



**Cyber Security (CYBER);
CRA;
Cybersecurity requirements for
Virtual Private Networks (VPNs)**

get full document from standards.iteh.ai

ReferenceDEN/CYBER-EUS-005

KeywordsCRA, cybersecurity, VPN

ETSI

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

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

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

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

Copyright Notification

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

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

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	19
Foreword.....	19
Modal verbs terminology	20
Introduction	20
1 Scope	21
2 References	21
2.1 Normative references	21
2.2 Informative references	21
3 Definition of terms, symbols, abbreviations and naming conventions	23
3.1 Terms	23
3.2 Symbols	24
3.3 Abbreviations.....	24
3.4 Naming conventions	25
4 Product context.....	25
4.1 Product Functions	25
4.1.1 Overview	25
4.1.2 Potential functions of a node	26
4.1.2.1 Authentication	26
4.1.2.2 Access control	26
4.1.2.3 Traffic encryption	26
4.1.2.4 Routing	26
4.1.2.5 Filtering	26
4.1.3 Potential roles of nodes	26
4.1.4 Capabilities of nodes	26
4.2 Product Architecture	27
4.2.1 Product overview	27
4.2.2 Network topology and relationship between nodes	27
4.2.3 VPN client.....	28
4.2.4 VPN server, VPN gateway	29
4.2.4.1 Server & gateway responsibilities	29
4.2.4.2 Server & gateway remote data processing.....	29
4.2.5 Management server	29
4.3 Operational Environment.....	29
4.3.1 General description	29
4.3.2 Hardware environment.....	29
4.3.3 Software environment	30
4.3.4 Connectivity aspects.....	31
4.4 Distribution of Security Functions.....	31
4.4.1 Cybersecurity function distribution overview	31
4.4.2 Cybersecurity Functionalities Offered to Integrated Components	32
4.4.3 Cybersecurity functions required from the environment.....	32
4.5 Users	32
4.6 Use Cases.....	33
4.6.1 Introduction to Use Cases	33
4.6.2 UC-1 Individual consumer	33
4.6.3 UC-2 Privacy conscious household.....	33
4.6.4 UC-3 Journalist, activist, legal professionals	33
4.6.5 UC-4 Small enterprise, small not-for-profit organization	34
4.6.6 UC-5 Large enterprise	34
4.6.7 UC-6 Enterprise with independent VPN infrastructure.....	34
4.6.8 UC-7 Mesh Network	34
5 Technical requirements for products	35

5.1	Introduction - Applicability of the requirements	35
5.2	Appropriate level of cybersecurity	37
5.2.1	Overview	37
5.2.1.1	CRA Relevance	37
5.2.1.2	Secure software design and development	37
5.2.2	REQ-SSD-01 Memory access error prevention	37
5.2.2.1	Requirement	37
5.2.2.2	Applicability	37
5.2.3	REQ-SSD-02 Resilience against potentially untrusted inputs	38
5.2.3.1	Requirement	38
5.2.3.2	Applicability	38
5.2.4	REQ-SSD-03 Applicability of Annex R	38
5.2.4.1	Requirement	38
5.2.4.2	Applicability	38
5.2.4.3	Guidance	39
5.2.5	Mapping of requirements to use cases	39
5.3	No known exploitable vulnerabilities	39
5.3.1	Overview	39
5.3.2	REQ-KEV-01 Testing for known exploitable vulnerabilities	39
5.3.2.1	Requirement	39
5.3.2.2	Applicability	39
5.3.2.3	Guidance	40
5.3.3	Mapping of requirements to use cases	40
5.4	Secure by default configuration	40
5.4.1	Overview	40
5.4.2	REQ-SBD-01 Unintentional disabling of cybersecurity features	40
5.4.2.1	Requirement	40
5.4.2.2	Applicability	40
5.4.3	Mapping of requirements to use cases	41
5.5	Security updates	41
5.5.1	Overview	41
5.5.2	REQ-SU-01 Automatic secure update before or during first use	41
5.5.2.1	Requirement	41
5.5.2.2	Applicability	41
5.5.3	REQ-SU-02 Automatic secure update via operational environment before or during first use	41
5.5.3.1	Requirement	41
5.5.3.2	Applicability	41
5.5.4	REQ-SU-03 Secure update via product	42
5.5.4.1	Requirement	42
5.5.4.2	Applicability	42
5.5.5	REQ-SU-04 Automatic secure update via product	42
5.5.5.1	Requirement	42
5.5.5.2	Applicability	42
5.5.6	REQ-SU-05 Secure update provided by operational environment	43
5.5.6.1	Requirement	43
5.5.6.2	Applicability	43
5.5.7	REQ-SU-06 Automatic secure update provided by operational environment	43
5.5.7.1	Requirement	43
5.5.7.2	Applicability	43
5.5.8	REQ-SU-07 Updates are signed and verified before installation	44
5.5.8.1	Requirement	44
5.5.8.2	Applicability	44
5.5.9	REQ-SU-08 Only authorized software updates	44
5.5.9.1	Requirement	44
5.5.9.2	Applicability	44
5.5.10	REQ-SU-09 Secure update has validly signed hash	44
5.5.10.1	Requirement	44
5.5.10.2	Applicability	44
5.5.10.3	Guidance	45
5.5.11	REQ-SU-10 Invalidated update is rejected	45
5.5.11.1	Requirement	45
5.5.11.2	Applicability	45

