Draft ETSI EN 304 636 V1.0.0 (2026-07)

HARMONISED EUROPEAN STANDARD

Cybersecurity (CYBER);
CRA;
Cybersecurity requirements for firewalls,
intrusion detection and/or prevention systems

Reference
DEN/CYBER-EUS-0020

Keywords
CRA, cybersecurity, firewall

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

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

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

Proposed national transposition dates	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	18 months after doa

Modal verbs terminology

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

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

Introduction

The present document covers cybersecurity for firewalls, intrusion detection systems, and intrusion prevention systems. These products are identified in Annex III, Class II, point 2 of Regulation (EU) 2024/2847 [i.1], known as the Cyber Resilience Act (CRA).

The present document provides a structured approach to identify the applicable cybersecurity requirements for the products in scope, following a risk-based approach. Security controls are therefore proportionate to the intended purpose, reasonably foreseeable use, deployment context, and threat exposure of the products.

Clause 4 describes the product architecture and intended purpose, and defines the use cases for the main deployment scenarios under reasonably foreseeable use.

Clause 5 specifies the technical cybersecurity requirements for the product to mitigate the identified risks.

Clause 6 specifies the assessment criteria and compliance verification procedures for the requirements of clause 5.

Annex A maps the technical requirements of the present document to the corresponding cybersecurity requirements of the CRA [i.1].

Annex B describes the methodology used to assess the security risks of the products in their context. Where a product does not clearly correspond to one of the use cases defined in clause 4, the risk assessment methodology of Annex B may be used to determine the applicable cybersecurity requirements.

1 Scope

The present document specifies vulnerability handling activities, technical requirements and corresponding assessment criteria for firewalls, intrusion detection systems, and intrusion prevention systems related to cybersecurity. The products with digital elements in scope:

- are specified within the "technical description" of the "category of product" in Class II, point 2 by the Commission Implementing Regulation (EU) 2025/2392 [i.2] 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.1] as:
  - "Firewalls are products with digital elements that protect a connected network or system from unauthorised access by monitoring and restricting data communication traffic to and from that network.

    This category includes but is not limited to network firewalls and application firewalls such as web application firewalls or filters and anti-spam gateways.";
  - "Intrusion detection systems are products with digital elements that monitor traffic once it has entered the network environment for suspicious activity and detect or identify that an intrusion has been attempted, is occurring, or has occurred on a connected network or system.

    This category includes but is not limited to network-based intrusion detection systems and host-based intrusion detection systems.";
  - "Intrusion prevention systems are products with digital elements composed of an intrusion detection system that actively responds to an intrusion to a connected network or system.

    This category includes but is not limited to network-based intrusion prevention systems and host-based intrusion prevention systems.";
- are only covered within the product context described in clause 4.

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

Firewalls, intrusion detection systems, and intrusion prevention systems fall within the scope of the present document, whether deployed as physical appliances or software. The present document applies when the intended purpose or reasonably foreseeable use involves monitoring, analysing, or controlling network traffic for security purposes. Products that detect access attempts made without authorisation, identify malicious activity, or enforce traffic controls to protect networks and systems from intrusions are within scope.

Firewalls, intrusion detection systems, and intrusion prevention systems intended for use in the industrial OT (Operational Technology) domain are excluded from the scope of the present document, see prEN 50770-1 [i.7].

The present document does not specify how products detect threats, classify traffic, or implement inspection algorithms. Detection accuracy rates, false positive thresholds, and signature effectiveness metrics are outside scope. Security requirements for the robustness of protocol parsing engines, the integrity of inspection processes, and vulnerability management remain within scope.

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.

[1] ENISA European Cybersecurity Certification Group, Sub-group on Cryptography: "Agreed Cryptographic Mechanisms", Version 2.0, April 2025.

[2] ETSI TS 119 312 (V2.1.1) (06-2026): "Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites".

[3] ETSI TS 133 210 (V19.3.0) (02-2026): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 19.3.0 Release 19)".

2.2 Informative 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.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding but are not required for conformance to the present document.

[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).

[i.2] 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.3] Standardisation request M/606 - C(2025)618: "Commission Implementing decision of 3.2.2025 on a standardisation request to the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (Cenelec) and the European Telecommunications Standards Institute (ETSI) as regards products with digital elements in support of Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)".

[i.4] prEN 40000-1-1: "Cybersecurity requirements for products with digital elements - Vocabulary", (produced by CEN CENELEC).

NOTE: Version and date to be added upon its publication by CEN CENELEC.

[i.5] NIST SP 800-133 Rev. 2 (June 2020): "Recommendation for Cryptographic Key Generation".

[i.6] ISO/IEC/IEEE 24765:2017: "Systems and software engineering - Vocabulary".

[i.7] prEN 50770-1: "Security for Operational Technologies - Part 1: Security Profile for firewalls and intrusion detection and prevention systems", (produced by CEN CENELEC).

NOTE: Version and date to be added upon its publication by CEN CENELEC.

[i.8] ENISA European Vulnerability Database (EUVD), established pursuant to Article 12(2) of Directive (EU) 2022/2555.

[i.9] ENISA: "Single Reporting Platform (SRP)" established for Regulation (EU) 2024/2847.

[i.10] BSI TR-02102-1 (Version 2026-01, 31 January 2026): "Cryptographic Mechanisms: Recommendations and Key Lengths".

[i.11] ANSSI Référentiel Général de Sécurité, Annex B2: "Choice and Sizing of Cryptographic Mechanisms".

[i.12] Canadian Centre for Cyber Security ITSP.40.062: "Guidance on Securely Configuring Network Protocols".

[i.13] NIST SP 800-131A Rev. 2 (March 2019): "Transitioning the Use of Cryptographic Algorithms and Key Lengths".

[i.14] Arm Limited: "Arm CCA Security Model 1.0" (DEN0096).

[i.15] IRTF RFC 8439: "ChaCha20 and Poly1305 for IETF Protocols".

[i.16] IETF RFC 4418: "UMAC: Message Authentication Code using Universal Hashing".

[i.17] IETF RFC 9106: "Argon2 Memory-Hard Function for Password Hashing and Proof-of-Work Applications".

[i.18] IETF RFC 7914: "The scrypt Password-Based Key Derivation Function".

[i.19] IETF RFC 8410: "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure".

[i.20] IRTF RFC 8032: "Edwards-Curve Digital Signature Algorithm (EdDSA)".

[i.21] IETF RFC 8420: "Using the Edwards-Curve Digital Signature Algorithm (EdDSA) in the Internet Key Exchange Protocol Version 2 (IKEv2)".

[i.22] IETF RFC 9000: "QUIC: A UDP-Based Multiplexed and Secure Transport".

[i.23] IETF RFC 3411: "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks".

[i.24] IETF RFC 5590: "Transport Subsystem for the Simple Network Management Protocol (SNMP)".

[i.25] IEEE 802.1AR™-2018: "IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity".

[i.26] IEEE 1588™-2019: "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[i.27] IETF RFC 8915: "Network Time Security for the Network Time Protocol".

[i.28] BSI TR-02102-2 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Transport Layer Security (TLS)".

[i.29] BSI TR-02102-3 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)".

[i.30] BSI TR-02102-4 (Version 2026-01): "Cryptographic Mechanisms: Recommendations and Key Lengths - Use of Secure Shell (SSH)".

[i.31] IEEE 802.11™-2024: "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in Regulation (EU) 2024/2847 [i.1], prEN 40000-1-1 [i.4] and the following apply:

audit event: timestamped, structured record of activities including authentication attempts, configuration changes, and product errors

critical security parameter: confidential information whose disclosure or modification can compromise product security

EXAMPLE: Secret cryptographic keys, authentication values such as passwords, PINs, private components of certificates.

cryptographic algorithm: sequence of instructions based on mathematical properties to protect confidentiality, integrity or authenticity against attacks

diagnostic: pertaining to the detection and isolation of faults or failures

NOTE: As defined in ISO/IEC/IEEE 24765 [i.6], clause 3.1190.

diagnostic interface: interface used for diagnostic or troubleshooting purposes, not part of the intended function of the product

EXAMPLE: UART, JTAG, and SWD.

factory reset: mechanism that restores the product to product factory default state

fail-open operation: operation of the product in which traffic that cannot be inspected is forwarded without applying a fail-secure action

NOTE: Fail-open operation can result from software configuration, hardware bypass, inspection or signature update windows, or per-flow bypass configuration.

fail-secure action: configured action applied by the product to traffic that cannot be inspected, such that the traffic is not forwarded without inspection

NOTE: Typical fail-secure actions include drop, block, reject, and quarantine.

firewalls: products with digital elements that protect a connected network or system from access made without authorisation by monitoring and restricting data communication traffic to and from that network or between nodes of that network

NOTE: This includes but is not limited to network firewalls and application firewalls such as Web Application Firewalls (WAF), anti-spam gateways and content filtering systems.

firmware: software stored in non-volatile memory that controls product operation

NOTE 1: Firmware includes boot sequences, operating system components, inspection engines, and management interfaces.

NOTE 2: Firmware can include persistent configuration data required for product operation.

intrusion detection systems: products with digital elements that monitor traffic once it has entered the network environment for suspicious activity and detect or identify that an intrusion has been attempted, is occurring, or has occurred on a connected network or system

NOTE: This includes but is not limited to network-based intrusion detection systems and host-based intrusion detection systems.

intrusion prevention systems: products with digital elements composed of an intrusion detection system that actively responds to an intrusion to a connected network or system

NOTE: This includes but is not limited to network-based intrusion prevention systems and host-based intrusion prevention systems.

legacy protocol: network protocol whose specification lacks state of the art cryptography to ensure the authenticity, integrity or confidentiality of security-relevant exchanges, where a secure alternative protocol or profile is widely available, and which is retained in the product exclusively to maintain interoperability with deployed systems

EXAMPLE: Protocols whose role is limited to local IP address configuration, local neighbour and address discovery, and name and service resolution are not considered legacy protocols for the purposes of the present document, irrespective of their cryptographic properties. These protocols are designed under explicit assumptions that specific risks are managed by the operational environment in which they are deployed, and are required for basic network attachment and reachability.

NOTE: A vulnerability in a specific implementation of a protocol does not, by itself, make the protocol a legacy protocol. Vulnerabilities associated with a legacy protocol can originate in its specification, in a specific implementation, or in both.

legacy system: system that operates using at least one legacy protocol

management override: deliberate configuration action by a privileged management account that (i) enables a non-default product behaviour; and (ii) is distinguishable from routine product configuration

NOTE: Mechanisms that satisfy management override include confirmation prompts acknowledging the consequence of the override, reauthentication for the override action, and separate management workflows for non-default behaviours. Default configuration values and settings inherited from templates are not management overrides.

network interface: physical interface that can be used to access the functionality of firewall, IDS or IPS via a network

product: firewall, intrusion detection system, or intrusion prevention system within the scope of the present document

product factory default state: state of the product as provided after manufacturing, reflecting the default configuration established by the manufacturer, to which the product returns after a factory reset

NOTE 1: Depending on the product design and business model, security functionalities, for example secure boot, trust anchors, or security policies, can be enabled by the manufacturer prior to delivery, or activated and configured by the customer or authorised operator during initial setup.

NOTE 2: The product can be delivered by the manufacturer to an importer or distributor that subsequently sells it to customers or puts it into service. In that case additional steps, for example finalisation of configuration, can be required before the product enters an operational state.

product operational state: state in which the product can operate within its intended purpose and reasonably foreseeable use with its current active configuration, whether this configuration corresponds to the preconfigured default settings or has been modified by the user

remote data processing solution: data processing at a distance for which the software is designed and developed by the manufacturer, or under the responsibility of the manufacturer, and the absence of which would prevent the product from performing one of its functions

NOTE: As defined in Regulation (EU) 2024/2847, Article 3, point 2 [i.1].

reboot: specific management operation or autonomous reaction to product state that triggers a product restart

secure channel: path for transferring data between two entities or components that ensures confidentiality, integrity, and replay protection, as well as mutual authentication between the entities or components

NOTE 1: The secure channel can be provided using cryptographic, physical, or procedural methods or a combination thereof.

NOTE 2: As defined in NIST SP 800-133 Rev. 2 [i.5].

secure-by-default configuration: configuration in which the product satisfies requirements in clause 5.4.1

security rule: specific statement or entry that specifies source, destination, protocol, port, action, and matching criteria for traffic classification

NOTE: Multiple rules can collectively express a single set of security decisions.

signature database: collection of patterns, heuristics, and indicators used by the product to detect known threats during traffic inspection

software bill of materials: formally structured list of all software components, libraries, and dependencies included in the product, with version identifiers

3.2 Symbols

Void.

3.3 Abbreviations

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

ACM	Agreed Cryptographic Mechanisms
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
API	Application Programming Interface
CAVP	Cryptographic Algorithm Validation Program
CCA	Confidential Compute Architecture
CFB	Cipher Feedback
CRA	Cyber Resilience Act
CTR	Counter
DMZ	DeMilitarised Zone
DoS	Denial of Service
EAP	Extensible Authentication Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-curve Digital Signature Algorithm
EU	European Union
EUVD	European Vulnerability Database
GMAC	Galois Message Authentication Code
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPR	Intellectual Property Rights
IPS	Intrusion Prevention System
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
IT	Information Technology
ITSP	Information Technology Security Publication
JTAG	Joint Test Action Group
KDF	Key Derivation Function
LWE	Learning With Errors
MiB	Mebibyte
NTP	Network Time Protocol
NTS	Network Time Security
PAC	Pointer Authentication Code
PTP	Precision Time Protocol
QUIC	Quick UDP Internet Connections
RDPS	Remote Data Processing Solution

RSA	Rivest-Shamir-Adleman
SBOM	Software Bill of Materials
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SIV	Synthetic Initialization Vector
SNMP	Simple Network Management Protocol
SOC	Security Operations Centre
SRP	Secure Remote Password
SSH	Secure Shell
SWD	Serial Wire Debug
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Type-Length-Value
UART	Universal Asynchronous Receiver-Transmitter
UMAC	Universal Message Authentication Code
VPN	Virtual Private Network
WAF	Web Application Firewall

4 Product context

4.1 Introduction

Firewalls, intrusion detection systems, and intrusion prevention systems protect network boundaries by inspecting traffic and enforcing configured rules. Their position at network boundaries protects integrity, confidentiality, and availability.

Compromise of these products can affect the security of all networks and systems that depend on them for protection. Security measures scale with deployment context whilst maintaining baseline protections.

Firewalls filter traffic using rules and stateful inspection. Intrusion detection systems monitor traffic and generate alerts. Intrusion prevention systems actively block threats. All three analyse traffic, maintain state information, balance detection accuracy against false positives, and protect themselves whilst performing security functions. Products can be deployed as dedicated appliances, built into the network infrastructure, obtained as a managed service, or installed on individual hosts. Security measures protect both the inspection function and management interfaces based on product capabilities and deployment.

Manufacturers add functionality such as threat intelligence, machine learning analytics, and cloud management. Each adds attack surfaces that require security assessment and maintenance.

4.2 Product functions

4.2.1 General product functions

4.2.1.1 General

The product functions in this clause apply to firewalls, intrusion detection systems, and intrusion prevention systems and are not specific to any single product category.

4.2.1.2 [FN-G-01] Configuration and management

These functions provide management interfaces such as command-line, web-based, and API interfaces. They handle security policies, rule sets, signature and threat-intelligence sources, logging configuration, and maintenance tasks. They maintain consistent settings across all components and block changes without authorisation.

4.2.1.3 [FN-NC-01] Network connectivity

These functions provide the capability for the product to perform Layer 2 forwarding or Layer 3 routing to enable integration with network infrastructures and act as network boundaries. These capabilities allow the firewall, IDS, or IPS to enforce security policies at network boundaries while maintaining network reachability and segmentation.

4.2.1.4 [FN-LG-01] Logging

These functions generate detailed audit trails and logs for all decisions, supporting compliance and forensic analysis.

4.2.1.5 [FN-TI-01] Traffic inspection and analysis

Deep inspection identifies threats, enforces rules, and detects anomalies by examining traffic across protocol layers. Inspection covers packet headers, stateful protocols, application identification, and content analysis for malware and violations.

4.2.1.6 [FN-SM-01] Signature and intelligence management

Products maintain signature and rule databases for threat detection. Management retrieves updates, validates integrity and compatibility, stages signatures for testing, manages custom and vendor rules, and optimises for performance.

4.2.2 Product functions implemented by firewalls and intrusion prevention systems

4.2.2.1 General

The product function described in this clause applies to firewalls and intrusion prevention systems that enforce traffic decisions and is not applicable to intrusion detection systems.

4.2.2.2 [FN-SP-01] Traffic access control and decision making

This function applies configured access control rules to network traffic, determining what traffic is permitted, blocked, logged, or modified. The rule engine evaluates rules in priority order, handles conflicts consistently, applies default actions to unmatched traffic, and generates audit trails.

4.2.2.3 [FN-SG-01] Traffic segmentation

These functions enforce security boundaries between different network zones such as internal, external, and DMZ, controlling traffic flow between them to prevent access without authorisation and lateral movement within the network.

4.2.3 Product functions implemented by intrusion detection systems and intrusion prevention systems

4.2.3.1 General

The product function described in this clause applies to intrusion detection systems and intrusion prevention systems that identify threats from inspected traffic and is not applicable to firewalls that do not perform threat detection beyond rule-based enforcement.

4.2.3.2 [FN-TD-01] Threat detection and pattern matching

Detection mechanisms identify known and unknown threats through complementary techniques. Signature-based detection matches traffic against databases of attack patterns. Anomaly-based detection establishes behaviour baselines and identifies deviations indicating compromise.

4.3 Product architecture

4.3.1 General

Products inspect traffic and enforce configured rules across one or more protocol layers. Network firewalls and intrusion prevention systems operate inline, processing traffic between network segments. Application firewalls operate at the application layer, inspecting protocol-specific content. Products may use dedicated hardware, custom engines, and distributed designs.

The software architecture builds on specialised operating systems optimised for security processing and real-time traffic analysis. Security engines implement signature-based pattern matching, behavioural analysis, and threat detection algorithms. Management software provides configuration tools, rule management, and logging. Security controls span management access, encrypted channels, and inline inspection.

Manufacturers add further capabilities such as threat intelligence, cloud management, and security orchestration. Each adds attack surfaces that require security assessment and maintenance.

4.3.2 Product assets

[AS-FW-01] Security policies and rule sets

[AS-FW-02] Signature databases and threat intelligence

[AS-FW-03] Inspection engine state

[AS-FW-04] Audit event records

4.3.3 Product capabilities

[CAP-FW-01] Deep packet inspection

[CAP-FW-02] Stateful traffic analysis

[CAP-FW-03] Signature-based threat detection

[CAP-FW-04] Inline traffic enforcement

4.4 Operational environment

4.4.1 General description

Products covered by the present document operate in diverse environments. Environments differ by product type as described in clause 4.1, by the deployment form, and by the operational context. Deployment forms include physical appliances, virtual machines, and containers. Relevant factors are network architecture, trust boundaries, segmentation, traffic volumes, tolerance for downtime, and the level of integration with security ecosystems.

Products operate at network enforcement points processing traffic between networks with different trust levels. They inspect traffic that may be malicious while themselves being targets of attack.

4.4.2 Physical environment

Physical environments range from data centres with strict access controls and dedicated equipment rooms to branch offices and retail locations. Physical appliances may be rack-mounted in secured facilities or deployed as desktop units in office environments. Physical protection varies from controlled-access server rooms to open office spaces where the product may be accessible to non-technical personnel.

4.4.3 Logical environment

Products are deployed at network boundaries, between internal segments, or as host-based agents. In perimeter deployments, the product is the primary security boundary between different zones such as internal, external, and DMZ. In segmentation deployments, products enforce trust boundaries between internal zones. Virtual and cloud deployments may share compute resources with protected workloads.

Management access is provided through dedicated management interfaces, in-band management over the data network, or cloud-based management platforms. The choice of management architecture affects the attack surface and the distribution of security functions.

4.4.4 Connectivity aspects

Products connect to multiple network segments simultaneously. In perimeter deployments, products connect to at least one untrusted external network and one or more internal networks. In segmentation deployments, products connect to two or more internal network segments, isolating broad trust zones such as employee, guest, and management. Host-based products connect to the host operating system network stack.

Integration with security ecosystems can include SIEM platforms, threat intelligence feeds, orchestration systems, and incident response tools. These integrations require network connectivity to external services and introduce additional interfaces that the product exposes.

4.5 Distribution of security functions

Security functions of firewalls, intrusion detection systems, and intrusion prevention systems relate to the assets and capabilities described in clause 4.3. The security function deployment can be categorised as follows:

- Integration of security functions. In this case, the security functions rely on resources provided outside the product itself, such as remote data processing solutions for cloud management, threat intelligence, signature distribution, or log collection as described in clause 5.13, and where applicable on third-party platform assets such as the host operating system network stack for host-based deployments or the underlying virtualisation infrastructure for virtual appliances. The present document addresses such security functions through integration requirements.

- Product-intrinsic deployment of security functions. In this case, the security functions rely on assets and capabilities that are part of the product design itself, such as security policies and rule sets [AS-FW-01], signature databases [AS-FW-02], inspection engine state [AS-FW-03], and audit event records [AS-FW-04], and capabilities such as deep packet inspection [CAP-FW-01], stateful traffic analysis [CAP-FW-02], signature-based threat detection [CAP-FW-03], and inline traffic enforcement [CAP-FW-04]. The present document addresses such security functions through requirements directly applicable to the products.

Security functions of firewalls, intrusion detection systems, and intrusion prevention systems can be associated with the assets and capabilities described in clause 4.3. The risk factors defined in clause B.3 determine which security requirements from clause 5 apply to a specific product based on its intended purpose, reasonably foreseeable use, and conditions of use.

4.6 Users

Firewalls, intrusion detection systems, and intrusion prevention systems may be accessed by multiple categories of users each having different roles, needs and privileges.

Security administrators configure access control rules, update signatures, and modify system settings determining permitted or blocked traffic. They have deep knowledge of security architectures, threat landscapes, and risk tolerance. This role requires strong authentication and comprehensive audit logging. Significant configuration changes may be subject to multiple approvals from security and network teams.

Security analysts and incident responders monitor alerts continuously, investigate threats, and tune detection rules to reduce false positives. They require read access to security events, packet captures, and threat intelligence, plus limited write access for suppression rules and alert acknowledgement. This role requires strong authentication and comprehensive audit logging.

Network administrators require limited access for troubleshooting connectivity issues or coordinating changes affecting traffic flows. Whilst not primarily responsible for security functions, they need visibility into rules blocking legitimate traffic and ability to request modifications through documented channels. Access is restricted to viewing relevant rules and logs without modifying security controls.

Compliance auditors and security assessors require read-only access to verify correct configuration and effective operation. They review rules, examine audit logs, and generate compliance reports without modifying configurations. Access can be temporary, restricted to compliance functions, with all activities logged.

Automated systems and orchestration platforms interact through APIs requiring service accounts with scoped permissions. They update threat intelligence, deploy configuration changes, collect logs, or implement response actions. Access requires strong authentication using certificates or API keys, with permissions limited to necessary functions. Compromise of automated accounts could disable security controls across multiple products simultaneously.

SOC personnel work in staffed environments and monitor multiple products through centralised consoles. They require streamlined interfaces for rapid threat identification and response across multiple customer environments. Access patterns involve shift handovers, escalation procedures, and coordinated incident response. SOC operators have read-only access with limited ability to implement temporary countermeasures under change control.

Security product users understand threat landscapes, attack techniques, and defensive strategies. Products cannot rely on intuitive interfaces alone but provide detailed information about threats, rule logic, and detection confidence for informed decisions. Misconfigurations cause security breaches, not just service disruptions. User training and clear documentation are essential.

4.7 Use cases

4.7.1 General

This clause identifies use cases for firewalls, intrusion detection systems, and intrusion prevention systems. The use cases presented are neither exhaustive nor mutually exclusive. A single product can support multiple use cases. The list of use cases can be extended in future revisions of the present document.

