
964 Examples of when a software update might be considered to no longer be valid include:

- 965       • An old software release is determined to have a critical and remotely-exploitable vulnerability; if that version  
966       of software is installed and connected to a network, it is very likely to be compromised.
- 967       • An attacker manages to execute a targeted software supply chain attack, and releases a compromised version of  
968       a package.

- 969       • A product is used in a safety-critical context, and needs to constantly be updated to the latest released version  
 970       of its firmware to remain in contractual or regulatory compliance for its specific industrial context. The  
 971       manufacturer therefore repudiates/revokes all previous software versions as soon as they release a new one.

972       If the update system makes use of a signed metadata file as suggested in the guidance for MI-SUVH, revoking a  
 973       particular update is simply a matter of removing it from the metadata file, updating the metadata file's version number,  
 974       and signing the new version. The product can then download and check the metadata file from the repository.

- 975       • Reference: TR-SCUD
- 976       • Objective: Prevent "rollback attacks" by rejecting previously-valid packages that contain vulnerabilities
- 977       • Preparation: Create an update image that was formerly valid but has been revoked from the repository  
 978       metadata
- 979       • Activities: Attempt to install the revoked update
- 980       • Verdict: Update is not installed => PASS, otherwise FAIL
- 981       • Evidence: Revoked update image, error message, before and after comparison of any data that would have  
 982       been altered if it had been installed

983       NOTE: Multiple different versions of software that are *simultaneously* endorsed/trusted for installation do not  
 984       constitute a "rollback attack". This mitigation specifically applies to the scenario where the software  
 985       updater on the product/device can be tricked into trusting a software package that is *no longer* valid, or  
 986       tricked into thinking that an older software version is actually a new update.

#### 987   5.2.4.11       MI-SURC: Signing keys have strictly scoped usage

988       The key or keys authorized to sign Repository Metadata shall be keys restricted to this specific purpose. Update clients  
 989       shall verify that the key or keys that sign the Repository Metadata are keys authorized for that specific purpose.

990       **Guidance:** Signing software updates is a very sensitive role. As such, the software update system needs effective  
 991       controls to ensure that the key used to sign repository metadata is the key intended for that role. This can be  
 992       accomplished via specifying roles in root metadata as defined in Uptane/TUF (IEEE-ISTO 6100.1.00) [i.9], or can be  
 993       specified using a PKI system, for example via extended role attributes in an X.509 [i.10] software signing certificate.

- 994       • Reference: TR-SCUD
- 995       • Objective: Ensure keys are only used for their designated roles and prevent role confusion attacks
- 996       • Preparation: Create Repository Metadata signed with a valid key that is intended for a different role
- 997       • Activities: Send the incorrectly-signed Repository Metadata to the device during an update check
- 998       • Verdict: Update check fails and error is reported => PASS, otherwise FAIL
- 999       • Evidence: Error message, before and after comparison showing local metadata is not changed

#### 1000   5.2.4.12       MI-SUSR: Signing keys have not been revoked or otherwise marked 1001       untrusted

1002       The update client shall check for signing key revocation and any other cybersecurity-relevant changes to the chain of  
 1003       trust, each time it checks for an update.

1004       **Guidance:** If keys are compromised, it is critical that they are revoked as soon as possible, and that the revocation  
 1005       reaches each client of the update system. Therefore, the update system needs to check revocation information as part of  
 1006       the update check, and fail closed if revocation information is not available. Uptane/TUF checks would meet this  
 1007       requirement. If using X.509 CRLs, it is important to fail closed if the CRL cannot be fetched. OCSP stapling is possible  
 1008       here as well, but due care should be taken in designing the validity period of the OCSP response. An OCSP response  
 1009       with an extended validity period provides a long attack window in the case of compromised keys.

1010       Some possible reasons (non-exhaustive) the information in a signature envelope could be discovered to be invalid or  
 1011       insufficient for attesting the validity of the signed content at time of update check:

- 1012 • X.509 cert for one of the signing keys has expired
- 1013 • X.509 cert for one of the signing keys has been revoked by its issuing authority
- 1014 • Authority that issued the X.509 cert for one of the signing keys has been revoked
- 1015 • Signing key has been removed from the set of valid signing keys in TUF/Uptane root metadata
- 1016 • Reference: TR-SCUD
- 1017 • Objective: Ensure keys have not been revoked and are still valid, including their complete chain of trust
- 1018 • Preparation: Create Repository Metadata signed with a formerly valid key that has been revoked
- 1019 • Activities: Send the Repository Metadata signed with the revoked key to the device during an update check
- 1020 • Verdict: Update check fails and error is reported => PASS, otherwise FAIL
- 1021 • Evidence: Error message, before and after comparison showing local metadata is not changed

#### 1022 5.2.4.13 MI-SUMV: Reject update to current or previous version

1023 The product shall reject Repository Metadata if its version number is equal to or less than the highest version number  
1024 the update client has seen.

1025 NOTE: This requirement is about repository metadata. Repository metadata should never be permitted to roll  
1026 back; it merely communicates the attested validity of a set of software. Software itself can often be  
1027 permitted to roll back; see also the guidance on MI-SURP (The product shall reject an update file that has  
1028 been indicated to no longer be valid).

- 1029 • Reference: TR-SCUD
- 1030 • Objective: Prevent rollback attacks by rejecting older versions of Repository Metadata
- 1031 • Preparation: Have the device perform an update check to obtain the latest Repository Metadata, then prepare  
1032 an older version of Repository Metadata
- 1033 • Activities: Send the older version of Repository Metadata to the device during another update check
- 1034 • Verdict: Update check fails and error is reported => PASS, otherwise FAIL
- 1035 • Evidence: Error message, before and after comparison showing update metadata is not changed

#### 1036 5.2.4.14 MI-SUED: Updates not applied from expired sources

1037 Repository Metadata shall have an expiry date included in the signed portion of the metadata. The update client shall  
1038 verify that repository metadata is not expired before using it.

- 1039 • Reference: TR-SCUD
- 1040 • Objective: Prevent use of expired metadata that could enable rollback attacks
- 1041 • Preparation: Create expired Repository Metadata and configure the update server to provide it
- 1042 • Activities: Have the device perform an update check with the expired metadata
- 1043 • Verdict: Update check fails and error is reported => PASS, otherwise FAIL
- 1044 • Evidence: Error message, before and after comparison showing update metadata is not changed

1045 **5.2.5 TR-ROUT: VPN traffic routed only through VPN connection during**  
 1046 **VPN connection**

1047 **5.2.5.1 Requirement**

1048 From the moment the user activates the VPN connection until the user knowingly deactivates the VPN connection, no  
 1049 network traffic intended for the VPN connection shall exit the endpoint via anything other than the VPN connection,  
 1050 whether or not it is functioning.

1051 Out of scope for the following requirements are other software on the user's endpoint with elevated privileges, users  
 1052 with administrator privileges, as well as the operating system itself that could change relevant network configuration  
 1053 (network interfaces, routes, DNS) or circumvent the VPN tunnel due to elevated privileges.

1054 **5.2.5.2 MI-ROUT-1 VPN routing stays in effect until VPN connection deactivated**

1055 The product shall only report that the VPN connection is established after it has configured the system in such a way  
 1056 that all traffic intended to be routed through the VPN connection will only exit through the VPN connection until the  
 1057 user or administrator knowingly deactivates the VPN connection.

- 1058 • Reference: TR-ROUT
- 1059 • Objective: Prevent VPN traffic leaks
- 1060 • Preparation: None
- 1061 • Activities: Start the VPN connection, after it reports that it is connected, force the VPN connection to end in a  
 1062 way that does not allow it to execute any VPN connection shutdown tasks, then attempt to transmit data that  
 1063 should only go through the VPN connection
- 1064 • Verdict: No network traffic intended for the VPN exits the host
- 1065 • Evidence: Configuration of VPN client, method used to force connection to end without allowing shutdown  
 1066 tasks to run, network configuration, log of actions, error messages, packet capture with annotations

1067 **5.2.5.3 MI-ROUT-2 VPN routing stays in effect during network-level tunnel failure**

1068 The product shall ensure that when the connection to the VPN server is lost at the network level (e.g., due to firewall  
 1069 rules or network outage), no traffic intended for the VPN connection can exit the endpoint outside of the tunnel.

- 1070 • Reference: TR-ROUT
- 1071 • Objective: Prevent VPN traffic leaks during tunnel failure
- 1072 • Preparation: None
- 1073 • Activities: Start the VPN connection, after it reports that it is connected, induce a network-level tunnel failure  
 1074 by blocking traffic to the VPN server's IP address using a host-based firewall, then attempt to transmit data that  
 1075 should only go through the VPN connection.
- 1076 • Verdict: No network traffic intended for the VPN exits the host via a non-VPN interface
- 1077 • Evidence: Method used to induce tunnel failure, network configuration, log of actions, error messages, packet  
 1078 capture with annotations

1079 **5.2.5.4 MI-ROUT-3 Tunnel all traffic by default**

1080 The VPN client shall by default be configured to route all network traffic from the endpoint through the VPN  
 1081 connection. If the client offers a configuration that only tunnels traffic from specific applications (e.g., "split tunnelling"  
 1082 or "browser-only mode"), this shall not be the default configuration. Where the user or administrator is responsible for  
 1083 configuration of tunnel policy, the user must be clearly informed of its limitations before enabling it.

- 1084 • Reference: TR-ROUT
- 1085 • Objective: Prevent user confusion and unexpected traffic leaks from non-tunnelled applications

- 1086 • Preparation: Perform a factory reset or new installation of the VPN client.
- 1087 • Activities: Start the VPN connection using the default configuration. Generate traffic from multiple
- 1088 applications (e.g., a web browser and a separate command-line tool). Capture traffic on all interfaces.
- 1089 • Verdict: All traffic from all applications is routed through the VPN connection.
- 1090 • Evidence: Packet capture showing traffic from multiple applications going through the VPN interface.

## 1091 5.2.6 TR-CONF: VPN client preserves system configuration

### 1092 5.2.6.1 Requirement

1093 The establishment and ending of a VPN connection shall not result in functional changes to the system configuration  
1094 unless explicitly authorized by the user or administrator.

### 1095 5.2.6.2 MI-CONF-1 VPN client restores any system configuration it changes to its 1096 previous state after the VPN connection ends

1097 After the user or administrator knowingly deactivates the VPN connection, the VPN client shall restore any system  
1098 configuration it modified to its state prior to activating the VPN connection.

- 1099 • Reference: TR-CONF
- 1100 • Objective: Preserve integrity of system configuration
- 1101 • Preparation: List all items of system configuration that the VPN client may alter
- 1102 • Activities:
  - 1103 ○ For each item of system configuration that the VPN client may alter, configure the VPN in a way that
  - 1104 would alter that item.
  - 1105 ○ Collect the state of all system configuration the product may alter.
  - 1106 ○ Start the VPN connection. After it reports that it is connected, stop the VPN connection.
  - 1107 ○ Collect the system configuration again and compare with previous version.
- 1108 • Verdict: System configuration modified by VPN matches its state prior to VPN connection => PASS,  
1109 otherwise FAIL
- 1110 • Evidence: Collected system configuration, annotations of any configuration changes explaining why they aren't  
1111 functional, log messages from tests

### 1112 5.2.6.3 MI-CONF-2 VPN client provides a method to restore any system 1113 configuration it changes to its previous state

1114 The VPN client shall provide a user or administrator documentation to restore any system configuration it has changed  
1115 to a state that is functionally equivalent to the state it was in before the VPN connection began, regardless of whether a  
1116 previous VPN connection was able to complete connection shutdown tasks.

- 1117 • Reference: TR-CONF
- 1118 • Objective: Preserve integrity of system configuration
- 1119 • Preparation: List all items of system configuration that the VPN client may alter
- 1120 • Activities:
  - 1121 ○ For each item of system configuration that the VPN client may alter, configure the VPN in a way that
  - 1122 would alter that item.
  - 1123 ○ Collect the state of all system configuration the product may alter.

- 1124 ○ Start the VPN connection.
- 1125 ○ After the VPN reports that it is connected, force the VPN connection to end in a way that does not
- 1126 allow it to execute any VPN connection shutdown tasks.
- 1127 ○ Execute the method to restore system configuration.
- 1128 ○ Collect the system configuration again and compare with previous version.
- 1129 ● Verdict: All system configuration collected is functionally the same before and after the VPN connection starts
- 1130 and the system configuration restoration method completes => PASS, otherwise FAIL
- 1131 ● Evidence: Collected system configuration, annotations of any configuration changes explaining why they aren't
- 1132 functional, log messages from tests, method used to force connection to end without allowing shutdown tasks
- 1133 to run, method used to restore system configuration

#### 1134 5.2.6.4 MI-CONF-3 VPN client does not degrade system security

1135 The VPN client shall not reduce system security after the end of the VPN connection, even if normal connection  
1136 shutdown tasks have not completed.

1137 NOTE: This is a "fail-closed" requirement—if the VPN connection experiences an unexpected failure, it is better  
1138 to end with a more restricted/secure network configuration than the configuration before the VPN  
1139 connection started, than a less restricted network configuration.

- 1140 ● Reference: TR-CONF
- 1141 ● Objective: Preserve cybersecurity of system
- 1142 ● Preparation: List all items of system configuration that the VPN client may alter
- 1143 ● Activities:
  - 1144 ○ For each item of system configuration that the VPN client may alter, configure the VPN in a way that
  - 1145 would alter that item.
  - 1146 ○ Collect the state of all system configuration the product may alter.
  - 1147 ○ Start the VPN connection.
  - 1148 ○ After the VPN reports that it is connected, force the VPN connection to end in a way that does not
  - 1149 allow it to execute any VPN connection shutdown tasks.
  - 1150 ○ Collect the system configuration again and compare with previous version.
- 1151 ● Verdict: All system configuration collected is at least as secure/restricted as before the VPN connection started  
1152 => PASS, otherwise FAIL
- 1153 ● Evidence: Collected system configuration, annotations of any configuration changes explaining why they are  
1154 more restricted/secure, log messages from tests, method used to force connection to end without allowing  
1155 shutdown tasks to run

#### 1156 5.2.6.5 MI-CONF-4 VPN client shall not require unnecessary permissions

1157 Custom VPN clients shall not require permissions that they do not need.

1158 NOTE: The VPN product should be able to operate without a wide set of permissions—eg, a VPN does not  
1159 require access to files/folders (like ~/Downloads) nor would it need access to the local network.

- 1160 ● Reference: TR-CONF
- 1161 ● Objective: Operate on a least privilege principle
- 1162 ● Preparation: List all the permissions that may be granted to applications
- 1163 ● Activities:

- 1164 ○ Collect all the permissions that may be requested by the VPN.
- 1165 ○ For each permission, lookup the state after the product installation.
- 1166 ○ Start the VPN connection.
- 1167 ○ Collect the permission states again and compare with previous version.
- 1168 • Verdict: The VPN client did not request permissions beyond those necessary for its documented functionality  
1169 => PASS, otherwise FAIL.
- 1170 • Evidence: Collected permission states, annotations of any permission requests explaining why they are more  
1171 restricted/secure, log messages from tests

### 1172 5.2.6.6 MI-CONF-5: User interfaces shall prevent unintentional disabling of 1173 cybersecurity features

1174 User interfaces, especially in regard to settings, shall be designed in a manner that prevents unintentional disabling of  
1175 default cybersecurity features.