5.5.11.3	Guidance	45
5.5.12	REQ-SU-11 Signing keys have strictly scoped usage	46
5.5.12.1	Requirement	46
5.5.12.2	Applicability	46
5.5.12.3	Guidance	46
5.5.13	REQ-SU-12 Signing keys have not been revoked or otherwise marked untrusted	46
5.5.13.1	Requirement	46
5.5.13.2	Applicability	46
5.5.13.3	Guidance	47
5.5.14	REQ-SU-13 Reject update to current or previous version	47
5.5.14.1	Requirement	47
5.5.14.2	Applicability	47
5.5.15	REQ-SU-14 Updates not applied from expired sources	48
5.5.15.1	Requirement	48
5.5.15.2	Applicability	48
5.5.16	Mapping of requirements to use cases	48
5.6	Authentication and access control	48
5.6.1	Overview	48
5.6.2	REQ-AAC-01 Authentication of cybersecurity-relevant nodes	49
5.6.2.1	Requirement	49
5.6.2.2	Applicability	49
5.6.2.3	Guidance	49
5.6.3	REQ-AAC-02 Encryption of transmitted credentials	49
5.6.3.1	Requirement	49
5.6.3.2	Applicability	49
5.6.4	REQ-AAC-03 Authentication timeout	49
5.6.4.1	Requirement	49
5.6.4.2	Applicability	50
5.6.5	REQ-AAC-04 Cloned credentials detection	50
5.6.5.1	Requirement	50
5.6.5.2	Applicability	50
5.6.6	REQ-AAC-05 Forced revocation of authorization of endpoints	50
5.6.6.1	Requirement	50
5.6.6.2	Applicability	51
5.6.7	REQ-AAC-06 Brute force protection	51
5.6.7.1	Requirement	51
5.6.7.2	Applicability	51
5.6.8	REQ-AAC-07 Authorization of endpoints	51
5.6.8.1	Requirement	51
5.6.8.2	Applicability	52
5.6.9	REQ-AAC-08 Fine-grain access control	52
5.6.9.1	Requirement	52
5.6.9.2	Applicability	52
5.6.10	Mapping of requirements to use cases	52
5.7	Confidentiality protection	53
5.7.1	Overview	53
5.7.1.1	CRA relevance	53
5.7.1.2	Confidentiality of DNS queries	53
5.7.2	REQ-CON-01 VPN routing stays in effect until VPN connection deactivated	53
5.7.2.1	Requirement	53
5.7.2.2	Applicability	53
5.7.3	REQ-CON-02 VPN routing stays in effect during network-level tunnel failure	54
5.7.3.1	Requirement	54
5.7.3.2	Applicability	54
5.7.4	REQ-CON-03 Tunnel all traffic by default	54
5.7.4.1	Requirement	54
5.7.4.2	Applicability	54
5.7.5	REQ-CON-04 Endpoint to endpoint encryption	54
5.7.5.1	Requirement	54
5.7.5.2	Applicability	55
5.7.6	REQ-CON-05 Inform user of visibility of DNS queries	55
5.7.6.1	Requirement	55