The description of each use case is limited to those characteristics considered relevant for the identification of threats. Characteristics may be both the user categories and their properties as described in clause 4.6 as well as the operational environments and their properties as described in clause 4.4.

4.7.2 Perimeter security deployments

This use case covers deployments where firewalls establish the primary security boundary between internal networks, DMZ networks, and untrusted external networks. External networks in this context include the public internet. The firewall is positioned as the sole traffic path, blocking all traffic except explicitly permitted communications. Products inspect both inbound and outbound traffic. Inbound inspection protects internal resources; outbound inspection identifies data exfiltration or malware communication. Deployments face continuous automated attacks and reconnaissance, requiring robust logging, alerting, and automated response. Mission-critical perimeter deployments may use redundant product clusters with state synchronisation and automatic failover.

4.7.3 Internal segmentation deployments

This use case covers deployments where firewalls and intrusion prevention systems are deployed between internal network segments to enforce zero-trust rules and limit lateral movement after compromise. Internal boundaries separate departments, isolate critical systems, and create demilitarised zones for public services. Products handle high east-west traffic volumes at low latency. They detect abnormal behaviour, access attempts between segments made without authorisation, and lateral movement.

4.7.4 Data centre security deployments

This use case covers deployments where products protect virtualised workloads within data centre environments. Products operate as virtual appliances or are integrated into the virtualisation infrastructure. Deployments protect workloads that migrate between hosts and share compute resources. Products enforce segmentation between tenant environments and between production, development, and management zones.

4.7.5 Cloud security deployments

This use case covers deployments where security inspection is distributed through cloud-native controls and container-native firewalls. Products integrate with orchestration platforms and SDN controllers. Workloads scale dynamically and exist temporarily. Rules follow workloads across cloud infrastructure. Where these deployments rely on remote data processing solutions, clause 5.13 applies.

4.7.6 Distributed branch office protection

This use case covers deployments at branch offices providing local inspection without backhauling traffic to centralised data centres. Deployments range from small, unified threat management appliances protecting few users to regional hubs aggregating traffic from multiple locations. Branch deployments run with minimal local IT support. They require simple management interfaces, automated threat response, and centralised configuration management.

4.7.7 Network forensics deployments

This use case covers deployments of dedicated intrusion detection systems for post-incident forensic analysis. Sensors capture and record network traffic for evidence preservation and historical investigation. Deployments emphasise comprehensive packet capture, metadata generation, and long-term storage. Products operate in passive mode observing all traffic without blocking.

4.7.8 Threat hunting deployments

This use case covers deployments where intrusion detection systems support proactive searching for threats that evade automated detection. Analysts use the product to test hypotheses about attacker presence by querying traffic patterns, correlating events, and identifying anomalies. Products provide visibility into network activity and support integration with threat intelligence for indicator matching.

4.7.9 Host-based security deployments

This use case covers products installed on individual servers, workstations, or endpoints rather than as dedicated network appliances. Host-based products inspect traffic at the operating system level. They enforce rules based on the local application context. They protect individual systems against threats that bypass network-level inspection, such as lateral movement within a trusted segment.

4.7.10 Application security deployments

This use case covers products that inspect traffic at the application layer. Web application firewalls protect web services by inspecting HTTP and HTTPS traffic for injection attacks, cross-site scripting, and protocol violations. Anti-spam gateways and content filtering systems inspect email and web traffic for unwanted or malicious content. These products operate as reverse proxies or inline filters and require application-layer protocol awareness beyond network packet inspection.

4.7.11 Managed security service deployments

This use case covers managed security service providers that protect multiple customer networks through shared or dedicated products. Customer traffic is isolated. Products support virtual domains, separate routing tables, and isolated rule sets. Information does not leak between customers. Where these deployments rely on remote data processing solutions, clause 5.13 applies.

5 Technical requirements for the products

5.1 Introduction - Applicability of the requirements

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

Not all requirements are universally applicable. The applicability of requirements may be based on use cases or specific capabilities of the product.

5.2 Appropriate level of cybersecurity

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

The present document provides an appropriate level of cybersecurity based on the risks by:

- describing in clause 4 the product context, including the product functions, architecture, operational environments, users, and use cases;
- describing in Annex B the threats associated with that product context and the risk factors that affect their applicability and likelihood; and
- conditioning the applicability of the technical requirements in the subsequent subclauses on those use cases and risk factors, so that the security controls required of a product are proportionate to the risks arising from its intended purpose, reasonably foreseeable use, deployment context, and threat exposure.

The security controls required by the applicable technical requirements of the present document shall be integrated into the product such that no security property required by one control is bypassed or weakened by the implementation or operation of another control or product function.

5.3 No known exploitable vulnerabilities

5.3.1 [KEV-1] No known exploitable vulnerabilities

5.3.1.1 General

Products made available on the market are free of known exploitable vulnerabilities. The manufacturer maintains a software bill of materials covering all product components and third-party dependencies. The assessor verifies the software bill of materials against known vulnerability databases.

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

NOTE: Vulnerability classes that warrant particular attention for these products are parsing flaws in deep-packet-inspection engines, resource exhaustion in signature and regular-expression engines, rule-evaluation bypasses, and traffic evasion through fragmentation or encoding. The corresponding threats are listed in Annex B.

5.3.1.2 Requirements

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

[REQ-KEV-1-01] The product shall provide, for each product version, a software bill of materials in a machine-readable format.

NOTE: Implementability of assessment is not given considering that upstream component suppliers do not have a legal mandate to make full SBOM available downstream. However, manufacturers are recommended to have a proof from the third-party that a component is free from vulnerabilities at the point in time the product was released to market. The proof can contain all mitigations which are received during the development time of the product.

[REQ-KEV-1-02] The product shall contain no known exploitable vulnerabilities in each product version when made available on the market.

[REQ-KEV-1-03] The product shall provide, for each product version when made available on the market, evidence of checks against known vulnerability databases for each third-party component.

5.4 Secure by default configuration

5.4.1 [DEFAULT-1] Secure by default configuration

5.4.1.1 General

Products include security controls that are configured and enabled from initial deployment. This protects against exploitation attempts that can occur within minutes of network connection. The default configuration establishes the security baseline that many deployments operate with unchanged throughout the product lifecycle.

5.4.1.2 Requirements

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

The requirements [REQ-DEFAULT-1-09] and [REQ-DEFAULT-1-10] apply, at the protocol layer, the legacy-interoperability framework set out in clause K.2.4 (2) of the present document for non-CRY-SOTA cryptographic algorithms.

[REQ-DEFAULT-1-01] The product, in its product factory default state, shall enforce the applicable requirements of the present document. The product need not enforce a requirement when (i) that requirement renders the initial product setup process non-functional; and (ii) the instructions to the user document the exception.

[REQ-DEFAULT-1-02] The product, in its product factory default state, shall enable only those interfaces and services that product setup requires.

NOTE 1: Some products in their product factory default state limit which network interfaces can be used for product setup. Other products place no restrictions on which network interfaces can be used for product setup.

[REQ-DEFAULT-1-03] The product, in its product factory default state, shall restrict access to management accounts and methods, as documented in the instructions to the user.

[REQ-DEFAULT-1-04] The product, in its product operational state, shall require authenticated and authorised access to management accounts.

[REQ-DEFAULT-1-05] The product, in its product factory default state, shall disable all diagnostic interfaces.

[REQ-DEFAULT-1-06] The product shall require authentication and authorisation for any management action that enables a diagnostic interface.

[REQ-DEFAULT-1-07] The product, in its product factory default state, shall generate audit events for (i) authentication attempts; (ii) configuration changes; and (iii) product errors, if those do not affect the recording.

[REQ-DEFAULT-1-08] The product, in its product factory default state, shall require state of the art cryptography for all cryptographic functions.

[REQ-DEFAULT-1-09] The product, in its product factory default state, shall (i) not enable any network-accessible service that relies on a legacy protocol; and (ii) require an explicit management action to activate a legacy protocol.

[REQ-DEFAULT-1-10] Where the product supports a legacy protocol, the manufacturer shall record (i) the protocol; (ii) security features no longer considered state of the art; (iii) legacy systems requiring it; and (iv) the constraint preventing a state of the art alternative.

NOTE 2: For the present context, the record forms part of the technical documentation referred to in Annex VII of Regulation (EU) 2024/2847.

[REQ-DEFAULT-1-11] The product shall enforce the principle of least privilege during normal operation.

[REQ-DEFAULT-1-12] The product shall store audit events in persistent memory that survives a reboot.

5.4.2 [RESET-1] Factory reset

5.4.2.1 General

Factory reset mechanisms remove all data and user configurations while leaving the current running software and the firmware versions in place. The factory reset also deletes the user login credentials, leading to the initial setup procedures.

NOTE 1: Factory reset does not include other types of reset procedures, such as what is commonly known as "operational reset" or "operator reset", where user data and configuration are preserved.

NOTE 2: In virtual environments, an alternative to factory reset of an existing instance can be to launch a new instance with the default configuration.

5.4.2.2 Requirements

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

[REQ-RESET-1-01] The product shall provide a factory reset mechanism that restores the product to its secure-by-default configuration.

NOTE 1: The product can provide a physical factory reset mechanism that does not require authentication.

[REQ-RESET-1-02] The product shall provide a factory reset mechanism that maintains the currently installed firmware version and all installed security updates.

[REQ-RESET-1-03] The product shall not retain (i) non-default configuration; (ii) user data; or (iii) user-instantiated or modified critical security parameters after factory reset.

NOTE 2: Connection information to an ISP administrated product belongs to the default configuration information.

5.5 Security updates

5.5.1 [UPDATE-1] Update mechanisms

5.5.1.1 General

This clause establishes requirements for delivering and installing security updates to address vulnerabilities throughout the product lifetime. Products may remain deployed for extended periods and may serve as critical infrastructure. Robust update mechanisms maintain security against evolving threats.

5.5.1.2 Requirements

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

[REQ-UPDATE-1-01] The product shall provide a mechanism to receive security updates.

[REQ-UPDATE-1-02] The product shall prevent installation of security updates without authentication and authorisation.

NOTE: The update process is initiated either (a) manually by an authorised and authenticated user or administrator, or (b) automatically by verification of authenticity and integrity of the update package.

[REQ-UPDATE-1-03] The product shall provide a mechanism to install a received security update and report the installed version.

[REQ-UPDATE-1-04] When the product is not designed for configuration and maintenance by professional network administrators, the product shall automatically check for security remedy updates according to the documented default schedule. Otherwise, the procedure for checking for security updates shall be included in the instructions to the user.

[REQ-UPDATE-1-05] When the product is not designed for configuration and maintenance by professional network administrators, the security update mechanism shall be automated and enabled by default. Otherwise, the procedure for performing the security update shall be included in the instructions to the user.

[REQ-UPDATE-1-06] The product shall verify security update integrity using state of the art cryptography before installation.

[REQ-UPDATE-1-07] The product shall generate audit events for (i) security update availability; (ii) security update download initiation, completion, or failure; and (iii) security update installation success or failure.

5.6 Authentication and access control

5.6.1 [AUTH-1] Authentication

5.6.1.1 General

Authentication is the fundamental security barrier against product modification without authorisation. These products play a critical role in network security enforcement. Compromise of access controls can disable threat detection, bypass security rules, or grant access to protected networks. This clause establishes requirements to ensure only authorised users can access product management functions.

5.6.1.2 Requirements

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

[REQ-AUTH-1-01] The product shall require user authentication on all interfaces providing management access to the product.

[REQ-AUTH-1-02] The product shall eliminate shared default credentials by either (i) generating credentials during secure production; (ii) enforcing mandatory credential creation during initial setup; or (iii) using non-password based authentication credentials.

NOTE 1: The generation of qualified individual user credentials can be supported by a product feature, or the product supports credential import.

[REQ-AUTH-1-03] Where the product transmits critical security parameters, the product shall protect their transmission over a secure channel.

[REQ-AUTH-1-04] The product shall protect critical security parameters using state of the art cryptography.

[REQ-AUTH-1-05] When supporting password-based credentials, the product shall enforce minimum credential entropy.

NOTE 2: Minimum credential entropy can be achieved by character complexity and minimum length requirements.

[REQ-AUTH-1-06] The product shall enforce authentication failure protection, including (i) progressive delays between failed attempts; and (ii) temporary account lockout after a configurable number of failed attempts.

[REQ-AUTH-1-07] When supporting password-based credentials, the product shall support maintaining the history of previously used passwords, in their processed form, to prevent reuse. The minimal number of previous passwords that shall be kept is one. The manufacturer may enable the user configuration of password history limit or increase this default based on the risk assessment. Password changes shall be validated against the configured password history limit before acceptance.

5.6.2 [AUTH-2] Authorisation

5.6.2.1 General

This clause establishes requirements for controlling what authenticated users can do on the product. While authentication verifies user identity, authorisation ensures users can only perform actions permitted by their privilege level. This is critical for the product as different users require different privileges.

5.6.2.2 Requirements

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

[REQ-AUTH-2-01] Where the product supports more than one privilege level, the product shall enforce privilege separation.

[REQ-AUTH-2-02] The product shall restrict each user to their authorised privilege level.

[REQ-AUTH-2-03] The product shall enforce authorisation control on all interfaces providing management access to the product.

[REQ-AUTH-2-04] The product shall deny execution of any command that is not authorised for the privilege level of the user issuing it.

5.6.3 [AUTH-3] Authenticated session lifecycle

5.6.3.1 General

This clause establishes requirements for managing the lifecycle of authenticated sessions, from establishment through termination. The product maintains the security context created through authentication as specified in clause 5.6.1 and authorisation as specified in clause 5.6.2 throughout the interaction. Session management prevents access without authorisation through session compromise.

Products remain accessible continuously and may be managed from multiple locations and interfaces. Robust session controls prevent configuration changes without authorisation that could compromise entire network segments. Vulnerabilities such as session hijacking, fixation, or replay attacks can lead to full product compromise, even when strong authentication is in place.

5.6.3.2 Requirements

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

[REQ-AUTH-3-01] The product shall enforce session timeout with configurable idle timeout periods and default values.

[REQ-AUTH-3-02] The product shall invalidate sessions immediately upon (i) user-initiated logout; (ii) timeout expiration; (iii) authentication credential change; (iv) expiry of a credential's validity; or (v) management termination. Session invalidation shall securely remove all session data.

[REQ-AUTH-3-03] The product shall limit concurrent sessions to a configurable maximum per user account.

[REQ-AUTH-3-04] The product shall deny privilege escalation attempts without authorisation within active sessions.

5.6.4 [AUTH-4] Protocol access control

5.6.4.1 General

This clause establishes requirements for management control over network protocols available on the product. Only authenticated and authorised users can enable, disable, or configure network protocols. Once enabled by an authorised user, protocols may operate according to their specifications. This applies to protocols that inherently lack authentication mechanisms for protocol-level interactions.

5.6.4.2 Requirements

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

Requirement [REQ-AUTH-4-05] applies, at the protocol layer, the legacy-interoperability framework set out in clause K.2.4 (2) of the present document for non-CRY-SOTA cryptographic algorithms.

Where risk factor [RF-B-06] is present, requirement [REQ-AUTH-4-01] applies.

[REQ-AUTH-4-01] The product shall enable only management protocols using state of the art cryptography in product factory default state and in product operational state.

NOTE 1: In this clause, "product operational state" refers to product operation in unmodified factory default setting. The user can decide to operate the product with legacy protocols.

Where any of risk factors [RF-B-05], [RF-TI-02] is present, requirement [REQ-AUTH-4-02] applies.

[REQ-AUTH-4-02] The product shall implement rate limiting and source validation for unauthenticated protocol requests to mitigate DoS attacks against management plane and control plane interfaces.

NOTE 2: The specific operational state for this assessment includes but is not limited to operational state prior to DoS conditions.

Where risk factor [RF-B-06] is present, requirement [REQ-AUTH-4-03] applies.

[REQ-AUTH-4-03] The product shall provide capability to configure state of the art cryptography and to disable protocols that do not use state of the art cryptography.

[REQ-AUTH-4-04] The product shall (i) validate trust establishment using additional mechanisms; and (ii) generate audit events for all trust relationship changes.

[REQ-AUTH-4-05] Where the product has activated a legacy protocol it supports, the product shall provide a user-facing indication that the legacy protocol is in use.

NOTE 3: For the present context, the mitigations recognised in publicly available specifications or in guidance from a recognised body should be preferred. Recognised bodies include those listed in clause K.1.1 (ii) of the present document, together with IETF Best Current Practice documents and applicable ETSI Technical Specifications.

5.7 Confidentiality protection

5.7.1 General

This clause establishes requirements for data confidentiality, integrity, and minimisation throughout the product lifecycle. Data protection rests on three principles. Confidentiality ensures data is accessible only to authorised entities. Integrity ensures data cannot be modified without authorisation. Data minimisation limits collection and retention to what the intended functions require. These principles apply to all data types processed by the product. Traffic content accessed during security inspection is subject to the same protections.

NOTE 1: Data necessary for intended security inspection functions, or for any additional product capabilities described in clause 4.3.3, includes connection state tables, signature matching results, threat detection metadata, security rule evaluation context, and session tracking data. It also includes inspection engine state, rule decision logs, and alert correlation data.

NOTE 2: Data considered beyond the intended purpose includes long-term retention of full packet payloads beyond real-time inspection, per-device behavioural analytics such as browsing habits or usage patterns, device fingerprinting beyond what access control requires, and diagnostic or telemetry data sent to the manufacturer or third parties.

5.7.2 Requirements

This clause addresses the requirements in the CRA [i.1], Annex I, Part I (2) (e), (2) (f) and (2) (g).

[REQ-DATA-1-01] The product shall protect the confidentiality of data at rest by one or more of the following: (i) encryption of the data using CRY-SOTA cryptography (see Annex K); (ii) access controls that prevent read access to the stored data by unauthorised entities; or (iii) another technical means that provides protection of data-at-rest confidentiality against unauthorised disclosure equivalent to (i) or (ii), where the product's technical documentation identifies the means and demonstrates how that protection is achieved.

NOTE 1: Point (iii) reflects the CRA [i.1], Annex I, Part I, point (2)(e), under which confidentiality can be protected by encryption or by other technical means. Point (iii) is technology-neutral and presupposes no specific implementation; examples include constructions in which the data is present in readable form only transiently during operation, or in which no interface exposes a command to read out the stored data.

NOTE 2: Where the demonstration under point (iii) is not provided, or is not sufficient to establish protection equivalent to point (i) or point (ii), the data at rest cannot be considered protected and is assessed under [AC-DATA-1-01] as if stored in plaintext.

[REQ-DATA-1-02] The product shall protect management communications and control plane traffic using state of the art cryptography.

[REQ-DATA-1-03] The product shall prevent modification of configuration and firmware without authorisation.

[REQ-DATA-1-04] The product shall implement data protection measures ensuring the product processes and retains only the minimum data required for its intended (i) firewall; (ii) intrusion detection; or (iii) intrusion prevention functions; or (iv) any additional product capabilities, including those described in clause 4.3.3.

[REQ-DATA-1-05] The product shall require explicit opt-in configuration of any diagnostic or telemetry data collection beyond the product's intended purpose, with such collection disabled by default.

5.8 Availability protection

5.8.1 General

This clause establishes requirements for protecting the availability of essential product functions during and after security incidents. Products detect, withstand, and recover from attacks while preserving security functions.

5.8.2 Requirements

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

[REQ-AVAIL-1-01] The product shall enforce rate limiting for each network protocol terminated by the product.

NOTE 1: The specific operational state for this assessment includes but is not limited to operational state prior to DoS conditions.

[REQ-AVAIL-1-02] The product shall enforce connection throttling for each connection-oriented network protocol terminated by the product.

NOTE 2: The specific operational state for this assessment includes but is not limited to operational state prior to DoS conditions.

[REQ-AVAIL-1-03] The product shall automatically recover to specific operational state when DoS conditions cease, without requiring manual intervention.

5.9 Non-interference

5.9.1 General

This clause establishes requirements for minimising the negative impact of the product on the availability of services provided by other products or networks. Products operating inline with network traffic can disrupt dependent systems through excessive resource consumption or uncontrolled failure modes.

5.9.2 Requirements

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

[REQ-IM-1-01] The product shall generate audit events when (i) resource utilisation exceeds the documented high utilisation threshold and (ii) resource utilisation returns below the documented high utilisation threshold.

NOTE: The high utilisation threshold levels are an implementation option and can be set by the manufacturer or be available as a user-configurable setting.

5.10 Attack surface minimalisation

5.10.1 [INTEGRITY-1] System integrity and boot process

5.10.1.1 General

This clause establishes requirements for product integrity throughout the operational lifecycle, from initial power-on through runtime operation. System integrity is the foundational trust anchor on which all other security controls depend. A compromised boot process or runtime environment can subvert authentication, bypass access controls, and grant persistent access without authorisation that survives reboots and firmware updates.

The boot process is a critical attack surface for persistent implants, security control bypass, and extraction of cryptographic material. Products operate autonomously for extended periods and control critical security functions. Boot integrity and runtime security prevent attacks during these periods and thus can prevent the compromise of entire network segments.

5.10.1.2 Requirements

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

[REQ-INTEGRITY-1-01] The product shall verify boot integrity using state of the art cryptography.

[REQ-INTEGRITY-1-02] The product shall in the factory default state enforce a secure boot chain where (i) each stage of the boot chain verifies the next stage before transferring execution control; (ii) the trusted code which is the first stage of the secure boot chain is protected against unauthorised modification; (iii) the product enters a predefined failure state on verification failure; and (iv) only verified code executes during boot.

NOTE 1: The product can provide a management mechanism by which the initial or subsequent trust materials used for enforcing the trust chain can be changed by at least, but not limited to, the authorised user.

NOTE 2: The verification can be based on cryptographic signatures, hashes or measured boot.

[REQ-INTEGRITY-1-03] The product shall generate audit events, from the moment the audit storage is available, including at least the result and status of the booting procedure.

NOTE 3: The generation of audit events at booting phases has constraints as the corresponding functionalities are not operational at early stages. An integrity validation failure through these early phases is constrained by the absence of essential components and causes execution to halt or triggers a hard reset. As a consequence, audit events for such early errors cannot be stored.

[REQ-INTEGRITY-1-04] The product shall protect recovery and maintenance modes by using methods documented in the instructions to the user.

5.10.2 [PACKET-1] Default packet disposition

5.10.2.1 General

These products differ fundamentally from general network infrastructure. Their primary purpose is security enforcement, not connectivity. The default-deny stance is their core operational principle. Products block traffic unless it has been explicitly validated. This applies even during resource exhaustion, parsing failures, or other exceptional conditions.

5.10.2.2 Requirements

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

[REQ-PACKET-1-01] Where the product cannot inspect traffic, the product shall apply the fail-secure action to that traffic.

[REQ-PACKET-1-02] The product shall enable fail-open operation only through management override.

[REQ-PACKET-1-03] Where stateful inspection is active, the product shall drop packets (i) that violate expected protocol state transitions; or (ii) that the product cannot reassemble for inspection.

NOTE: This requirement applies to network-layer stateful inspection.

[REQ-PACKET-1-04] The product shall (i) generate security events; (ii) increment bypass counters; and (iii) block the traffic where explicit per-flow configuration does not permit bypass, when traffic bypasses inspection.

[REQ-PACKET-1-05] The product shall drop packets that violate applicable protocol standards.

5.10.3 [EXPOSURE-1] Interface and service exposure minimisation

5.10.3.1 General

This clause establishes requirements to limit exposed interfaces and services. Products expose only what their intended operation requires. Each exposed interface is an attack vector; reducing unnecessary exposure reduces risk.

5.10.3.2 Requirements

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

[REQ-EXPOSURE-1-01] The product shall enable only those interfaces and services that have been configured, regardless of the product state.

[REQ-EXPOSURE-1-02] The product shall provide capability to selectively enable or disable individual services and interfaces through configuration.