- 1176 • Applicability: VPNs featuring user-installable software which includes a graphical user interface
- 1177 • Reference: TR-CONF
- 1178 • Objective: Prevent attack exposure from misconfigured VPN software
- 1179 • Preparation: Access preferences or settings of VPN client
- 1180 • Activities: Attempt to configure the software in a way which exposes the user or their traffic to an attacker
- 1181 • Verdict: The VPN client does not permit reduced cybersecurity via configuration, or provides a clear,  
1182 recallable warning about the impact of the user's configuration actions => PASS, otherwise FAIL
- 1183 • Evidence: Recorded configuration options, annotation of settings which provided warning

## 1184 5.2.7 TR-NUTI: No untrusted traffic in the VPN connection

### 1185 5.2.7.1 Requirement

1186 Traffic from an unauthorized or unauthenticated source shall not be permitted to transit the VPN connection.

### 1187 5.2.7.2 MI-NUTI-1 Policy-driven traffic exclusion

1188 The VPN client and server shall be able to be configured to enforce granular packet filtering by application and  
1189 destination address & port, and shall only permit traffic explicitly authorized to transit the VPN connection.

- 1190 • Reference: TR-NUTI
- 1191 • Objective: Prevent unauthorized traffic in the VPN connection
- 1192 • Preparation: None
- 1193 • Activities: Attempt to send traffic that is explicitly blocked by configuration directly to the network port used  
1194 to route traffic into the VPN connection on the VPN client, repeat on VPN server
- 1195 • Verdict: The traffic does not enter the VPN connection, and does not exit it => PASS, otherwise FAIL
- 1196 • Evidence: Configuration file including the deny rule, packet capture of both incoming and outgoing interface,  
1197 log message recording the denied traffic

### 1198 5.2.7.3 MI-NUTI-2 Protocol validity checks

1199 The VPN client and server shall implement data validity checks on all incoming packets to ensure they conform to the  
1200 expected format and protocol of the restricted network.

- 1201 • Reference: TR-NUTI
- 1202 • Objective: Prevent unauthorized and/or malicious traffic in the VPN connection
- 1203 • Preparation: Create packets for each protocol supported by the traffic policy engine that have invalid or  
1204 malformed headers designed to bypass the traffic policy
- 1205 • Activities: For each malformed packet, inject the packet into the receiving interface of the VPN client or server
- 1206 • Verdict: Packet does not exit the VPN interface => PASS, otherwise FAIL
- 1207 • Evidence: Malformed packets, packet capture, any log messages showing packet was dropped

## 1208 5.2.8 TR-AUTH: Authentication of nodes

### 1209 5.2.8.1 Requirement

1210 All elements of the product that connect to nodes providing cybersecurity-relevant services shall authenticate the node  
1211 before using any services from the node.

### 1212 5.2.8.2 MI-AUTH-1 Authentication of cybersecurity-relevant nodes

1213 The VPN client shall require the use of pre-shared secrets, certificates, or fingerprints to authenticate the identity of any  
1214 cybersecurity-relevant node involved in the VPN connection and establish an initial secure connection.

1215 Guidance: Some options may be: TLS certificates already installed on the platform, configuration files containing  
1216 secrets, credentials provided as part of the product, fingerprints of keys that are distributed on a website or in  
1217 accompanying documentation, along with instructions to the user on how to verify them.

- 1218 • Reference: TR-AUTH
- 1219 • Objective: Prevent client trusting a masquerading node
- 1220 • Preparation: For each method of authenticating the cybersecurity-relevant node's identity, set up a test node  
1221 that provides invalid secrets, certificates, or fingerprints
- 1222 • Activities: For each method of authentication, make the VPN client to attempt to connect to the test node using  
1223 this method of authentication, and follow user instructions on how to approve authentication, if any
- 1224 • Verdict: VPN client does not connect to node => PASS, otherwise FAIL
- 1225 • Evidence: Invalid authentication materials, log messages for connection attempt, packet capture, log of user  
1226 actions, if any

### 1227 5.2.8.3 MI-AUTH-2 Transmitted credentials must be encrypted

1228 The VPN client shall by default encrypt all transmitted user credentials or sensitive authentication material used for any  
1229 supported authentication method or transport protocol.

- 1230 • Reference: TR-AUTH
- 1231 • Objective: Confidentiality of credentials
- 1232 • Preparation: None
- 1233 • Activities: For each supported authentication and transport method, authenticate a user while capturing the  
1234 network traffic for the entire authentication process, search the captured traffic for a plaintext string matching  
1235 the user's credential
- 1236 • Verdict: No plaintext string matching the user's credential is found => PASS, otherwise FAIL
- 1237 • Evidence: The authentication method and transport used, a packet capture, the plain text of the user's  
1238 credential, and the output of a search for the credential in the packet capture

#### 1239 5.2.8.4 MI-AUTH-3 Authentication timeout

1240 The VPN client, server, or other nodes shall not use session credentials with indefinite validity.

- 1241 • Reference: TR-AUTH
- 1242 • Objective: Protect VPN connection from unauthorised use
- 1243 • Preparation: Inspect, obtain or configure the session lifetime
- 1244 • Activities: Obtain a session credential. After the configured session credential validity periode, attempt to  
1245 connect to the VPN server.
- 1246 • Verdict: Connection is rejected => PASS, otherwise FAIL
- 1247 • Evidence: Log messages showing VPN connection establishment, authentication timeout or rejection, packet  
1248 capture with timestamps synchronised with log messages

#### 1249 5.2.8.5 MI-AUTH-4 Cloned credentials detection

1250 VPN server or mesh node shall detect when multiple VPN clients are using credentials that should be unique to a VPN  
1251 client and notify the users of both VPN clients or only allow one connection per credential.

- 1252 • Applicability: VPN handles credentials and VPN client credentials can be duplicated
- 1253 • Reference: TR-AUTH
- 1254 • Objective: Protect VPN connection from unauthorized use
- 1255 • Preparation: Configure two VPN clients with identical credentials that should be unique to a VPN client
- 1256 • Activities: Connect to the VPN with both VPN clients
- 1257 • Verdict: Notification of both VPN clients or only one connection is active at a time => PASS, otherwise FAIL
- 1258 • Evidence: Configuration of clients, log messages showing notifications and/or connection status

#### 1259 5.2.8.6 MI-AUTH-5 Forced revocation of authorization of endpoints

1260 The VPN service shall provide a method to force revocation, temporary or permanent, of authorization of an endpoint  
1261 by an authorized user. The revocation of authorization of the VPN client shall end the VPN connection for that client by  
1262 the time the revocation indicates it has completed.

- 1263 • Reference: TR-AUTH
- 1264 • Objective: Protect VPN connection from unauthorized use
- 1265 • Preparation: None
- 1266 • Activities: Authorize an endpoint to connect to the VPN, connect it to the VPN, revoke its authorization, then  
1267 attempt to access the VPN connection from the revoked client
- 1268 • Verdict: Revoked client cannot access the VPN connection => PASS, otherwise FAIL
- 1269 • Evidence: Logs or screenshots of authorization and revocation, packet capture

#### 1270 5.2.8.7 MI-AUTH-6 Brute force protection

1271 TODO: Mitigation documenting that the operational environment must provide  
1272 brute force protection.

- 1273 • Reference: TR-AUTH
- 1274 • Objective: Protect VPN connection from unauthorized use
- 1275 • Preparation:

- 1276 • Activities:
- 1277 • Verdict:
- 1278 • Evidence:

## 1279 5.2.9 TR-DNSL: DNS leak prevention

### 1280 5.2.9.1 Requirement

1281 Special attention to DNS queries is required, because they are usually transmitted in plaintext and could be  
 1282 eavesdropped on by an attacker on the wire or the DNS server itself and disclose which domains the user is trying to  
 1283 connect to.

1284 DNS leaks occur if the client does not or only partially tunnels cleartext DNS traffic through the VPN connection. This  
 1285 could either happen due to misconfiguration, system overwrites, or by design for example in case only partial traffic is  
 1286 tunnelled, so-called split tunnelling.

1287 Further, the user might want to set special DNS configuration either configured by the enterprise or custom configured  
 1288 in a consumer context. The VPN provider then must honour this DNS configuration.

1289 A DNS server is authorised if:

- 1290 1. the DNS server is configured by administrating user, or
- 1291 2. the DNS server is provided by the VPN manufacturer

1292 NOTE: is an evolution away plaintext DNS to secure DNS, with platforms, browsers and/or applications  
 1293 increasingly using "secure DNS" that is transported over TLS or HTTPS. Unlike cleartext DNS that uses  
 1294 port 53, use of secure DNS can be harder to identify, inhibiting the enforcement of specific policies to use  
 1295 a specifically configured DNS server.

1296 The following requirements apply to DNS traffic intended for the VPN connection. DNS queries for connection  
 1297 establishment, maintenance or restoration of the VPN tunnel are excluded.

1298 NOTE: The network configuration of a system is frequently changed by multiple different pieces of software,  
 1299 many of which the VPN client has no control over or insight into.

### 1300 5.2.9.2 MI-DNSL-1 Inform user of visibility of DNS queries

1301 The VPN client shall prominently inform the user of the handling of their plaintext DNS queries under the current  
 1302 configuration and their consequences in simple plain language, focusing on the potential risk and impact to the user of  
 1303 such handling and, where applicable, potential steps to resolve this risk.

1304 The product shall require the user to actively confirm that they have read the information before being able to use the  
 1305 VPN connection.

- 1306 • Applicability: Journalist & Activity, Privacy Cautious Households
- 1307 • Reference: TR-DNSL
- 1308 • Objective: Consent to and transfer of risk of loss of confidentiality to the user
- 1309 • Preparation: None
- 1310 • Activities: Start the VPN client, configure the VPN in such a way that DNS queries are not routed exclusively  
 1311 through the VPN and read any information displayed. Attempt to use the VPN connection before confirming  
 1312 that the user has read the information
- 1313 • Verdict: Information is displayed is clear and complete, VPN connection is not usable until the user confirms
- 1314 • Evidence: Logs, screenshots, screen recordings, packet captures

### 1315 5.2.9.3 MI-DNSL-2 Configurable exclusive DNS routing

1316 Unless DNS traffic is routed exclusively through the VPN at all times, the VPN client shall offer a configuration option  
1317 to route all DNS queries using well-known ports through the VPN connection.

- 1318 • Reference: TR-DNSL
  - 1319 • Objective: Prevent plaintext DNS query leaks outside of VPN connection
  - 1320 • Preparation: Configure the VPN to route all DNS queries using well-known ports through the VPN connection
  - 1321 • Activities: Start the VPN connection and perform a DNS lookup while capturing traffic on all network  
1322 interfaces
  - 1323 • Verdict: All plaintext DNS traffic shall be routed exclusively through the VPN connection => PASS, otherwise  
1324 FAIL
  - 1325 • Evidence: VPN client configuration, a packet capture showing the destination of all DNS queries using  
1326 well-known ports
- 1327 NOTE: Excluded from this verdict are DNS queries which are transmitted using DoH, DoT or other DNS query  
1328 hiding techniques.

### 1329 5.2.9.4 MI-DNSL-3 Exclusive DNS routing by default

1330 By default, the VPN client shall route all DNS queries using well-known ports through the VPN connection.

- 1331 • Reference: TR-DNSL
- 1332 • Objective: Prevent DNS query leaks using well-known ports outside of VPN connection
- 1333 • Activities: Start the VPN connection and perform a DNS lookup while capturing traffic on all network  
1334 interfaces
- 1335 • Verdict: All plaintext DNS traffic shall be routed exclusively through the VPN connection => PASS, otherwise  
1336 FAIL
- 1337 • Evidence: A packet capture showing that no DNS query using well-known ports is transmitted outside the  
1338 VPN tunnel

### 1339 5.2.9.6 MI-DNSL-5 Monitoring of DNS configuration

1340 The VPN client shall monitor changes in the local DNS configuration and take a user-configurable action when it  
1341 detects that the DNS configuration has changed from the one the VPN client specified. By default, the configurable  
1342 option shall be to disable network traffic outside the system.

1343 This requirement is only applicable, if changes in the local DNS configuration would affect the plaintext DNS query  
1344 visibility outside the tunnel to third parties of the system.

- 1345 • Reference: TR-DNSL
- 1346 • Objective: Prevent plaintext DNS query leaks outside of VPN connection
- 1347 • Preparation: Configure the VPN client to use exclusive DNS routing to authorized DNS servers
- 1348 • Activities: Start the VPN client and capture network packages on all interfaces, then alter the DNS  
1349 configuration to stop using the authorized DNS servers
- 1350 • Verdict: Analyse network packages, if DNS packages are leaked outside the tunnel, then within 30 seconds of  
1351 the configuration change, networking is disabled
- 1352 • Evidence: Logs, before and after configuration files, packet captures

### 1353 5.2.9.7 MI-DNSL-6 Secure DNS protocols

1354 The VPN client shall block or notify users of potential VPN bypass via encrypted DNS protocols, including when using  
1355 the dedicated port for DNS over TLS (DoT), if the traffic is routed via the VPN connection based on DNS policies.

- 1356 • Reference: TR-DNSL
- 1357 • Objective: Prevent DNS query leaks outside of VPN connection
- 1358 • Preparation: None
- 1359 • Activities: Start the VPN connection, configure DNS-based policy routing, then for each of DNS over TLS  
1360 (DoT), configure the operating system or an application to use a well-known public DNS provider for that  
1361 protocol using the well-known port 853, then generate DNS requests while capturing traffic on all network  
1362 interfaces. If using notifications rather than blocking, observe the client UI or documentation for static  
1363 warnings regarding encrypted DNS protocols.
- 1364 • Verdict: For all tests, either DNS connections to well-known public DNS providers should be blocked, or the  
1365 user should be notified that some software on their OS could be using encrypted DNS protocols with servers  
1366 that don't belong to the VPN manufacturer
- 1367 • Evidence: A description of the method used to prevent or notify the user about DNS over TLS (DoT) leaks, a  
1368 list of authorized DNS server IP addresses, a packet capture showing the destination of all DNS queries, or a  
1369 copy of the static notification provided to the user.

### 1370 5.2.9.8 MI-DNSL-7 No DNS leaks during network-level tunnel failure

1371 The VPN client shall ensure that DNS queries using well-known ports intended for the VPN tunnel are not sent to  
1372 non-authorized DNS servers when the connection to the VPN server is lost at the network level.

- 1373 • Reference: TR-DNSL
- 1374 • Objective: Prevent DNS query leaks during tunnel failure
- 1375 • Preparation: Start the VPN connection with exclusive DNS routing enabled.
- 1376 • Activities: Induce a network-level tunnel failure by blocking traffic to the VPN server's IP address using a  
1377 host-based firewall. Attempt to resolve a domain name while capturing traffic on all network interfaces.
- 1378 • Verdict: No DNS queries using well-known ports are sent to DNS servers outside the VPN connection.
- 1379 • Evidence: Method used to induce tunnel failure, packet capture, log messages.

## 1380 5.2.10 TR-EISO: Endpoint isolation

### 1381 5.2.10.1 Requirement

1382 The VPN shall by default not establish routes between different client endpoints.

### 1383 5.2.10.2 MI-EISO: No route between different endpoints

1384 The VPN shall by default not establish routes between different client endpoints.

- 1385 • Reference: TR-EISO
- 1386 • Objective: Prevent unauthorized network access to endpoints
- 1387 • Preparation: None
- 1388 • Activities: Connect two endpoints and attempt to connect to a port on the other endpoint
- 1389 • Verdict: Connection not possible or connection fails => PASS, otherwise FAIL
- 1390 • Evidence: Log messages, packet capture

## 1391 5.2.11 TR-TRAF: No traffic through the node unless explicitly approved

### 1392 5.2.11.1 Requirement

1393 The VPN client shall not route traffic through the endpoint from sources/destinations other than the endpoint without  
1394 the user's explicit informed consent, and such routing shall not be necessary for the use of any unrelated function.

### 1395 5.2.11.2 MI-TRAF-1: No capability to route traffic from other sources

1396 The VPN client shall not implement the capability for routing traffic from sources/destinations other than the endpoint  
1397 through an endpoint.

- 1398 • Reference: TR-TRAF
- 1399 • Objective: Prevent unauthorized network access to endpoints
- 1400 • Preparation: None
- 1401 • Activities: Connect an endpoint and capture the traffic on all interfaces
- 1402 • Verdict: No traffic originating from the VPN for sources/destinations other than the endpoint => PASS,  
1403 otherwise FAIL
- 1404 • Evidence: Packet capture with annotations of origin of packet

### 1405 5.2.11.3 MI-TRAF-2: Route traffic from other sources disabled by default

1406 The VPN client shall disable by default the capability for routing traffic from sources/destinations other than the  
1407 endpoint through an endpoint.