5.7.6.2	Applicability	55
5.7.7	REQ-CON-06 Configurable exclusive DNS routing	55
5.7.7.1	Requirement	55
5.7.7.2	Applicability	56
5.7.8	REQ-CON-07 Exclusive DNS routing by default.....	56
5.7.8.1	Requirement	56
5.7.8.2	Applicability	56
5.7.9	REQ-CON-08 DNS configuration consistency	56
5.7.9.1	Requirement	56
5.7.9.2	Applicability	56
5.7.10	REQ-CON-09 Secure DNS protocols	57
5.7.10.1	Requirement	57
5.7.10.2	Applicability	57
5.7.11	REQ-CON-10 No DNS leaks during network-level tunnel failure	57
5.7.11.1	Requirement	57
5.7.11.2	Applicability	57
5.7.12	REQ-CON-11 Block IPv6 if Unsupported.....	57
5.7.12.1	Requirement	57
5.7.12.2	Applicability	58
5.7.13	REQ-CON-12 Full Support if Claimed	58
5.7.13.1	Requirement	58
5.7.13.2	Applicability	58
5.7.14	REQ-CON-13 Use conformant cryptography	58
5.7.14.1	Requirement	58
5.7.14.2	Applicability	58
5.7.15	REQ-CON-14 Protect confidentiality of data stored on the product.....	59
5.7.15.1	Requirement	59
5.7.15.2	Applicability	59
5.7.16	REQ-CON-15 Inform user of limits of privacy protection	59
5.7.16.1	Requirement	59
5.7.16.2	Applicability	60
5.7.17	Mapping of requirements to use cases.....	60
5.8	Integrity protection	60
5.8.1	Overview	60
5.8.2	REQ-INT-01 VPN client restores any system configuration it changes to its previous state after the VPN connection ends.....	60
5.8.2.1	Requirement	60
5.8.2.2	Applicability	61
5.8.3	REQ-INT-02 VPN client provides a method to restore any system configuration it changes to its previous state.....	61
5.8.3.1	Requirement	61
5.8.3.2	Applicability	61
5.8.4	REQ-INT-03 VPN client does not degrade system security	61
5.8.4.1	Requirement	61
5.8.4.2	Applicability	61
5.8.5	REQ-INT-04 Application protocol validity checks.....	62
5.8.5.1	Requirement	62
5.8.5.2	Applicability	62
5.8.6	REQ-INT-05 Application protocol validity checks by operational environment.....	62
5.8.6.1	Requirement	62
5.8.6.2	Applicability	62
5.8.7	Mapping of requirements to use cases.....	63
5.9	Data minimisation.....	63
5.9.1	Overview	63
5.9.2	REQ-DM-01 Data minimisation across the product	63
5.9.2.1	Requirement	63
5.9.2.2	Applicability	63
5.9.3	REQ-DM-02 No Personal Data sent outside endpoint.....	63
5.9.3.1	Requirement	63
5.9.3.2	Applicability	64
5.9.4	REQ-DM-03 Minimise Personal Data required for service provisioning and payment.....	64
5.9.4.1	Requirement	64

5.9.4.2	Applicability	64
5.9.5	REQ-DM-04 Minimise Personal Data stored.....	64
5.9.5.1	Requirement	64
5.9.5.2	Applicability	64
5.9.6	REQ-DM-05 No data persistence or storage enabled on exit nodes	65
5.9.6.1	Requirement	65
5.9.6.2	Applicability	65
5.9.7	Mapping of requirements to use cases.....	65
5.10	Availability protection	65
5.10.1	Overview	65
5.10.2	REQ-AP-01 Fast packet drop.....	65
5.10.2.1	Requirement	65
5.10.2.2	Applicability	66
5.10.3	REQ-AP-02 Limit memory usage	66
5.10.3.1	Requirement	66
5.10.3.2	Applicability	66
5.10.4	REQ-AP-03 Availability protection provided by operational environment	66
5.10.4.1	Requirement	66
5.10.4.2	Applicability	66
5.10.5	REQ-AP-04 Rate limit unauthenticated traffic	67
5.10.5.1	Requirement	67
5.10.5.2	Applicability	67
5.10.6	Mapping of requirements to use cases.....	67
5.11	Non-interference	67
5.11.1	Overview	67
5.11.2	REQ-IM-01 No route between different endpoints by default	67
5.11.2.1	Requirement	67
5.11.2.2	Applicability	68
5.11.3	REQ-IM-02: Minimise data transmitted to unverified sources	68
5.11.3.1	Requirement	68
5.11.3.2	Applicability	68
5.11.3.3	Guidance.....	68
5.11.4	Mapping of requirements to use cases.....	68
5.12	Attack surface minimisation	69
5.12.1	Overview	69
5.12.2	REQ-MAS-01 Unnecessary VPN client permissions	69
5.12.2.1	Requirement	69
5.12.2.2	Applicability	69
5.12.2.3	Guidance.....	69
5.12.3	Mapping of requirements to use cases.....	69
5.13	Exploit mitigation	69
5.13.1	Overview	69
5.13.2	REQ-EMM-01 Route traffic from other sources/destination disabled by default.....	70
5.13.2.1	Requirement	70
5.13.2.2	Applicability	70
5.13.3	REQ-EMM-02 Notify user if routing traffic from other sources/destination	70
5.13.3.1	Requirement	70
5.13.3.2	Applicability	70
5.13.4	REQ-EMM-03 No routing traffic from other sources/destination if not necessary for services	70
5.13.4.1	Requirement	70
5.13.4.2	Applicability	70
5.13.5	Mapping of requirements to use cases.....	71
5.14	Monitoring	71
5.14.1	Overview	71
5.14.1.1	CRA requirement.....	71
5.14.1.2	Minimum scope	71
5.14.1.3	Monitoring restrictions	71
5.14.2	REQ-LOG-01 Local event logging	72
5.14.2.1	Requirement	72
5.14.2.2	Applicability	72
5.14.3	REQ-LOG-02 Internal event logging.....	72
5.14.3.1	Requirement	72