5.11 Monitoring and logging

5.11.1 General

This clause covers requirements for recording and monitoring. These products serve as primary sensors in security architectures. Records support incident detection, threat response, forensic analysis, and compliance checks. The following activities are logged: authentication attempts, configuration changes, threat detections, blocked attacks, and management actions. Event data is protected against modification or deletion without authorisation.

5.11.2 Requirements

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

[REQ-LOG-1-01] The product shall generate audit events for authentication activities including but not limited to (i) successful or failed authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change attempts.

[REQ-LOG-1-02] The product shall generate audit events for all session lifecycle activities including (i) session establishment with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv) concurrent session limit violations.

[REQ-LOG-1-03] The product shall implement command authorisation that generates audit events whenever execution of unauthorised command is requested.

5.12 Data management

5.12.1 [TRANSFER-1] Secure data export and transfer

5.12.1.1 General

This clause addresses secure data transfer between products. Users require the ability to migrate configurations, operational data, and system state without loss of security. Configuration files contain critical security parameters and need protection during export and transfer.

NOTE: This does not limit the choice of users to import or export data using legacy protocols maintained for backward compatibility.

5.12.1.2 Requirements

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

[REQ-TRANSFER-1-01] The product shall provide capability to transfer exported data over a channel protected by state of the art cryptography.

[REQ-TRANSFER-1-02] The product shall provide capability to transfer imported data over a channel protected by state of the art cryptography.

[REQ-TRANSFER-1-03] The product shall require management access for data export and data import operations.

[REQ-TRANSFER-1-04] The product shall generate audit events for all data export and data import operations.

5.12.2 [SIGNATURE-1] Signature update and validation

5.12.2.1 General

This clause covers signature database retrieval, validation, and application. Compromised or outdated signatures can disable detection or introduce false negatives. Products maintain signature integrity and support secure distribution.

5.12.2.2 Requirements

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

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-01] applies.

[REQ-SIGNATURE-1-01] The product shall verify signature database update integrity using state of the art cryptography before installation.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-02] applies.

[REQ-SIGNATURE-1-02] The product shall verify signature database integrity using state of the art cryptography before use.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-03] applies.

[REQ-SIGNATURE-1-03] The product shall prevent installation of signature database versions older than the currently installed version.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-04] applies.

[REQ-SIGNATURE-1-04] The product shall restore the signature database from backup when integrity verification fails.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-05] applies.

[REQ-SIGNATURE-1-05] The product shall preserve user-created signatures when installing manufacturer-supplied signature database updates.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-06] applies.

[REQ-SIGNATURE-1-06] The product shall check for signature database updates at configurable intervals.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-07] applies.

[REQ-SIGNATURE-1-07] The product shall defer signature database updates outside configured maintenance windows.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-08] applies.

[REQ-SIGNATURE-1-08] The product shall limit signature database update download bandwidth to configurable thresholds.

Where any of risk factors [RF-UI-02], [RF-UI-03] is present, requirement [REQ-SIGNATURE-1-09] applies.

[REQ-SIGNATURE-1-09] The product shall retry failed signature database downloads within 24 hours.

5.13 Remote data processing solutions

5.13.1 General

This clause establishes requirements for products that depend on remote data processing solutions as defined in Article 3, point 2, of Regulation (EU) 2024/2847. For firewalls, intrusion detection systems, and intrusion prevention systems, RDPS dependencies commonly arise from cloud-based management, threat intelligence feeds, signature distribution, and log collection services. Compromise of RDPS connectivity or authentication can disable security functions, inject rules without authorisation, poison threat intelligence, or expose protected data.

5.13.2 Requirements

Where risk factor [RF-RDPS-01] is present, requirement [REQ-RDPS-1-01] applies.

[REQ-RDPS-1-01] The manufacturer shall document all remote data processing solutions on which the product depends.

Where risk factor [RF-RDPS-01] is present, requirement [REQ-RDPS-1-02] applies.

[REQ-RDPS-1-02] Where the product communicates with a remote data processing solution, the product shall protect that communication over a secure channel.

Where risk factor [RF-RDPS-01] is present, requirement [REQ-RDPS-1-03] applies.

[REQ-RDPS-1-03] Where the product communicates with a remote data processing solution, the product shall authenticate the remote data processing solution before transmitting data to it.

Where risk factor [RF-RDPS-01] is present, requirement [REQ-RDPS-1-04] applies.

[REQ-RDPS-1-04] Where the product communicates with a remote data processing solution, the product shall retry failed communications with the remote data processing solution as documented in the instructions to the user.

Where risk factor [RF-RDPS-01] is present, requirement [REQ-RDPS-1-05] applies.

[REQ-RDPS-1-05] The product shall generate audit events for communication failures with a remote data processing solution.

6 Assessment criteria for compliance with technical requirements

6.1 Introduction to the assessment and compliance criteria

This clause details the assessment process for compliance with the requirements in clause 5 of the present document.

NOTE: In the following clauses, *documentation* means any documentation provided to the assessor. This includes, but is not limited to, the technical specification, test results, and instructions to the user.

6.2 Appropriate level of cybersecurity

As stated in clause 5.2 of the present document, the requirements set out in clauses 5.3 to 5.14 have been developed to cover the corresponding requirement defined in the CRA [i.1], Annex I, Part I (1), given the security analysis methodology described in Annex B and its application to the use cases in clause 4.7 through the threats and risk factors identified in Annex B over the product assets defined in clause 4.2. The same coverage therefore applies to the assessments defined in the following clauses of the present document, which are associated with the cybersecurity requirements in clause 5.

6.3 No known exploitable vulnerabilities

6.3.1 [KEV-1] No known exploitable vulnerabilities

6.3.1.1 Requirement assessments

[AC-KEV-1-01] Verify that a software bill of materials is available, in a machine-readable format, for each product version.

Assessment reference

Requirement [REQ-KEV-1-01].

Assessment objective

Confirm that the software bill of materials for the product version under assessment is available in a machine-readable format and that its declared version matches the installed version reported by the product.

Assessment preparation

1) The product is in specific operational state.
2) The software bill of materials for the product is available.
3) Documentation describing the software bill of materials maintenance process is available.

Assessment activities

1) Review documentation to identify the software bill of materials maintenance process.
2) Inspect the software bill of materials and the installed version reported by the product. Verify that the version declared in the software bill of materials matches the installed version reported by the product, and that the software bill of materials is in a machine-readable format.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the software bill of materials maintenance process.

2) The product does not provide a software bill of materials in a machine-readable format, or its declared version does not match the installed version reported by the product.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the software bill of materials maintenance process.

2) The product provides a software bill of materials in a machine-readable format whose declared version matches the installed version reported by the product.

Assessment evidence

1) Documentation describing the software bill of materials maintenance process.

2) The software bill of materials and the installed version reported by the product.

[AC-KEV-1-02] Verify that the product contains no known exploitable vulnerabilities in each product version when made available on the market.

Assessment reference

Requirement [REQ-KEV-1-02].

Assessment objective

Confirm that no component of the product contains a known exploitable vulnerability in each product version when made available on the market.

Assessment preparation

1) The product is in product factory default state.

2) Documentation describing the vulnerability assessment process is available.

3) The software bill of materials is available.

Assessment activities

1) Review the software bill of materials. Verify that all product components and third-party dependencies are listed with version identifiers.

2) Cross-reference each component in the software bill of materials against known vulnerability databases. Verify that no listed component has a known exploitable vulnerability at the time of assessment.

3) Verify that the software bill of materials is maintained in a machine-readable format.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) The product does not provide a software bill of materials that lists all product components and third-party dependencies with version identifiers.

2) The product contains a known exploitable vulnerability in one or more components listed in the software bill of materials.

3) The product does not provide a software bill of materials in a machine-readable format.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) The product provides a software bill of materials that lists all product components and third-party dependencies with version identifiers.

2) The product does not contain a known exploitable vulnerability in any component listed in the software bill of materials.

3) The product provides a software bill of materials in a machine-readable format.

Assessment evidence

1) Documentation showing the software bill of materials lists all product components and third-party dependencies with version identifiers.

2) Test results showing no component listed in the software bill of materials contains a known exploitable vulnerability.

3) Documentation showing the format of the software bill of materials.

[AC-KEV-1-03] Verify that the product provides, for each product version when made available on the market, evidence of checks against known vulnerability databases for each third-party component.

Assessment reference

Requirement [REQ-KEV-1-03].

Assessment objective

Confirm that, for each product version when made available on the market, the product provides records of checks against known vulnerability databases covering every third-party component listed in the software bill of materials.

Assessment preparation

1) Documentation describing the third-party component verification process is available.

2) The software bill of materials is available.

Assessment activities

1) Review documentation to identify the third-party component verification process applied before each product version is made available on the market.

2) Inspect the software bill of materials and the verification records provided by the product. Verify that every third-party component listed in the software bill of materials has a corresponding record of a check against known vulnerability databases.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the third-party component verification process.

2) The product does not provide verification records covering every third-party component listed in the software bill of materials.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the third-party component verification process.

2) The product provides verification records covering every third-party component listed in the software bill of materials.

Assessment evidence

1) Documentation describing the third-party component verification process.

2) Verification records provided by the product showing checks of every third-party component listed in the software bill of materials against known vulnerability databases.

6.4 Secure by default configuration

6.4.1 [DEFAULT-1] Secure by default configuration

6.4.1.1 Requirement assessments

[AC-DEFAULT-1-01] Verify that the product enforces the applicable requirements of the present document in product factory default state, and that each excepted requirement (i) renders the initial product setup process non-functional; and (ii) the instructions to the user document the exception.

Assessment reference

Requirement [REQ-DEFAULT-1-01].

Assessment objective

Confirm that the product enforces the applicable requirements of the present document in product factory default state, and that each excepted requirement (i) renders the initial product setup process non-functional; and (ii) the instructions to the user document the exception.

Assessment preparation

1) The product is in product factory default state.
2) Documentation listing applicable requirements and their conformance status in product factory default state is available.
3) Instructions to the user are available.

Assessment activities

1) Review documentation to identify the applicable requirements that are excepted from product factory default state.
2) Review documentation for each excepted requirement to confirm the stated justification that conforming to it renders the initial product setup process non-functional.
3) Inspect the product in product factory default state to identify all requirements that are not conformed to. Verify that each non-conformed requirement is listed in documentation as excepted.
4) Inspect the product in product factory default state to verify that all non-excepted requirements are conformed to.
5) Enforce conformance to each excepted requirement individually and attempt setup. Verify that setup fails.
6) Review instructions to the user to verify that each excepted requirement is listed.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all applicable requirements excepted from product factory default state.
2) Documentation does not describe the justification that conforming to each excepted requirement renders the initial product setup process non-functional.
3) The product does not document any non-conformed requirement in product factory default state as excepted.
4) Any non-excepted requirement is not conformed to in product factory default state.
5) The product does not fail setup when any excepted requirement is individually enforced.
6) Instructions to the user do not document every excepted requirement.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all applicable requirements excepted from product factory default state.
2) Documentation describes the justification that conforming to each excepted requirement renders the initial product setup process non-functional.
3) The product documents every non-conformed requirement in product factory default state as excepted.
4) All non-excepted requirements are conformed to in product factory default state.
5) The product fails setup when each excepted requirement is individually enforced.
6) Instructions to the user document every excepted requirement.

Assessment evidence

1) Documentation listing all applicable requirements excepted from product factory default state.
2) Documentation describing the justification that conforming to each excepted requirement renders the initial product setup process non-functional.
3) Test results showing the product documents every non-conformed requirement in product factory default state as excepted.
4) Test results showing all non-excepted requirements are conformed to in product factory default state.
5) Test results showing setup failure when each excepted requirement is individually enforced.
6) Instructions to the user listing all excepted requirements.

[AC-DEFAULT-1-02] Verify that the product, in its product factory default state, enables only those interfaces and services that product setup requires.

Assessment reference

Requirement [REQ-DEFAULT-1-02].

Assessment objective

Confirm that the product enables only the interfaces and services that product setup requires in product factory default state, and that no additional interfaces or services are active.

Assessment preparation

1) The product is in product factory default state.
2) Documentation describing the network interfaces and services required for product setup is available.

Assessment activities

1) Review documentation to identify all network interfaces and services required for product setup.
2) Inspect the product in product factory default state. Verify the product enables only network interfaces and services documented as required for setup and does not initiate undocumented outbound connections.
3) Complete the product setup process using only the documented interfaces and services. Verify that setup succeeds.
4) Attempt to access a network interface or service not documented as required for setup in product factory default state. Verify that access is denied or the interface is inactive.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all interfaces and services required for product setup.

2) Any active network interface in product factory default state is not documented as required for setup.

3) Any listening network service in product factory default state is not documented as required for setup.

4) The product initiates an undocumented outbound connection in product factory default state.

5) The product does not complete setup successfully using only documented interfaces and services.

6) The product does not deny access to network interfaces and services not required for setup in product factory default state.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all interfaces and services required for product setup.

2) All active network interfaces in product factory default state are documented as required for setup.

3) All listening network services in product factory default state are documented as required for setup.

4) The product does not initiate any undocumented outbound connection in product factory default state.

5) The product completes setup successfully using only documented interfaces and services.

6) The product denies access to network interfaces and services not required for setup in product factory default state.

Assessment evidence

1) Documentation listing all interfaces and services required for product setup.

2) Test results showing all active network interfaces in product factory default state are documented as required for setup.

3) Test results showing all listening network services in product factory default state are documented as required for setup.

4) Test results showing the product does not initiate any undocumented outbound connection in product factory default state.

5) Test results showing setup completes successfully using only documented interfaces and services.

6) Test results showing non-setup network interfaces and services are inaccessible in product factory default state.

[AC-DEFAULT-1-03] Verify that the product, in its product factory default state, restricts access to management accounts and methods, as documented in the instructions to the user.

Assessment reference

Requirement [REQ-DEFAULT-1-03].

Assessment objective

Confirm that the product restricts access to management accounts and methods as documented in the instructions to the user, and that no undocumented management accounts or access methods exist.

Assessment preparation

1) The product is in product factory default state.

2) Instructions to the user describing factory default management accounts and methods are available.

Assessment activities

1) Review instructions to the user to identify all factory default management accounts and methods.

2) Attempt access using each management account and method documented in the instructions to the user. Verify that access is granted.

3) Attempt access using management accounts and methods not documented in the instructions to the user. Verify that the product restricts access by denying undocumented management accounts and methods.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Instructions to the user do not identify all factory default management accounts and methods.

2) Any management account or method documented in the instructions to the user is not functional in product factory default state.

3) The product does not deny access using undocumented management accounts and methods.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Instructions to the user identify all factory default management accounts and methods.

2) All management accounts and methods documented in the instructions to the user are functional in product factory default state.

3) The product denies access using undocumented management accounts and methods.

Assessment evidence

1) Instructions to the user listing all factory default management accounts and methods.

2) Test results showing all management accounts and methods documented in the instructions to the user are functional in product factory default state.

3) Test results showing undocumented management accounts and methods are denied.

[AC-DEFAULT-1-04] Verify that the product, in its product operational state, requires authenticated and authorised access to management accounts.

Assessment reference

Requirement [REQ-DEFAULT-1-04].

Assessment objective

Confirm that access to management accounts in product operational state is granted only after successful authentication and that the authenticated identity is authorised for the requested management account.

Assessment preparation

1) The product is in product operational state with at least one management account configured by the user.

2) Documentation describing authentication and authorisation mechanisms for management accounts is available.

Assessment activities

1) Review documentation to identify authentication and authorisation mechanisms applied to management accounts.

2) Attempt access to a management account using valid authentication credentials of an identity authorised for that account. Verify that access is granted.

3) Attempt access to a management account without providing authentication credentials or with invalid credentials. Verify that the product denies access.

4) Attempt access to a management account using valid authentication credentials of an identity that is not authorised for that account. Verify that the product denies access.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe authentication and authorisation mechanisms applied to management accounts.

2) The product does not grant access to the management account when authentication succeeds and the authenticated identity is authorised.

3) The product does not deny access to the management account when authentication is absent or fails.

4) The product does not deny access to the management account when the authenticated identity is not authorised.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes authentication and authorisation mechanisms applied to management accounts.

2) The product grants access to the management account when authentication succeeds and the authenticated identity is authorised.

3) The product denies access to the management account when authentication is absent or fails.

4) The product denies access to the management account when the authenticated identity is not authorised.

Assessment evidence

1) Documentation describing authentication and authorisation mechanisms for management accounts.

2) Test results showing access is granted to a management account on successful authentication and authorisation.

3) Test results showing access to a management account is denied when authentication is absent or fails.

4) Test results showing access to a management account is denied when the authenticated identity is not authorised.

[AC-DEFAULT-1-05] Verify that the product disables all diagnostic interfaces in product factory default state.

Assessment reference

Requirement [REQ-DEFAULT-1-05].

Assessment objective

Confirm that all diagnostic interfaces are disabled in product factory default state.

Assessment preparation

1) The product is in product factory default state.

2) Documentation listing all diagnostic interfaces is available.

Assessment activities

1) Review documentation to identify all diagnostic interfaces.

2) Inspect the product in product factory default state to verify that each documented diagnostic interface is disabled.

3) Attempt to access each documented diagnostic interface in product factory default state. Verify that access is denied or the interface is inactive.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all diagnostic interfaces.
2) Any documented diagnostic interface is enabled in product factory default state.
3) Any documented diagnostic interface does not deny access in product factory default state.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all diagnostic interfaces.
2) All documented diagnostic interfaces are disabled in product factory default state.
3) All documented diagnostic interfaces deny access in product factory default state.

Assessment evidence

1) Documentation listing all diagnostic interfaces.
2) Test results showing all documented diagnostic interfaces are disabled in product factory default state.
3) Test results showing all documented diagnostic interfaces deny access in product factory default state.

[AC-DEFAULT-1-06] Verify that the product requires authentication and authorisation for any management action that enables a diagnostic interface.

Assessment reference

Requirement [REQ-DEFAULT-1-06].

Assessment objective

Confirm that the product requires authentication and authorisation for any management action that enables a diagnostic interface.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing the management actions used to enable diagnostic interfaces is available.

Assessment activities

1) Review documentation to identify all management actions used to enable diagnostic interfaces.
2) Attempt to perform each management action to enable a diagnostic interface without authentication. Verify that the product denies the action.
3) Attempt to perform each management action to enable a diagnostic interface with credentials below the required authorisation level. Verify that the product denies the action.
4) Perform each management action to enable a diagnostic interface with credentials at the required authorisation level. Verify that the action succeeds.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe all management actions used to enable diagnostic interfaces.
2) The product does not deny access without authentication to any diagnostic interface.
3) The product does not deny access with insufficient authorisation to any diagnostic interface.
4) The product does not grant access with authentication and authorisation to any diagnostic interface.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes all management actions used to enable diagnostic interfaces.
2) The product denies access without authentication to each diagnostic interface.
3) The product denies access with insufficient authorisation to each diagnostic interface.
4) The product grants access with authentication and authorisation to each diagnostic interface.

Assessment evidence

1) Documentation describing all management actions used to enable diagnostic interfaces.
2) Test results showing the product denies access without authentication to each diagnostic interface.
3) Test results showing the product denies access with insufficient authorisation to each diagnostic interface.
4) Test results showing the product grants access with authentication and authorisation to each diagnostic interface.

[AC-DEFAULT-1-07] Verify that the product, in its product factory default state, generates audit events for (i) authentication attempts; (ii) configuration changes; and (iii) product errors, if those do not affect the recording.

Assessment reference

Requirement [REQ-DEFAULT-1-07].

Assessment objective

Confirm that the product, in its product factory default state, generates audit events for authentication attempts, configuration changes, and product errors that do not affect the recording.

Assessment preparation

1) The product is in product factory default state.
2) Documentation describing audit events generated for authentication attempts, configuration changes, and product errors is available.

Assessment activities

1) Review documentation to identify the audit events generated for authentication attempts, configuration changes, and product errors.
2) Trigger each authentication attempt scenario described in the documentation. Verify that the product generates an audit event for each attempt.
3) Perform each configuration change scenario described in the documentation. Verify that the product generates an audit event for each change.
4) Trigger each product error condition described in the documentation that does not affect audit recording. Verify that the product generates an audit event for the error.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the audit events generated for authentication attempts, configuration changes, or product errors.
2) The product does not generate an audit event for any authentication attempt.
3) The product does not generate an audit event for any configuration change.
4) The product does not generate an audit event for any product error that does not affect audit recording.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the audit events generated for authentication attempts, configuration changes, and product errors.

2) The product generates an audit event for each authentication attempt.

3) The product generates an audit event for each configuration change.

4) The product generates an audit event for each product error that does not affect audit recording.

Assessment evidence

1) Documentation describing the audit events generated for authentication attempts, configuration changes, and product errors.

2) Test results showing the product generates audit events for each authentication attempt.

3) Test results showing the product generates audit events for each configuration change.

4) Test results showing the product generates audit events for product errors that do not affect audit recording.

[AC-DEFAULT-1-08] Verify that the product, in its product factory default state, requires state of the art cryptography for all cryptographic functions.

Assessment reference

Requirement [REQ-DEFAULT-1-08].

Assessment objective

Confirm that the product, in its product factory default state, requires state of the art cryptography for all cryptographic functions, and that no deprecated or weak cryptography is enabled.

Assessment preparation

1) Documentation describing the cryptographic configuration is available.

Assessment activities

1) Review documentation to identify the cryptographic configuration.

2) Inspect the product in product factory default state to verify the active cryptographic configuration matches the documented cryptographic configuration and is state of the art.

3) Inspect the product in product operational state to verify the active cryptographic configuration matches the documented cryptographic configuration and is state of the art.

4) Verify that where cryptographic negotiation is supported, the default order does not prefer deprecated cryptography over recognised cryptography, and that where only fixed configuration is used, no negotiation occurs.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the cryptographic configuration.

2) The product does not use state of the art cryptography in product factory default state.

3) The product does not use state of the art cryptography in product operational state.

4) The product does not prioritise recognised cryptography over deprecated cryptography in the default negotiation order where negotiation is supported.

5) The product performs cryptographic negotiation where only fixed configuration is used.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the cryptographic configuration.
2) The product uses state of the art cryptography in product factory default state.
3) The product uses state of the art cryptography in product operational state.
4) The product prioritises recognised cryptography over deprecated cryptography in the default negotiation order where negotiation is supported.
5) The product does not perform cryptographic negotiation where only fixed configuration is used.

Assessment evidence

1) Documentation describing the cryptographic configuration.
2) Test results showing the cryptographic configuration is state of the art in product factory default state.
3) Test results showing the cryptographic configuration is state of the art in product operational state.
4) Test results showing the default negotiation order does not prefer deprecated cryptography over recognised cryptography where negotiation is supported.
5) Test results showing no cryptographic negotiation occurs where only fixed configuration is used.

[AC-DEFAULT-1-09] Verify that the product, in its product factory default state, does not enable any network-accessible service that relies on a legacy protocol, and that activation of a legacy protocol requires an explicit management action.

Assessment reference

Requirement [REQ-DEFAULT-1-09].

Assessment objective

Confirm that the product enables no network-accessible service that relies on a legacy protocol in product factory default state, and that the product requires an explicit management action to activate a legacy protocol.

Assessment preparation

1) The product is in product factory default state.
2) Documentation describing the legacy protocols supported by the product is available.

Assessment activities

1) Review documentation to list each legacy protocol supported by the product.
2) Scan the product in product factory default state to enumerate network-accessible services. Verify that no enabled network-accessible service relies on a legacy protocol.
3) Scan the product in product factory default state to enumerate active protocols. Verify that each documented legacy protocol is disabled.
4) Attempt to activate each documented legacy protocol without performing the documented management action. Verify that the legacy protocol remains disabled.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list each legacy protocol supported by the product.
2) The product enables a network-accessible service that relies on a legacy protocol in product factory default state.
3) Any documented legacy protocol is enabled in product factory default state.

4) Any documented legacy protocol becomes enabled when activation is attempted without the documented management action.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists each legacy protocol supported by the product.