- 1408 • Reference: TR-TRAF
- 1409 • Objective: Prevent unauthorized network access to endpoints
- 1410 • Preparation: None
- 1411 • Activities: Connect an endpoint and capture the traffic on all interfaces
- 1412 • Verdict: No traffic originating from the VPN for sources/destinations other than the endpoint => PASS,  
1413 otherwise FAIL
- 1414 • Evidence: Packet capture with annotations of origin of packet

### 1415 5.2.11.4 MI-TRAF-3: Notify user if routing traffic from other sources

1416 The VPN client shall alert the user if the endpoint is allowing traffic from sources/destinations other than the endpoint  
1417 to be routed through the endpoint.

- 1418 • Reference: TR-TRAF
- 1419 • Objective: Prevent unauthorized network access to endpoints
- 1420 • Preparation: None
- 1421 • Activities: Connect an endpoint, enable the routing of external traffic through it, and observe the UI and  
1422 system
- 1423 • Verdict: User receives some alert or notification that clearly indicates forwarding is enabled => PASS,  
1424 otherwise FAIL
- 1425 • Evidence: Record of UI change

1426 **5.2.11.5 MI-TRAF-4: No routing traffic from other sources if not necessary for services**

1427 The VPN client shall not require routing of traffic from sources/destinations other than the endpoint to use services that  
1428 do not require such routing.

- 1429 • Reference: TR-TRAF
- 1430 • Objective: Prevent unauthorized network access to endpoints
- 1431 • Preparation: None
- 1432 • Activities: Create a list of services that can only be used if routing of external traffic is enabled, and document  
1433 why each service requires routing of external traffic to function
- 1434 • Verdict: All such services are documented, explanation is convincing => PASS, otherwise FAIL
- 1435 • Evidence: Documentation of services

1436 **5.2.12 TR-DMIN: Data minimization**

1437 **5.2.12.1 Requirement**

1438 The product shall not collect data unnecessary for the operation of the product.

1439 **5.2.12.2 MI-NPER-1: No Personal Data collected without authorization**

1440 The product shall not collect Personal Data without explicit authorization.

- 1441 • Reference: TR-DMIN
- 1442 • Objective: Data minimization
- 1443 • Preparation: Packet capture during typical hour of use and document all data sent to the VPN manufacturer,  
1444 label it all as to Personal Data or not, and justify all Personal Data sent, and document if it is kept or not, for  
1445 how long, who it is shared with, how it is stored, how the user consents to it, record of user consent
- 1446 • Activities: Review the documentation of the packet capture for Personal Data and see if any of it was collected  
1447 without authorization
- 1448 • Verdict: All Personal Data collected has a record of authorization by the user => PASS, otherwise FAIL
- 1449 • Evidence: Packet capture, documentation of Personal Data, authorization, justification

1450 **5.2.12.3 MI-NPER-2: No Personal Data sent outside endpoint**

1451 VPN shall not send Personal Data outside of the endpoint at all.

- 1452 • Reference: TR-DMIN
- 1453 • Objective: Data minimization
- 1454 • Preparation: Packet capture during typical hour of use and document all data sent to the VPN manufacturer
- 1455 • Activities: Review the documentation of the packet capture for any form of Personal Data
- 1456 • Verdict: There is no Personal Data collected => PASS, otherwise FAIL
- 1457 • Evidence: Packet capture

1458 **5.2.12.4 MI-NPER-3: Minimize Personal Data required for use, service provisioning  
1459 and payment**

1460 The VPN shall minimize the required Personal Data for use of the product, collecting only the Personal Data strictly  
1461 necessary for the service provider to process the payment, manage the subscription and fulfill contractual obligations.

- 1462 • Reference: TR-DMIN
- 1463 • Objective: Data minimization
- 1464 • Preparation: Follow the instructions to use the product and start a VPN connection, selecting the options that  
1465 require the least Personal Data, recording all data entered
- 1466 • Activities: Examine the data entered looking for Personal Data. Review the manufacturer's provided  
1467 justification for the necessity of this data in relation to providing the service, processing payment or managing  
1468 the subscription.
- 1469 • Verdict: If there is any excessive Personal Data recorded or Personal Data recorded without a justified,  
1470 documented operational reason essential for the delivery of the service or payment processing => FAIL,  
1471 otherwise PASS
- 1472 • Evidence: The record of data entered with a short description indicating whether the particular data element  
1473 alone or in combination with other data elements allows for singling out the individual in accordance with the  
1474 definition of personal data under the applicable law. Where this is the case, the reason why the data element is  
1475 required should also be documented.

#### 1476 5.2.12.5 MI-NPER-4: No Personal Data stored on remote data processing systems

1477 The VPN shall not store any Personal Data of the user on remote data processing systems.

1478 NOTE: VPN manufacturers may use remote systems to handle support tickets, e-mail and a knowledge base. The  
1479 VPN manufacturer shall not store any Personal Data in remote data processing systems without  
1480 abundantly clear and explicit permission from the user.

- 1481 • Applicability: (optional, for requirements that depend on a feature)
- 1482 • Reference: TR-DMIN
- 1483 • Objective: Confidentiality
- 1484 • Preparation: Gather internal written policy on what data may be stored, samples of all types of information  
1485 stored by the manufacturer that may contain Personal Data, covering at least one instance of all types of  
1486 activities conducted by the user
- 1487 • Activities: Examine the written policy and samples of stored data and look for Personal Data
- 1488 • Verdict: Policy is consistent with not storing Personal Data and samples of stored data contain no Personal  
1489 Data
- 1490 • Evidence: Policy, samples of stored data, documentation of why the samples don't contain Personal Data

### 1491 5.2.13 TR-IPV6: Secure IPv6 Handling

#### 1492 5.2.13.1 Requirement

1493 The VPN product shall handle IPv6 traffic in a secure manner that prevents data leaks.

#### 1494 5.2.13.2 MI-IPV6-1 Block IPv6 if Unsupported

1495 If the VPN does not support IPv6, the VPN client shall block all IPv6 traffic to prevent it from leaking outside the VPN  
1496 tunnel.

- 1497 • Applicability: VPN does not support IPv6
- 1498 • Reference: TR-IPV6
- 1499 • Objective: Prevent IPv6 traffic leaks
- 1500 • Preparation: None

1501 • Activities: On a network with IPv6 connectivity, connect to the VPN and attempt to access an IPv6-only  
1502 service.

1503 • Verdict: The connection to the IPv6-only service fails.

1504 • Evidence: Packet capture showing that no IPv6 traffic is leaving the device.

### 1505 5.2.13.3 MI-IPV6-2 Full Support if Claimed

1506 If the VPN claims to support IPv6, it shall provide full, native IPv6 connectivity, and all cybersecurity requirements in  
1507 this standard shall apply to IPv6 traffic.

1508 • Reference: TR-IPV6

1509 • Objective: Ensure full IPv6 support if claimed

1510 • Preparation: None

1511 • Activities: On a network with IPv6 connectivity, connect to the VPN and verify that the client has a globally  
1512 routable IPv6 address assigned by the VPN. All tests in this standard should be repeated over the IPv6  
1513 connection.

1514 • Verdict: The client has a globally routable IPv6 address and all tests in this standard pass over IPv6.

1515 • Evidence: Network configuration details, packet captures, and test results for all requirements over IPv6.

## 1516 5.2.14 TR-CRYPT: Use strong, VPN specific cryptography

### 1517 5.2.14.1 Requirement

1518 The VPN shall use strong cryptography.

### 1519 5.2.14.3 MI-CRYPT-1: Use conformant cryptography

1520 The product shall use cryptographic primitives and parameters as defined in Annex K.

1521 • Reference: TR-CRYPT

1522 • Objective: Confidentiality

1523 • Preparation: Perform a factory reset or new installation of the VPN client.

1524 • Activities: Start the VPN connection using the default configuration. Capture traffic on all interfaces.

1525 • Verdict: The traffic pertaining to the VPN connection uses the primitives and parameters as described in  
1526 Annex K.

1527 • Evidence: Packet capture showing the encryption headers.

## 1528 5.2.15 TR-LOGG: Logging and monitoring

### 1529 5.2.15.1 Requirement

1530 The product shall record cybersecurity-relevant internal events, including but not limited to changes to configuration  
1531 and Change to access or modification of data, services or functions. The product shall provide an opt-out mechanism.

### 1532 5.2.15.2 MI-LOGG-1: Logging

1533 In accordance with the requirement to monitor access or modification of data, services, or functions, the product shall  
1534 record log messages indicating specific cybersecurity-relevant internal events in an internal log.

1535 The minimum scope of cybersecurity-relevant events logged by the VPN client may include, but not limited to:

1536 • successful and failed authentication attempts,

- 1537 • establishment, termination, or unexpected drops of the VPN connection,
  - 1538 • modifications to the VPN client's configuration or security settings,
  - 1539 • changes applied by the VPN client to the host system's network configuration technically relevant for the VPN
  - 1540 service provision, or
  - 1541 • software update successes or failures.
- 1542 The log messages shall not include any confidential information such as Personal Data, network traffic content,  
 1543 connection metadata (e.g., destination IPs, DNS queries), secrets, or credentials. These logs shall be retained locally on  
 1544 the endpoint. To comply with data minimisation requirements, the VPN client shall not transmit these logs to the remote  
 1545 data processing solutions of the VPN manufacturer by default. Transmission of local logs to the manufacturer (e.g., for  
 1546 technical support or troubleshooting) shall require explicit, informed user authorisation (e.g. explicit opt-in).
- 1547 • Reference: TR-LOGG, TR-DMIN
  - 1548 • Objective: Monitoring and recording cybersecurity-relevant events
  - 1549 • Preparation: Review the manufacturer's documentation to confirm the scope of cybersecurity-relevant internal
  - 1550 events implemented in the logging mechanism.
  - 1551 • Activities: For each type of cybersecurity-relevant internal event (authentication, connection state change,  
 1552 configuration modification, etc.), trigger the event on the endpoint. Attempt to locate any automated  
 1553 transmission of these logs to the manufacturer without explicit user consent.
  - 1554 • Verdict: For each triggered event, the local log contains a message indicating the event, log message does not  
 1555 include any information likely to be confidential, and logs are not transmitted to the manufacturer without  
 1556 explicit user authorisation => PASS, otherwise FAIL
  - 1557 • Evidence: Method of triggering events, log messages with annotations, and packet captures demonstrating no  
 1558 unauthorised transmission of logs.
- 1559 NOTE: One type of event for which log messages must take care to not accidentally include a secret is failed  
 1560 password authentication attempts. Since users often type their password into the username field, including  
 1561 the username field in the log message may result in including a secret in the log message. Additionally,  
 1562 the product may provide an easy-to-use opt-out mechanism for users who do not wish to have internal  
 1563 activity recorded locally

### 1564 5.2.15.3 MI-LOGG-2: Remote Logging

- 1565 The product shall transfer log messages indicating cybersecurity-relevant internal events to a remote logging server.  
 1566 The log messages shall not include any confidential information such as Personal Data, secrets, or credentials, or any  
 1567 information which might reasonably be expected to include such items.
- 1568 • Reference: TR-LOGG
  - 1569 • Objective: Transfer log messages regarding cybersecurity-relevant events to mitigate local tampering
  - 1570 • Preparation: List all types of cybersecurity-relevant internal events
  - 1571 • Activities: For each type of cybersecurity-relevant internal event, trigger the event
  - 1572 • Verdict: For each triggered event, the log contains a message indicating the event, log message does not  
 1573 include any information likely to be confidential => PASS, otherwise FAIL
  - 1574 • Evidence: Method of triggering events, log messages with annotations
- 1575 NOTE: One type of event for which log messages must take care to not accidentally include a secret is failed  
 1576 password authentication attempts. Since users often type their password into the username field, including  
 1577 the username field in the log message may result in including a secret in the log message.

#### 1578 5.2.15.4 MI LOGG 3: No-Logs Policy and Traffic Anonymization

1579 The remote data processing solutions of the VPN manufacturer shall technically enforce a strict "no-logs" policy. The  
 1580 solutions shall ensure that no information about the user's network traffic is persistently stored; this includes Personal  
 1581 Data, the client's source IP, or connection metadata, such as destination IPs and other plaintext connection information  
 1582 (e.g., DNS queries, Ports or SNI Headers).

- 1583 • Reference: TR-LOGG, TR-DMIN
- 1584 • Objective: Data minimization and Confidentiality of data.
- 1585 • Preparation: Gather the technical documentation detailing the logging architecture of the remote data  
 1586 processing solutions, and obtain administrative access to a test instance of the VPN server configured  
 1587 identically to the production environment
- 1588 • Activities: Examine the server and routing software configuration files to verify that the logging of connection  
 1589 metadata and Personal Data is disabled or discarded, start a VPN connection from a client and generate  
 1590 network traffic, and inspect the remote server's persistent storage for the client's source IP, destination IPs, or  
 1591 plaintext connection information.
- 1592 • Verdict: If the server configuration permits the persistent storage of user network traffic data, or if any  
 1593 Personal Data or connection metadata is found persistently stored on the remote data processing system after  
 1594 generating traffic => FAIL, otherwise PASS.
- 1595 • Evidence: Copies of the relevant server configuration files demonstrating that logging is disabled, a description  
 1596 of the test traffic generated, and the output of the server storage/log inspection confirming the absence of the  
 1597 specified data.

#### 1598 5.2.15.5 MI LOGG 3: No data persistence or storage enabled on exit nodes

1599 The remote data processing solutions (e.g., exit nodes) of the VPN manufacturer shall utilize an ephemeral  
 1600 infrastructure architecture to technically prevent the persistent storage of user data, traffic metadata, or system logs at  
 1601 the hardware and operating system level. Servers shall operate exclusively using volatile memory (e.g., RAM disks or  
 1602 NVRAM) for temporary processing and system logs, without writing to non-volatile disk-based storage. To satisfy  
 1603 cybersecurity monitoring requirements, any non-Personal Data cybersecurity-relevant events shall be logged in volatile  
 1604 memory or securely transmitted to a remote logging system in accordance with MI-LOGG-2

- 1605 • Reference: TR-LOGG, TR-DMIN
- 1606 • Objective: Minimization of data compromise due to equipment compromise, Confidentiality of data
- 1607 • Preparation: Obtain the technical documentation detailing the server provisioning architecture for the remote  
 1608 data processing solutions. Obtain administrative access to a test instance of the VPN exit node configured  
 1609 identically to the production environment.
- 1610 • Activities: Perform steps in sequence:
  - 1611 1. Examine the server's operating system configuration (e.g., filesystem table/fstab, boot parameters) to  
 1612 verify that all system directories (including /var/log and temporary storage) are mounted exclusively  
 1613 on volatile memory (RAM disks).
  - 1614 2. Verify that unencrypted non-volatile swap partitions are disabled.  
 1615
  - 1616 3. Generate network traffic through the test node, then power cycle (reboot) the server and inspect the  
 1617 storage.
- 1618 • Verdict: If the server utilizes non-volatile disk-based storage for system logs, swap, or temporary processing,  
 1619 or if any data persists across a power cycle => FAIL, otherwise PASS.
- 1620 • Evidence: Copies of the relevant server configuration files demonstrating the use of RAM disks, and the output  
 1621 of the storage inspection after the power cycle.
- 1622 NOTE: NOTE: "Minimization of data compromise due to equipment compromise" is a completely NEW  
 1623 OBJECTIVE

## 1624 5.2.16 TR-SCDL: Secure deletion

### 1625 5.2.16.1 Requirement

1626 The product shall provide a method of deleting all user data and settings and resetting the product to its  
1627 secure-by-default configuration.