5.14.3.2	Applicability	72
5.14.4	REQ-LOG-03 Remote Logging to RDPS	73
5.14.4.1	Requirement	73
5.14.4.2	Applicability	73
5.14.4.3	Guidance	73
5.14.5	REQ-LOG-04 Privacy-preserving logs policy and traffic anonymization	73
5.14.5.1	Requirement	73
5.14.5.2	Applicability	73
5.14.6	Mapping of requirements to use cases	74
5.15	Factory reset and data portability	74
5.15.1	Overview	74
5.15.2	REQ-DRT-01 Secure deletion via "factory reset"	74
5.15.2.1	Requirement	74
5.15.2.2	Applicability	74
5.15.3	REQ-DRT-02 Secure deletion via reinstallation	75
5.15.3.1	Requirement	75
5.15.3.2	Applicability	75
5.15.4	REQ-DRT-03 Secure data read from product	75
5.15.4.1	Requirement	75
5.15.4.2	Applicability	75
5.15.5	REQ-DRT-04 Secure data export	75
5.15.5.1	Requirement	75
5.15.5.2	Applicability	76
5.15.6	Mapping of requirements to use cases	76
6	Assessment criteria for compliance with technical requirements	76
6.1	Introduction to the assessment and compliance criteria	76
6.2	Appropriate level of cybersecurity	78
6.2.1	Overview	78
6.2.2	REQ-SSD-01 Memory access error prevention	78
6.2.2.0	Overview	78
6.2.2.1	Objective	78
6.2.2.2	Preparation	78
6.2.2.3	Activities	78
6.2.2.4	Verdict	79
6.2.2.5	Evidence	79
6.2.2.6	Guidance for "risk-based approach"	80
6.2.3	REQ-SSD-02 Resilience against potentially untrusted inputs	80
6.2.3.1	Objective	80
6.2.3.2	Preparation	80
6.2.3.3	Activities	81
6.2.3.4	Verdict	81
6.2.3.5	Evidence	81
6.2.3.6	Guidance	81
6.2.4	REQ-SSD-03 Applicability of Annex R	81
6.3	No known exploitable vulnerabilities	81
6.3.1	Overview	81
6.3.2	REQ-KEV-01 Testing for known exploitable vulnerabilities	82
6.3.2.1	Objective	82
6.3.2.2	Preparation	82
6.3.2.3	Activities	82
6.3.2.4	Verdict	82
6.3.2.5	Evidence	82
6.4	Secure by default configuration	82
6.4.1	Overview	82
6.4.2	REQ-SBD-01 Unintentional disabling of cybersecurity features	82
6.4.2.1	Objective	82
6.4.2.2	Preparation	83
6.4.2.3	Activities	83
6.4.2.4	Verdict	83
6.4.2.5	Evidence	83
6.5	Security updates	83