2) The product does not enable any network-accessible service that relies on a legacy protocol in product factory default state.

3) Each documented legacy protocol remains disabled in product factory default state.

4) Each documented legacy protocol remains disabled when activation is attempted without the documented management action.

Assessment evidence

1) Documentation listing each legacy protocol supported by the product.

2) Test results showing no enabled network-accessible service relies on a legacy protocol in product factory default state.

3) Test results showing each documented legacy protocol is disabled in product factory default state.

4) Test results showing each documented legacy protocol remains disabled when activation is attempted without the documented management action.

[AC-DEFAULT-1-10] Verify that the manufacturer records in the technical documentation referred to in Annex VII of Regulation (EU) 2024/2847 [i.1], for each legacy protocol supported by the product, (i) the legacy protocol; (ii) the security features that are no longer considered state of the art; (iii) the specific legacy system or systems for which the protocol is required; and (iv) the constraint preventing the use of a state of the art alternative.

Assessment reference

Requirement [REQ-DEFAULT-1-10].

Assessment objective

Confirm that the technical documentation records, for each legacy protocol supported by the product, (i) the legacy protocol; (ii) the security features that are no longer considered state of the art; (iii) the specific legacy system or systems for which the protocol is required; and (iv) the constraint preventing the use of a state of the art alternative.

Assessment preparation

1) The product is in product operational state.

2) The technical documentation referred to in Annex VII of Regulation (EU) 2024/2847 [i.1] is available.

Assessment activities

1) Review documentation to list each legacy protocol supported by the product.

2) Review documentation for the security features that are no longer considered state of the art for each documented legacy protocol.

3) Review documentation for the legacy system or systems for which each documented legacy protocol is required.

4) Review documentation for the constraint preventing the use of a state of the art alternative for each documented legacy protocol.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list each legacy protocol supported by the product.

2) Documentation does not list the security features that are no longer considered state of the art for any documented legacy protocol.

3) Documentation does not list the legacy system or systems for any documented legacy protocol.

4) Documentation does not describe the constraint preventing the use of a state of the art alternative for any documented legacy protocol.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists each legacy protocol supported by the product.

2) Documentation lists the security features that are no longer considered state of the art for each documented legacy protocol.

3) Documentation lists the legacy system or systems for which each documented legacy protocol is required.

4) Documentation describes the constraint preventing the use of a state of the art alternative for each documented legacy protocol.

Assessment evidence

1) Documentation listing each legacy protocol supported by the product.

2) Documentation listing the security features that are no longer considered state of the art for each documented legacy protocol.

3) Documentation listing the legacy system or systems for which each documented legacy protocol is required.

4) Documentation describing the constraint preventing the use of a state of the art alternative for each documented legacy protocol.

[AC-DEFAULT-1-11] Verify that the product enforces the principle of least privilege during normal operation.

Assessment reference

Requirement [REQ-DEFAULT-1-11].

Assessment objective

Confirm that the product enforces the principle of least privilege by defining distinct privilege levels, restricting each account to its assigned privileges, and preventing privilege escalation without authorisation.

Assessment preparation

1) The product is in specific operational state with initialisation complete.

2) Documentation describing the role and permission model is available.

3) Accounts for each defined role are available or can be created.

Assessment activities

1) Review documentation to identify all defined roles and their assigned operations.

2) Authenticate with an account of each defined role. Verify that all assigned operations are available.

3) Authenticate with each defined role in turn and attempt operations assigned to a higher-privilege role. Verify that access is denied for each attempt.

4) Attempt privilege escalation without authorisation. Verify that the product rejects the attempt.

5) Inspect running processes and services on the product where accessible to verify they run with minimum required privileges and not as root or equivalent unless documented as necessary.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all roles, their privilege levels, and assigned operations.
2) Any defined role does not perform all its assigned operations.
3) The product does not deny operations assigned to higher-privilege roles to lower-privilege accounts.
4) The product does not reject privilege escalation attempts without authorisation.
5) The product does not run all inspected processes with minimum required privileges where process listing is accessible.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all roles, their privilege levels, and assigned operations.
2) Each defined role performs all its assigned operations.
3) The product denies operations assigned to higher-privilege roles to lower-privilege accounts.
4) The product rejects privilege escalation attempts without authorisation.
5) The product runs all inspected processes with minimum required privileges where process listing is accessible.

Assessment evidence

1) Documentation listing all roles, privilege levels, and assigned operations.
2) Test results showing each defined role performs all its assigned operations.
3) Test results showing the product denies operations assigned to higher-privilege roles to lower-privilege accounts.
4) Test results showing the product rejects privilege escalation attempts without authorisation.
5) Test results showing the product runs all inspected processes with minimum required privileges where process listing is accessible.

[AC-DEFAULT-1-12] Verify that the product stores audit events in persistent memory that survives a reboot.

Assessment reference

Requirement [REQ-DEFAULT-1-12].

Assessment objective

Confirm that the product stores audit events in persistent memory that survives the reboot.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing audit event storage mechanisms is available.

Assessment activities

1) Review documentation to identify the audit event storage mechanism.
2) Perform a reboot. Verify that audit events recorded before the reboot are present and intact after the reboot.
3) Perform a power cycle. Verify that audit events recorded before the power cycle are present and intact after the power cycle.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list the audit event storage mechanism.
2) The product does not store audit events in persistent memory that survives a reboot.
3) The product does not store audit events in persistent memory that survives a power cycle.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

4) Documentation lists the audit event storage mechanism.
5) The product stores audit events in persistent memory that survives a reboot.
6) The product stores audit events in persistent memory that survives a power cycle.

Assessment evidence

1) Documentation listing the audit event storage mechanism.
2) Test results showing the product stores audit events in persistent memory that survives a reboot.
3) Test results showing the product stores audit events in persistent memory that survives a power cycle.

6.4.2 [RESET-1] Factory reset

6.4.2.1 Requirement assessments

[AC-RESET-1-01] Verify that the product provides a factory reset mechanism that restores the product to its secure-by-default configuration.

Assessment reference

Requirement [REQ-RESET-1-01].

Assessment objective

Confirm that the product provides a factory reset mechanism that restores the product to its secure-by-default configuration.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing the factory reset mechanism and procedure is available.

Assessment activities

1) Review documentation to identify the factory reset mechanism and procedure. Verify the product provides a documented factory reset mechanism.
2) Perform a factory reset. Verify that the product is restored to its secure-by-default configuration.
3) Perform the assessments in clause 5.4.1 on the post-reset product. Verify that all assessments pass.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the factory reset mechanism or procedure.
2) The product does not restore its secure-by-default configuration after factory reset.
3) The product does not pass all assessments in clause 5.4.1 after factory reset.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the factory reset mechanism and procedure.
2) The product restores its secure-by-default configuration after factory reset.
3) The product passes all assessments in clause 5.4.1 after factory reset.

Assessment evidence

1) Documentation describing the factory reset mechanism and procedure.
2) Test results showing the product is restored to its secure-by-default configuration after factory reset.
3) Test results showing the product passes all assessments in clause 5.4.1 after factory reset.

[AC-RESET-1-02] Verify that the product maintains the currently installed firmware version and all installed security updates after factory reset.

Assessment reference

Requirement [REQ-RESET-1-02].

Assessment objective

Confirm that the product provides a factory reset mechanism that maintains the currently installed firmware version and all installed security updates, without reverting to the firmware version when made available on the market.

Assessment preparation

1) The product is in specific operational state with at least one security update applied beyond the firmware version when made available on the market.
2) Documentation describing factory reset behaviour for firmware version and security updates is available.

Assessment activities

1) Review documentation to confirm the product provides a factory reset mechanism that preserves firmware version and security updates.
2) Perform factory reset. Verify that the product maintains (i) the currently installed firmware version; and (ii) all installed security updates.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe that factory reset preserves firmware version and installed security updates.
2) The product does not maintain the currently installed firmware version after factory reset.
3) Any installed security update does not remain applied after factory reset.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes that factory reset preserves firmware version and installed security updates.
2) The product maintains the currently installed firmware version after factory reset.
3) All installed security updates remain applied after factory reset.

Assessment evidence

1) Documentation describing factory reset behaviour for firmware and installed security updates.
2) Test results showing the product maintains the currently installed firmware version after factory reset.
3) Test results showing all installed security updates remain applied after factory reset.

[AC-RESET-1-03] Verify that the product does not retain (i) non-default configuration; (ii) user data; or (iii) user-instantiated or modified critical security parameters after factory reset.

Assessment reference

Requirement [REQ-RESET-1-03].

Assessment objective

Confirm that the product does not retain (i) non-default configuration; (ii) user data; or (iii) user-instantiated or modified critical security parameters after factory reset.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing factory reset behaviour is available.

Assessment activities

1) Review documentation to identify data retained and data removed during factory reset.
2) Modify the product configuration to a non-default state, create user data, and configure user-instantiated or modified critical security parameters. Verify the modifications are present before factory reset.
3) Perform factory reset. Attempt to retrieve the previously modified configuration through the product.
4) Attempt to retrieve the previously created user data through the product after factory reset.
5) Attempt to retrieve the previously configured user-instantiated or modified critical security parameters through the product after factory reset.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe data retained and data removed during factory reset.
2) The product does not contain non-default configuration, user data, or user-instantiated or modified critical security parameters before factory reset.
3) The product retains non-default configuration after factory reset.
4) The product retains user data after factory reset.
5) The product retains user-instantiated or modified critical security parameters after factory reset.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes data retained and data removed during factory reset.
2) The product contains non-default configuration, user data, and user-instantiated or modified critical security parameters before factory reset.
3) The product does not retain non-default configuration after factory reset.
4) The product does not retain user data after factory reset.
5) The product does not retain user-instantiated or modified critical security parameters after factory reset.

Assessment evidence

1) Documentation describing data retained and data removed during factory reset.
2) Test results showing the product contains non-default configuration, user data, and user-instantiated or modified critical security parameters before factory reset.
3) Test results showing the product does not retain non-default configuration after factory reset.

4) Test results showing the product does not retain user data after factory reset.

5) Test results showing the product does not retain user-instantiated or modified critical security parameters after factory reset.

6.5 Security updates

6.5.1 [UPDATE-1] Update mechanisms

6.5.1.1 Requirement assessments

[AC-UPDATE-1-01] Verify that the product provides a mechanism to receive security updates.

Assessment reference

Requirement [REQ-UPDATE-1-01].

Assessment objective

Confirm that the product provides a mechanism to receive security updates through on-product delivery, off-the-product delivery, or both.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the security update delivery method is available.

Assessment activities

1) Review documentation to identify whether the product supports on-product delivery, off-the-product delivery, or both.

2) For products not designed for configuration and maintenance by professional network administrators, verify that the product downloads the security update through the on-product mechanism, where the product supports on-product delivery.

3) For products not designed for configuration and maintenance by professional network administrators, obtain a security update through the documented off-the-product procedure, where the product supports off-the-product delivery.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the security update delivery method.

2) The product does not download the security update through the on-product mechanism.

3) The product does not provide a mechanism to receive security updates through the documented off-the-product procedure.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the security update delivery method.

2) The product downloads the security update through the on-product mechanism.

3) The product provides a mechanism to receive security updates through the documented off-the-product procedure.

Assessment evidence

1) Documentation describing the security update delivery method.

2) Test results showing the product downloads the security update through the on-product mechanism.

3) Test results showing the product provides a mechanism to receive security updates through the off-the-product procedure.

[AC-UPDATE-1-02] Verify that the product prevents installation of security updates without authentication and authorisation.

Assessment reference

Requirement [REQ-UPDATE-1-02].

Assessment objective

Confirm that the product prevents installation of security updates without authentication and authorisation.

Assessment preparation

1) The product is in specific operational state.

2) For products not designed for configuration and maintenance by professional network administrators, documentation describing authentication and authorisation requirements for security update installation is available.

Assessment activities

1) Review documentation to identify the authentication and authorisation requirements for security update installation.

2) Attempt to install a security update without authentication. Verify that the product prevents the installation.

3) Attempt to install a security update without authorisation. Verify that the product prevents the installation.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the authentication and authorisation requirements for security update installation.

2) For products not designed for configuration and maintenance by professional network administrators, the product does not prevent security update installation without authentication.

3) The product does not prevent security update installation without authorisation.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the authentication and authorisation requirements for security update installation.

2) For products not designed for configuration and maintenance by professional network administrators, the product prevents security update installation without authentication.

3) The product prevents security update installation without authorisation.

Assessment evidence

1) Documentation describing the authentication and authorisation requirements for security update installation.

2) Test results showing the product prevents security update installation without authentication.

3) Test results showing the product prevents security update installation without authorisation.

[AC-UPDATE-1-03] Verify that the product provides a mechanism to install a received security update, that the mechanism installs the update, and that the product reports the installed version.

Assessment reference

Requirement [REQ-UPDATE-1-03].

Assessment objective

Confirm that the product provides a mechanism to install a received security update, that exercising the mechanism installs the update, and that the product reports the installed version after installation.

Assessment preparation

1) The product is in specific operational state.

2) A security update has been received through the documented delivery method.

Assessment activities

1) Review documentation to identify the security update installation procedure and the version reporting mechanism.

2) Install the received security update. Verify that the product reports the installed version after installation.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the security update installation procedure and the version reporting mechanism.

2) The product does not install the security update.

3) The product does not report the installed version.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the security update installation procedure and the version reporting mechanism.

2) The product installs the security update.

3) The product reports the installed version.

Assessment evidence

1) Documentation describing the security update installation procedure and the version reporting mechanism.

2) Test results showing the product installs the security update.

3) Test results showing the product reports the installed version.

[AC-UPDATE-1-04] Verify that when the product is not designed for configuration and maintenance by professional network administrators, the product automatically checks for security remedy updates according to the documented default schedule. Otherwise, verify that the procedure for checking for security updates is included in the instructions to the user.

Assessment reference

Requirement [REQ-UPDATE-1-04].

Assessment objective

Confirm that when the product is not designed for configuration and maintenance by professional network administrators, the product automatically checks for security remedy updates according to the documented default schedule, and otherwise that the instructions to the user include the procedure for checking for security updates.

Assessment preparation

1) The product is in specific operational state.

2) Documentation identifying whether the product is designed for configuration and maintenance by professional network administrators is available.

3) For products not designed for configuration and maintenance by professional network administrators, documentation describing the default schedule for checking security remedy updates is available.

4) For products designed for configuration and maintenance by professional network administrators, instructions to the user are available.

Assessment activities

1) Review documentation to identify whether the product is designed for configuration and maintenance by professional network administrators and to identify the applicable update checking information.

2) Where the product is not designed for configuration and maintenance by professional network administrators, inspect the product in specific operational state and verify that it automatically checks for security remedy updates according to the documented default schedule.

3) Where the product is designed for configuration and maintenance by professional network administrators, follow the documented procedure for checking for security updates and verify that the procedure enables checking for security updates.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not identify whether the product is designed for configuration and maintenance by professional network administrators.

2) Documentation does not describe the default schedule for checking security remedy updates where the product is not designed for configuration and maintenance by professional network administrators.

3) Instructions to the user do not describe the procedure for checking for security updates where the product is designed for configuration and maintenance by professional network administrators.

4) The product does not check for security remedy updates automatically according to the documented default schedule where the product is not designed for configuration and maintenance by professional network administrators.

5) The documented procedure does not enable checking for security updates where the product is designed for configuration and maintenance by professional network administrators.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation identifies whether the product is designed for configuration and maintenance by professional network administrators.

2) Documentation describes the default schedule for checking security remedy updates where the product is not designed for configuration and maintenance by professional network administrators.

3) Instructions to the user describe the procedure for checking for security updates where the product is designed for configuration and maintenance by professional network administrators.

4) The product checks for security remedy updates automatically according to the documented default schedule where the product is not designed for configuration and maintenance by professional network administrators.

5) The documented procedure enables checking for security updates where the product is designed for configuration and maintenance by professional network administrators.

Assessment evidence

1) Documentation identifying whether the product is designed for configuration and maintenance by professional network administrators.

2) Documentation describing the default schedule for checking security remedy updates where the product is not designed for configuration and maintenance by professional network administrators.

3) Instructions to the user describing the procedure for checking for security updates where the product is designed for configuration and maintenance by professional network administrators.

4) Test results showing the product checks for security remedy updates automatically according to the documented default schedule where the product is not designed for configuration and maintenance by professional network administrators.

5) Test results showing the documented procedure enables checking for security updates where the product is designed for configuration and maintenance by professional network administrators.

[AC-UPDATE-1-05] Verify that when the product is not designed for configuration and maintenance by professional network administrators, the security update mechanism is automated and enabled by default. Otherwise, verify that the procedure for performing the security update is included in the instructions to the user.

Assessment reference

Requirement [REQ-UPDATE-1-05].

Assessment objective

Confirm that when the product is not designed for configuration and maintenance by professional network administrators, the security update mechanism is automated and enabled by default, and otherwise that the instructions to the user include the procedure for performing the security update.

Assessment preparation

1) The product is in product factory default state.

2) Documentation identifying whether the product is designed for configuration and maintenance by professional network administrators is available.

3) For products designed for configuration and maintenance by professional network administrators, instructions to the user are available.

4) A security update is available through the documented delivery method.

Assessment activities

1) Review documentation to identify whether the product is designed for configuration and maintenance by professional network administrators and to identify the applicable security update mechanism or procedure.

2) Where the product is not designed for configuration and maintenance by professional network administrators, inspect the product in product factory default state and verify that the security update mechanism is automated and enabled by default.

3) Where the product is designed for configuration and maintenance by professional network administrators, follow the documented procedure for performing the security update and verify that the procedure enables the security update to be performed.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not identify whether the product is designed for configuration and maintenance by professional network administrators.

2) Documentation does not describe the automated and enabled-by-default security update mechanism where the product is not designed for configuration and maintenance by professional network administrators.

3) Instructions to the user do not describe the procedure for performing the security update where the product is designed for configuration and maintenance by professional network administrators.

4) The product does not provide a security update mechanism that is automated and enabled by default where the product is not designed for configuration and maintenance by professional network administrators.

5) The documented procedure does not enable the security update to be performed where the product is designed for configuration and maintenance by professional network administrators.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation identifies whether the product is designed for configuration and maintenance by professional network administrators.

2) Documentation describes the automated and enabled-by-default security update mechanism where the product is not designed for configuration and maintenance by professional network administrators.

3) Instructions to the user describe the procedure for performing the security update where the product is designed for configuration and maintenance by professional network administrators.

4) The product provides a security update mechanism that is automated and enabled by default where the product is not designed for configuration and maintenance by professional network administrators.

5) The documented procedure enables the security update to be performed where the product is designed for configuration and maintenance by professional network administrators.

Assessment evidence

1) Documentation identifying whether the product is designed for configuration and maintenance by professional network administrators.

2) Documentation describing the automated and enabled-by-default security update mechanism where the product is not designed for configuration and maintenance by professional network administrators.

3) Instructions to the user describing the procedure for performing the security update where the product is designed for configuration and maintenance by professional network administrators.

4) Test results showing the product provides a security update mechanism that is automated and enabled by default where the product is not designed for configuration and maintenance by professional network administrators.

5) Test results showing the documented procedure enables the security update to be performed where the product is designed for configuration and maintenance by professional network administrators.

[AC-UPDATE-1-06] Verify that the product verifies security update integrity using state of the art cryptography before installation.

Assessment reference

Requirement [REQ-UPDATE-1-06].

Assessment objective

Confirm that the product verifies security update integrity using state of the art cryptography before installation.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the security update integrity verification mechanism is available.

Assessment activities

1) Review documentation to identify the security update integrity verification mechanism.

2) Inspect the documented security update verification mechanism. Verify the cryptography used is state of the art.

3) Install a valid security update. Verify the product performs cryptographic verification before installation proceeds.

4) Attempt to install a tampered security update. Verify that the product rejects the installation.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the security update integrity verification mechanism.
2) The product does not use state of the art cryptography for security update verification.
3) The product does not perform cryptographic verification before installing the security update.
4) The product does not reject installation of a tampered security update.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the security update integrity verification mechanism.
2) The product uses state of the art cryptography for security update verification.
3) The product performs cryptographic verification before installing the security update.
4) The product rejects installation of a tampered security update.

Assessment evidence

1) Documentation describing the security update integrity verification mechanism.
2) Test results showing the security update verification uses state of the art cryptography.
3) Test results showing the product performs cryptographic verification before installing the security update.
4) Test results showing the product rejects installation of a tampered security update.

[AC-UPDATE-1-07] Verify that the product generates audit events for (i) security update availability; (ii) security update download initiation, completion, or failure; and (iii) security update installation success or failure.

Assessment reference

Requirement [REQ-UPDATE-1-07].

Assessment objective

Confirm that the product generates audit events for (i) security update availability; (ii) security update download initiation, completion, or failure; and (iii) security update installation success or failure.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing audit events generated for security update activities is available.

Assessment activities

1) Review documentation to identify the audit events generated for security update activities.
2) Trigger a security update availability notification. Verify that the product generates an audit event for security update availability.
3) Initiate and complete a security update download. Verify that the product generates audit events for security update download initiation, completion, or failure.
4) Perform a security update installation. Verify that the product generates an audit event for security update installation success or failure.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe audit events for security update activities.

2) The product does not generate an audit event for security update availability.

3) The product does not generate audit events for security update download initiation, completion, or failure.

4) The product does not generate an audit event for security update installation success or failure.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes audit events for security update activities.

2) The product generates an audit event for security update availability.

3) The product generates audit events for security update download initiation, completion, or failure.

4) The product generates an audit event for security update installation success or failure.

Assessment evidence

1) Documentation describing audit events generated for security update activities.

2) Test results showing the product generates an audit event for security update availability.

3) Test results showing the product generates audit events for security update download initiation, completion, or failure.

4) Test results showing the product generates an audit event for security update installation success or failure.

6.6 Authentication and access control

6.6.1 [AUTH-1] Authentication

6.6.1.1 Requirement assessments

[AC-AUTH-1-01] Verify that the product requires user authentication on all interfaces providing management access to the product.

Assessment reference

Requirement [REQ-AUTH-1-01].

Assessment objective

Confirm that the product requires user authentication on all interfaces providing management access to the product, and that access without authentication is denied.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the user authentication mechanism is available.

Assessment activities

1) Review documentation to identify all authentication mechanisms and management interfaces on which authentication is required.

2) Attempt to access the product on each management interface without providing credentials. Verify access is denied.

3) Authenticate using valid credentials on each management interface. Verify access is granted.

4) Authenticate using valid credentials and perform a series of operations without re-authenticating. Verify the product maintains authentication state throughout the session without requiring repeated credential entry.

5) Attempt to access the product on each management interface with invalid credentials. Verify access is denied.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the authentication mechanism, method, or management interfaces requiring authentication.

2) The product does not deny access without authentication on any management interface.

3) The product does not grant access with valid credentials on any management interface.

4) The product does not maintain authentication state throughout the session without requiring repeated credential entry.

5) The product does not reject invalid credentials on any management interface.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the authentication mechanism, method, and all management interfaces requiring authentication.

2) The product denies access without authentication on all management interfaces.

3) The product grants access with valid credentials on each management interface.

4) The product maintains authentication state throughout the session without requiring repeated credential entry.

5) The product rejects invalid credentials on each management interface.

Assessment evidence

1) Documentation describing the authentication mechanism, method, and all management interfaces requiring authentication.

2) Test results showing access without authentication is denied on each management interface.

3) Test results showing valid credentials grant access on each management interface.

4) Test results showing the product maintains authentication state throughout the session using valid credentials without re-authenticating.

5) Test results showing the product rejects invalid credentials on each management interface.

[AC-AUTH-1-02] Verify that the product eliminates shared default credentials by either (i) generating credentials during secure production; (ii) enforcing mandatory credential creation during initial setup; or (iii) using non-password based authentication credentials.

Assessment reference

Requirement [REQ-AUTH-1-02].

Assessment objective

Confirm that the product eliminates shared default credentials by either (i) generating credentials during secure production; (ii) enforcing mandatory credential creation during initial setup; or (iii) using non-password based authentication credentials, and that no two product units share default credentials.