1628 NOTE: Overwriting all user-writable storage or encrypting all user data and deleting the key are two secure  
1629 deletion mechanisms.

### 1630 5.2.16.2 MI-RSET: Secure deletion via reset

1631 The product shall reset to its secure-by-default state after a power cycle or reset command.

- 1632 • Applicability: Product has the capability for the user to write data and/or settings
- 1633 • Reference: TR-SCDL
- 1634 • Objective: Secure deletion
- 1635 • Preparation: Document every type of stored data or setting that may be changed by the user on the product,  
1636 how to store it on the product, and how to read it from the product
- 1637 • Activities: For each type of user data or setting that may be stored and changed by the user on the product,  
1638 write an instance of the data or setting stored on the product that is different from the default and read it from  
1639 the product; once all types of data have been written and read, power cycle or reset the product, and read each  
1640 type of data again
- 1641 • Verdict: If any data or setting is the same for both of the reads => FAIL, otherwise PASS
- 1642 • Evidence: Record of each type of data or setting, what data or setting was written, what data or setting was  
1643 returned by the first read, and what data or setting was returned by the second read, comparison of each one

### 1644 5.2.16.3 MI-INST: Secure deletion via reinstallation

1645 The product shall reset to its secure-by-default state after a reinstallation that securely deletes all previous user data or  
1646 settings.

- 1647 • Applicability: Product has the capability for the user to write data and/or settings
- 1648 • Reference: TR-SCDL
- 1649 • Objective: Secure deletion
- 1650 • Preparation: Document every type of data or setting that may be stored and changed by the user on the product,  
1651 how to store it on the product, and how to read it from the product
- 1652 • Activities: For each type of user data or setting that may be stored and changed by the user on the product,  
1653 write an instance of the data or setting stored on the product that is different from the default and read it from  
1654 the product; once a breadth of data points have been written and read, reinstall the product with the secure  
1655 delete option, and read the data or settings again
- 1656 • Verdict: If any data or setting is the same for both of the reads => FAIL, otherwise PASS
- 1657 • Evidence: Record of each type of data or setting, what data or setting was written, what data or setting was  
1658 returned by the first read, and what data or setting was returned by the second read, comparison of each one

### 1659 5.2.16.4 MI-DELE: Secure deletion via secure deletion function

1660 The product shall reset to its secure-by-default state after the secure deletion function is used.

- 1661 • Applicability: Product has the capability for the user to write data and/or settings
- 1662 • Reference: TR-SCDL

- 1663
- Objective: Secure deletion
- 1664
- Preparation: Document every type of data or setting that may be stored and changed by the user on the product, how to store it on the product, and how to read it from the product
- 1665
- 1666
- Activities: For each type of user data or setting that may be stored and changed by the user on the product, write an instance of the data or setting stored on the product that is different from the default and read it from the product; once all types of data have been written and read, activate the secure deletion function, and read the data or settings again
- 1667
- 1668
- 1669
- 1670
- Verdict: If any data or setting is the same for both of the reads => FAIL, otherwise PASS
- 1671
- Evidence: Record of each type of data or setting, what data or setting was written, what data or setting was returned by the first read, and what data or setting was returned by the second read, comparison of each one
- 1672

## 1673 5.2.17 TR-SDTR: Secure data read and transfer

### 1674 5.2.17.1 Requirement

1675 The product shall provide a method to read all data and settings from the product, and if provided, securely transfer data  
1676 and settings to another product.

### 1677 5.2.17.2 MI-SDRF: Secure data read from product

1678 The product shall provide a method by which an authorized user can securely read all data and settings from the  
1679 product.

- 1680
- Applicability: Product has the capability for the user to write data and/or settings
- 1681
- Reference: TR-SDTR
- 1682
- Objective: Secure data read
- 1683
- Preparation: List all data and settings
- 1684
- Activities: For each type of data or setting, read the data or setting as an authorized user, then attempt read the  
1685 data or setting as an unauthorized user, if any exists
- 1686
- Verdict: All data and settings can be read by the authorized user, and no data or setting can be read by an  
1687 unauthorized user => PASS, otherwise FAIL
- 1688
- Evidence: List of data and settings, log message showing success or failure of each read by the authorized user  
1689 and, if applicable, the unauthorized user

### 1690 5.2.17.3 MI-SDTR: Secure data transfer to another product

1691 If the product provides a method to transfer data and settings to another product, it shall do so securely.

- 1692
- Applicability: Product has the capability for the user to write data and/or settings and to transfer them to  
1693 another product.
- 1694
- Reference: TR-SDTR
- 1695
- Objective: Secure data transfer
- 1696
- Preparation: Prepare methods by which an unauthorized user could read the data during transfer as outlined in  
1697 the risk assessment
- 1698
- Activities: Read the data or settings, initiate the data transfer, attempt to read or alter the transferred data and  
1699 settings as an unauthorized user, read the new data and settings on the target product
- 1700
- Verdict: No data or settings could be read or altered by an an unauthorized user, and the data and settings read  
1701 from the original product and target product are the same wherever technically possible => PASS, otherwise  
1702 FAIL

- 1703       • Evidence: List of data and settings, log messages from the attempts to read or alter data as the unauthorized  
1704 user, data and settings as read from the source product and as read from the target product, comparison  
1705 explaining technical reasons for any differences in the two versions

## 1706 5.2.18 Intentionally left blank

## 1707 5.2.19 TR-AVAI: Availability

### 1708 5.2.19.1 Requirement

1709 The product shall protect the availability of essential functions.

### 1710 5.2.19.2 MI-FDRP: Fast packet drop

1711 The product shall check network traffic from untrusted sources for validity and discard it efficiently, using reasonable  
1712 efforts to minimize use of system resources on invalid packets.

1713 NOTE: One method of minimizing resource use on invalid packets is to do the least resource-intensive validity  
1714 checks first, and to do validity checks before using system resources based on possibly invalid data. For  
1715 example, verifying that the length of a packet is valid should be done before verifying that the source  
1716 address is valid, and both should be done before allocating memory necessary to process a packet of that  
1717 length.

- 1718       • Reference: TR-AVAI

- 1719       • Objective: Maintain service availability during denial-of-service attacks

- 1720       • Preparation: Using packet generation software to bypass operating system level interference, create a selection  
1721 of invalid packets and enable some type of instrumentation or logging in the packet validity checking code

- 1722       • Activities: For each invalid packet, send the packet to the product and record the checks it makes and its use of  
1723 system resources before it drops the packet

- 1724       • Verdict: For each invalid packet, if the packet used resources that were not reasonably required to reject the  
1725 packet, or the packet was not rejected => FAIL, otherwise PASS

- 1726       • Evidence: Invalid packets and their descriptions, logs of processing, annotations explaining why the order of  
1727 operations is the most efficient reasonable way to process the packet.

### 1728 5.2.19.3 MI-LMEM: Limit memory usage

1729 The product shall limit and fairly allocate memory usage triggered by untrusted input to maintain availability of product  
1730 functions and the functions of the underlying platform and other products sharing system resources.

1731 NOTE: The product should range-check untrusted input fields that trigger memory allocations and rate-limit or  
1732 drop input that would allocate enough memory to impair the functions of any part of the system.

- 1733       • Reference: TR-AVAI

- 1734       • Objective: Maintain service availability during denial-of-service attacks

- 1735       • Preparation: Identify input fields from untrusted input that are used to calculate the size of memory allocations,  
1736 and create a set of inputs that, if processed as fast as possible, would significantly degrade the function of the  
1737 product due to overallocation of memory

- 1738       • Activities: For each set of inputs, send them to the product, while simultaneously measuring the availability of  
1739 the product functions and the functions of the underlying platform

- 1740       • Verdict: For each set of inputs, the product functions and the platform functions remain acceptably available  
1741 => PASS, otherwise FAIL

- 1742       • Evidence: Set of inputs, logs of measurements, explanation of availability metrics

1743 **5.2.19.5 MI-DOST: Document risk transfer to operational environment for denial of**  
 1744 **service**

1745 The product shall be accompanied by documentation informing the user that denial-of-service protection must be  
 1746 provided by the environment, in a form appropriate for a typical user for the intended purpose and reasonably  
 1747 foreseeable use and misuse of the product.

- 1748 • Reference: TR-AVAI
- 1749 • Objective: Maintain service availability during denial-of-service attacks
- 1750 • Preparation: None
- 1751 • Activities: Examine documentation
- 1752 • Verdict: Documentation exists and is appropriate to the typical user => PASS, otherwise FAIL
- 1753 • Evidence: Documentation, analysis of documentation, documentation of intended purpose

1754 **5.2.19.6 MI-DOST: Rate limit unauthenticated traffic**

1755 The product shall rate limit traffic from unauthenticated endpoints to nodes.

- 1756 • Reference: TR-AVAI
- 1757 • Objective: Maintain service availability during denial-of-service attacks
- 1758 • Preparation: None
- 1759 • Activities: Start capturing on all interfaces, repeatedly flood the node with unauthenticated traffic, observe any  
 1760 traffic rejections or package dropping
- 1761 • Verdict: Rate limiting can be observed => PASS, otherwise FAIL
- 1762 • Evidence: Network package capture, log messages

1763 **5.2.19.7 MI-DOST: Automatic traffic handling during denial-of-service attack**

1764 Unless the product relies on a single node or dedicated IP address, the product shall support multiple nodes which act as  
 1765 possible alternative fallbacks if a node becomes reachable.

1766 NOTE 1: A product may relay on a single node or dedicated IP address if the production function requires such  
 1767 setup. Such instances could be a dedicated IP address assigned to one VPN server, a dedicated IP address  
 1768 assigned to a cluster of VPN servers, or a mesh node which usually doesn't have a fallback.

1769 NOTE 2: Instances of such attack where a whole IP address becomes unavailable are Border Gateway Protocol  
 1770 (BGP) hijacking, (distributed) denial-of-service attacks making an IP address or a node unavailable, or IP  
 1771 address blocking by a network adversary.

- 1772 • Applicability: Not for mesh nodes
- 1773 • Reference: TR-AVAI
- 1774 • Objective: Maintain service availability during denial-of-service attacks
- 1775 • Preparation: None
- 1776 • Activities: Capture traffic on all interfaces, start the VPN connection, shutdown or disable traffic to the  
 1777 currently connected VPN server, observe automatic reconnection or traffic rerouting to the next available VPN  
 1778 server
- 1779 • Verdict: If connection automatically restored => PASS, otherwise FAIL
- 1780 • Evidence: Network package capture, log messages

## 1781 5.2.20 TR-CDST: Confidentiality of data stored on the product

### 1782 5.2.20.1 Requirement

1783 The product shall protect data stored on the product from unauthorized access.

### 1784 5.2.20.2 MI-CDST: Protect confidentiality of data stored on the product

1785 NOTE: This threat is currently only covered by a single high-level mitigation, more detailed and specific  
1786 mitigations will be added in future drafts.

1787 The product shall protect data stored on the product from unauthorized access.

1788 • Reference: TR-CDST

1789 • Objective: Confidentiality of data

1790 • Preparation: List all types of data that may be stored on the product that should not be readable without  
1791 authorization, what methods of ensuring confidentiality are appropriate for each type, all methods of accessing  
1792 that data available to an attacker based on the risk assessment, and what the allowable authorization methods  
1793 are for that access method

1794 • Activities: For each type of data and each access mechanism, determine the method of ensuring confidentiality  
1795 used, and attempt to read the data without authorization

1796 • Verdict: If all methods of ensuring confidentiality match the type of the data stored, and all the attempts to read  
1797 confidential data without authorization fail => PASS, otherwise FAIL

1798 • Evidence: Logs of determination of type of data and method of confidentiality and attempts to read  
1799 confidential data without authorization

1800 NOTE: Data may be protected by the environment, permissions, encryption, salting and hashing, offline storage,  
1801 or hardware-backed secrets.

## 1802 5.3 Risk mitigation sets

### 1803 5.3.1 General

1804 This clause lists all the mitigations necessary to meet requirements for each security profile. Security profiles are  
1805 derived from the Use Cases in 4.7. See Annex C for more information.

### 1806 5.3.2 SP-1 Individual consumer required mitigations

1807 1. (KEVD or KEVA)

1808 2. KEVT

1809 3. (SUVP or SUAP or SUOE or SUA0)

1810 4. AUTH-6

1811 5. CDST

1812 6. LOGG-1

1813 7. ROUT-3

1814 8. SCFS

1815 9. SSCA

1816 10. VULH

### 1817 5.3.3 SP-2 Privacy conscious household required mitigations

- 1818 1. KEVT
- 1819 2. (SUAP or SUA0)
- 1820 3. (TRAF-1 or (TRAF-2 and TRAF-3 and TRAF-4))
- 1821 4. AUTH-1
- 1822 5. AUTH-2
- 1823 6. AUTH-3
- 1824 7. AUTH-5
- 1825 8. AUTH-6
- 1826 9. CDST
- 1827 10. CONF-1
- 1828 11. CONF-2
- 1829 12. CONF-3
- 1830 13. CONF-4
- 1831 14. CONF-5
- 1832 15. DNSL-1
- 1833 16. DNSL-2
- 1834 17. DNSL-7
- 1835 18. DOST
- 1836 19. EISO
- 1837 20. FDRP
- 1838 21. IPv6-1
- 1839 22. IPv6-2
- 1840 23. KEVA
- 1841 24. KEVD
- 1842 25. LMEM
- 1843 26. LOGG-1
- 1844 27. LOGG-4
- 1845 28. LOGG-5
- 1846 29. NPER-1
- 1847 30. ROUT-1
- 1848 31. ROUT-2
- 1849 32. ROUT-3
- 1850 33. SCFS
- 1851 34. SSCA

1852	35. SUAU
1853	36. SUCS
1854	37. SUED
1855	38. SUMV
1856	39. SURC
1857	40. SURP
1858	41. SUSR
1859	42. SUVH
1860	43. VULH

#### 1861 5.3.4 SP-3 Journalist or activist required mitigations

1862	1. (FZ95 or BTIN or IMSL)
1863	2. KEVT
1864	3. (RSET or INST or DELE)
1865	4. (SUAP or SUA0)
1866	5. AUTH-1
1867	6. AUTH-2
1868	7. AUTH-3
1869	8. AUTH-4
1870	9. AUTH-5
1871	10. AUTH-6
1872	11. CDST
1873	12. CONF-1
1874	13. CONF-2
1875	14. CONF-3
1876	15. CONF-4
1877	16. CONF-5
1878	17. CRYPT-1
1879	18. DNSL-1
1880	19. DNSL-2
1881	20. DNSL-3
1882	21. DNSL-4
1883	22. DNSL-5
1884	23. DNSL-6
1885	24. DNSL-7
1886	25. DOST

1887	26. EISO
1888	27. FAIR
1889	28. FDRP
1890	29. IPv6-1
1891	30. IPv6-2
1892	31. KEVA
1893	32. KEVD
1894	33. LMEM
1895	34. LOGG-1
1896	35. LOGG-2
1897	36. LOGG-4
1898	37. LOGG-5
1899	38. NPER-1
1900	39. NPER-2
1901	40. NPER-3
1902	41. NPER-4
1903	42. NUTI-1
1904	43. NUTI-2
1905	44. ROUT-1
1906	45. ROUT-2
1907	46. ROUT-3
1908	47. SCFS
1909	48. SDRF
1910	49. SDTR
1911	50. SSCA
1912	51. SUAUA
1913	52. SUCS
1914	53. SUED
1915	54. SUMV
1916	55. SURC
1917	56. SURP
1918	57. SUSR
1919	58. SUVH
1920	59. TRAF-1
1921	60. VULH