6.5.1	Overview	83
6.5.2	REQ-SU-01 Automatic secure update before or during first use	83
6.5.2.1	Objective	83
6.5.2.2	Preparation.....	83
6.5.2.3	Activities	83
6.5.2.4	Verdict.....	83
6.5.2.5	Evidence	84
6.5.3	REQ-SU-02 Automatic secure update via operational environment before or during first use	84
6.5.3.1	Objective	84
6.5.3.2	Preparation.....	84
6.5.3.3	Activities	84
6.5.3.4	Verdict.....	84
6.5.3.5	Evidence	84
6.5.4	REQ-SU-03 Secure update via product.....	85
6.5.4.1	Objective	85
6.5.4.2	Preparation.....	85
6.5.4.3	Activities	85
6.5.4.4	Verdict.....	85
6.5.4.5	Evidence	85
6.5.5	REQ-SU-04 Automatic secure update via product.....	85
6.5.5.1	Objective	85
6.5.5.2	Preparation.....	85
6.5.5.3	Activities	85
6.5.5.4	Verdict.....	86
6.5.5.5	Evidence	86
6.5.6	REQ-SU-05 Secure update provided by operational environment.....	86
6.5.6.1	Objective	86
6.5.6.2	Preparation.....	86
6.5.6.3	Activities	86
6.5.6.4	Verdict.....	86
6.5.6.5	Evidence	86
6.5.7	REQ-SU-06 Automatic secure update provided by operational environment.....	86
6.5.7.1	Objective	86
6.5.7.2	Preparation.....	86
6.5.7.3	Activities	86
6.5.7.4	Verdict.....	87
6.5.7.5	Evidence	87
6.5.8	REQ-SU-07 Updates are signed and verified before installation	87
6.5.8.1	Objective	87
6.5.8.2	Preparation.....	87
6.5.8.3	Activities	87
6.5.8.4	Verdict.....	87
6.5.8.5	Evidence	87
6.5.9	REQ-SU-08 Only authorized software updates.....	87
6.5.9.1	Objective	87
6.5.9.2	Preparation.....	87
6.5.9.3	Activities	87
6.5.9.4	Verdict.....	88
6.5.9.5	Evidence	88
6.5.10	REQ-SU-09 Secure update has validly signed hash.....	88
6.5.10.1	Objective	88
6.5.10.2	Preparation.....	88
6.5.10.3	Activities	88
6.5.10.4	Verdict.....	88
6.5.10.5	Evidence	88
6.5.11	REQ-SU-10 Invalidated update is rejected	88
6.5.11.1	Objective	88
6.5.11.2	Preparation.....	88
6.5.11.3	Activities	88
6.5.11.4	Verdict.....	89
6.5.11.5	Evidence	89
6.5.12	REQ-SU-11 Signing keys have strictly scoped usage.....	89

6.5.12.1	Objective	89
6.5.12.2	Preparation.....	89
6.5.12.3	Activities	89
6.5.12.4	Verdict.....	89
6.5.12.5	Evidence	89
6.5.13	REQ-SU-12 Signing keys have not been revoked or otherwise marked untrusted	89
6.5.13.1	Objective	89
6.5.13.2	Preparation.....	89
6.5.13.3	Activities	90
6.5.13.4	Verdict.....	90
6.5.13.5	Evidence	90
6.5.14	REQ-SU-13 Reject update to current or previous version	90
6.5.14.1	Objective	90
6.5.14.2	Preparation.....	90
6.5.14.3	Activities	90
6.5.14.4	Verdict.....	90
6.5.14.5	Evidence	90
6.5.15	REQ-SU-14 Updates not applied from expired sources.....	90
6.5.15.1	Objective	90
6.5.15.2	Preparation.....	91
6.5.15.3	Activities	91
6.5.15.4	Verdict.....	91
6.5.15.5	Evidence	91
6.6	Authentication and access control	91
6.6.1	Overview	91
6.6.2	REQ-AAC-01 Authentication of cybersecurity-relevant nodes	91
6.6.2.1	Objective	91
6.6.2.2	Preparation.....	91
6.6.2.3	Activities	91
6.6.2.4	Verdict.....	91
6.6.2.5	Evidence	91
6.6.3	REQ-AAC-02 Encryption of transmitted credentials.....	92
6.6.3.1	Objective	92
6.6.3.2	Preparation.....	92
6.6.3.3	Activities	92
6.6.3.4	Verdict.....	92
6.6.3.5	Evidence	92
6.6.4	REQ-AAC-03 Authentication timeout.....	92
6.6.4.1	Objective	92
6.6.4.2	Preparation.....	92
6.6.4.3	Activities	92
6.6.4.4	Verdict.....	93
6.6.4.5	Evidence	93
6.6.5	REQ-AAC-04 Cloned credentials detection	93
6.6.5.1	Objective	93
6.6.5.2	Preparation.....	93
6.6.5.3	Activities	93
6.6.5.4	Verdict.....	93
6.6.5.5	Evidence	93
6.6.6	REQ-AAC-05 Forced revocation of authorization of endpoints	93
6.6.6.1	Objective	93
6.6.6.2	Preparation.....	93
6.6.6.3	Activities	93
6.6.6.4	Verdict.....	94
6.6.6.5	Evidence	94
6.6.7	REQ-AAC-06 Brute force protection.....	94
6.6.7.1	Objective	94
6.6.7.2	Preparation.....	94
6.6.7.3	Activities	94
6.6.7.4	Verdict.....	94
6.6.7.5	Evidence	94
6.6.8	REQ-AAC-07 Authorization of endpoints.....	94