Assessment preparation

1) The product is in product factory default state.

2) Documentation describing the credential provisioning approach is available.

Assessment activities

1) Review documentation to identify whether credentials are provisioned by per-unit production generation, by mandatory setup-time change, or by using non-password based authentication credentials.

2) When the product uses password-based credentials, start the initial setup process where setup-enforced credentials are used. Verify mandatory credential creation is enforced before access is granted and that credential creation cannot be skipped.

3) When the product uses password-based credentials, verify the product does not allow normal operation with shared default credentials.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not identify whether credentials are provisioned by per-unit production generation or by mandatory setup-time change.

2) Where setup-enforced credentials are used, the product does not enforce mandatory credential creation before granting access.

3) Where setup-enforced credentials are used, the product permits the mandatory credential creation step to be skipped.

4) The product operates with shared default credentials.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation identifies whether credentials are provisioned by per-unit production generation or by mandatory setup-time change.

2) Where setup-enforced credentials are used, the product enforces mandatory credential creation before access is granted.

3) Where setup-enforced credentials are used, the product does not permit the mandatory credential creation step to be skipped.

4) The product does not operate with shared default credentials.

Assessment evidence

1) Documentation describing whether credentials are provisioned by per-unit production generation or by mandatory setup-time change, or documentation identifying that the product does not use password-based credentials.

2) Test results showing mandatory credential creation is enforced before access is granted where setup-enforced.

3) Test results showing credential creation cannot be skipped.

4) Test results confirming shared default credentials do not provide access.

[AC-AUTH-1-03] Verify that where the product transmits critical security parameters, the product protects their transmission over a secure channel and prevents disclosure of critical security parameters over an unencrypted channel.

Assessment reference

Requirement [REQ-AUTH-1-03].

Assessment objective

Confirm that where the product transmits critical security parameters, the product protects their transmission over a secure channel and prevents disclosure of critical security parameters over an unencrypted channel.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the critical security parameter transmission mechanism and secure channel is available.

Assessment activities

1) Review documentation to identify the secure channel used for critical security parameter transmission.

2) Capture network traffic during an authentication attempt on each interface that accepts critical security parameters. Verify the product transmits critical security parameters over a secure channel.

3) Attempt to force critical security parameter transmission over an unencrypted channel. Verify that the product prevents disclosure of critical security parameters.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the secure channel used for critical security parameter transmission.

2) The product does not protect critical security parameters over a secure channel on any interface.

3) The product does not prevent disclosure of critical security parameters over an unencrypted channel.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the secure channel used for critical security parameter transmission.

2) The product protects critical security parameters over a secure channel on all interfaces.

3) The product prevents disclosure of critical security parameters over an unencrypted channel.

Assessment evidence

1) Documentation describing the secure channel used for critical security parameter transmission.

2) Test results showing the product protects critical security parameters over a secure channel when transmitting on all interfaces.

3) Test results showing the product prevents disclosure of critical security parameters when an unencrypted channel is forced.

[AC-AUTH-1-04] Verify that the product protects critical security parameters using state of the art cryptography.

Assessment reference

Requirement [REQ-AUTH-1-04].

Assessment objective

Confirm that the product protects critical security parameters using state of the art cryptography.

Assessment preparation

1) The product is in specific operational state with at least one user account configured.

2) Documentation describing the critical security parameter storage mechanism is available.

Assessment activities

1) Review documentation to identify the cryptographic method used for critical security parameter storage and its parameters. Verify the documented method is state of the art.

2) Inspect stored critical security parameters where storage is accessible, verifying they are not in plaintext and that a known-credential stored representation is consistent with the documented method. Inspect manufacturer technical documentation or source code where direct storage access is not available to confirm the implementation matches the documented method.

3) Attempt to retrieve critical security parameters in plaintext through available interfaces without required authorisation. Verify the product protects critical security parameters by denying retrieval.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the critical security parameter storage method.
2) The product does not use a state of the art critical security parameter storage method.
3) The product stores critical security parameters in plaintext.
4) The product does not store critical security parameters consistently with the documented method.
5) The product permits retrieval of critical security parameters in plaintext without authorisation.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the critical security parameter storage method.
2) The product uses a state of the art critical security parameter storage method.
3) The product does not store critical security parameters in plaintext.
4) The product stores critical security parameters consistently with the documented method.
5) The product does not permit retrieval of critical security parameters in plaintext without authorisation.

Assessment evidence

1) Documentation describing the critical security parameter storage method, parameters, and standard reference.
2) Test results showing the storage method is state of the art.
3) Test results showing critical security parameters are not stored in plaintext, where direct access is available.
4) Test results showing stored representation matches the documented method.
5) Test results showing the implementation matches the documented storage method, where direct storage access is not available.
6) Test results showing critical security parameters cannot be retrieved in plaintext without authorisation.

[AC-AUTH-1-05] When supporting password-based credentials, verify that the product enforces minimum credential entropy.

Assessment reference

Requirement [REQ-AUTH-1-05].

Assessment objective

When supporting password-based credentials, confirm that the product enforces minimum credential entropy, for example through minimum length and character complexity requirements sufficient to ensure entropy, and rejects credentials that do not meet these requirements.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing minimum credential entropy requirements is available.

Assessment activities

1) Review documentation to identify the minimum credential entropy requirements.
2) Attempt to create or change a credential that does not meet the documented minimum entropy. Verify the product rejects the credential.
3) Create or change a credential that meets the minimum entropy. Verify the product accepts it.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the minimum credential entropy requirements.
2) The product does not reject credentials that do not meet the minimum entropy.
3) The product does not accept credentials meeting the minimum entropy.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the minimum credential entropy requirements.
2) The product rejects credentials that do not meet the minimum entropy.
3) The product accepts credentials meeting the minimum entropy.

Assessment evidence

1) Documentation describing the minimum credential entropy requirements.
2) Test results showing credentials that do not meet the minimum entropy are rejected.
3) Test results showing credentials meeting the minimum entropy are accepted.

[AC-AUTH-1-06] Verify that the product enforces authentication failure protection by (i) progressive delays between failed attempts; and (ii) temporary account lockout after a configurable number of failed attempts.

Assessment reference

Requirement [REQ-AUTH-1-06].

Assessment objective

Confirm that the product enforces authentication failure protection by (i) progressive delays between failed attempts; and (ii) temporary account lockout after a configurable number of failed attempts, and that both mechanisms are documented with specific thresholds and durations.

Assessment preparation

1) The product is in specific operational state with at least one user account.
2) Documentation describing the authentication failure protection mechanisms is available.

Assessment activities

1) Review documentation to identify the authentication failure protection parameters.
2) Perform consecutive failed authentication attempts using invalid credentials and measure the delay between allowed attempts. Verify the delay increases progressively with consecutive failures.
3) Reset the authentication failure counter by successfully authenticating, then perform consecutive failed attempts from a clean zero-failure state until the documented lockout threshold is reached. Verify the account is temporarily locked and the lockout duration matches the documented value.
4) Wait for lockout to expire and authenticate with valid credentials. Verify access is granted and failure counters are reset.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe authentication failure protection mechanisms.
2) Documentation does not list lockout threshold and duration values.
3) The product does not apply a delay between consecutive failed authentication attempts.

4) The product does not increase the delay with each consecutive failure.

5) The product does not lock the account after consecutive failed authentication attempts reach the documented lockout threshold.

6) The product does not enforce the documented lockout duration.

7) The product does not restore access with valid credentials after lockout expires.

8) The product does not reset the failure counter after successful authentication following lockout.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes authentication failure protection mechanisms.

2) Documentation lists lockout threshold and duration values.

3) The product applies a delay between consecutive failed authentication attempts.

4) The product increases the delay with each consecutive failure.

5) The product locks the account after consecutive failed authentication attempts reach the documented lockout threshold.

6) The product enforces the documented lockout duration.

7) The product restores access with valid credentials after lockout expires.

8) The product resets the failure counter after successful authentication following lockout.

Assessment evidence

1) Documentation describing authentication failure protection mechanisms.

2) Documentation listing lockout threshold and duration values.

3) Test results showing the product applies progressive delays between consecutive failed authentication attempts.

4) Test results showing the delay increases with each consecutive failure.

5) Test results from resetting the failure counter and performing consecutive failed authentication attempts showing the product locks the account after the documented lockout threshold is reached.

6) Test results showing the product enforces the documented lockout duration.

7) Test results showing the product restores access with valid credentials after lockout expires.

8) Test results showing the product resets the failure counter after successful authentication following lockout.

[AC-AUTH-1-07] Verify that the product supports maintaining the history of previously used passwords, in their processed form, to prevent reuse, with a minimum of one previous password kept, and that password changes are validated against this history before acceptance.

Assessment reference

Requirement [REQ-AUTH-1-07].

Assessment objective

Confirm that the product supports maintaining the history of previously used passwords in their processed form, retains at least one previous password, and rejects password changes that attempt to reuse a password present in the history.

Assessment preparation

1) The product is in specific operational state with at least one user account.

2) Documentation describing the password history mechanism is available.

Assessment activities

1) Review documentation to identify the number of previous passwords retained and the storage form or documentation to enable the user configuration of password history limit.

2) Review documentation to identify the password history depth and the cryptographic method used for storage.

3) Verify the documented password history depth meets the graduated minimum for the applicable risk factors.

4) Use the password change interface to (i) set a known password; (ii) change it to a different value; and (iii) attempt to change it back to the original value. Verify the product rejects the change and informs the user that the password is already present in the password history.

5) Change the password to a value that is not present in the password history. Verify the change is accepted.

6) Inspect the password history where storage is accessible. Verify previous passwords are stored using state of the art cryptographic password encryption or hashes.

7) Test password history isolation across accounts by (i) configuring two separate user accounts; (ii) changing the password on one account; and (iii) attempting to reuse that same password on the other account. Verify the history of one account does not affect password validation on the other.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the number of previous passwords retained or the storage form.

2) Documentation does not describe the password history mechanism or cryptographic storage method.

3) The product does not store the graduated minimum number of previous passwords for the applicable risk level.

4) The product does not reject password changes to passwords present in the history.

5) The product does not inform the user of the rejection reason.

6) The product does not accept new passwords not present in the history.

7) The product does not store password history using state of the art cryptographic password encryption or hashes.

8) The product does not isolate password history across accounts.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the number of previous passwords retained and the storage form.

2) Documentation describes the password history mechanism and cryptographic storage method.

3) The product stores the graduated minimum number of previous passwords for the applicable risk level.

4) The product rejects password changes to passwords present in the history.

5) The product informs the user of the rejection reason.

6) The product accepts new passwords not present in the history.

7) The product stores password history using state of the art cryptographic password encryption or hashes.

8) The product isolates password history across accounts.

Assessment evidence

1) Documentation describing the number of previous passwords retained and the storage form.

2) Documentation describing the password history mechanism, depth, and cryptographic storage method.

3) Test results showing the product stores the graduated minimum number of previous passwords for the applicable risk level.

4) Test results showing passwords present in the password history are rejected.

5) Test results showing the user is informed of the rejection reason.

6) Test results showing new passwords not present in history are accepted.

7) Test results showing the product stores password history using state of the art cryptographic password encryption or hashes.

8) Test results showing the product isolates password history across accounts.

6.6.2 [AUTH-2] Authorisation

6.6.2.1 Requirement assessments

[AC-AUTH-2-01] Verify that where the product supports more than one privilege level, the product enforces privilege separation.

Assessment reference

Requirement [REQ-AUTH-2-01].

Assessment objective

Confirm that where the product supports more than one privilege level, the product enforces privilege separation.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the privilege levels is available, where the product supports more than one privilege level.

Assessment activities

Review documentation to identify whether the product supports more than one privilege level. Verify that the documentation describes all privilege levels and the authentication mechanism for management access, where applicable.

Attempt to access management functions without authentication, where the product supports more than one privilege level. Verify access is denied.

Authenticate with non-management credentials and attempt to access management functions, where the product supports more than one privilege level. Verify access is denied.

Authenticate with management credentials, where the product supports more than one privilege level. Verify management functions are accessible.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe all supported privilege levels or the authentication mechanism for management access.

2) The product does not deny access without authentication to management functions.

3) The product grants management access with non-management credentials.

4) The product does not grant access to management functions with management credentials.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes all supported privilege levels and the authentication mechanism for management access.
2) The product denies access without authentication to management functions.
3) The product does not grant management access with non-management credentials.
4) The product grants access to management functions with management credentials.

Assessment evidence

1) Documentation describing all supported privilege levels and the authentication mechanism for management access.
2) Test results showing management access attempts without authentication are denied.
3) Test results showing non-management credentials cannot access management functions.
4) Test results showing management credentials grant access to management functions.

[AC-AUTH-2-02] Verify that the product restricts each user to their authorised privilege level.

Assessment reference

Requirement [REQ-AUTH-2-02].

Assessment objective

Confirm that the product restricts each user to their authorised privilege level.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing all privilege levels and the operations assigned to each level is available.

Assessment activities

1) Review documentation to identify all privilege levels and the operations assigned to each.
2) Authenticate with an account at each privilege level and attempt all documented operations for that level. Verify they succeed.
3) Authenticate with an account at each defined privilege level in turn and attempt operations assigned to a higher privilege level. Verify each attempt is denied.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe all privilege levels.
2) Documentation does not describe the operations assigned to each privilege level.
3) The product does not permit each user to perform all operations within their assigned privilege level.
4) The product does not restrict users from performing operations above their assigned privilege level.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes all privilege levels.
2) Documentation describes the operations assigned to each privilege level.
3) The product permits each user to perform all operations within their assigned privilege level.
4) The product restricts users from performing operations above their assigned privilege level.

Assessment evidence

1) Documentation describing all privilege levels.

2) Documentation describing the operations assigned to each privilege level.

3) Test results showing the product permits each user to perform all operations within their assigned privilege level.

4) Test results showing the product restricts users from performing operations above their assigned privilege level.

[AC-AUTH-2-03] Verify that the product enforces authorisation control on all interfaces providing management access to the product.

Assessment reference

Requirement [REQ-AUTH-2-03].

Assessment objective

Confirm that the product enforces authorisation control on all interfaces providing management access to the product.

Assessment preparation

1) The product is in specific operational state.

2) Documentation listing all interfaces providing management access to the product and the access control mechanisms on each is available.

Assessment activities

1) Review documentation to identify all interfaces providing management access to the product and the access control mechanism on each.

2) Attempt access on each interface providing management access to the product. Verify that the product enforces access control on each interface.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe all interfaces providing management access to the product and their access control mechanisms.

2) The product does not enforce access control on any interface providing management access to the product.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes all interfaces providing management access to the product and their access control mechanisms.

2) The product enforces access control on each interface providing management access to the product.

Assessment evidence

1) Documentation describing all interfaces providing management access to the product and the access control mechanism for each.

2) Test results showing the product enforces access control on each interface providing management access to the product.

[AC-AUTH-2-04] Verify that the product denies execution of any command that is not authorised for the privilege level of the user issuing it.

Assessment reference

Requirement [REQ-AUTH-2-04].

Assessment objective

Confirm that the product denies execution of any command that is not authorised for the privilege level of the user issuing it.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the command authorisation mechanism is available.

Assessment activities

1) Review documentation to identify the command authorisation mechanism and the privilege level required for each command category.

2) Authenticate with a lower-privilege account and attempt to execute commands from each higher-privilege category. Verify each is denied before execution.

3) Authenticate with an authorised account and execute commands from the authorised category. Verify they succeed.

4) Attempt to bypass command authorisation by modifying command parameters or injecting commands through alternative input paths. Verify the product denies execution.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the command authorisation mechanism or privilege requirements per command category.

2) The product does not validate privilege levels before command execution.

3) The product does not reject higher-privilege commands from lower-privilege users.

4) The product does not execute authorised commands successfully.

5) The product does not deny execution when command parameters are modified or commands are injected through alternative input paths.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the command authorisation mechanism and privilege requirements per command category.

2) The product validates privilege levels before command execution.

3) The product rejects higher-privilege commands from lower-privilege users.

4) The product executes authorised commands successfully.

5) The product denies execution when command parameters are modified or commands are injected through alternative input paths.

Assessment evidence

1) Documentation describing the command authorisation mechanism and privilege requirements per command category.

2) Test results showing the product validates privilege levels before command execution.

3) Test results showing the product rejects higher-privilege commands from lower-privilege users.

4) Test results showing authorised commands execute successfully for authorised accounts.

5) Test results showing the product denies execution when command parameters are modified or commands are injected through alternative input paths.

6.6.3 [AUTH-3] Authenticated session lifecycle

6.6.3.1 Requirement assessments

[AC-AUTH-3-01] Verify that the product enforces session timeout with configurable idle timeout periods and default values.

Assessment reference

Requirement [REQ-AUTH-3-01].

Assessment objective

Confirm that the product enforces session timeout with configurable idle timeout periods and default values.

Assessment preparation

1) The product is in specific operational state with at least one authenticated session.
2) Documentation describing session timeout mechanisms, default timeout values, and configuration options is available.

Assessment activities

1) Review documentation to identify the default idle timeout value and the configurable range.
2) Retrieve the default idle timeout value from documentation or product configuration and leave an authenticated session idle for that timeout period. Verify that the product terminates the session and requires re-authentication.
3) Establish a new session and perform an operation during the timeout period. Verify the timeout counter resets and the session remains active.
4) Configure the timeout period to a shorter value. Verify that the session terminates after the new period.
5) Attempt to reuse a timed-out session. Verify that the product denies access.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the default idle timeout value and configurable range.
2) The product does not terminate sessions after the default idle timeout period.
3) The product does not require re-authentication after session termination by idle timeout.
4) The product does not reset the timeout counter when user activity occurs, or the session does not remain active.
5) The product does not enforce configurable timeout periods.
6) The product does not apply newly configured timeout values.
7) The product does not deny access when a timed-out session is reused.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the default idle timeout value and configurable range.
2) The product terminates sessions after the default idle timeout period.
3) The product requires re-authentication after session termination by idle timeout.
4) The product resets the timeout counter when user activity occurs and the session remains active.
5) The product enforces configurable timeout periods.

6) The product applies newly configured timeout values.

7) The product denies access when a timed-out session is reused.

Assessment evidence

1) Documentation describing the session timeout mechanism, default idle timeout value, and configurable range.

2) Test results showing the product terminates sessions after the default idle timeout period.

3) Test results showing the product requires re-authentication after session termination by idle timeout.

4) Test results showing the timeout counter resets on user activity and the session remains active.

5) Test results showing the product enforces configurable timeout periods.

6) Test results showing the product applies newly configured timeout values.

7) Test results showing access is denied when a timed-out session is reused.

[AC-AUTH-3-02] Verify that the product invalidates sessions immediately upon (i) user-initiated logout; (ii) timeout expiration; (iii) authentication credential change; (iv) expiry of a credential's validity; or (v) management termination, and that session invalidation securely removes all session data.

Assessment reference

Requirement [REQ-AUTH-3-02].

Assessment objective

Confirm that the product invalidates sessions immediately upon (i) user-initiated logout; (ii) timeout expiration; (iii) authentication credential change; (iv) expiry of a credential's validity; or (v) management termination, that session invalidation securely removes all session data, and that invalidated sessions cannot be reused.

Assessment preparation

1) The product is in specific operational state with at least one authenticated session.

2) Documentation describing session invalidation triggers and data removal mechanisms is available.

Assessment activities

1) Review documentation to identify all session invalidation triggers and data removal mechanisms.

2) Establish an authenticated session and perform a logout. Establish a second session and terminate it through the management interface. Verify that the product denies access when either session identifier is reused.

3) Establish a session and change the authentication credential for the account. Verify that the product invalidates the existing session and requires re-authentication.

4) Allow an established session to time out. Verify that the product denies access when the session identifier is reused.

5) Trigger each session invalidation type in sequence and time each invalidation from trigger event to denial of the session identifier. Verify no observable delay occurs.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe all invalidation triggers and data removal mechanisms.

2) The product does not invalidate sessions upon logout or termination.

3) The product does not reject invalidated session identifiers on subsequent use.

4) The product does not invalidate sessions upon authentication credential change.

5) The product does not invalidate sessions upon timeout expiration.

6) The product does not invalidate sessions without observable delay for all triggers.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes all invalidation triggers and data removal mechanisms.

2) The product invalidates sessions upon logout or termination.

3) The product rejects invalidated session identifiers on subsequent use.

4) The product invalidates sessions upon authentication credential change.

5) The product invalidates sessions upon timeout expiration.

6) The product invalidates sessions without observable delay for all triggers.

Assessment evidence

1) Documentation describing all session invalidation triggers and data removal mechanisms.

2) Test results showing the product invalidates sessions upon logout or termination.

3) Test results showing the product rejects invalidated session identifiers on subsequent use.

4) Test results showing the product invalidates sessions upon authentication credential change.

5) Test results showing the product invalidates sessions upon timeout expiration.

6) Test results showing the product invalidates sessions without observable delay for all triggers.

[AC-AUTH-3-03] Verify that the product limits concurrent sessions to a configurable maximum per user account.

Assessment reference

Requirement [REQ-AUTH-3-03].

Assessment objective

Confirm that the product limits concurrent sessions to a configurable maximum per user account.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the concurrent session limit mechanism is available.

Assessment activities

1) Review documentation to identify the default concurrent session limit and the configurable range.

2) Establish sessions up to the documented limit. Verify that all are active.

3) Attempt to establish one session beyond the limit. Verify that the product denies the additional session.

4) Change the concurrent session limit to a different value. Verify the new limit is enforced.

5) Verify the limit is enforced per user account.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the default concurrent session limit, configurable range, and behaviour when the limit is exceeded.

2) The product does not accept sessions up to the documented concurrent session limit.

3) The product does not deny session establishment beyond the configured concurrent session limit.

4) The product does not enforce the newly configured concurrent session limit.

5) The product does not enforce the concurrent session limit independently per user account.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the default concurrent session limit, configurable range, and behaviour when the limit is exceeded.

2) The product accepts sessions up to the documented concurrent session limit.

3) The product denies session establishment beyond the configured concurrent session limit.

4) The product enforces the newly configured concurrent session limit.

5) The product enforces the concurrent session limit independently per user account.

Assessment evidence

1) Documentation describing the concurrent session limit, configurable range, and behaviour when the limit is exceeded.

2) Test results showing sessions up to the documented limit are active.

3) Test results showing the product denies session establishment beyond the configured concurrent session limit.

4) Test results showing the product enforces the newly configured concurrent session limit.

5) Test results showing the concurrent session limit applies independently to each user account.

[AC-AUTH-3-04] Verify that the product denies privilege escalation attempts without authorisation within active sessions.

Assessment reference

Requirement [REQ-AUTH-3-04].

Assessment objective

Confirm that the product denies privilege escalation attempts without authorisation within active sessions.

Assessment preparation

1) The product is in specific operational state with at least one non-management authenticated session.

2) Documentation describing the privilege escalation denial mechanism is available.

Assessment activities

1) Review documentation to identify the privilege escalation denial mechanism.

2) Attempt privilege escalation from a non-management session through (i) parameter manipulation; and (ii) session attribute tampering. Verify the product denies each attempt.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the privilege escalation denial mechanism.

2) The product does not deny privilege escalation attempts without authorisation from non-management sessions.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the privilege escalation denial mechanism.

2) The product denies privilege escalation attempts without authorisation from non-management sessions.

Assessment evidence

1) Documentation describing the privilege escalation denial mechanism.

2) Test results showing the product denies privilege escalation attempts without authorisation from non-management sessions.

6.6.4 [AUTH-4] Protocol access control

6.6.4.1 Requirement assessments

[AC-AUTH-4-01] Verify that the product enables only management protocols using state of the art cryptography in product factory default state and in product operational state.

Assessment reference

Requirement [REQ-AUTH-4-01].

Assessment objective

Confirm that the product enables only management protocols using state of the art cryptography in product factory default state and in product operational state.

Assessment preparation

1) The product is in product factory default state.