### 1922 5.3.5 SP-4 Small organization required mitigations

- 1923 1. (FZ95 or BTIN or IMSL)
- 1924 2. KEVT
- 1925 3. (NUTI-1 or TRAF-1 or (TRAF-2 and TRAF-3 and TRAF-4))
- 1926 4. (RSET or INST or DELE)
- 1927 5. (SUAP or SUA0)
- 1928 6. AUTH-1
- 1929 7. AUTH-2
- 1930 8. AUTH-3
- 1931 9. AUTH-4
- 1932 10. AUTH-5
- 1933 11. AUTH-6
- 1934 12. CDST
- 1935 13. CONF-1
- 1936 14. CONF-2
- 1937 15. CONF-3
- 1938 16. CONF-4
- 1939 17. CONF-5
- 1940 18. CRYPT-1
- 1941 19. DNSL-1
- 1942 20. DNSL-2
- 1943 21. DNSL-3
- 1944 22. DNSL-4
- 1945 23. DNSL-5
- 1946 24. DNSL-6
- 1947 25. DNSL-7
- 1948 26. DOST
- 1949 27. FAIR
- 1950 28. FDRP
- 1951 29. IPv6-1
- 1952 30. IPv6-2
- 1953 31. KEVX
- 1954 32. KEVD
- 1955 33. LMEM
- 1956 34. LOGG-1

1957	35. LOGG-2
1958	36. NPER-1
1959	37. NUTI-1
1960	38. NUTI-2
1961	39. ROUT-1
1962	40. ROUT-2
1963	41. ROUT-3
1964	42. SCFS
1965	43. SDRF
1966	44. SDTR
1967	45. SSCA
1968	46. SUAUA
1969	47. SUCS
1970	48. SUED
1971	49. SUMV
1972	50. SURC
1973	51. SURP
1974	52. SUSR
1975	53. SUVH
1976	54. VULH

### 1977 5.3.5 SP-5 Large enterprise required mitigations

1978	1. (FZ95 or BTIN or IMSL)
1979	2. KEVT
1980	3. (RSET or INST or DELE)
1981	4. (SUAP or SUAUA)
1982	5. AUTH-1
1983	6. AUTH-2
1984	7. AUTH-3
1985	8. AUTH-4
1986	9. AUTH-5
1987	10. AUTH-6
1988	11. CDST
1989	12. CONF-1
1990	13. CONF-2
1991	14. CONF-3

1992	15. CONF-4
1993	16. CONF-5
1994	17. CRYPT-1
1995	18. DNSL-1
1996	19. DNSL-2
1997	20. DNSL-3
1998	21. DNSL-4
1999	22. DNSL-5
2000	23. DNSL-6
2001	24. DNSL-7
2002	25. DOST
2003	26. FAIR
2004	27. FDRP
2005	28. IPv6-1
2006	29. IPv6-2
2007	30. KEVE
2008	31. KEVD
2009	32. LMEM
2010	33. LOGG-1
2011	34. LOGG-2
2012	35. NPER-1
2013	36. NUTI-1
2014	37. NUTI-2
2015	38. ROUT-1
2016	39. ROUT-2
2017	40. SCFS
2018	41. SDRF
2019	42. SDTR
2020	43. SSCA
2021	44. SUAUA
2022	45. SUCS
2023	46. SUED
2024	47. SUMV
2025	48. SURC
2026	49. SURP

- 2027 50. SUSR
- 2028 51. SUVH
- 2029 52. VULH

### 2030 5.3.6 SP-6 Enterprise independent client mitigations

2031 TODO: update security analysis to better allow for this security profile's needs be met (without overprescribing)

- 2032 1. (FZ95 or BTIN or IMSL)
- 2033 2. KEVT
- 2034 3. TRAF-1 or (TRAF-2 and TRAF-4)
- 2035 4. (RSET or INST or DELE)
- 2036 5. SUDC
- 2037 6. (SUAP or SUA0)
- 2038 7. AUTH-1
- 2039 8. AUTH-2
- 2040 9. CDST
- 2041 10. CONF-1
- 2042 11. CONF-2
- 2043 12. CONF-3
- 2044 13. CONF-4
- 2045 14. DNSL-7 \*
- 2046 15. IPv6-1
- 2047 16. LOGG-1
- 2048 17. ROUT-1
- 2049 18. ROUT-2
- 2050 19. SCFS
- 2051 20. SDRF
- 2052 21. SDTR
- 2053 22. SSCA
- 2054 23. SUA0
- 2055 24. SUCS
- 2056 25. SUED
- 2057 26. SUMV
- 2058 27. SURC
- 2059 28. SURP
- 2060 29. SUSR
- 2061 30. SUVH

2062 31. VULH

### 2063 5.3.X SP-7 Mesh VPN required mitigations

2064 1. (FZ95 or BTIN or IMSL)

2065 2. KEVT

2066 3. (RSET or INST or DELE)

2067 4. (SUAP or SUA0)

2068 5. AUTH-1

2069 6. AUTH-2

2070 7. AUTH-3

2071 8. AUTH-4

2072 9. AUTH-5

2073 10. AUTH-6

2074 11. CDST

2075 12. CONF-1

2076 13. CONF-2

2077 14. CONF-3

2078 15. CONF-4

2079 16. CONF-5

2080 17. CRYPT-1

2081 18. DNSL-1

2082 19. DNSL-2

2083 20. DNSL-3

2084 21. DNSL-4

2085 22. DNSL-5

2086 23. DNSL-6

2087 24. DNSL-7

2088 25. DOST

2089 26. EISO

2090 27. FAIR

2091 28. FDRP

2092 29. IPv6-1

2093 30. IPv6-2

2094 31. KEVA

2095 32. KEVD

2096	33. LMEM
2097	34. LOGG-1
2098	35. LOGG-2
2099	36. NPER-1
2100	37. NUTI-1
2101	38. NUTI-2
2102	39. ROUT-1
2103	40. ROUT-2
2104	41. SCFS
2105	42. SDRF
2106	43. SDTR
2107	44. SSCA
2108	45. SUAU
2109	46. SUCS
2110	47. SUED
2111	48. SUMV
2112	49. SURC
2113	50. SURP
2114	51. SUSR
2115	52. SUVH
2116	53. TRAF-2
2117	54. TRAF-3
2118	55. TRAF-4
2119	56. VULH

---

## 2120 6 Assessment criteria for compliance with technical 2121 requirements

2122 *It has been agreed across vertical standards to define each assessment criteria following the common structure:*

- 2123 • *Requirement reference*
- 2124 • *Objective*
- 2125 • *Preparation*
- 2126 • *Activities*
- 2127 • *Verdict*
- 2128 • *Evidence*

2129 *The assessment criteria clause shall be structured by requirement defined in clause 5.*

## 2130 6.1 Introduction to the assessment and compliance criteria

2131 This clause provides objective and reproducible assessment criteria to determine whether a product complies with the  
2132 technical security requirements of clause 5, based on the UC and/or the Security Profile it may belong towards its  
2133 placement in the EU market.

2134 For each cybersecurity requirements defined in Clause 5, the following clauses specify assessment criteria to determine  
2135 if the technical requirement is met.

2136 Please ensure that there is an easy, clear and unambiguous mapping of the requirements in clause 5 to the relevant  
2137 assessment criteria in clause 6.

2138 The assessment criteria for each security requirements are described in a structured manner, as follows:

- 2139 • **Assessment Objective:** Defines the security property or capability that shall be verified, ensuring that the  
2140 assessment remains focused on the intent of the requirement. It includes the reference index of the  
2141 requirement(s) it aims to assess.
- 2142 • **Assessment Preparation:** Describes the environment, setup, and preconditions required before executing the  
2143 test. It includes the following elements as applicable:
  - 2144 ○ Test environment: Describe the hardware, software, and network setup used for the assessment,  
2145 including versions, topology, and any relevant dependencies.
  - 2146 ○ Preconditions: Specify any configurations, credentials, or operational states that should be established  
2147 before the test (e.g. product initialized, certificates loaded, user roles created).
  - 2148 ○ Required tools: Identify the tools or software necessary to perform the assessment (e.g. vulnerability  
2149 scanners, protocol fuzzers, traffic analyzers, static code analyzers, cryptographic test suites).
  - 2150 ○ Required information/documentation for the assessment: Specify all information that is necessary to  
2151 perform the assessment
  - 2152 ○ Reference any vendor-provided setup guides, configuration instructions, or operational manuals, as  
2153 well as any relevant standards or technical notes, that define how the product shall be configured or  
2154 operated for the assessment.
- 2155 • **Assessment Activities:** Provides execution steps to be performed. Assessment activities may include, as  
2156 applicable:
  - 2157 ○ Review information/documentation for the assessment to confirm that the described implementation  
2158 matches the requirement (e.g. verify that the security architecture document specifies TLS 1.2 or  
2159 higher for all external interfaces, or that the password policy aligns with the defined threshold).
  - 2160 ○ Perform security functional tests to verify the completeness and correctness of the  
2161 information/documentation for the assessment
  - 2162 ○ Perform security functional or penetration tests to verify that implemented controls are correctly  
2163 implemented e.g. to prevent unauthorized access or data modification (e.g. via attempting to log in  
2164 with invalid credentials to test lockout enforcement or trying to modify protected configuration files  
2165 without administrative privileges).
  - 2166 ○ Analyse code or binaries to identify potential security weaknesses or misconfigurations (e.g. perform  
2167 static analysis to detect hardcoded credentials or use dynamic analysis tools to identify buffer  
2168 overflow or injection vulnerabilities).
  - 2169 ○ Inspect configurations to ensure that required security parameters are correctly applied (e.g. check  
2170 that weak cipher suites are disabled, two-factor authentication is enabled, and least-privilege access  
2171 controls are configured in the system).
  - 2172 ○ Observe runtime behaviour to confirm that protections such as encryption, authentication, and  
2173 integrity verification operate as intended (e.g. monitor network traffic to ensure data in transit is  
2174 encrypted or observe system logs to verify successful validation of digital signatures during startup).
- 2175 • **Assignment of Verdict:** Defines the pass/fail criteria.

- 2176 ○ **Pass:** The assessment is considered passed if the product demonstrably fulfils the requirement and  
 2177 meets the defined security thresholds. Examples of such thresholds include:
- 2178 ▪ Minimum cryptographic strength (e.g. AES-128 or higher);
  - 2179 ▪ Password policy limits (e.g. minimum of 12 characters);
  - 2180 ▪ Login protection mechanisms (e.g. account lockout after five consecutive failed attempts);
  - 2181 ▪ Resistance to a specified attack potential (e.g. equivalent to CSA High/AVA\_VAN.3 or  
 2182 higher).
- 2183 ○ **Fail:** The assessment is considered failed if the requirement is not fulfilled, or if the defined security  
 2184 thresholds are not achieved (e.g. insufficient key length, missing authentication enforcement, or  
 2185 inadequate resistance to the required attack potential).

- 2186 • **Supporting Evidence :** Defines the artefacts and documentation collected to demonstrate that the requirement  
 2187 has been assessed and fulfilled. The evidence shall be sufficient to enable independent verification of the  
 2188 assessment results and to demonstrate compliance with the relevant CRA essential requirements. The  
 2189 supporting evidence include, where applicable:
  - 2190 ○ Test or assessment reports showing the steps performed and results obtained;
  - 2191 ○ Logs, configuration files, or audit traces demonstrating the implementation of the requirement;
  - 2192 ○ Screenshots, captures, or console outputs confirming the correct execution or protection behaviour;
  - 2193 ○ Relevant vendor or design documentation describing the applied security measures;

2194 *It would be very useful to use a common structure for the assessment criteria definition clause 6. The following is a*  
 2195 *proposal - to be discussed among rapporteurs.*

2196 *The assessment criteria shall be indexed, to facilitate their referencing, preferably using a common indexing structure*  
 2197 *throughout all standards and enabling an easy mapping with the requirements of Clause 5.*

2198 *Proposed structure for indexing the assessment criteria:*

2199 *ACC - PP - ESR - NNN*

2200 *ACC: Used to identify assessment and compliance criteria in the text*

2201 *PP : Product short name added only if relevant when the product category may be divided in sub categories*

2202 *ESR :Proposed abbreviations referring to the different essential requirements of the regulation*

2203 *NNNN - Incremental and unique sequence of numbers and letters - could be the same as for the corresponding*  
 2204 *requirement (if one-to-one match), otherwise a mapping would be needed*

## 2205 6.2 No known exploitable vulnerabilities

2206 Proposed ESR code: KEV

## 2207 6.3 Secure by design

2208 Proposed ESR code SBD

## 2209 6.4 Secure Updates

2210 Proposed ESR code: SU

## 2211 6.5 Authentication and Access Control

2212 Proposed ESR code: AAC

2213 **6.6 Confidentiality**

2214 Proposed ESR code: CON

2215 In this clause, reference can be made to the Annex K (normative), specifying State Of The Art Cryptography  
2216 assessment criteria.

2217 **6.7 Integrity**

2218 Proposed ESR code: INT

2219 **6.8 Data Minimisation**

2220 Proposed ESR code: DM

2221 **6.9 Availability Protection**

2222 Proposed ESR code: AP

2223 **6.10 Impact Minimisation**

2224 Proposed ESR code: IM

2225 **6.11 Minimisation of Attack Surfaces**

2226 Proposed ESR code: MAS

2227 **6.12 Exploitation Mitigation Mechanisms**

2228 Proposed ESR code: EMM

2229 **6.13 Logging and Monitoring**

2230 Proposed ESR code: LOG

2231 **6.14 Data Removal and Transparency**

2232 Proposed ESR code: DRT

2233 **6.15 Vulnerability Handling**

2234 The assessment criteria specified in CEN/CLC JT013090:2026 (CEN/CLC prEN 40000-1-3) [2] shall be met for the  
2235 product

2236

2237 **Annex A (informative):**  
 2238 **Relationship between the present document and the**  
 2239 **requirements of EU Regulation (EU) 2024/2847 - the**  
 2240 **Cyber Resilience Act**

2241 The present document has been prepared in response to the Commission's standardisation request C(2025)618 [i.3] to  
 2242 provide, in additions to its other uses, one voluntary means of conforming to the essential requirements of Regulation  
 2243 (EU) 2024/2847 [i.2] known as the Cyber Resilience Act (CRA).

2244 Once the present document is cited in the Official Journal of the European Union under Regulation (EU) 2024/2847  
 2245 [i.2], conformance with the normative clauses of the present document given in the tables in Annex A confers, to  
 2246 products with digital elements in the scope of the present document, a presumption of conformity with the  
 2247 corresponding essential requirements of that Regulation and associated EFTA regulations.

2248 **Table A.1: Relationship between the present document and**  
 2249 **the requirements of Regulation (EU) 2024/2847 - the Cyber Resilience Act**

CRA requirement	Cybersecurity requirements(s)
No known exploitable vulnerabilities	NKEV, SSSD, SCUD, NUTI, LOGG
Secure design, development, production	SSDD
Secure by default configuration	ROUT, DNSL, EISO, TRAF
Secure updates	SCUD
Authentication and access control mechanisms	AUTH
Confidentiality protection	AUTH, ROUT, DNSL, EISO, IPV6, CRYPT
Integrity protection for data and configuration	CONF, DNSL
Data minimisation	DMIN
Availability protection	AVAI
Minimise impact on other devices or services	NUTI
Limit attack surface	EISO, NUTI
Exploit mitigation by limiting incident impact	SSD, EISO, NUTI
Logging and monitoring mechanisms	LOGG
Secure deletion and data transfer	SCDL, SDTR
Vulnerability handling	VULH

2250  
 2251 NOTE 1: The table cannot indicate direct relationship between the relevant legal requirement and *other* standards  
 2252 or normative clauses contained in *other* standards.

2253 NOTE 2: If the standard is developed according to the structure in the present skeleton document, then the number  
 2254 of the clauses in the table below don't need to be changed.

2255 NOTE 3: The last two columns shall be either filled with details and the reference of the table(s) mapping the  
 2256 applicability of the technical cybersecurity requirements, or deleted all together.

2257 **Key to columns:**

2258 **Requirement:**

2259 No A unique identifier for one row of the table which may be used to identify a requirement.

2260 **Description** A textual reference to the requirement.