6.6.8.1	Objective	94
6.6.8.2	Preparation.....	94
6.6.8.3	Activities	95
6.6.8.4	Verdict.....	95
6.6.8.5	Evidence	95
6.6.9	REQ-AAC-08 Fine-grain access control.....	95
6.6.9.1	Objective	95
6.6.9.2	Preparation.....	95
6.6.9.3	Activities	95
6.6.9.4	Verdict.....	95
6.6.9.5	Evidence	95
6.7	Confidentiality protection	95
6.7.1	Overview	95
6.7.2	REQ-CON-01 VPN routing stays in effect until VPN connection deactivated.....	96
6.7.2.1	Objective	96
6.7.2.2	Preparation.....	96
6.7.2.3	Activities	96
6.7.2.4	Verdict.....	96
6.7.2.5	Evidence	96
6.7.3	REQ-CON-02 VPN routing stays in effect during network-level tunnel failure.....	96
6.7.3.1	Objective	96
6.7.3.2	Preparation.....	96
6.7.3.3	Activities	96
6.7.3.4	Verdict.....	97
6.7.3.5	Evidence	97
6.7.4	REQ-CON-03 Tunnel all traffic by default.....	97
6.7.4.1	Objective	97
6.7.4.2	Preparation.....	97
6.7.4.3	Activities	97
6.7.4.4	Verdict.....	97
6.7.4.5	Evidence	97
6.7.5	REQ-CON-04 Endpoint to endpoint encryption	97
6.7.5.1	Objective	97
6.7.5.2	Preparation.....	98
6.7.5.3	Activities	98
6.7.5.4	Verdict.....	98
6.7.5.5	Evidence	98
6.7.6	REQ-CON-05 Inform user of visibility of DNS queries	98
6.7.6.1	Objective	98
6.7.6.2	Preparation.....	98
6.7.6.3	Activities	98
6.7.6.4	Verdict.....	98
6.7.6.5	Evidence	98
6.7.7	REQ-CON-06 Configurable exclusive DNS routing	99
6.7.7.1	Objective	99
6.7.7.2	Preparation.....	99
6.7.7.3	Activities	99
6.7.7.4	Verdict.....	99
6.7.7.5	Evidence	99
6.7.8	REQ-CON-07 Exclusive DNS routing by default.....	99
6.7.8.1	Objective	99
6.7.8.2	Preparation.....	99
6.7.8.3	Activities	99
6.7.8.4	Verdict.....	99
6.7.8.5	Evidence	99
6.7.9	REQ-CON-08 DNS configuration consistency	100
6.7.9.1	Objective	100
6.7.9.2	Preparation.....	100
6.7.9.3	Activities	100
6.7.9.4	Verdict.....	100
6.7.9.5	Evidence	100
6.7.10	REQ-CON-09 Secure DNS protocols	100

6.7.10.1	Objective	100
6.7.10.2	Preparation.....	100
6.7.10.3	Activities	100
6.7.10.4	Verdict.....	101
6.7.10.5	Evidence	101
6.7.11	REQ-CON-10 No DNS leaks during network-level tunnel failure	101
6.7.11.1	Objective	101
6.7.11.2	Preparation.....	101
6.7.11.3	Activities	101
6.7.11.4	Verdict.....	101
6.7.11.5	Evidence	101
6.7.12	REQ-CON-11 Block IPv6 if Unsupported.....	101
6.7.12.1	Objective	101
6.7.12.2	Preparation.....	102
6.7.12.3	Activities	102
6.7.12.4	Verdict.....	102
6.7.12.5	Evidence	102
6.7.13	REQ-CON-12 Full Support if Claimed	102
6.7.13.1	Objective	102
6.7.13.2	Preparation.....	102
6.7.13.3	Activities	102
6.7.13.4	Verdict.....	102
6.7.13.5	Evidence	102
6.7.14	REQ-CON-13 Use conformant cryptography	102
6.7.14.1	Objective	102
6.7.14.2	Preparation.....	103
6.7.14.3	Activities	103
6.7.14.4	Verdict.....	103
6.7.14.5	Evidence	103
6.7.15	REQ-CON-14 Confidentiality of data stored on the product	103
6.7.15.1	Objective	103
6.7.15.2	Preparation.....	103
6.7.15.3	Activities	103
6.7.15.4	Verdict.....	103
6.7.15.5	Evidence	103
6.7.16	REQ-CON-15 Inform user of limits of privacy protection	104
6.7.16.1	Objective	104
6.7.16.2	Preparation.....	104
6.7.16.3	Activities	104
6.7.16.4	Verdict.....	104
6.7.16.5	Evidence	104
6.8	Integrity protection	104
6.8.1	Overview	104
6.8.2	REQ-INT-01 VPN client restores any system configuration it changes to its previous state after the VPN connection ends	104
6.8.2.1	Objective	104
6.8.2.2	Preparation.....	104
6.8.2.3	Activities	104
6.8.2.4	Verdict.....	105
6.8.2.5	Evidence	105
6.8.3	REQ-INT-02 VPN client provides a method to restore any system configuration it changes to its previous state.....	105
6.8.3.1	Objective	105
6.8.3.2	Preparation.....	105
6.8.3.3	Activities	105
6.8.3.4	Verdict.....	105
6.8.3.5	Evidence	105
6.8.4	REQ-INT-03 VPN client does not degrade system security	106
6.8.4.1	Objective	106
6.8.4.2	Preparation.....	106
6.8.4.3	Activities	106
6.8.4.4	Verdict.....	106