2) Documentation describing management protocols is available.

Assessment activities

1) Review documentation to identify all management protocols and their cryptographic protection.

2) Inspect the product in product factory default state to enumerate all enabled management protocols. Verify each uses state of the art cryptography.

3) Complete product initialisation without user modification and inspect the product in product operational state to enumerate all enabled management protocols. Verify each uses state of the art cryptography.

4) Capture network traffic during a management session on each enabled protocol in product operational state without user modification. Verify the captured traffic uses state of the art cryptography.

5) Attempt to enable a management protocol that does not use state of the art cryptography. Verify that the product denies the protocol activation or informs the user.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all management protocols or their cryptographic protection.

2) Any management protocol enabled in product factory default state does not use state of the art cryptography.

3) Any management protocol enabled in product operational state without user modification does not use state of the art cryptography.

4) Any enabled management protocol does not use state of the art cryptography in product operational state without user modification.

5) The product does not deny activation of protocols terminated by the product that do not use state of the art cryptography.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all management protocols and their cryptographic protection.

2) All management protocols enabled in product factory default state use state of the art cryptography.

3) All management protocols enabled in product operational state without user modification use state of the art cryptography.

4) All enabled management protocols use state of the art cryptography in product operational state without user modification.

5) The product denies activation of protocols terminated by the product that do not use state of the art cryptography.

Assessment evidence

1) Documentation listing all management protocols and their cryptographic protection.

2) Test results showing all management protocols enabled in product factory default state use state of the art cryptography.

3) Test results showing all management protocols enabled in product operational state without user modification use state of the art cryptography.

4) Test results from network traffic captures confirming all enabled management protocols use state of the art cryptography in product operational state without user modification.

5) Test results showing the product denies activation of protocols terminated by the product that do not use state of the art cryptography.

[AC-AUTH-4-02] Verify that the product implements rate limiting and source validation where possible, for unauthenticated protocol requests to mitigate DoS attacks against management plane and control plane interfaces.

Assessment reference

Requirement [REQ-AUTH-4-02].

Assessment objective

Confirm that the product implements rate limiting and source validation where possible, for unauthenticated protocol requests to mitigate DoS attacks against management plane and control plane interfaces.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the rate limiting mechanism is available.

Assessment activities

1) Review documentation to identify the rate limiting thresholds for each protocol that accepts requests without authentication.

2) Exceed the documented rate limiting threshold on each protocol that accepts requests without authentication. Verify the product drops requests after the threshold is reached.

3) Send requests without authentication below the documented rate limiting threshold on each protocol. Verify the product does not block them.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list rate limiting thresholds for any protocol that accepts requests without authentication.

2) The product does not drop requests that exceed the documented rate limiting threshold.

3) The product blocks requests below the documented rate limiting threshold.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists rate limiting thresholds for each protocol that accepts requests without authentication.
2) The product drops requests that exceed the documented rate limiting threshold.
3) The product does not block requests below the documented rate limiting threshold.

Assessment evidence

1) Documentation listing rate limiting thresholds for each protocol that accepts requests without authentication.
2) Test results showing the product enforces rate limiting by dropping requests exceeding the documented threshold.
3) Test results showing requests below the documented rate limiting threshold are not blocked.

[AC-AUTH-4-03] Verify that the product provides capability to configure state of the art cryptography and to disable protocols that do not use state of the art cryptography.

Assessment reference

Requirement [REQ-AUTH-4-03].

Assessment objective

Confirm that the product provides capability to configure state of the art cryptography and to disable protocols that do not use state of the art cryptography.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing cryptographic configuration and weak protocol versions is available.

Assessment activities

1) Review documentation to identify all protocols that do not use state of the art cryptography and the available configuration options.
2) Use the configuration interface to disable a protocol that does not use state of the art cryptography, where the documentation states disabling is operationally feasible. Verify the product refuses a connection using the disabled protocol.
3) Disable a weak protocol version using the configuration interface. Verify that the strong protocol version continues to function by completing a management session using it.
4) Verify that the documentation provides a justification for each weak protocol version where disabling is not operationally feasible.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe all protocols that do not use state of the art cryptography and the available configuration options.
2) The product does not provide configuration options to disable protocols that do not use state of the art cryptography where operationally feasible.
3) The product does not refuse connections on disabled protocols.
4) The product does not continue to support strong protocol versions after weak versions are disabled.
5) Documentation does not list a justification for each weak protocol version where disabling is not operationally feasible.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes all protocols that do not use state of the art cryptography and the available configuration options.

2) The product provides configuration options to disable protocols that do not use state of the art cryptography where operationally feasible.

3) The product refuses connections on disabled protocols.

4) The product continues to support strong protocol versions after weak versions are disabled.

5) Documentation lists a justification for each weak protocol version where disabling is not operationally feasible.

Assessment evidence

1) Documentation describing all protocols that do not use state of the art cryptography and the available configuration options.

2) Test results showing the product provides configuration options to disable protocols that do not use state of the art cryptography where operationally feasible.

3) Test results showing the product refuses connections on disabled protocols.

4) Test results showing the strong protocol version continues to function after weak versions are disabled.

5) Documentation listing a justification for each weak protocol version where disabling is not operationally feasible.

[AC-AUTH-4-04] Verify that the product validates trust establishment using additional mechanisms and generates audit events for all trust relationship changes.

Assessment reference

Requirement [REQ-AUTH-4-04].

Assessment objective

Confirm that the product validates trust establishment using additional mechanisms and that the product generates audit events for all trust relationship changes.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing trust establishment protocols and validation mechanisms is available.

Assessment activities

1) Review documentation to identify protocols that establish trust without cryptographic verification and the additional validation mechanisms for each.

2) Trigger a trust establishment event for each identified protocol. Verify the additional validation mechanism operates.

3) Attempt to establish a trust relationship through a spoofed source or a source without authorisation. Verify the validation mechanism detects or mitigates the attempt.

4) Verify that the product generates audit events for all trust relationship changes.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list trust establishment protocols or their additional validation mechanisms.

2) The product does not operate additional validation mechanisms during trust establishment events.

3) The product does not detect or mitigate spoofed trust establishment attempts via validation mechanisms.

4) The product does not generate audit events for all trust relationship changes.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists trust establishment protocols and their additional validation mechanisms.

2) The product operates additional validation mechanisms during trust establishment events.

3) The product detects or mitigates spoofed trust establishment attempts via validation mechanisms.

4) The product generates audit events for all trust relationship changes.

Assessment evidence

1) Documentation listing trust establishment protocols and their additional validation mechanisms.

2) Test results showing additional validation mechanisms operate during trust establishment events.

3) Test results showing the product detects or mitigates spoofed trust establishment attempts via validation mechanisms.

4) Test results showing audit events are generated for all trust relationship changes.

[AC-AUTH-4-05] Verify that the product provides a user-facing indication that the legacy protocol is in use, where the product has activated a legacy protocol it supports.

Assessment reference

Requirement [REQ-AUTH-4-05].

Assessment objective

Confirm that the product provides a user-facing indication that the legacy protocol is in use whenever a supported legacy protocol is active on the product.

Assessment preparation

1) The product is in product operational state.

2) Documentation describing the legacy protocols supported by the product and the user-facing indication mechanism is available.

Assessment activities

1) Review documentation to identify the user-facing indication mechanism for each legacy protocol supported by the product.

2) Enable each documented legacy protocol in turn using the documented management action. Verify that the product presents the user-facing indication that the legacy protocol is in use.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the user-facing indication mechanism for any legacy protocol supported by the product.

2) The product does not present a user-facing indication that the legacy protocol is in use for any enabled legacy protocol.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the user-facing indication mechanism for each legacy protocol supported by the product.

2) The product presents a user-facing indication that the legacy protocol is in use for each enabled legacy protocol.

Assessment evidence

1) Documentation describing the user-facing indication mechanism for each legacy protocol supported by the product.

2) Test results showing the product presents a user-facing indication that the legacy protocol is in use for each enabled legacy protocol.

6.7 Confidentiality protection

6.7.1 Requirement assessments

[AC-DATA-1-01] Verify that the product protects the confidentiality of data at rest by one or more of the means in [REQ-DATA-1-01].

Assessment reference

Requirement [REQ-DATA-1-01].

Assessment objective

Confirm that, for each category of data stored by the product, the confidentiality of the data at rest is protected by (i) CRY-SOTA encryption, (ii) access controls preventing read access by unauthorised entities, or (iii) another technical means demonstrated to provide equivalent protection against unauthorised disclosure.

Assessment preparation

1) The product is in a specified operational state with at least one user account configured.

2) Documentation is available that, for each category of data stored by the product, identifies the protection applied and which of points (i), (ii) or (iii) of [REQ-DATA-1-01] is relied upon.

3) Where point (iii) is relied upon, documentation is available that identifies the technical means and demonstrates how it protects data-at-rest confidentiality against unauthorised disclosure equivalently to (i) or (ii).

Assessment activities

1) Review documentation to identify all categories of data stored by the product and, for each, the protection relied upon and the point of [REQ-DATA-1-01] invoked.

2) For data relying on (i): verify that the cryptography is CRY-SOTA in accordance with Annex K; inspect storage to verify that the stored representation is not plaintext and is consistent with the documented protection.

3) For data relying on (ii): verify that the documented access controls prevent read access to the stored data by unauthorised entities, and confirm by inspection or testing that the data cannot be read through the interfaces available to such entities.

4) For data relying on (iii): verify that the documentation demonstrates how the technical means protects confidentiality against unauthorised disclosure equivalently to (i) or (ii), and verify the correctness of that demonstration. Where there is any uncertainty or ambiguity in the demonstration, request additional information before reaching a verdict. Confirm by inspection or testing that the protected data cannot be disclosed to unauthorised entities under the conditions the means is claimed to cover.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not identify all categories of data stored by the product, the protection relied upon for each, and the point of [REQ-DATA-1-01] invoked.

2) Any category of stored data is left without any of the protections (i), (ii) or (iii).

3) The cryptography is not CRY-SOTA, the stored representation is plaintext, or it is inconsistent with the documented protection.

4) The access controls do not prevent read access by unauthorised entities, or testing shows that the data can be read by such an entity.

5) The documentation does not demonstrate protection equivalent to (i) or (ii), the demonstration cannot be verified as correct, or testing shows that the data can be disclosed to an unauthorised entity; in any of these cases the data at rest is assessed as if stored in plaintext.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation identifies all categories of data stored by the product, the protection relied upon for each, and the point of [REQ-DATA-1-01] invoked.

2) Every category of stored data is covered by at least one of (i), (ii) or (iii).

3) The cryptography is CRY-SOTA, the stored representation is not plaintext, and the stored representation is consistent with the documented protection.

4) The access controls prevent read access by unauthorised entities, and testing shows that the data cannot be read by such an entity.

5) The documentation demonstrates protection equivalent to (i) or (ii), the demonstration is verified as correct, and testing shows that the data cannot be disclosed to an unauthorised entity.

Assessment evidence

1) Documentation listing all categories of data stored by the product, the protection relied upon for each, and the point of [REQ-DATA-1-01] invoked.

2) Test results showing CRY-SOTA cryptography and the absence of plaintext storage.

3) Documentation and test results showing that access controls prevent read access by unauthorised entities.

4) The technical documentation demonstrating equivalent protection, and test results showing that the protected data cannot be disclosed to unauthorised entities.

[AC-DATA-1-02] Verify that the product protects management communications and control plane traffic using state of the art cryptography.

Assessment reference

Requirement [REQ-DATA-1-02].

Assessment objective

Confirm that the product protects management communications and control plane traffic using state of the art cryptography.

Assessment preparation

1) The product is in specific operational state with management and control plane traffic actively flowing.

2) Documentation describing management communication channels and control plane protocols is available.

Assessment activities

1) Review documentation to identify all management communication channels and control plane protocols. Verify the documented cryptography is state of the art.

2) Inspect network traffic during active management and control plane exchanges. Verify the captured traffic uses state of the art cryptography.

3) Attempt to disable the cryptographic protection of management communications and control plane traffic. Verify the product does not permit this silently or without documented justification.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all management channels or control plane protocols.
2) The product does not use state of the art cryptography for any management channel or control plane protocol.
3) The product does not use state of the art cryptography for management communications or control plane traffic.
4) The product permits cryptographic protection of management communications to be disabled.
5) The product permits cryptographic protection of control plane traffic to be disabled.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all management channels and control plane protocols.
2) The product uses state of the art cryptography for all management channels and control plane protocols.
3) The product uses state of the art cryptography for management communications and control plane traffic.
4) The product does not permit cryptographic protection of management communications to be disabled.
5) The product does not permit cryptographic protection of control plane traffic to be disabled.

Assessment evidence

1) Documentation listing all management channels and control plane protocols.
2) Test results showing state of the art cryptography for all management channels and control plane protocols.
3) Test results from network traffic captures during management and control plane exchanges showing state of the art cryptography.
4) Test results showing the product does not permit cryptographic protection of management communications to be disabled.
5) Test results showing the product does not permit cryptographic protection of control plane traffic to be disabled.

[AC-DATA-1-03] Verify that the product prevents modification of configuration and firmware without authorisation.

Assessment reference

Requirement [REQ-DATA-1-03].

Assessment objective

Confirm that the product prevents modification of configuration and firmware without authorisation.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing the integrity verification mechanisms for configuration files and firmware images is available.

Assessment activities

1) Review documentation to identify the integrity verification mechanisms and the authorisation level required for modification of each.
2) Attempt to modify a configuration file using an authorised account. Verify that the modification succeeds.

3) Attempt to modify a configuration file using an insufficiently privileged account. Verify the modification is denied.

4) Modify a configuration file directly on the storage medium where direct storage access is feasible. Verify the product detects, rejects, or reverts the modification.

5) Attempt to install a tampered firmware image. Verify that the product detects the modification and rejects installation.

6) Install the valid firmware image using an authorised account. Verify installation succeeds.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe integrity verification mechanisms for configuration files or firmware images.

2) Documentation does not describe the authorisation level required for modification of each.

3) The product does not accept configuration modifications by authorised accounts.

4) The product does not deny configuration modifications by insufficiently privileged accounts.

5) The product does not detect or prevent direct storage modification of configuration files.

6) The product does not detect and reject tampered firmware images.

7) The product does not install valid firmware successfully with an authorised account.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes integrity verification mechanisms for configuration files and firmware images.

2) Documentation describes the authorisation level required for modification of each.

3) The product accepts configuration modifications by authorised accounts.

4) The product denies configuration modifications by insufficiently privileged accounts.

5) The product detects or prevents direct storage modification of configuration files.

6) The product detects and rejects tampered firmware images.

7) The product installs valid firmware successfully with an authorised account.

Assessment evidence

1) Documentation describing the integrity verification mechanisms for configuration files and firmware images.

2) Documentation describing the authorisation level required for modification of each.

3) Test results showing the product accepts configuration modifications by authorised accounts.

4) Test results showing the product denies configuration modifications by insufficiently privileged accounts.

5) Test results showing that direct storage modification of configuration files is detected or rejected where feasible.

6) Test results showing that the product detects and rejects a tampered firmware image.

7) Test results showing that valid firmware installation succeeds with an authorised account.

[AC-DATA-1-04] Verify that the product implements data protection measures ensuring the product processes and retains only the minimum data required for its intended (i) firewall; (ii) intrusion detection; or (iii) intrusion prevention functions; or (iv) any additional product capabilities, including those described in clause 4.3.3.

Assessment reference

Requirement [REQ-DATA-1-04].

Assessment objective

Confirm that the product implements data protection measures ensuring the product processes and retains only the minimum data required for its intended (i) firewall; (ii) intrusion detection; or (iii) intrusion prevention functions; or (iv) any additional product capabilities, including those described in clause 4.3.3.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the intended product functions, additional product capabilities, and the categories of data each function or capability processes and retains is available.

Assessment activities

1) Review documentation to identify the intended product functions, additional product capabilities, and the categories of data that each function or capability processes and retains.

2) Inspect the product and review its data protection measures. Verify that the product implements data protection measures ensuring data processing and retention are limited to the minimum required for the intended functions and additional capabilities.

3) Attempt to retrieve retained data through the product. Verify data categories are consistent with documented intended functions and additional product capabilities.

4) Capture outbound network traffic during operation. Verify the product transmits only data consistent with documented intended functions and additional product capabilities.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list the intended product functions, additional product capabilities, or the categories of data processed and retained for each.

2) The product does not implement data protection measures that limit data processing and retention to the minimum required for the intended functions and additional capabilities.

3) The product does not restrict retained data to categories consistent with documented intended functions and additional product capabilities.

4) The product does not restrict transmitted data to categories consistent with documented intended functions and additional product capabilities.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists the intended product functions, additional product capabilities, and the categories of data processed and retained for each.

2) The product implements data protection measures that limit data processing and retention to the minimum required for the intended functions and additional capabilities.

3) The product restricts retained data to categories consistent with documented intended functions and additional product capabilities.

4) The product restricts transmitted data to categories consistent with documented intended functions and additional product capabilities.

Assessment evidence

1) Documentation listing the intended product functions, additional product capabilities, and the categories of data each function or capability processes and retains.

2) Documentation and test results showing the product implements data protection measures limiting data processing and retention to the minimum required.

3) Test results showing the product restricts retained data to categories consistent with documented intended functions and additional product capabilities.

4) Test results from traffic capture confirming transmitted data is consistent with documented intended functions and additional product capabilities.

[AC-DATA-1-05] Verify that the product requires explicit opt-in configuration of any diagnostic or telemetry data collection beyond the product's intended purpose, and that such collection is disabled by default.

Assessment reference

Requirement [REQ-DATA-1-05].

Assessment objective

Confirm that the product requires explicit opt-in configuration of any diagnostic or telemetry data collection beyond the product's intended purpose, and that such collection is disabled by default.

Assessment preparation

1) The product is in product factory default state.

2) Documentation describing any diagnostic or telemetry data collection beyond the product's intended purpose, the opt-in configuration mechanism, and the default state of such collection is available.

Assessment activities

1) Review documentation to identify any diagnostic or telemetry data collection beyond the product's intended purpose, the opt-in configuration mechanism, and the default state of such collection.

2) Inspect the product in product factory default state. Capture outbound network traffic and verify that no diagnostic or telemetry data beyond the product's intended purpose is collected or transmitted.

3) Attempt to enable diagnostic or telemetry data collection beyond the product's intended purpose. Verify that enabling requires explicit opt-in configuration by an authorised user, distinct from accepting default settings.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe diagnostic and telemetry data collection beyond the product's intended purpose, the opt-in configuration mechanism, and the default state of such collection.

2) The product collects or transmits diagnostic or telemetry data beyond the product's intended purpose in product factory default state.

3) The product does not require explicit opt-in configuration to enable diagnostic or telemetry data collection beyond the product's intended purpose.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes diagnostic and telemetry data collection beyond the product's intended purpose, the opt-in configuration mechanism, and the default state of such collection.

2) The product does not collect or transmit any diagnostic or telemetry data beyond the product's intended purpose in product factory default state.

3) The product requires explicit opt-in configuration to enable diagnostic or telemetry data collection beyond the product's intended purpose.

Assessment evidence

1) Documentation describing diagnostic and telemetry data collection beyond the product's intended purpose, the opt-in configuration mechanism, and the default state of such collection.

2) Test results from traffic capture confirming no diagnostic or telemetry data beyond the product's intended purpose is collected or transmitted in product factory default state.

3) Test results showing the product requires explicit opt-in configuration to enable diagnostic or telemetry data collection beyond the product's intended purpose.

6.8 Availability protection

6.8.1 Requirement assessments

[AC-AVAIL-1-01] Verify that the product enforces rate limiting for each network protocol terminated by the product.

Assessment reference

Requirement [REQ-AVAIL-1-01].

Assessment objective

Confirm that the product enforces rate limiting for each network protocol terminated by the product.

Assessment preparation

1) The product is in specific operational state with at least one network protocol actively handling traffic.

2) Documentation describing the rate limiting mechanisms and their configured thresholds and parameters is available.

Assessment activities

1) Review documentation to identify all rate limiting mechanisms, protected protocols, and their configured thresholds and parameters.

2) Send legitimate traffic through the product at normal rates and record baseline throughput, response time, and resource utilisation.

3) Send requests to a protected protocol at a rate exceeding the documented threshold. Verify the product begins rejecting or delaying excess requests and that the documented threshold and time window match the observed enforcement point.

4) Initiate a simulated traffic flood against the product from one source and simultaneously send legitimate traffic from a separate source. Verify that throughput and response time for the legitimate traffic confirm it continues to be processed and that essential forwarding and management functions remain operational.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all rate limiting mechanisms, protected protocols, thresholds, and parameters.

2) The product does not maintain stable throughput, response time, or resource utilisation under normal traffic.

3) The product does not implement rate limiting.

4) The product does not enforce the documented rate limiting thresholds.

5) The product does not reject or delay excess requests beyond rate limiting thresholds.

6) The product does not enforce a rate limiting time window that matches the documented value.

7) The product does not continue to process legitimate traffic during simulated attack.

8) The product does not maintain essential forwarding and management functions during attack.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all rate limiting mechanisms, protected protocols, thresholds, and parameters.
2) The product maintains stable throughput, response time, and resource utilisation under normal traffic.
3) The product implements rate limiting.
4) The product enforces the documented rate limiting thresholds.
5) The product rejects or delays excess requests beyond rate limiting thresholds.
6) The product enforces a rate limiting time window that matches the documented value.
7) The product continues to process legitimate traffic during simulated attack.
8) The product maintains essential forwarding and management functions during attack.

Assessment evidence

1) Documentation listing all rate limiting mechanisms, protected protocols, thresholds, and parameters.
2) Test results showing baseline throughput, response time, and resource utilisation are recorded.
3) Test results showing the product implements rate limiting.
4) Test results showing the product enforces the documented rate limiting thresholds.
5) Test results showing the product rejects or delays excess requests beyond rate limiting thresholds.
6) Test results showing the observed rate limiting time window matches the documented value.
7) Test results showing legitimate traffic continues to be processed during simulated attack.
8) Test results showing forwarding and management functions remain operational during attack.

[AC-AVAIL-1-02] Verify that the product enforces connection throttling for each connection-oriented network protocol terminated by the product.

Assessment reference

Requirement [REQ-AVAIL-1-02].

Assessment objective

Confirm that the product enforces connection throttling for each connection-oriented network protocol terminated by the product.

Assessment preparation

1) The product is in specific operational state with at least one connection-establishing network protocol actively handling traffic.
2) Documentation describing the connection throttling mechanisms and their configured parameters is available.

Assessment activities

1) Review documentation to identify all connection throttling mechanisms, protected protocols, and their configured parameters.
2) Initiate new connections to the product at a rate exceeding the documented connection throttling parameter. Verify the product limits new connections.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all connection throttling mechanisms, protected protocols, and parameters.

2) The product does not implement connection throttling.

3) The product does not enforce the documented connection throttling parameters.

4) The product does not limit excess connections beyond throttling parameters.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all connection throttling mechanisms, protected protocols, and parameters.

2) The product implements connection throttling.

3) The product enforces the documented connection throttling parameters.

4) The product limits excess connections beyond throttling parameters.

Assessment evidence

1) Documentation listing all connection throttling mechanisms, protected protocols, and parameters.

2) Test results showing the product implements connection throttling.

3) Test results showing the product enforces the documented connection throttling parameters.

4) Test results showing the product limits excess connections beyond throttling parameters.

[AC-AVAIL-1-03] Verify that the product automatically recovers to specific operational state when DoS conditions cease, without requiring manual intervention.

Assessment reference

Requirement [REQ-AVAIL-1-03].

Assessment objective

Confirm that the product automatically recovers to specific operational state when DoS conditions cease, without requiring manual intervention, within the documented recovery time.

Assessment preparation

1) The product has DoS protection mechanisms activated by a simulated attack.

2) Documentation describing the automatic recovery behaviour, the specific operational state reached after recovery, and the expected recovery time is available. The specific operational state includes but is not limited to the operational state of the product prior to the DoS conditions.