2261 **Requirements of Regulation** Identification of article(s) defining the requirement in the Regulation.

2262 **Clause(s) of the present document** Identification of clause(s) defining the requirement in the present document unless  
 2263 another document is referenced explicitly.

2264 **Requirement Conditionality:**

2265 U/C Indicates whether the requirement is unconditionally applicable (U) or is conditional upon the manufacturer's  
 2266 claimed functionality of the equipment (C).

2267 **Condition** Explains the conditions when the requirement is or is not applicable for a requirement which is classified  
 2268 "conditional".

- 2269 Presumption of conformity stays valid only as long as a reference to the present document is maintained in the list  
2270 published in the Official Journal of the European Union. Users of the present document should consult frequently the  
2271 latest list published in the Official Journal of the European Union.
- 2272 Other Union legislation may be applicable to the product(s) falling within the scope of the present document.
- 2273

---

2274 **Annex C (informative):**  
2275 **Cybersecurity threat landscape, risk identification**  
2276 **and assessment methodology**

2277 **C.1 Assets**

2278 **C.1.1 Data**

- 2279 • Data transmitted over the VPN network
- 2280 • Management and configuration data
  - 2281 ○ Configuration data
  - 2282 ○ Management application certificates
  - 2283 ○ CA information, certificates & keys (public, private, PSK)
  - 2284 ○ End-point details including authentication, location, and potential Personal Data
- 2285 • Statistics and telemetry data
  - 2286 ○ Network configuration audit logs
  - 2287 ○ Network flow logs and other statistics about data transferred over the network
  - 2288 ○ Debugging logs from end-points and VPN gateways
- 2289 • Software applications
  - 2290 ○ Device-native applications for connecting to the network (Client or Node software)

2291 **C.1.2 Product functions**

2292 A basic overview of VPN functions follows. See clause 4.2 for a detailed overview of the essential functions of a VPN  
2293 product.

- 2294 • Edge: uses a public network to communicate with the restricted use network
- 2295 • Gateway: provides link between public network and restricted
- 2296 • Router: forward traffic between nodes in the restricted use network
- 2297 • Filter: select which traffic may transit this node
- 2298 • Relays: assist nodes in connecting to the restricted use network
- 2299 • Auth: grant nodes access to the restricted network

2300 **C.2 Risk factors**

2301 **C.2.1 General**

2302 Risk factors determine which mitigation(s) satisfy each of the cybersecurity requirements in clause 5.2. The assessor of  
2303 a product determines the level of each risk factor via the development of a threat model and risk profile based on the  
2304 intended and foreseeable use and misuse of the VPN.

2305 Risk factors may increase the likelihood of an incident, increase the impact of an incident, or both. As a result, different  
2306 mitigation strategies may be more or less relevant to different risk factors.

2307 The overall risk related to each use case should be considered as a result of combining risk factors affecting both  
2308 likelihood and impact of an incident.

## 2309 C.2.2 RF-CFG: End-point configuration

2310 Description: Affects likelihood of threats involving misconfiguration.

2311 Rationale: The complexity of the end-point configuration can directly affect the likelihood of threats

- 2312 • [CFG-0] End-point requires no configuration
- 2313 • [CFG-1] End-point requires simple configuration, such as selecting an established VPN protocol or choosing a  
2314 region to connect to
- 2315 • [CFG-2] End-point requires configuration by a skilled administrator

## 2316 C.2.3 RF-AUT: Account management and authentication of endpoints

2317 Description: Affects likelihood of threats involving authentication.

2318 Rationale: An improper account management and authentication implementation can directly impact with a successful  
2319 breach

- 2320 • [AUT-0] User employs a third party identity and authentication provider
- 2321 • [AUT-1] Identity and authentication are managed through a user-owned and managed centralised identity  
2322 system
- 2323 • [AUT-2] Each system utilised by the user involves its own set of account information and secrets

## 2324 C.2.5 RF-FUN: Sensitivity of functions

2325 Description: Affects impact of threats involving loss of availability of product functions.

2326 Rationale: Loss of product functions' availability can have a major impact on threats.

- 2327 • [FUN-0] Loss of function would be a minor annoyance (e.g. preventing accessing unimportant web sites)
- 2328 • [FUN-1] Loss of function would impede daily activities
- 2329 • [FUN-2] Loss of function would threaten human rights of user

## 2330 C.2.6 RF-ADM: Availability of administration

2331 Description: What the availability and skill of administration is for the product.

2332 Rationale: Skilled, fully resourced administration allows more risk transfer and can reduce the impact of incidents.

- 2333 • [ADM-0] Skilled administration, fully resourced
- 2334 • [ADM-1] Skilled administration, partially resourced
- 2335 • [ADM-2] Unskilled administration

## 2336 C.2.7 RF-RDP: Manufacturer infrastructure isolation

2337 Description: Exposure of manufacturer infrastructure responsible for essential functions of the product

2338 Rationale: More users with physical access to manufacturer infrastructure increases likelihood of an attack via hardware  
2339 interfaces.

- 2340 • [RDP-0] Manufacturer does not provide any remote data processing
- 2341 • [RDP-1] Manufacturer provides RDPS via self-hosted infrastructure.
- 2342 • [RDP-2] Manufacturer infrastructure located in a multi-tenant SaaS system

## 2343 C.2.8 RF-DNC: Difficulty of network configuration

2344 Description: Difficulty of configuring, controlling, and monitoring the configuration of the network connection on the  
2345 platform the product is running on.

2346 Rationale: The more difficult it is to configure the network connection, maintain control over that configuration, and  
2347 learn about changes to the configuration, the more likely it is that the configuration will become insecure.

- 2348 • [DNC-0] Product has complete control over the network configuration
- 2349 • [DNC-1] Product is using a well-defined, predictable platform service to configure the network connection
- 2350 • [DNC-2] Other software can change network configuration without notification or permission from the  
2351 product

## 2352 C.2.9 RF-COM: Complexity of feature set

2353 Description: How complex the features necessary for the product's foreseeable use are.

2354 Rationale: More features mean more code and more interfaces mean attack surface.

- 2355 • [COM-0] Usage requires only basic features to tunnel encrypted traffic
- 2356 • [COM-1] Usage requires a few additional features related to tunnelling encrypted traffic
- 2357 • [COM-2] Usage requires many additional features

## 2358 C.2.10 RF-CON: Connectivity offered

2359 Description: Whether the VPN connects different endpoints to each other via a private network or simply provides a  
2360 tunnel from a single endpoint to a public network

2361 Rationale: Different connectivity requirements create different risks and mitigations.

- 2362 • [CON-0] Usage is a single endpoint connecting only to a public network
- 2363 • [CON-1] Usage is one or more endpoints connecting to other endpoints or hosts via a private network
- 2364 • [CON-2] Usage is multiple endpoints connecting to each other via a private network, in addition to connecting  
2365 to a public network

## 2366 C.2.11 RF-PER: Consequences of Protected Data compromise

2367 Description: What the consequences of an attacker acquiring Protected Data (personal or enterprise) via the product are.

2368 Rationale: Different consequences change the impact of compromise of Protected Data stored or transmitted by the  
2369 product.

- 2370 • [PER-0] Usage is no or low consequences for compromise of Protected Data stored or transmitted by the  
2371 product
- 2372 • [PER-1] Usage is moderate consequences for compromise of Protected Data stored or transmitted by the  
2373 product, e.g. financial or reputational loss, or disclosure of private enterprise data
- 2374 • [PER-2] Foreseeable use is high consequences for compromise of Protected Data stored or transmitted by the  
2375 product, e.g. loss of life or human rights, or disclosure of highly confidential enterprise data

## 2376 C.3 Assumptions

### 2377 C.3.1 Platform

2378 [AS-PP]: The platform the product is running on is trustworthy.

## 2379 C.3.2 Proper administrator

2380 [AS-PA]: The product administrator is not intentionally hostile and is engaging in good faith efforts to administer the  
2381 product properly.

## 2382 C.3.3 Attacker has limited physical access to product

2383 [AS-LP]: An attacker will have only temporary physical access to the platform running the product.

## 2384 C.3.4 Attacker has limited resources

2385 [AS-LR]: An attacker will use limited resources in proportion to the value of the assets of the product in each security  
2386 profile.

# 2387 C.4 Threats and security analysis

## 2388 C.4.1 General

2389 The approach to listing threats is to separate them by mitigation so that they may be associated with risk factors more  
2390 directly.

2391 For the purposes of the list of threats, the product includes:

- 2392 • VPN software operating on an end-user node
- 2393 • VPN software operating as a VPN server on any hardware
- 2394 • software used to manage VPN network topology

## 2395 C.4.2 Security analysis methodology

2396 Risk factor levels for each security profile are determined by reading the descriptions for each risk factor level and  
2397 choosing the one that most accurately represents the highest risk for the use case.

2398 For each threat, a formula based on the risk factor levels is used to calculate the Likelihood and Impact of the threat, on  
2399 a scale of Low, Medium, and High.

2400 For each threat, both likelihood and impact must be Low before the risk is considered sufficiently mitigated. If the  
2401 calculated levels are not already Low, then mitigations must be applied until they are both Low. The mitigation sets that  
2402 will accomplish this are listed in each threat description.

## 2403 C.4.3 TH-UEVU: Unknown exploitable vulnerabilities

2404 Attacker may use unknown exploitable vulnerabilities in the product implementation to get unauthorised access to  
2405 product assets.

2406 **Table C.4.3-1: Unknown exploitable vulnerabilities**

Risk factors	Likelihood	Security profiles
max(PER, FUN, COM) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-1, SP-2

2407

2408 **Table C.4.3-2: Unknown exploitable vulnerabilities**

Risk factors	Impact	Security profiles
max(PER, FUN, COM) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-1, SP-2

2409

2410 Requirements that mitigate this threat: SSDD, NUTI, LOGG

2411 Mitigations for Likelihood:

- 2412 • Medium to Low: SSCA, SCFS

- 2413 • High to Low: SSCA, (FZ95 or BTIN or IMSL), SCFS, NUTI-1, NUTI-2

2414 Mitigations for Impact:

- 2415 • Medium to Low: LOGG-1, CDST

- 2416 • High to Low: LOGG-1, LOGG-2, CDST

#### 2417 C.4.4 TH-KEVU: Known exploitable vulnerabilities

2418 Attacker may use known exploitable vulnerabilities in the product implementation to get unauthorised access to product  
2419 assets.

2420 **Table C.4.4-1: Known exploitable vulnerabilities**

Risk factors	Likelihood	Security profiles
max(PER, FUN, COM) > 0	High	SP-2, SP-3, SP-4, SP-5
all others	Medium	SP-1

2421

2422 **Table C.4.4-2: Known exploitable vulnerabilities**

Risk factors	Impact	Security profiles
max(PER, FUN) > 0	High	SP-2, SP-3, SP-4, SP-5
all others	Medium	SP-1

2423

2424 Requirements that mitigate this threat: NKEV, SSDD, SCUD, NUTI, LOGG, VULH

2425 All mitigations from TH-UEVU apply (using that requirement's risk formula), in addition to:

2426 Mitigations for Likelihood:

2427 TODO KEVX - the more enterprise-appropriate version of KEVA

- 2428 • Medium to Low: (KEVD or KEVA or KEVX), (KEVT or SCAN), (SUVP or SUAP or SUOE or SUA0),  
2429 VULH

- 2430 • High to Low: KEVD, (KEVA or KEVX), (KEVT or SCAN), (SUAP or SUA0), SUCS, SUA0, SUVH,  
2431 SURP, SURC, SUSR, SUMV, SUED, VULH

#### 2432 C.4.5 TH-UEAC: Unauthorised endpoint access

2433 Attacker may gain unauthorised access to an endpoint in a manner not under control of the product, exposing product  
2434 assets.

2435 **Table C.4.5-1: Unauthorised endpoint access**

Risk factors	Likelihood	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
max (PER, FUN) = 0	Low	SP-1

2436

2437 **Table C.4.5-2: Unauthorised endpoint access**

Risk factors	Impact	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
max (PER, FUN) = 0	Low	SP-1

2438

2439 Requirements that mitigate this threat: AUTH, DMIN, CDST

2440 Mitigations for Likelihood:

- 2441 • Medium to Low: TODO: add risk transfer to environment

- 2442 • High to Low: TODO: add risk transfer to environment

2443 Mitigations for Impact:

- 2444 • Medium to Low: AUTH-3, AUTH-5, CDST

- 2445 • High to Low: AUTH-3, AUTH-4, AUTH-5, CDST

## 2446 C.4.6 TH-RDOS: Denial of service on remote data processing

2447 Attacker launches denial of service attack on remote data processing solution.

2448 **Table C.4.6-1: Denial of service on remote data processing**

Risk factors	Likelihood	Security profiles
RDP = 2 & max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
RDP = 0 or PER = 0 or FUN = 0	Low	SP-1

2449

2450 **Table C.4.6-2: Denial of service on remote data processing**

Risk factors	Impact	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
max (PER, FUN) = 0	Low	SP-1

2451

2452 Requirements that mitigate this threat: AVAI

2453 Mitigations for Likelihood:

- 2454 • Medium to Low: DOST

- 2455 • High to Low: DOST

2456 Mitigations for Impact:

- 2457 • Medium to Low: FDRP, LMEM

- 2458 • High to Low: FDRP, LMEM, FAIR

## 2459 C.4.7 TH-MITM: Machine-in-the-middle

2460 Attacker may read or modify traffic by capturing and relaying activity to and from endpoints.

2461 **Table C.4.7-1: Machine-in-the-middle**

Risk factors	Likelihood	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
max(PER, FUN) = 0	Low	SP-1

2462

2463 **Table C.4.7-2: Machine-in-the-middle**

Risk factors	Impact	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
max (PER, FUN) = 0	Low	SP-1

2464

2465 Table: *Table C.10*

2466 Requirements that mitigate this threat: CRYPT, LOGG

2467 Mitigations for Likelihood:

- 2468 • Medium to Low: CRYPT-2
- 2469 • High to Low: CRYPT-1, CRYPT-2

2470 Mitigations for Impact:

- 2471 • Medium to Low: LOGG-1
- 2472 • High to Low: LOGG-1, LOGG-2

## 2473 C.4.8 TH-LEAK: Sensitive data leaks

2474 Attacker may read sensitive data sent outside the VPN connection by the product.

2475 **Table C.4.8-1: Sensitive data leaks**

Risk factors	Likelihood	Security profiles
DNC = 2 & max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
DNC = 0 or max(PER, FUN) = 0	Low	SP-1

2476

2477 **Table C.4.8-2: Sensitive data leaks**

Risk factors	Impact	Security profiles
PER = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-1, SP-2

2478

2479 Requirements that mitigate this threat: ROUT, CONF, DNSL, IPv6, CRYPT

2480 Mitigations for Likelihood:

- 2481 • Medium to Low: ROUT-1, ROUT-2, CONF-1, CONF-2, CONF-3, CONF-4, CONF-5, DNSL-1, DNSL-2,  
2482 DNSL-7, IPv6-1, IPv6-2
- 2483 • High to Low: ROUT-1, ROUT-2, ROUT-3, CONF-1, CONF-2, CONF-3, CONF-4, CONF-5, DNSL-1,  
2484 DNSL-2, DNSL-3, DNSL-4, DNSL-5, DNSL-6, DNSL-7, IPv6-1, IPv6-2

2485 Mitigations for Impact:

- 2486 • Medium to Low: LOGG-1
- 2487 • High to Low: LOGG-1, LOGG-2

## 2488 C.4.9 TH-PLNS: Transmitting sensitive data in the clear in a single endpoint 2489 VPN

2490 Attacker may read sensitive data transmitted without encryption in a single endpoint VPN.

2491 **Table C.4.9-1: Transmitting sensitive data in the clear in a single endpoint VPN**

Risk factors	Likelihood	Security profiles
CON = 0 & CFG > 0 & max(PER, FUN) = 2	High	SP-3
all others	Medium	SP-2
CON > 0 or CFG = 0 or max(PER, FUN) = 0	Low	SP-1, SP-4, SP-5

2492

2493 **Table C.4.9-2: Transmitting sensitive data in the clear in a single endpoint VPN**

Risk factors	Impact	Security profiles
CON = 0 & max(PER, FUN) = 2	High	SP-3
all others	Medium	SP-2
CON > 0 or max(PER, FUN) = 0	Low	SP-1, SP-4, SP-5

2494

2495 Requirements that mitigate this threat: EISO, CRYPT, AUTH, ROUT, DNSL

2496 Mitigations for Likelihood:

- 2497 • Medium to Low: EISO, CRYPT-2, ROUT-1, AUTH-1, AUTH-2
- 2498 • High to Low: EISO, DNSL-6, CRYPT-1, CRYPT-2, ROUT-1, ROUT-2, ROUT-3, AUTH-1, AUTH-2,  
2499 AUTH-3, AUTH-4, AUTH-5, AUTH-6

2500 Mitigations for Impact:

- 2501 • Medium to Low: LOGG-1
- 2502 • High to Low: LOGG-1, LOGG-2

## 2503 C.4.10 TH-PLNM: Transmitting sensitive data in the clear in multi-endpoint 2504 VPN

2505 Attacker may read sensitive data transmitted without encryption in a VPN which connects multiple endpoints to each  
2506 other.