6.8.4.5	Evidence	106
6.8.5	REQ-INT-04 Protocol validity checks	106
6.8.5.1	Objective	106
6.8.5.2	Preparation.....	106
6.8.5.3	Activities	106
6.8.5.4	Verdict.....	107
6.8.5.5	Evidence	107
6.8.6	REQ-INT-05 Application protocol validity checks by operational environment.....	107
6.8.6.1	Objective	107
6.8.6.2	Preparation.....	107
6.8.6.3	Activities	107
6.8.6.4	Verdict.....	107
6.8.6.5	Evidence	107
6.9	Data minimisation.....	107
6.9.1	Overview	107
6.9.2	REQ-DM-01 Data minimisation across the product	107
6.9.2.1	Objective	107
6.9.2.2	Preparation.....	108
6.9.2.3	Activities	108
6.9.2.4	Verdict.....	108
6.9.2.5	Evidence	108
6.9.3	REQ-DM-02 No Personal Data sent outside endpoint.....	108
6.9.3.1	Objective	108
6.9.3.2	Preparation.....	108
6.9.3.3	Activities	108
6.9.3.4	Verdict.....	109
6.9.3.5	Evidence	109
6.9.4	REQ-DM-03 Minimise Personal Data required service provisioning and payment	109
6.9.4.1	Objective	109
6.9.4.2	Preparation.....	109
6.9.4.3	Activities	109
6.9.4.4	Verdict.....	109
6.9.4.5	Evidence	110
6.9.5	REQ-DM-04 Minimise Personal Data stored.....	110
6.9.5.1	Objective	110
6.9.5.2	Preparation.....	110
6.9.5.3	Activities	110
6.9.5.4	Verdict.....	110
6.9.5.5	Evidence	110
6.9.6	REQ-DM-05 No data persistence or storage enabled on exit nodes	110
6.9.6.1	Objective	110
6.9.6.2	Preparation.....	110
6.9.6.3	Activities	111
6.9.6.4	Verdict.....	111
6.9.6.5	Evidence	111
6.10	Availability protection	111
6.10.1	Overview	111
6.10.2	REQ-AP-01 Fast packet drop.....	111
6.10.2.1	Objective	111
6.10.2.2	Preparation.....	111
6.10.2.3	Activities	111
6.10.2.4	Verdict.....	111
6.10.2.5	Evidence	112
6.10.3	REQ-AP-02 Limit memory usage.....	112
6.10.3.1	Objective	112
6.10.3.2	Preparation.....	112
6.10.3.3	Activities	112
6.10.3.4	Verdict.....	112
6.10.3.5	Evidence	112
6.10.4	REQ-AP-03 Availability protection provided by operational environment.....	112
6.10.4.1	Objective	112
6.10.4.2	Preparation.....	113