Assessment activities

1) Review documentation to identify the automatic recovery behaviour, the specific operational state to which the product recovers, and the expected recovery time.

2) Initiate a simulated traffic flood to activate the DoS protection mechanisms of the product. Verify that protections are engaged, then cease the simulated attack entirely and record the cessation timestamp.

3) Measure the time until rate limiting, connection throttling, and legitimate traffic throughput return to normal parameters after the simulated attack ceases.

4) Verify that recovery occurred without manual intervention.

5) Verify all essential functions are operational after recovery. Verify the product has not remained in a degraded state.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the automatic recovery behaviour, the specific operational state, or the expected recovery time.

2) The product does not activate DoS protection mechanisms when a simulated traffic flood is initiated.

3) The product does not engage protections during the simulated traffic flood.

4) The product does not restore rate limiting and connection throttling to normal parameters automatically.

5) The product does not restore legitimate traffic throughput to baseline.

6) The product does not recover within the documented recovery period.

7) The product does not recover without manual intervention when DoS conditions cease.

8) Any essential function does not resume normal operation after recovery.

9) The product remains in a degraded state.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the automatic recovery behaviour, the specific operational state, and the expected recovery time.

2) The product activates DoS protection mechanisms when a simulated traffic flood is initiated.

3) The product engages protections during the simulated traffic flood.

4) The product restores rate limiting and connection throttling to normal parameters automatically.

5) The product restores legitimate traffic throughput to baseline.

6) The product recovers within the documented recovery period.

7) The product recovers without manual intervention when DoS conditions cease.

8) Each essential function resumes normal operation after recovery.

9) The product does not remain in a degraded state.

Assessment evidence

1) Documentation describing the automatic recovery behaviour, the specific operational state, and the expected recovery time.

2) Test results showing the product activates DoS protection mechanisms when a simulated traffic flood is initiated.

3) Test results showing the product engages protections during the simulated traffic flood.

4) Test results showing rate limiting and connection throttling return to normal parameters automatically after attack cessation.

5) Test results showing legitimate traffic throughput returns to baseline after attack cessation.

6) Test results showing recovery occurs within the documented recovery period.

7) Test results showing recovery occurred without manual intervention when DoS conditions ceased.

8) Test results showing all essential functions resume normal operation after recovery.

9) Test results showing the product does not remain in a degraded state after recovery.

6.9 Non-interference

6.9.1 Requirement assessments

[AC-IM-1-01] Verify that the product generates audit events when (i) resource utilisation exceeds the documented high utilisation threshold; and (ii) resource utilisation returns below the documented high utilisation threshold.

Assessment reference

Requirement [REQ-IM-1-01].

Assessment objective

Confirm that the product generates audit events when (i) resource utilisation exceeds the documented high utilisation threshold; and (ii) resource utilisation returns below the documented high utilisation threshold.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the resources monitored and their high utilisation thresholds is available.

Assessment activities

1) Review documentation to identify the monitored resources and their high utilisation thresholds.

2) Record baseline utilisation for each monitored resource and artificially increase utilisation above the documented threshold for each resource.

3) Inspect audit events. Verify that an audit event is generated for each resource that exceeds its documented high utilisation threshold.

4) Apply artificial load to drive each monitored resource above its documented high utilisation threshold, then cease the load and allow utilisation to return below the threshold. Inspect audit events for a threshold recovery audit event for each resource.

5) Retrieve the audit event via the documented access interface. Verify that all utilisation audit events are present and that no audit events are truncated.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list monitored resources and their high utilisation thresholds.

2) Any monitored resource does not report baseline utilisation.

3) Any monitored resource does not reach utilisation above the documented threshold under artificial load.

4) The product does not generate an audit event when each monitored resource exceeds its documented high utilisation threshold.

5) The product does not generate a threshold recovery audit event when each monitored resource returns below the documented high utilisation threshold.

6) Any utilisation audit event is not present in the audit log.

7) The product does not expose audit events via the documented access interface.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists monitored resources and their high utilisation thresholds.

2) Each monitored resource reports baseline utilisation.

3) Each monitored resource reaches utilisation above the documented threshold under artificial load.

4) The product generates an audit event when each monitored resource exceeds its documented high utilisation threshold.

5) The product generates a threshold recovery audit event when each monitored resource returns below the documented high utilisation threshold.

6) Each utilisation audit event is present in the audit log.

7) The product exposes audit events via the documented access interface.

Assessment evidence

1) Documentation listing monitored resources and their high utilisation thresholds.
2) Test results showing each monitored resource reports baseline utilisation.
3) Test results showing each monitored resource reaches utilisation above the documented threshold under artificial load.
4) Test results showing an audit event is generated for each resource that exceeds its high utilisation threshold.
5) Test results showing a threshold recovery audit event is generated for each resource after utilisation returns below the documented high utilisation threshold.
6) Test results showing each utilisation audit event is present in the audit log.
7) Test results showing the product exposes audit events via the documented access interface.

6.10 Attack surface and mitigation

6.10.1 [INTEGRITY-1] System integrity and boot process

6.10.1.1 Requirement assessments

[AC-INTEGRITY-1-01] Verify that the product verifies boot integrity using state of the art cryptography.

Assessment reference

Requirement [REQ-INTEGRITY-1-01].

Assessment objective

Confirm that the product verifies boot integrity using state of the art cryptography.

Assessment preparation

1) The product is in product factory default state with the boot process ready to be initiated.
2) Documentation describing boot components subject to cryptographic verification is available.

Assessment activities

1) Review documentation to identify the boot verification scheme and failure behaviour. Verify the documented cryptography is state of the art.
2) Boot the product and check the logging file that the booting procedure is documented. Check also whether the record shows fail or success.
3) Modify one software boot component that is accessible for modification and attempt to boot the product. Verify the product detects the modification, refuses to execute the modified component, and enters the predefined failure state.
4) Modify a software boot component that is accessible for modification, then restore the original. Verify the product completes normally after the original component is restored.
5) Inspect the verification key storage. Verify the key is stored in the documented protected location and is not modifiable through normal product interfaces.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all boot components, verification scheme, and failure behaviour.

2) The product does not use state of the art cryptography for boot component verification.

3) The product does not log the booting procedure or does not record the result.

4) The product does not detect or does not refuse to execute a modified boot component.

5) The product does not enter the predefined failure state on verification failure.

6) The product does not complete the boot process after restoring the original boot component during cryptographic verification testing.

7) The product does not store the verification key in the documented protected location.

8) The product permits modification of the verification key through normal product interfaces.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all boot components, verification scheme, and failure behaviour.

2) The product uses state of the art cryptography for boot component verification.

3) The product logs the booting procedure and records the result as fail or success.

4) The product detects and refuses to execute a modified boot component.

5) The product enters the predefined failure state on verification failure.

6) The product completes the boot process after restoring the original boot component during cryptographic verification testing.

7) The product stores the verification key in the documented protected location.

8) The product does not permit modification of the verification key through normal product interfaces.

Assessment evidence

1) Documentation listing all boot components, verification scheme, and failure behaviour.

2) Test results showing the boot verification uses state of the art cryptography.

3) Test results showing the logging file documents the booting procedure and the result.

4) Test results showing the product detects and refuses to execute a modified boot component.

5) Test results showing the product enters the predefined failure state on verification failure.

6) Test results showing the product completes the boot process after restoring the original boot component during cryptographic verification testing.

7) Test results showing the verification key is stored in the documented protected location.

8) Test results showing the verification key is not modifiable through normal product interfaces.

[AC-INTEGRITY-1-02] Verify that the product in the factory default state enforces a secure boot chain where (i) each stage of the boot chain verifies the next stage before transferring execution control; (ii) the trusted code which is the first stage of the secure boot chain is protected against unauthorised modification; (iii) the product enters a predefined failure state on verification failure; and (iv) only verified code executes during boot.

Assessment reference

Requirement [REQ-INTEGRITY-1-02].

Assessment objective

Confirm that the product in the factory default state enforces a secure boot chain where (i) each stage of the boot chain verifies the next stage before transferring execution control; (ii) the trusted code which is the first stage of the secure boot chain is protected against unauthorised modification; (iii) the product enters a predefined failure state on verification failure; and (iv) only verified code executes during boot.

Assessment preparation

1) The product is in product factory default state with the boot process ready to be initiated.

2) Documentation describing the boot chain architecture is available.

Assessment activities

1) Review documentation to identify all boot stages and the verification mechanism for each stage transition.

2) Attempt to modify the trusted code which is the first stage of the secure boot chain through software means. Verify the product rejects the modification.

3) Inspect the storage medium of the trusted code which is the first stage of the secure boot chain where physically feasible. Verify the protection matches the documented mechanism.

4) Boot the product and check the logging file that the booting procedure is documented. Check also whether the record shows fail or success.

5) Restore all components. Verify the product completes the boot process.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe all boot stages, verification mechanisms, and protection of the trusted code which is the first stage of the secure boot chain.

2) The product does not prevent modification of the trusted code which is the first stage of the secure boot chain through software.

3) The product does not store the trusted code which is the first stage of the secure boot chain using the documented protection mechanism.

4) The product does not log the booting procedure or does not record the result.

5) The product does not complete the boot process after restoring all modified components.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes all boot stages, verification mechanisms, and protection of the trusted code which is the first stage of the secure boot chain.

2) The product prevents modification of the trusted code which is the first stage of the secure boot chain through software.

3) The product stores the trusted code which is the first stage of the secure boot chain using the documented protection mechanism.

4) The product logs the booting procedure and records the result as fail or success.

5) The product completes the boot process after restoring all modified components.

Assessment evidence

1) Documentation describing all boot stages, verification mechanisms, and protection of the trusted code which is the first stage of the secure boot chain.

2) Test results from modification attempt show the product rejects modification of the trusted code which is the first stage of the secure boot chain through software.

3) Test results from storage inspection of the trusted code which is the first stage of the secure boot chain show the storage matches the documented protection mechanism.

4) Test results showing the logging file documents the booting procedure and the result.

5) Test results showing the product completes the boot process after restoring all modified components.

[AC-INTEGRITY-1-03] Verify that the product records the result and status of the booting procedure.

Assessment reference

Requirement [REQ-INTEGRITY-1-03].

Assessment objective

Confirm that the product generates audit events recording the result and status of the booting procedure from the moment the audit storage is available.

Assessment preparation

1) The product is in product factory default state with the boot process ready to be initiated.

2) Documentation describing the audit events recorded for the booting procedure is available.

Assessment activities

1) Review documentation to identify the audit events recorded for the booting procedure, including the result and status.

2) Boot the product and inspect the audit events after boot completion. Verify the product records the result and status of the booting procedure.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the audit events recorded for the booting procedure or does not cover the result and status.

2) The product does not record the result and status of the booting procedure.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the audit events recorded for the booting procedure, including the result and status.

2) The product records the result and status of the booting procedure.

Assessment evidence

1) Documentation describing the audit events recorded for the booting procedure.

2) Test results showing the product records the result and status of the booting procedure.

[AC-INTEGRITY-1-04] Verify that the product requires authentication and authorisation before granting access to recovery and maintenance modes, where such modes are present.

Assessment reference

Requirement [REQ-INTEGRITY-1-04].

Assessment objective

Confirm that the product protects recovery and maintenance modes, by using methods documented in the instructions to the user.

Assessment preparation

1) The product is in product operational state.

2) Documentation describing recovery and maintenance modes is available.

Assessment activities

1) Review documentation to determine whether recovery mode and maintenance mode are present and to identify the methods to protect each present mode.

2) Attempt to enter each present mode without following documented methods. Verify access is denied.

3) Attempt to enter each present mode following documented methods. Verify access is granted.

4) Inspect the product for undocumented recovery or maintenance entry points where documentation states no such modes are present. Verify that none exist.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe recovery or maintenance mode presence.

2) The product does not protect recovery and maintenance modes by using methods documented in the instructions to the user.

3) Any present mode is accessible without following documented methods.

4) The product does not grant access to any present mode following documented methods.

5) An undocumented recovery or maintenance entry point exists where documentation states no such modes are present.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation identifies recovery and maintenance mode presence, entry methods, and requirements.

2) The product protects recovery and maintenance modes by using methods documented in the instructions to the user.

3) The product denies access to each present mode when not following documented methods.

4) The product grants access to each present mode following documented methods.

5) No undocumented recovery or maintenance entry points exist where documentation states no such modes are present.

Assessment evidence

1) Documentation describing recovery and maintenance mode presence and the documented protection mechanisms in the instructions to the user.

2) Test results from not following documented methods showing access is denied for each present mode.

3) Test results confirming access is granted following documented methods.

4) Test results from the undocumented entry point probe confirming no undocumented recovery or maintenance entry points exist where no modes are declared.

6.10.2 [PACKET-1] Default packet disposition

6.10.2.1 Requirement assessments

[AC-PACKET-1-01] Verify that where the product cannot inspect traffic, the product applies the fail-secure action to that traffic.

Assessment reference

Requirement [REQ-PACKET-1-01].

Assessment objective

Confirm that where the product cannot inspect traffic, the product applies the fail-secure action to that traffic.

Assessment preparation

1) The product is in specific operational state with inspection rules configured.

2) Documentation describing the fail-secure action and the conditions treated as traffic that cannot be inspected is available.

3) Network traffic generation tools capable of exceeding inspection capacity and of exercising each inspection subsystem are available.

Assessment activities

1) Review documentation to identify the fail-secure action and the conditions treated as traffic that cannot be inspected.

2) Submit traffic at a load exceeding the documented inspection capacity and verify the product applies the configured fail-secure action to the affected traffic.

3) Trigger a failure of the deep packet inspection, signature-matching, or packet-reassembly subsystem and verify the product applies the fail-secure action to traffic that was reliant on the failed subsystem.

4) Submit traffic to which a configured security rule requires decryption under conditions where decryption cannot be performed, and verify the product applies the configured fail-secure action to the affected traffic.

5) Submit traffic that the product cannot classify conclusively as a known protocol or application where protocol-aware or application-aware inspection is configured, and verify the product applies the configured fail-secure action to the affected traffic.

6) Configure a verdict-determination time constraint and submit traffic that cannot receive a security verdict within that constraint. Verify the product applies the configured fail-secure action to the affected traffic.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the fail-secure action or the conditions treated as traffic that cannot be inspected.

2) The product does not apply the configured fail-secure action to traffic when inspection capacity is exceeded.

3) The product does not apply the configured fail-secure action to traffic when an inspection subsystem fails.

4) The product does not apply the configured fail-secure action to traffic when security-rule-required decryption cannot be performed.

5) The product does not apply the configured fail-secure action to traffic when protocol or application cannot be identified conclusively.

6) The product does not apply the configured fail-secure action to traffic when a security verdict cannot be determined within configured time constraints.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the fail-secure action and the conditions treated as traffic that cannot be inspected.

2) The product applies the configured fail-secure action to traffic when inspection capacity is exceeded.

3) The product applies the configured fail-secure action to traffic when an inspection subsystem fails.

4) The product applies the configured fail-secure action to traffic when security-rule-required decryption cannot be performed.

5) The product applies the configured fail-secure action to traffic when protocol or application cannot be identified conclusively.

6) The product applies the configured fail-secure action to traffic when a security verdict cannot be determined within configured time constraints.

Assessment evidence

1) Documentation describing the fail-secure action and the conditions treated as traffic that cannot be inspected.
2) Test results showing the product applies the configured fail-secure action to traffic when inspection capacity is exceeded.
3) Test results showing the product applies the configured fail-secure action to traffic when an inspection subsystem fails.
4) Test results showing the product applies the configured fail-secure action to traffic when security-rule-required decryption cannot be performed.
5) Test results showing the product applies the configured fail-secure action to traffic when protocol or application cannot be identified conclusively.
6) Test results showing the product applies the configured fail-secure action to traffic when a security verdict cannot be determined within configured time constraints.

[AC-PACKET-1-02] Verify that the product enables fail-open operation only through management override.

Assessment reference

Requirement [REQ-PACKET-1-02].

Assessment objective

Confirm that the product does not enable fail-open operation in product factory default state and enables fail-open operation only through management override.

Assessment preparation

1) The product is in product factory default state.
2) Documentation describing the management override required to enable fail-open operation is available.
3) A management account with sufficient privilege to enable fail-open operation is available.

Assessment activities

1) Review documentation to identify the management override required to enable fail-open operation and the privilege required to apply the override.
2) Inspect the product in product factory default state and verify fail-open operation is not enabled.
3) Attempt to enable fail-open operation without applying the management override and verify the attempt is rejected. Then apply the override using a management account with sufficient privilege and verify fail-open operation is enabled.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the management override required to enable fail-open operation.
2) Documentation does not describe the management privilege required to apply the override.
3) The product enables fail-open operation in product factory default state.
4) The product enables fail-open operation without the management override.
5) The product does not enable fail-open operation when the management override is applied by a privileged management account.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the management override required to enable fail-open operation.

2) Documentation describes the management privilege required to apply the override.

3) The product does not enable fail-open operation in product factory default state.

4) The product does not enable fail-open operation without the management override.

5) The product enables fail-open operation when the management override is applied by a privileged management account.

Assessment evidence

1) Documentation describing the management override required to enable fail-open operation.

2) Documentation describing the management privilege required to apply the override.

3) Test results showing fail-open operation is not enabled in product factory default state.

4) Test results showing the product does not enable fail-open operation without the management override.

5) Test results showing the product enables fail-open operation when the management override is applied.

[AC-PACKET-1-03] Verify that where stateful inspection is active, the product drops packets (i) that violate expected protocol state transitions; or (ii) that the product cannot reassemble for inspection.

Assessment reference

Requirement [REQ-PACKET-1-03].

Assessment objective

Confirm that where stateful inspection is active, the product drops packets (i) that violate expected protocol state transitions; or (ii) that the product cannot reassemble for inspection.

Assessment preparation

1) The product is in specific operational state with stateful inspection rules active.

2) Documentation describing stateful inspection behaviour is available.

Assessment activities

1) Review documentation to identify the stateful inspection behaviour for protocol state violation and reassembly failure conditions.

2) Send packets that violate expected TCP state transitions and verify the product drops the packets.

3) Send fragmented traffic that cannot be fully reassembled and verify the product drops unreassembled fragments rather than forwarding them.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe stateful inspection behaviour for protocol state violations or reassembly failures.

2) The product does not drop packets violating expected protocol state transitions.

3) The product does not drop packets that cannot be reassembled for inspection.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes stateful inspection behaviour for protocol state violations and reassembly failures.

2) The product drops packets violating expected protocol state transitions.

3) The product drops packets that cannot be reassembled for inspection.

Assessment evidence

1) Documentation describing stateful inspection behaviour for protocol state violations and reassembly failures.

2) Test results showing the product drops packets violating expected protocol state transitions.

3) Test results showing the product drops packets that cannot be reassembled for inspection.

[AC-PACKET-1-04] Verify that the product (i) generates security events; (ii) increments bypass counters; and (iii) blocks the traffic where explicit per-flow configuration does not permit bypass, when traffic bypasses inspection.

Assessment reference

Requirement [REQ-PACKET-1-04].

Assessment objective

Confirm that the product (i) generates security events; (ii) increments bypass counters; and (iii) blocks the traffic where explicit per-flow configuration does not permit bypass, when traffic bypasses inspection.

Assessment preparation

1) The product is in specific operational state with inspection rules active.

2) Documentation describing bypass detection and response behaviour is available.

Assessment activities

1) Review documentation to identify the bypass detection mechanisms and response behaviour.

2) Trigger traffic to bypass inspection and verify the product generates a security event and increments the bypass counter.

3) Verify the product blocks bypassed traffic by default and permits it only where explicit per-flow configuration is present.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe bypass detection mechanisms, security event generation, bypass counters, or default blocking of bypassed traffic.

2) The product does not generate a security event when traffic bypasses inspection.

3) The product does not increment the bypass counter when traffic bypasses inspection.

4) The product does not block bypassed traffic by default.

5) The product permits bypassed traffic without explicit per-flow configuration.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes bypass detection mechanisms, security event generation, bypass counters, and default blocking of bypassed traffic.

2) The product generates a security event when traffic bypasses inspection.

3) The product increments the bypass counter when traffic bypasses inspection.

4) The product blocks bypassed traffic by default.

5) The product does not permit bypassed traffic without explicit per-flow configuration.

Assessment evidence

1) Documentation describing bypass detection mechanisms, security event generation, bypass counters, and default blocking of bypassed traffic.

2) Test results showing the product generates a security event when traffic bypasses inspection.

3) Test results showing the product increments the bypass counter when traffic bypasses inspection.

4) Test results showing bypassed traffic is blocked by default.

5) Test results showing bypassed traffic is permitted only where explicit per-flow configuration is present.

[AC-PACKET-1-05] Verify that the product drops packets that violate applicable protocol standards.

Assessment reference

Requirement [REQ-PACKET-1-05].

Assessment objective

Confirm that the product drops packets that violate applicable protocol standards.

Assessment preparation

1) The product is in specific operational state with inspection rules active.

2) Documentation describing packet validation and dropping behaviour is available.

3) Network traffic generation tools capable of producing malformed packets are available.

Assessment activities

1) Review documentation to identify the packet validation criteria and dropping behaviour.

2) Send packets that violate applicable protocol standards and verify the product drops the packets.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the packet validation criteria or dropping behaviour.

2) The product does not drop packets that violate applicable protocol standards.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the packet validation criteria and dropping behaviour.

2) The product drops packets that violate applicable protocol standards.

Assessment evidence

1) Documentation describing the packet validation criteria and dropping behaviour.

2) Test results showing the product drops packets that violate applicable protocol standards.

6.10.3 [EXPOSURE-1] Interface and service exposure minimisation

6.10.3.1 Requirement assessments

[AC-EXPOSURE-1-01] Verify that the product enables only those interfaces and services that have been configured, regardless of the product state.

Assessment reference

Requirement [REQ-EXPOSURE-1-01].

Assessment objective

Confirm that the product enables only configured interfaces and services in each applicable product state, and that no additional interfaces or services are active.

Assessment preparation

1) The product can be placed in each applicable product state.

2) Documentation describing configurable interfaces and services and their configured state is available.

Assessment activities

1) Review documentation to identify all configurable interfaces and services and their configured state.

2) For each applicable product state, inspect enabled interfaces and services and compare the results against the configured state. Verify no unconfigured interface or service is enabled.

3) Change the configured state of selected interfaces and services, where supported, and verify the enabled interfaces and services follow the configured state in each applicable product state.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all configurable interfaces and services and their configured state.

2) Any enabled interface or service is not configured to be enabled in any applicable product state.

3) The product enables any unconfigured interface or service in any applicable product state.

4) The product enables any selected interface or service when configured to be disabled.

5) The product disables any selected interface or service when configured to be enabled.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all configurable interfaces and services and their configured state.

2) All enabled interfaces and services are configured to be enabled in each applicable product state.

3) The product does not enable any unconfigured interface or service in any applicable product state.

4) The product enables selected interfaces and services only when configured to be enabled.

5) The product disables selected interfaces and services when configured to be disabled.

Assessment evidence

1) Documentation listing all configurable interfaces and services and their configured state.

2) Test results showing all enabled interfaces and services are configured to be enabled in each applicable product state.

3) Test results showing the product does not enable any unconfigured interface or service in any applicable product state.

4) Test results showing selected interfaces and services follow their configured state.

[AC-EXPOSURE-1-02] Verify that the product provides capability to selectively enable or disable individual services and interfaces through configuration.

Assessment reference

Requirement [REQ-EXPOSURE-1-02].

Assessment objective

Confirm that the product provides capability to selectively enable or disable individual services and interfaces through configuration.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing configuration options for enabling and disabling services and interfaces is available.

Assessment activities

1) Review documentation to identify which services and interfaces can be individually enabled or disabled.

2) Disable and re-enable at least two configurable services. Verify the product provides the capability to disable and re-enable each through configuration.

3) Disable and re-enable at least two configurable interfaces. Verify each is not operational when disabled and operational when re-enabled.