2507 **Table C.4.10-1: Transmitting sensitive data in the clear in multi-endpoint VPN**

Risk factors	Likelihood	Security profiles
CON > 0 & CFG > 0 & max(PER, FUN) = 2	High	SP-4, SP-5
all others	Medium	none
CON = 0 or CFG = 0 or max(PER, FUN) = 0	Low	SP-1, SP-2, SP-3

2508

2509 **Table C.4.10-2: Transmitting sensitive data in the clear in multi-endpoint VPN**

Risk factors	Impact	Security profiles
CON > 0 & max(PER, FUN) = 2	High	SP-4, SP-5
all others	Medium	none
CON = 0 or max(PER, FUN) = 0	Low	SP-1, SP-2, SP-3

2510

2511 Requirements that mitigate this threat: CRYPT, AUTH, ROUT, DNSL

2512 Mitigations for Likelihood:

- 2513 • Medium to Low: CRYPT-2, ROUT-1, AUTH-1, AUTH-2
- 2514 • High to Low: DNSL-6, CRYPT-1, CRYPT-2, ROUT-1, ROUT-2, ROUT-3, AUTH-1, AUTH-2, AUTH-3,  
2515 AUTH-4, AUTH-5, AUTH-6

2516 Mitigations for Impact:

- 2517 • Medium to Low: LOGG-1
- 2518 • High to Low: LOGG-1, LOGG-2

## 2519 C.4.11 TH-UNAA: Unauthorised authentication

2520 Attacker may attempt to authenticate in an unauthorised manner to get access to product assets.

2521 **Table C.4.11-1: Unauthorised authentication**

Risk factors	Likelihood	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-1, SP-2

2522

2523

**Table C.4.11-2: Unauthorised authentication**

Risk factors	Impact	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2
max (PER, FUN) = 0	Low	SP-1

2524

2525 Requirements that mitigate this threat: AUTH, LOGG

2526

Mitigations for Likelihood:

2527

- Medium to Low: AUTH-6

2528

- High to Low: AUTH-6

2529

Mitigations for Impact:

2530

- Medium to Low: AUTH-3, LOGG-1

2531

- High to Low: AUTH-3, AUTH-4, AUTH-5, LOGG-1, LOGG-2

2532 **C.4.12 TH-LDEL: Attacker removes evidence of compromise**

2533

Attacker may remove evidence of compromise from the endpoint.

2534

**Table C.4.12-1: Attacker removes evidence of compromise**

Risk factors	Likelihood	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Low	SP-1, SP-2

2535

2536

**Table C.4.12-2: Attacker removes evidence of compromise**

Risk factors	Impact	Security profiles
max(PER, FUN) = 2	High	SP-3, SP-4, SP-5
all others	Low	SP-1, SP-2

2537

2538 Requirements that mitigate this threat: LOGG

2539

Mitigations for Likelihood:

2540

- Medium to Low: LOGG-2

2541

- High to Low: LOGG-2

2542

Mitigations for Impact:

2543

- Medium to Low: CDST

2544

- High to Low: CDST

2545 **C.4.13 TH-CNFS: Access to assets via configuration errors in single endpoint  
2546 VPN**

2547

Attacker may use configuration errors to get unauthorised access to product assets in a single endpoint VPN.

2548

**Table C.4.13-1: Access to assets via configuration errors in single endpoint VPN**

Risk factors	Likelihood	Security profiles
CON = 0 & CFG > 0 & max(ADM, COM) = 2 & max(PER, FUN) = 2	High	SP-3
all others	Medium	SP-2
CON > 0 or CFG = 0 or max(ADM, COM) = 0 or max(PER, FUN) = 0	Low	SP-1, SP-4, SP-5

2549

2550 **Table C.4.13-2: Access to assets via configuration errors in single endpoint VPN**

Risk factors	Impact	Security profiles
CON = 0 & max(PER, FUN) = 2	High	SP-3
all others	Medium	SP-2
CON > 0 or max(PER, FUN) = 0	Low	SP-1, SP-4, SP-5

2551

2552 Requirements that mitigate this threat: CONF, TRAF, IPv6, CDST, LOGG

2553 Mitigations for Likelihood:

2554 • Medium to Low: CONF-5, (TRAF-1 or (TRAF-2 and TRAF-3 and TRAF-4)), IPv6-1, IPv6-2

2555 • High to Low: TRAF-1, IPv6-1, IPv6-2

2556 Mitigations for Impact:

2557 • Medium to Low: AUTH-3, LOGG-1, CDST

2558 • High to Low: AUTH-3, AUTH-4, AUTH-5, LOGG-1, LOGG-2, CDST

2559 **C.4.14 TH-CNFM: Access to assets via configuration errors in a multi-**  
2560 **endpoint VPN**

2561 Attacker may use configuration errors to get unauthorised access to product assets in a multi-endpoint VPN.

2562 **Table C.4.14-1: Access to assets via configuration errors in a multi-endpoint VPN**

Risk factors	Likelihood	Security profiles
CON > 0 & CFG > 0 & max(ADM, COM) = 2 & max(PER, FUN) = 2	High	SP-5
all others	Medium	SP-4
CON = 0 or CFG = 0 or max(ADM, COM) = 0 or max(PER, FUN) = 0	Low	SP-1, SP-2, SP-3

2563

2564 **Table C.4.14-2: Access to assets via configuration errors in a multi-endpoint VPN**

Risk factors	Impact	Security profiles
CON > 0 & max(PER, FUN) = 2	High	SP-4, SP-5
all others	Medium	none
CON = 0 or max(PER, FUN) = 0	Low	SP-1, SP-2, SP-3

2565

2566 Requirements that mitigate this threat: CONF, TRAF, IPv6, CDST, LOGG

2567 Mitigations for Likelihood:

2568 • Medium to Low: CONF-5, (NUTI-1 or TRAF-1 or (TRAF-2 and TRAF-3 and TRAF-4)), IPv6-1, IPv6-2

2569 • High to Low: NUTI-1, NUTI-2, IPv6-1, IPv6-2

2570 Mitigations for Impact:

2571 • Medium to Low: AUTH-3, LOGG-1, CDST

2572 • High to Low: AUTH-3, AUTH-4, AUTH-5, LOGG-1, LOGG-2, CDST

2573 **C.4.15 TH-META: Compromise of Personal Data due to metadata and traffic**  
2574 **analysis**

2575 Attacker may use user metadata such as IP addresses and traffic analysis to compromise Personal Data.

2576 **Table C.4.15-1: Compromise of Personal Data due to metadata and traffic analysis**

Risk factors	Likelihood	Security profiles
PER = 2 & FUN = 2	High	SP-3
all others	Medium	SP-1, SP-2, SP-4, SP-5

2577

2578 **Table C.4.15-2: Compromise of Personal Data due to metadata and traffic analysis**

Risk factors	Impact	Security profiles
PER = 2	High	SP-3
all others	Medium	SP-1, SP-2, SP-4, SP-5

2579

2580 Requirements that mitigate this threat:

2581 Mitigations for Likelihood:

- 2582 • Medium to Low: TODO - transfer risk to user
- 2583 • High to Low: TODO - transfer risk to user

2584 Mitigations for Impact:

- 2585 • Medium to Low: LOGG-4, LOGG-5
- 2586 • High to Low: TODO - transfer risk to user

2587 **C.4.16 TH-RCOM: RDPS compromise and isolation**

2588 Attacker may use compromise or isolation errors in remote data processing system to gain access to product assets.

2589 **Table C.4.16-1: RDPS compromise and isolation**

Risk factors	Likelihood	Security profiles
RDP = 2 & PER = 2 & FUN = 2	High	SP-3, SP-5
all others	Medium	SP-4
RDP = 0 or PER = 0 or FUN = 0	Low	SP-1, SP-2

2590

2591 **Table C.4.16-2: RDPS compromise and isolation**

Risk factors	Impact	Security profiles
PER = 2 & FUN = 2	High	SP-3, SP-5
all others	Medium	SP-2, SP-4
PER = 0 & FUN = 0	Low	SP-1

2592

2593 Requirements that mitigate this threat: TODO

2594 Mitigations for Likelihood:

- 2595 • Medium to Low: TODO
- 2596 • High to Low: TODO

2597 Mitigations for Impact:

- 2598 • Medium to Low: LOGG-4, LOGG-5
- 2599 • High to Low: TODO

2600 **C.4.17 TH-USED: Access to data via access to used product**

2601 Attacker may get unauthorised access to confidential data stored on the product through access to or acquisition of a  
 2602 device containing the used product.

2603

**Table C.4.17-1: Access to data via access to used product**

Risk factors	Likelihood	Security profiles
ADM > 0 & PER = 2	High	SP-3, SP-4
all others	Medium	SP-2, SP-5
PER = 0	Low	SP-1

2604

2605

**Table C.4.17-1: Access to data via access to used product**

Risk factors	Impact	Security profiles
PER = 2	High	SP-3, SP-4, SP-5
all others	Medium	SP-2,
PER = 0	Low	SP-1

2606

2607 Requirements that mitigate this threat: AUTH, CDST, SCDL, SDRF

2608 Mitigations for Likelihood:

2609 • Medium to Low: (RSET or INST or DELE), SDRF, SDTR

2610 • High to Low: (RSET or INST or DELE), SDRF, SDTR

2611 Mitigations for Impact:

2612 • Medium to Low: AUTH-5, CDST

2613 • High to Low: AUTH-3, AUTH-4, AUTH-5, CDST

## 2614 C.4.18 TH-CPER: Compromise of Personal Data stored or transmitted by the 2615 product

2616 Attacker may get unauthorised access to Personal Data stored or transmitted by the product.

2617

**Table C.4.18-1: Compromise of Personal Data stored or transmitted by the product**

Risk factors	Likelihood	Security profiles
PER = 2 & FUN = 2	High	SP-3
all others	Medium	SP-1, SP-2, SP-4, SP-5

2618

2619

**Table C.4.18-2: Compromise of Personal Data stored or transmitted by the product**

Risk factors	Impact	Security profiles
PER = 2	High	SP-3
all others	Medium	SP-1, SP-2, SP-4, SP-5

2620

2621 Requirements that mitigate this threat: AUTH, DMIN, CRYPT, AUTH, ROUT, DNSL, CDST, SCDL, SDRF, LOGG

2622 All mitigations from TH-UEAC, TH-MITM, TH-LEAK, TH-PLNS, TH-PLNM, TH-UNAA, TH-CONF, TH-META,  
2623 TH-RCOM, TH-USED apply (using those requirement's risk formula), in addition to:

2624 Mitigations for Impact:

2625 • Medium to Low: NPER-1

2626 • High to Low: NPER-1, NPER-2, NPER-3, NPER-4, LOGG-4, LOGG-5

## 2627 C.5 Mapping of use cases to risk factors and security profiles

2628 **Table C.5-1: Mapping of use cases to risk factors and security profiles**

Use case	Description	CF G	AU T	FU N	AD M	RD P	DN C	CO M	CO N	PE R	SP
UC-1	Individual consumer	1	0	0	2	2	2	0	0	0	SP-1
UC-2	Privacy conscious household	1	0	1	1	1	2	1	0	1	SP-2
UC-3	Journalist or activist	1	1	2	2	2	2	1	0	2	SP-3
UC-4	Small organisation	2	2	1	1	2	2	2	1	1	SP-4
UC-5	Large enterprise	2	2	2	0	2	2	2	2	1	SP-4
UC-6	Enterprise client software	1	0	2	1	0	0	2	0	1	SP-6
UC-7	Mesh network	2	2	1	1	1	2	2	0	1	SP-7

2629

## 2630 C.6 Security profiles

### 2631 C.6.1 General

2632 Security profiles are an informative resource to the assessor. Each security profile is associated with a collection of  
 2633 levels of risk factors. Security profiles will be mapped to specific mitigations for each cybersecurity requirements  
 2634 necessary to treat the risk.

### 2635 C.6.2 Mapping of security profiles to risk factors

2636 **Table C.6.2-1: Mapping of security profiles to risk factors**

Security Profile	Description	CF G	AU T	FU N	AD M	RD P	DN C	CO M	CO N	PE R
SP-1	Individual consumer	1	0	0	2	2	2	0	0	0
SP-2	Privacy conscious household	1	0	1	1	0	2	1	0	1
SP-3	Journalist or activist	1	1	2	2	2	2	1	0	2
SP-4	Small organisation	2	2	1	1	1	2	2	1	1
SP-5	Large enterprise	2	2	2	0	1	2	2	2	1
SP-6	Enterprise client software	1	0	2	1	0	0	2	0	1
SP-7	Mesh network	2	2	1	1	1	2	2	0	1

2637

2638

---

2639 **Annex D (informative):**  
2640 **Risk evaluation guidance**

2641 **D.1 Explanation of Risk Modelling Approach**

2642 The risk modelling approach followed in this document can be applied to two situations:

- 2643 1. *Covered*: For Manufacturers of products with use cases that are present in the text of this document, it states  
2644 the mitigations which the product shall implement and provides guidance on how to verify that the mitigations  
2645 are implemented in a product. Furthermore, it describes why that unique set of mitigations is sufficient for the  
2646 use case.
- 2647 2. *Not Covered*: For Manufacturers of products whose use case does not precisely match use cases covered in the  
2648 present document, the methodology used herein may be further used to derive the appropriate set of  
2649 mitigations for a given product, and to communicate this justification in a structured way. This could inform  
2650 revisions of this document and the list of use cases over time.

2651 **Methodology**

2652 This clause describes the methodology followed in the current text.

- 2653 1. Document a comprehensive range of foreseeable use cases for products of this type.
- 2654 2. For a particular use case, document the inherent and product-specific risk factors likely to affect products of  
2655 that type which are not already covered by other relevant standards.
- 2656 3. For that use case, document environmental risk factors likely to affect products of that type which are not  
2657 already covered by other relevant standards.
- 2658 4. Document a comprehensive list of threats. For each threat, create a formula to estimate the risk level using the  
2659 risk factors.
- 2660 5. For each threat, document appropriate mitigations which should be present to mitigate the specific risk  
2661 depending on the risk level. For each mitigation, also document at least one verification methodology.
- 2662 6. Create a mapping between each use case and each risk factor, assigning a proportionality score. The scoring  
2663 range should start from zero, representing the inapplicability of a risk factor to a use case, and increase  
2664 monotonically based on both the likelihood and severity of potential harm or impact.
- 2665 7. Develop security profiles from the use cases, which are collections of risk factor levels that can be used to fully  
2666 describe the risk levels of all relevant threats. There may be one use case per security profile or multiple. There  
2667 should be as many security profiles as are useful to manufacturers.
- 2668 8. Using the risk factors in the security profiles and the risk formulas and mitigations for all threats, derive the  
2669 completed list of required mitigations for each security profile.