6.10.4.3	Activities	113
6.10.4.4	Verdict	113
6.10.4.5	Evidence	113
6.10.5	REQ-AP-04 Rate limit unauthenticated traffic	113
6.10.5.1	Objective	113
6.10.5.2	Preparation.....	113
6.10.5.3	Activities	113
6.10.5.4	Verdict.....	113
6.10.5.5	Evidence	113
6.11	Non-interference	114
6.11.1	Overview	114
6.11.2	REQ-IM-01 No route between different endpoints by default	114
6.11.2.1	Objective	114
6.11.2.2	Preparation.....	114
6.11.2.3	Activities	114
6.11.2.4	Verdict.....	114
6.11.2.5	Evidence	114
6.11.3	REQ-IM-02: Minimise data transmitted to unverified sources	114
6.11.3.1	Objective	114
6.11.3.2	Preparation.....	114
6.11.3.3	Activities	114
6.11.3.4	Verdict.....	115
6.11.3.5	Evidence	115
6.12	Attack surface minimisation	115
6.12.1	Overview	115
6.12.2	REQ-MAS-01 Unnecessary VPN client permissions	115
6.12.2.1	Objective	115
6.12.2.2	Preparation.....	115
6.12.2.3	Activities	115
6.12.2.4	Verdict.....	115
6.12.2.5	Evidence	115
6.13	Exploit mitigation	116
6.13.1	Overview	116
6.13.2	REQ-EMM-01 Route traffic from other sources/destination disabled by default	116
6.13.2.1	Objective	116
6.13.2.2	Preparation.....	116
6.13.2.3	Activities	116
6.13.2.4	Verdict.....	116
6.13.2.5	Evidence	116
6.13.3	REQ-EMM-02 Notify user if routing traffic from other sources/destination	116
6.13.3.1	Objective	116
6.13.3.2	Preparation.....	116
6.13.3.3	Activities	116
6.13.3.4	Verdict.....	117
6.13.3.5	Evidence	117
6.13.4	REQ-EMM-03 No routing traffic from other sources/destination if not necessary for services	117
6.13.4.1	Objective	117
6.13.4.2	Preparation.....	117
6.13.4.3	Activities	117
6.13.4.4	Verdict.....	117
6.13.4.5	Evidence	117
6.14	Monitoring	117
6.14.1	Overview	117
6.14.2	REQ-LOG-01 Local event logging	117
6.14.2.1	Objective	117
6.14.2.2	Preparation.....	118
6.14.2.3	Activities	118
6.14.2.4	Verdict.....	118
6.14.2.5	Evidence	118
6.14.3	REQ-LOG-02 Internal event logging	118
6.14.3.1	Objective	118
6.14.3.2	Preparation.....	118

6.14.3.3	Activities	118
6.14.3.4	Verdict	119
6.14.3.5	Evidence	119
6.14.4	REQ-LOG-03 Remote Logging	119
6.14.4.1	Objective	119
6.14.4.2	Preparation.....	119
6.14.4.3	Activities	119
6.14.4.4	Verdict.....	119
6.14.4.5	Evidence	119
6.14.5	REQ-LOG-04 Privacy-preserving logs policy and traffic anonymization	120
6.14.5.1	Objective	120
6.14.5.2	Preparation.....	120
6.14.5.3	Activities	120
6.14.5.4	Verdict.....	120
6.14.5.5	Evidence	120
6.15	Factory reset and data portability	120
6.15.1	Overview	120
6.15.2	REQ-DRT-01 Secure deletion via "factory reset"	120
6.15.2.1	Objective	120
6.15.2.2	Preparation.....	120
6.15.2.3	Activities	121
6.15.2.4	Verdict.....	121
6.15.2.5	Evidence	121
6.15.3	REQ-DRT-02 Secure deletion via reinstallation	121
6.15.3.1	Objective	121
6.15.3.2	Preparation.....	121
6.15.3.3	Activities	121
6.15.3.4	Verdict.....	121
6.15.3.5	Evidence	122
6.15.4	REQ-DRT-03 Secure data read from product	122
6.15.4.1	Objective	122
6.15.4.2	Preparation.....	122
6.15.4.3	Activities	122
6.15.4.4	Verdict.....	122
6.15.4.5	Evidence	122
6.15.5	REQ-DRT-04 Secure data export.....	122
6.15.5.1	Objective	122
6.15.5.2	Preparation.....	122
6.15.5.3	Activities	123
6.15.5.4	Verdict.....	123
6.15.5.5	Evidence	123
B.0	Overview	127
B.1	Assets	127
B.1.0	Overview	127
B.1.1	Data assets	127
B.1.2	Product functions	127
B.1.3	Digital assets	128
B.1.4	Human-associated assets.....	128
B.1.5	Hardware assets	128
B.2	Risk factors.....	128
B.2.1	General.....	128
B.2.2	RF-CFG: Endpoint configuration	129
B.2.3	RF-AUT: Account management and authentication of endpoints	129
B.2.4	RF-DTX: Sensitivity of data transmitted	129
B.2.5	RF-DST: Sensitivity of data stored	129
B.2.6	RF-FUN: Sensitivity of functions	129
B.2.7	RF-ADM: Availability and skill of administration	130
B.2.8	RF-RDP: Manufacturer infrastructure isolation.....	130
B.2.9	RF-DNC: Difficulty of network configuration	130
B.2.10	RF-COM: Complexity of feature set	130