## 2670 D.2 Mapping of risks to requirements

2671 **Table D.2-1: Mapping of risks to requirements**

Threat	Requirements
UEVU	SSDD, NUTI, LOGG
KEVU	NKEV, SSDD, SCUD, NUTI, LOGG, VULH
UEAC	AUTH, DMIN
RDOS	AVAI
MITM	CRYPT, LOGG
LEAK	ROUT, CONF, DNSL, IPv6, CRYPT
PLNS	EISO, CRYPT, AUTH, ROUT, DNSL
PLNM	CRYPT, AUTH, ROUT, DNSL
UNAA	AUTH, LOGG
LDEL	LOGG
CNFS	CONF, TRAF, IPv6, CDST, LOGG
CNFM	CONF, TRAF, IPv6, CDST, LOGG
META	TODO
RCOM	TODO
USED	AUTH, CDST, SCDL, SDRF
CPER	AUTH, DMIN, CRYPT, AUTH, ROUT, DNSL, CDST, SCDL, SDRF, LOGG

2672

## 2673 D.3 Risk acceptance criteria

2674 If the Likelihood and Impact of a risk are already Low or have been reduced to Low by application of mitigations, then  
 2675 the risk is acceptable. Alternatively, the risk may be transferred to the user or the operational environment, given proper  
 2676 justification.

## 2677 D.4 Risks not treated by the requirements

2678 For each risk untreated by the product itself, a corresponding mitigation has been created to explicitly permit the risk to  
 2679 be transferred to the user or operational environment. These are:

- 2680 • MI-DNSL-1
- 2681 • MI-KEVD
- 2682 • MI-SUDC
- 2683 • MI-SUOE
- 2684 • MI-SUAO
- 2685 • MI-DOST
- 2686 • MI-AUTH-6

2687

---

2688 **Annex G:**  
2689 **Guidelines on the implementation of the present**  
2690 **document (informative):**

2691 *This Annex is optional and may be referred to from the Introduction of the document to provide more information on*  
2692 *how to implement the standard.*

2693

## 2694 Annex K:

### 2695 Cryptography (Normative)

#### 2696 K.1.1 Requirement

2697 The default configuration for each security mechanism supported by the product shall use (*one or more*) public  
2698 available cryptographic algorithm, which are:

- 2699 i) listed in the ECCG Agreed Cryptographic Mechanism (ACM) catalogue [1] classified as [CRY-SOTA-listed] or
- 2700 ii) suitable for the corresponding use case, classified as [CRY-SOTA-unlisted] in Annex X

2701 [1] ENISA European Cybersecurity Certification Group: "Agreed Cryptographic Mechanisms, vers 2.0" (ACM)

2702 **NOTE 1:** The use of security mechanism as for example.

2703 *integrity, authentication, access control, secure communication, secure storage and secure update are described in the*  
2704 *main text of this standard.*

## 2705 K.2 Crypto agility

### 2706 K.2.1 Requirement

2707 Where a security mechanism supported by the product uses **in its** the default configuration **a cryptographic algorithm**  
2708 **that is:**

- 2709 i) listed in the CRY-SOTA catalogue; or
- 2710 ii) referenced in a crypto catalogue within the context of K.1.1.(ii) in accordance to the Cyber Resilience Act (CRA).

2711 **and that algorithm** is expected to be deprecated within the intended lifetime of the product, the product shall provide a  
2712 mechanism for updating the cryptographic algorithm or deprecating its usage.

2713 **EXAMPLE 1 :** Hybridization serves as a strategy to mitigate the case of deprecation, For instance , if within a secure  
2714 storage mechanism, it can involve combination classical asymmetric cryptographic algorithms with quantum.resistant  
2715 algorithm through dual encapsulation. This approach ensures data confidentiality data over a specific future time  
2716 horizon , assuming that at least one of the employed algorithm remains uncompromised during this period

2717 **NOTE 1:** To maintain SOTA for cryptographic algorithm within the intended lifetime of the product concepts to  
2718 consider are crypto agility additional to the capability of updating cryptographic algorithms on the product in  
2719 accordance to Secure Update and Secure Communication mechanism.

2720 **NOTE 2:** The [ACM] listing consist of wo classes of SOTA algorithms; Legacy mechanisms with an expiry date as  
2721 defined in ACM, and Recommended mechanisms with no set expiry date.

2722 **NOTE 3:** For products that cannot have their cryptographic algorithms updated for example if the implementation or  
2723 part uses a hardware-based root of trust, it is important to check if the intended lifetime of the equipment does not  
2724 exceed the recommended usage lifetime of their cryptographic algorithms. Thereby the implementation of an algorithm  
2725 can include the specific implementation of their parameters e.g. their key length.

2726 **NOTE 4:** If a component storing the algorithm or corresponding parameters of a main product is replaced by a new  
2727 component, the product is considered as a new product according to the New Legislative Framework Blue Guide, if the  
2728 replacement provides a substantial modification to the main product.

2729 *Last update on 2026-04-15*

2730 [1] e.g. BSI – BSI TR-02102-1, Cryptographic Mechanisms: Recommendations and Key Lengths , Vers. 2026-01,  
2731 January 31, 2026

2732 [2] e.g. EPC342-08 /Version 15.0 /Guidelines on cryptographic algorithms usage and key management - PPSG / 7  
2733 March 2025

2734 In addition to general cryptographic catalogues, certain industry sectors maintain their own specialized algorithm  
2735 catalogues optimized for specific threat models, hardware and/or software architectures or performance constraints.  
2736 These vertical use-case specific cryptographic algorithm catalogues may serve as supporting evidence when they  
2737 explicitly recognize algorithms as suitable for the intended use case, *e.g. the ARM Confidential Compute Architecture*  
2738 *(CCA) Security Model, Section 12.3.3 ("Memory Encryption")*, recommends specific algorithms for memory protection  
2739 in dedicated hardware environments, including: *QARMA-128 with a 256-bit key and AES-128-XEX with two*  
2740 *independent 128-bit keys* [3] European Vulnerability Database established pursuant

2741 to Article 12(2) of Directive (EU) 2022/2555, <https://euvd.enisa.europa.eu/ENISA>

2742 [4] SRP = , Single Reporting Platform CRA

2743 <https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp>

2744 [5] NCCA =

2745 [National Cybersecurity Certification Authorities](#)

2746

2747

2748 [6] defined in [ACM]

2749

---

2750 Annex R:  
2751 Remote Data Processing Solutions (Normative)  
2752

---

2753 Annex S:  
2754       Secure Updates (Normative)  
2755

2756 **Annex X:**  
 2757 **Product specific state of the art cryptography**  
 2758 **(Normative)**

2759 **X.1 State of the Art Cryptography (CRY-SOTA-unlisted)**

2760 This annex provides additional generic requirements around the use of state of the art cryptography. Annex K classifies  
 2761 cryptographic algorithm primitives as CRY-SOTA if they are listed in the ENISA ACM [REF] and are suitable for the  
 2762 implementation of supported security mechanisms of the product. This annex lists additional cryptographic algorithm  
 2763 primitives and schemes that are commonly existing on the market for VPNs that are classified as CRY-SOTA.

2764 **X.2 Symmetric atomic primitives**

2765 **X.2.1 Block ciphers**

2766 No additional primitives.

2767 **X.2.2 Stream ciphers**

2768 Block ciphers can be configured to behave like stream ciphers using counter (CTR) mode, as described in [ACM]  
 2769 clause 3.1. In addition, the stream ciphers included in Table X.2.2-1 are agreed as state of the art.

2770 Table: Table X.2.2-1: State of the art stream ciphers. | Primitive | Parameter's size | Notes | |-----|-----|  
 2771 -----|-----| ChaCha20 (RFC 8439) | 256 bit (key) | A modern stream cipher used in VPNs and TLS 1.3.  
 2772 Preferred for devices without AES hardware acceleration. Extending ChaCha20 with a larger 24-byte nonce  
 2773 (XChaCha20) to mitigate nonce collisions is included in this primitive. |

2774 **X.2.3 Hash Functions**

2775 The additional hash functions are included in table X.2.3-1 are agreed as state of the art.

2776 Table: Table X.2.3-1: State of the art hash functions. | Primitive | Parameter's size | Notes | |-----|-----|  
 2777 -----|-----| Blake2b (RFC7693, NIST IR 7896) | 512 bit | A modern cryptographic hash function which  
 2778 targets 64-bit platform (blake2s). | Blake2s (RFC7693, NIST IR 7896) | 256 bit | A modern cryptographic hash  
 2779 function which targets 64-bit platform. |

2780 **X.3 Symmetric constructions**

2781 **X.3.1 Confidentiality modes of operation: encryption/decryption modes**

2782 No additional schemes.

2783 **X.3.2 Specific confidentiality modes: disk encryption**

2784 No additional schemes.

2785 **X.3.3 Integrity modes: message authentication codes**

2786 The additional message authentication codes included in Table X.3.3-1 are agreed as state of the art.

2787 Table: Table X.3.3-1: State of the art message authentication codes. | Scheme | Parameter's size | Notes | |-----|-----|  
 2788 -----|-----| Poly1305 (RFC 8439) | 256 bit key | Paired with ChaCha20  
 2789 in TLS 1.3. | HMAC-blake2s (RFC 2104, RFC 7693) | 256 bit key | Used in modern VPN protocols. | UMAC (RFC  
 2790 4418) | 128 bit key | Used in SSH configurations for managing VPN servers |

2791 **X.3.4 Symmetric entity authentication schemes**

2792 No additional schemes.

### 2793 X.3.5 Authenticated encryption

2794 The additional authentication encryption schemes included in Table X.3.5-1 are agreed as state of the art.

2795 Table: Table X.3.5-1: State of the art authentication encryption schemes. | Scheme | Parameter's size | Notes | |  
 2796 |-----|-----| | ChaCha20-Poly1305 (RFC8439) | 256 bit(key) | Standard AEAD for TLS 1.3.  
 2797 Extending ChaCha20 with a larger 24-byte nonce (XChaCha20) to mitigate nonce collisions is included in this  
 2798 primitive. |

### 2799 X.3.6 Key protection

2800 No additional schemes.

### 2801 X.3.7 Key derivation functions

2802 The additional key derivation functions included in Table X.3.7-1 are agreed as state of the art.

2803 Table: Table X.3.7-1: State of the art key derivation functions. | Scheme | Parameter's size | Notes | |  
 2804 |-----|-----| | Blake2s (RFC 7693) | Key: 128 bit  
 2805 | Blake2s is used in modern VPN protocols. Blake supportes a keyed mode which makes it a suitable key derivation  
 2806 function. | | Blake2b (RFC 7693) | Key: 256 bit | Blake2b is used in modern VPN protocols. Blake supportes a keyed  
 2807 mode which makes it a suitable key derivation function. | | SipHash24 (<https://eprint.iacr.org/2012/351>) | Key: 128 bit |  
 2808 A pseudorandom random function (PRF) optimized for short inputs. Allowed use-cases for this PRF is limited to  
 2809 non-security critical use-cases, such as, for example, hash table creation and ID generation. For other use-cases, refere  
 2810 to other approved cryptographic functions. |

### 2811 X.3.8 Password protection/password hashing mechanisms

2812 The additional Password protection/password hashing mechanisms are included in table X.3.8-1 are agreed as state of  
 2813 the art.

2814 Every password based hashing mechansim shall include a unique random salt (at least 16 bytes) per user.

2815 Table: Table X.3.8-1: State of the art Password protection/password hashing mechanisms. | Primitive | Parameter's size |  
 2816 Notes | |-----| | Argon2id (RFC 9106, BSI-TR-02102-1) | (Output: 32  
 2817 bytes, OpsLimit: 2, Memory: 19 MiB, Threats: 1) or higher | A resource intensive hash function to protect passwords.  
 2818 Can also be used as a KDF to derive secret keys from passwords. Generated entropy depends on the entropy of the  
 2819 password. | | scrypt (RFC 7914) | (Cost:  $2^{17}$ , block size 1024 bytes, parallelization 1) or higher | A resource intensive  
 2820 hash function to protect passwords. Can also be used as a KDF to derive secret keys from passwords. Generated entropy  
 2821 depends on the entropy of the password. |

### 2822 X.3.9 Key combiners

## 2823 X.4 Asymmetric atomic primitives

### 2824 X.4.1 RSA/Integer factorization

2825 No additional primitives.

### 2826 X.4.2 Discrete logarithm in finite fields

2827 No additional primitives.

### 2828 X.4.3 Discrete logarithm in elliptic curves

2829 The additional elliptic curve parameters included in Table X.4.3-1 are agreed as state of the art.

2830 [!Note] It is noted that all mentioned curves in this sections are included in the  
 2831 ECDH umbrella and are thus usable for all applicable ECDH use cases.

2832 Table: Table X.4.3-1: Additional elliptic curve parameters agreed as start of the art. | Scheme | Curve | Notes | |  
 2833 |-----|-----| | X25519 / Ed25519 (RFC 8410) | Curve25519 | Standard for TLS 1.3, and SSH and  
 2834 various VPN protocols. |

## 2835 X.4.4 Learning with errors in (structured) lattices

2836 No additional LWE mechanisms.

## 2837 X.4.5 Hash function preimage resistance

2838 No additional schemes.

## 2839 X.4.6 Other intractable problems

2840 No additional schemes.

# 2841 X.5 Asymmetric constructions

## 2842 X.5.1 Asymmetric encryption scheme

2843 No additional schemes.

## 2844 X.5.2 Digital signature

2845 The additional digital signature schemes included in Table X.5.2-1 are agreed as state of the art.

2846 Table: Table X.5.2-1: State of the art digital signature schemes. | Scheme | Parameter's sizes | Notes | |-----|-----|  
2847 -----|-----| Ed25519 (RFC 8032) | 256 bit key | Used for TLS and formally known as EdDSA. |

## 2848 X.5.3 Asymmetric entity authentication schemes

2849 The additional asymmetric entity authentication schemes included in table X.5.3-1 are agreed as state of the art.

2850 **Table X.5.3-1: State of the art entity authentication schemes.** | Scheme | Parameter's sizes | Notes | |-----|-----|  
2851 -----|-----| Ed25519-256 with Curve25519 (RFC 8420) | 256 bit | Allowing Ed25519 in modern VPN  
2852 protocols. |

## 2853 X.5.4 Key establishment and key encapsulation

2854 No additional primitives.

# 2855 X.6 Cryptographic Industry Standards

2856 The following industry standards serve as a baseline for approved cryptographic algorithm and are considered approved  
2857 as CRY-SOTA.

2858 **Table X.6.1-1: National catalogues defined as CRY-SOTA.** | Cryptographic Mechanisms | Version | Notes | |-----|  
2859 -----|-----|-----|-----| BSI

2860 TR-02102-1 "Cryptographic Mechanisms: Recommendations and Key Lengths"

2861 (<https://www.bsi.bund.de/dok/TR-02102-en>) | 2026-01 | |

2862 | BSI TR-02102-2 "Cryptographic Mechanisms: Recommendations and Key Lengths: Use of Transport Layer Security

2863 (TLS)" (<https://www.bsi.bund.de/dok/TR-02102-en>) | 2026-01 | TLS is often used as a baseline for common tunneling

2864 protocols. | | BSI TR-02102-3 "Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Internet

2865 Protocol Security (IPsec) and Internet Key Exchange (IKEv2)" (<https://www.bsi.bund.de/dok/TR-02102-en>) | 2026-01 |

2866 | | BSI TR-02102-4 "Cryptographic Mechanisms: Recommendations and Key Lengths – Use of Secure Shell (SSH)" |

2867 2026-01 | SSH can act as tunnel, but mainly is used for node maintenance and deployments. |

2868

---

## 2869 History

2870 The following table will automatically be filled in by the ETSI Secretariat.

Document History		
Version	Date	Milestone
	<#>	

2871