4) Disable one service and one interface, then restart the product. Verify disabled configuration persists and re-enabled configuration persists after restart.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list which services and interfaces are individually enabled or disabled and the configuration procedure for each.

2) The product does not allow individual services to be disabled and re-enabled through configuration.

3) Any disabled service is accessible or any re-enabled service is not functional.

4) The product does not allow individual interfaces to be disabled and re-enabled through configuration.

5) Any disabled interface remains accessible.

6) Any re-enabled interface is not operational.

7) The product does not maintain service or interface configuration after restart.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists which services and interfaces are individually enabled or disabled and the configuration procedure for each.

2) The product allows individual services to be disabled and re-enabled through configuration.

3) Each disabled service is inaccessible and each re-enabled service is functional.

4) The product allows individual interfaces to be disabled and re-enabled through configuration.

5) Each disabled interface becomes inaccessible.

6) Each re-enabled interface becomes operational.

7) The product maintains service and interface configuration after restart.

Assessment evidence

1) Documentation listing which services and interfaces are individually enabled or disabled and the configuration procedure for each.

2) Test results showing the product allows individual services to be disabled and re-enabled through configuration.

3) Test results showing each disabled service is inaccessible and each re-enabled service is functional.

4) Test results showing the product allows individual interfaces to be disabled and re-enabled through configuration.

5) Test results showing each disabled interface becomes inaccessible.

6) Test results showing each re-enabled interface becomes operational.

7) Test results showing the product maintains service and interface configuration after restart.

6.11 Monitoring and logging

6.11.1 Requirement assessments

[AC-LOG-1-01] Verify that the product generates audit events for authentication activities including (i) successful or failed authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change attempts.

Assessment reference

Requirement [REQ-LOG-1-01].

Assessment objective

Confirm that the product generates audit events for authentication activities including (i) successful or failed authentication; (ii) account lockout triggers and releases; and (iii) authentication credential change attempts.

Assessment preparation

1) The product is in specific operational state with at least one user account configured and authentication failure protection enabled.

2) Documentation is available describing authentication-related audit events.

Assessment activities

1) Review documentation to identify all authentication-related audit event types.

2) Trigger each documented authentication event type in sequence including (i) successful authentication; (ii) failed authentication; (iii) account lockout trigger; (iv) account lockout release; (v) successful authentication credential change; and (vi) failed authentication credential change. Verify an audit event is generated for each.

3) Verify that all authentication audit events are accessible for review.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all authentication audit event types.

2) The product does not generate an audit event for each documented authentication event type including successful authentication, failed authentication, account lockout trigger, account lockout release, and authentication credential change attempt.

3) Any authentication audit event is not accessible for review.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all authentication audit event types.

2) The product generates an audit event for each documented authentication event type including successful authentication, failed authentication, account lockout trigger, account lockout release, and authentication credential change attempt.

3) All authentication audit events are accessible for review.

Assessment evidence

1) Documentation listing all authentication audit event types.

2) Test results showing an audit event is generated for each documented authentication event type triggered in sequence including successful authentication, failed authentication, lockout trigger, lockout release, and credential change attempt.

3) Test results showing all authentication audit events are present and retrievable.

[AC-LOG-1-02] Verify that the product generates audit events for all session lifecycle activities including (i) session establishment with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv) concurrent session limit violations.

Assessment reference

Requirement [REQ-LOG-1-02].

Assessment objective

Confirm that the product generates audit events for all session lifecycle activities including (i) session establishment with source details; (ii) session termination with reason; (iii) failed session validation attempts; and (iv) concurrent session limit violations.

Assessment preparation

1) The product is in specific operational state with at least one user account and session management configured with idle timeout and concurrent session limit.

2) Documentation is available describing session lifecycle audit events.

Assessment activities

1) Review documentation to identify all session lifecycle audit event types.

2) Establish a session. Verify the product generates an audit event for session establishment with source details.

3) Terminate a session by user-initiated logout, idle timeout, and management-initiated termination. Verify the product generates an audit event for each session termination with reason.

4) Attempt to use an invalid session identifier. Verify the product generates an audit event for the failed session validation attempt.

5) Exceed the concurrent session limit. Verify the product generates an audit event for the concurrent session limit violation.

6) Verify all session lifecycle audit events are accessible for review.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not list all session lifecycle audit event types.

2) The product does not generate an audit event for session establishment with source details.

3) The product does not generate an audit event for each session termination with reason.

4) The product does not generate an audit event for failed session validation attempts.

5) The product does not generate an audit event for concurrent session limit violations.

6) Any session lifecycle audit event is not accessible for review.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation lists all session lifecycle audit event types.

2) The product generates an audit event for session establishment with source details.

3) The product generates an audit event for each session termination with reason.

4) The product generates an audit event for failed session validation attempts.

5) The product generates an audit event for concurrent session limit violations.

6) All session lifecycle audit events are accessible for review.

Assessment evidence

1) Documentation listing all session lifecycle audit event types.

2) Test results showing the product generates an audit event for session establishment with source details.

3) Test results showing the product generates an audit event for each session termination with reason.

4) Test results showing the product generates an audit event for failed session validation attempts.

5) Test results showing the product generates an audit event for concurrent session limit violations.

6) Test results showing all session lifecycle audit events are accessible for review.

[AC-LOG-1-03] Verify that the product implements command authorisation that generates audit events whenever execution of an unauthorised command is requested.

Assessment reference

Requirement [REQ-LOG-1-03].

Assessment objective

Confirm that the product implements command authorisation that generates audit events whenever execution of an unauthorised command is requested, and that this operates consistently across all command-capable interfaces.

Assessment preparation

1) The product is in specific operational state with accounts at multiple privilege levels configured.

2) Documentation is available describing audit events generated for command without authorisation attempts.

3) A list of at least three commands requiring higher privileges than the test account possesses is available.

Assessment activities

1) Review documentation to identify the audit events generated for command without authorisation attempts.

2) Authenticate with a lower-privilege account on the primary command interface to test audit event generation for command without authorisation by (i) attempting at least three identified higher-privilege commands; and (ii) inspecting audit events to verify an audit event is generated for each attempt.

3) Repeat at least one command without authorisation attempt on a different command-capable interface and inspect audit events. Verify an audit event is generated and that all command authorisation audit events are accessible and not suppressed.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the audit events generated for command without authorisation attempts.

2) Any command without authorisation attempt from a lower-privilege account does not generate an audit event when attempting at least three identified higher-privilege commands.

3) The product does not generate audit events for command without authorisation attempts on secondary interfaces.

4) The product does not generate audit events consistently across all command-capable interfaces.

5) Any command authorisation audit event is not accessible for review.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the audit events generated for command without authorisation attempts.
2) Each command without authorisation attempt from a lower-privilege account generates an audit event when attempting at least three identified higher-privilege commands.
3) The product generates audit events for command without authorisation attempts on secondary interfaces.
4) The product generates audit events consistently across all command-capable interfaces.
5) All command authorisation audit events are accessible for review.

Assessment evidence

1) Documentation describing the audit events generated for command without authorisation attempts.
2) Test results showing each command without authorisation attempt from a lower-privilege account generates an audit event when attempting higher-privilege commands.
3) Test results showing the product generates audit events for command without authorisation attempts on secondary interfaces.
4) Test results showing the product generates audit events consistently across all command-capable interfaces.
5) Test results showing all command authorisation audit events are accessible for review.

6.12 Data management

6.12.1 [TRANSFER-1] Secure data export and transfer

6.12.1.1 Requirement assessments

[AC-TRANSFER-1-01] Verify that the product provides capability to transfer exported data over a channel protected by state of the art cryptography.

Assessment reference

Requirement [REQ-TRANSFER-1-01].

Assessment objective

Confirm that the product provides capability to transfer exported data over a channel protected by state of the art cryptography.

Assessment preparation

1) The product is in specific operational state.
2) Documentation describing the data export channel and the cryptography protecting it is available.

Assessment activities

1) Review documentation to identify the data export channel and the cryptography protecting it. Verify the documented cryptography is state of the art.
2) Initiate a data export operation and capture network traffic during the transfer. Verify that the traffic is carried over a channel protected by state of the art cryptography and that the data export completes successfully.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the data export channel or the cryptography protecting it.

2) The product does not use state of the art cryptography on the documented channel.

3) The product does not transfer exported data over a channel protected by state of the art cryptography.

4) The product does not complete data export operations successfully.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the data export channel and the cryptography protecting it.

2) The product uses state of the art cryptography on the documented channel.

3) The product transfers exported data over a channel protected by state of the art cryptography.

4) The product completes data export operations successfully.

Assessment evidence

1) Documentation describing the data export channel and the cryptography protecting it.

2) Test results from network traffic captures showing the data export channel is protected by state of the art cryptography.

3) Test results showing the data export operation completes successfully.

[AC-TRANSFER-1-02] Verify that the product provides capability to transfer imported data over a channel protected by state of the art cryptography.

Assessment reference

Requirement [REQ-TRANSFER-1-02].

Assessment objective

Confirm that the product provides capability to transfer imported data over a channel protected by state of the art cryptography.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing the data import channel and the cryptography protecting it is available.

Assessment activities

1) Review documentation to identify the data import channel and the cryptography protecting it. Verify the documented cryptography is state of the art.

2) Initiate a data import operation and capture network traffic during the transfer. Verify that the traffic is carried over a channel protected by state of the art cryptography and that the data import completes successfully.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the data import channel or the cryptography protecting it.

2) The product does not use state of the art cryptography on the documented channel.

3) The product does not transfer imported data over a channel protected by state of the art cryptography.

4) The product does not complete data import operations successfully.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the data import channel and the cryptography protecting it.

2) The product uses state of the art cryptography on the documented channel.

3) The product transfers imported data over a channel protected by state of the art cryptography.

4) The product completes data import operations successfully.

Assessment evidence

1) Documentation describing the data import channel and the cryptography protecting it.

2) Test results from network traffic captures showing the data import channel is protected by state of the art cryptography.

3) Test results showing the data import operation completes successfully.

[AC-TRANSFER-1-03] Verify that the product requires management access for data export and data import operations.

Assessment reference

Requirement [REQ-TRANSFER-1-03].

Assessment objective

Confirm that the product requires management access for data export and data import operations.

Assessment preparation

1) The product is in specific operational state.

2) Documentation describing access control requirements for data transfer operations is available.

Assessment activities

1) Review documentation to identify the access control requirements for data export and data import operations.

2) Attempt to initiate a data export operation without management access. Verify the attempt is denied.

3) Attempt to initiate a data import operation without management access. Verify the attempt is denied.

4) Authenticate with a management account and perform a data export and a data import operation. Verify both operations complete.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe management access requirements for data export and data import operations.

2) The product does not deny data export without management access.

3) The product does not deny data import without management access.

4) The product does not permit data export with management access.

5) The product does not permit data import with management access.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes management access requirements for data export and data import operations.

2) The product denies data export without management access.

3) The product denies data import without management access.

4) The product permits data export with management access.

5) The product permits data import with management access.

Assessment evidence

1) Documentation describing management access requirements for data export and data import operations.

2) Test results showing the product denies data export without management access.

3) Test results showing the product denies data import without management access.

4) Test results showing the product permits data export with management access.

5) Test results showing the product permits data import with management access.

[AC-TRANSFER-1-04] Verify that the product generates audit events for all data export and data import operations.

Assessment reference

Requirement [REQ-TRANSFER-1-04].

Assessment objective

Confirm that the product generates an audit event for every data export and data import operation whether successful or failed.

Assessment preparation

1) The product is in specific operational state.

2) Valid data for import is available.

3) Documentation describing the audit events generated for export and import operations is available.

4) Management and non-management credentials are available.

Assessment activities

1) Review documentation to identify the audit events generated for export and import operations.

2) Perform a data export with management credentials and inspect the audit event. Verify an audit event is generated for the operation.

3) Attempt a data export with non-management credentials or trigger a failure. Verify an audit event is generated for the failed attempt.

4) Perform a data import with management credentials using valid import data and inspect the audit event. Verify an audit event is generated for the operation.

5) Attempt a data import with non-management credentials or using invalid data. Verify an audit event is generated for the failed attempt and that all events are accessible for review.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the audit events generated for export and import operations.

2) Any successful export operation does not generate an audit event.

3) Any failed export attempt does not generate an audit event.

4) Any successful import operation does not generate an audit event.

5) Any failed import attempt does not generate an audit event.

6) Any import audit event is not accessible for review.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the audit events generated for export and import operations.

2) Each successful export operation generates an audit event.

3) Each failed export attempt generates an audit event.

4) Each successful import operation generates an audit event.

5) Each failed import attempt generates an audit event.

6) All import audit events are accessible for review.

Assessment evidence

1) Documentation describing the audit events generated for export and import operations.

2) Test results from audit event inspection show an audit event is generated for the successful export operation.

3) Test results from audit event inspection show an audit event is generated for the failed export attempt.

4) Test results from audit event inspection show an audit event is generated for the successful import operation.

5) Test results from audit event inspection show an audit event is generated for the failed import attempt.

6) Test results showing all export and import audit events are accessible for review.

6.12.2 [SIGNATURE-1] Signature update and validation

6.12.2.1 Requirement assessments

[AC-SIGNATURE-1-01] Verify that the product verifies signature database update integrity using state of the art cryptography before installation.

Assessment reference

Requirement [REQ-SIGNATURE-1-01].

Assessment objective

Confirm that the product verifies signature database update integrity using state of the art cryptography before installation.

Assessment preparation

1) The product is in specific operational state with signature database update functionality configured.

2) Documentation describing the signature database update integrity verification mechanism is available.

Assessment activities

1) Review documentation to identify the signature database update integrity verification mechanism.

2) Attempt to install a signature database update with a valid cryptographic signature. Verify the product installs it.

3) Attempt to install a signature database update with an invalid or missing cryptographic signature. Verify the product rejects it.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database update integrity verification mechanism.

2) The product does not install signature database updates with valid cryptographic signatures.

3) The product does not reject signature database updates with invalid or missing cryptographic signatures.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database update integrity verification mechanism.

2) The product installs signature database updates with valid cryptographic signatures.

3) The product rejects signature database updates with invalid or missing cryptographic signatures.

Assessment evidence

1) Documentation describing the signature database update integrity verification mechanism.
2) Test results showing the product installs signature database updates with valid cryptographic signatures.
3) Test results showing rejection of signature database updates with invalid or missing signatures.

[AC-SIGNATURE-1-02] Verify that the product verifies signature database integrity using state of the art cryptography before use.

Assessment reference

Requirement [REQ-SIGNATURE-1-02].

Assessment objective

Confirm that the product verifies signature database integrity using state of the art cryptography before use.

Assessment preparation

1) The product is in specific operational state with a signature database installed.
2) Documentation describing the signature database integrity verification mechanism is available.

Assessment activities

1) Review documentation to identify the signature database integrity verification mechanism.
2) Corrupt a portion of the signature database and restart the product or trigger a database reload. Verify the product detects the corruption and does not use the corrupted database for inspection.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database integrity verification mechanism.
2) The product does not verify signature database integrity before use.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database integrity verification mechanism.
2) The product verifies signature database integrity before use.

Assessment evidence

1) Documentation describing the signature database integrity verification mechanism.
2) Test results showing the product detects signature database corruption before operational use.

[AC-SIGNATURE-1-03] Verify that the product prevents installation of signature database versions older than the currently installed version.

Assessment reference

Requirement [REQ-SIGNATURE-1-03].

Assessment objective

Confirm that the product prevents rollback to older signature database versions.

Assessment preparation

1) The product is in specific operational state with a current signature database installed.

2) Documentation describing the signature database downgrade prevention mechanism is available.

Assessment activities

1) Review documentation to identify the signature database downgrade prevention mechanism.

2) Attempt to install a signature database version older than the currently installed version. Verify the product rejects it.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database downgrade prevention mechanism.

2) The product does not prevent installation of signature database versions older than the currently installed version.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database downgrade prevention mechanism.

2) The product prevents installation of signature database versions older than the currently installed version.

Assessment evidence

1) Documentation describing the signature database downgrade prevention mechanism.

2) Test results showing the product prevents installation of signature database versions older than the currently installed version.

[AC-SIGNATURE-1-04] Verify that the product restores the signature database from backup when integrity verification fails.

Assessment reference

Requirement [REQ-SIGNATURE-1-04].

Assessment objective

Confirm that the product automatically restores a known-good signature database from backup when integrity verification of the active database fails.

Assessment preparation

1) The product is in specific operational state with a signature database and backup available.

2) Documentation describing the signature database backup and restoration mechanism is available.

Assessment activities

1) Review documentation to identify the signature database backup and restoration mechanism.

2) Corrupt the active signature database and trigger an integrity check. Verify the product restores the database from backup and resumes inspection.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database backup and restoration mechanism.

2) The product does not restore the signature database from backup when integrity verification fails.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database backup and restoration mechanism.

2) The product restores the signature database from backup when integrity verification fails.

Assessment evidence

1) Documentation describing the signature database backup and restoration mechanism.

2) Test results showing signature database restoration from backup after integrity failure.

[AC-SIGNATURE-1-05] Verify that the product preserves user-created signatures when installing manufacturer-supplied signature database updates.

Assessment reference

Requirement [REQ-SIGNATURE-1-05].

Assessment objective

Confirm that the product preserves user-created signatures when installing manufacturer-supplied signature database updates.

Assessment preparation

1) The product is in specific operational state with both manufacturer-supplied and user-created signatures configured.

2) Documentation describing the user-created signature preservation mechanism is available.

Assessment activities

1) Review documentation to identify the user-created signature preservation mechanism.

2) Install a manufacturer-supplied signature database update. Verify that user-created signatures remain unmodified.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the user-created signature preservation mechanism.

2) The product does not preserve user-created signatures after installing a manufacturer-supplied signature database update.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the user-created signature preservation mechanism.

2) The product preserves user-created signatures after installing a manufacturer-supplied signature database update.

Assessment evidence

1) Documentation describing the user-created signature preservation mechanism.

2) Test results showing user-created signatures are preserved after a manufacturer-supplied signature database update.

[AC-SIGNATURE-1-06] Verify that the product checks for signature database updates at configurable intervals.

Assessment reference

Requirement [REQ-SIGNATURE-1-06].

Assessment objective

Confirm that the product checks for signature database updates at configurable intervals.

Assessment preparation

The product is in specific operational state with automatic signature database updates enabled.

Documentation describing the signature database update check interval configuration is available.

Assessment activities

1) Review documentation to identify the signature database update check interval configuration.
2) Verify the product checks for signature database updates within the configured interval.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database update check interval configuration.
2) The product does not check for signature database updates within the configured interval.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database update check interval configuration.
2) The product checks for signature database updates within the configured interval.

Assessment evidence

1) Documentation describing the signature database update check interval configuration.
2) Test results showing signature database update checks occur within the configured interval.

[AC-SIGNATURE-1-07] Verify that the product defers signature database updates outside configured maintenance windows.

Assessment reference

Requirement [REQ-SIGNATURE-1-07].

Assessment objective

Confirm that the product defers signature database updates outside configured maintenance windows.

Assessment preparation

1) The product is in specific operational state with a maintenance window configured.
2) Documentation describing the signature database update deferral mechanism is available.

Assessment activities

1) Review documentation to identify the signature database update deferral mechanism.
2) Trigger a signature database update outside the configured maintenance window. Verify the product defers the update.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database update deferral mechanism.
2) The product does not defer signature database updates outside the configured maintenance window.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database update deferral mechanism.
2) The product defers signature database updates outside the configured maintenance window.

Assessment evidence

1) Documentation describing the signature database update deferral mechanism.

2) Test results showing signature database updates are deferred outside maintenance windows.

[AC-SIGNATURE-1-08] Verify that the product limits signature database update download bandwidth to configurable thresholds.

Assessment reference

Requirement [REQ-SIGNATURE-1-08].

Assessment objective

Confirm that the product limits signature database update download bandwidth to configurable thresholds.

Assessment preparation

1) The product is in specific operational state with signature database update bandwidth limits configured.

2) Documentation describing the signature database update bandwidth limit configuration is available.

Assessment activities

1) Review documentation to identify the signature database update bandwidth limit configuration.

2) Configure a bandwidth limit and initiate a signature database update download. Verify the download rate does not exceed the configured threshold.

3) Inspect the default bandwidth limit. Verify the default value limits bandwidth.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database update bandwidth limit configuration.

2) The product does not limit signature database update download bandwidth to the configured threshold.

3) The product does not enforce a default bandwidth limit for signature database update downloads.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database update bandwidth limit configuration.

2) The product limits signature database update download bandwidth to the configured threshold.

3) The product enforces a default bandwidth limit for signature database update downloads.

Assessment evidence

1) Documentation describing the signature database update bandwidth limit configuration.

2) Test results showing signature database update download bandwidth does not exceed the configured threshold.

3) Test results showing the default bandwidth limit for signature database update downloads is enforced.

[AC-SIGNATURE-1-09] Verify that the product retries failed signature database downloads within 24 hours.

Assessment reference

Requirement [REQ-SIGNATURE-1-09].

Assessment objective

Confirm that the product retries failed signature database downloads within 24 hours.

Assessment preparation

1) The product is in specific operational state with signature database update functionality configured.
2) Documentation describing the signature database download retry mechanism is available.

Assessment activities

1) Review documentation to identify the signature database download retry mechanism.
2) Block the signature database update server and monitor retry attempts. Verify the product retries within 24 hours.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the signature database download retry mechanism.
2) The product does not retry failed signature database downloads within 24 hours.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the signature database download retry mechanism.
2) The product retries failed signature database downloads within 24 hours.

Assessment evidence

1) Documentation describing the signature database download retry mechanism.
2) Test results showing the product retries failed signature database downloads within 24 hours.

6.13 Remote data processing solutions

6.13.1 Requirement assessments

[AC-RDPS-1-01] Verify that the manufacturer documents all remote data processing solutions on which the product depends.

Assessment reference

Requirement [REQ-RDPS-1-01].

Assessment objective

Confirm that the manufacturer documents all remote data processing solutions used by the product.

Assessment preparation

1) Technical documentation is available.

Assessment activities

1) Review the technical documentation to verify that all remote data processing solutions on which the product depends are listed.
2) Inspect the product runtime configuration and verify that every remote data processing solution the product communicates with is listed in the technical documentation.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) The manufacturer does not document all remote data processing solutions on which the product depends.

2) The product communicates with a remote data processing solution that is not documented.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) The manufacturer documents all remote data processing solutions on which the product depends.

2) Each remote data processing solution the product communicates with is documented.

Assessment evidence

1) Documentation listing all remote data processing solutions on which the product depends.

2) Test results showing every remote data processing solution the product communicates with is documented.

[AC-RDPS-1-02] Verify that where the product communicates with a remote data processing solution, the product protects that communication over a secure channel.

Assessment reference

Requirement [REQ-RDPS-1-02].

Assessment objective

Confirm that where the product communicates with a remote data processing solution, the product protects that communication over a secure channel.

Assessment preparation

1) The product is in specific operational state with RDPS connectivity configured.

2) Documentation describing the secure channel mechanism used for communication with a remote data processing solution is available.

Assessment activities

1) Review documentation to identify the secure channel mechanism used for communication with a remote data processing solution.

2) Capture network traffic between the product and a remote data processing solution. Verify the product protects the communication over a secure channel.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the secure channel mechanism used for communication with a remote data processing solution.

2) The product does not protect communication with a remote data processing solution over a secure channel.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the secure channel mechanism used for communication with a remote data processing solution.

2) The product protects communication with a remote data processing solution over a secure channel.

Assessment evidence

1) Documentation describing the secure channel mechanism used for communication with a remote data processing solution.

2) Test results showing the product protects communication with a remote data processing solution over a secure channel.

[AC-RDPS-1-03] Verify that where the product communicates with a remote data processing solution, the product authenticates the remote data processing solution before transmitting data to it.

Assessment reference

Requirement [REQ-RDPS-1-03].

Assessment objective

Confirm that where the product communicates with a remote data processing solution, the product authenticates the remote data processing solution before transmitting data to it.

Assessment preparation

1) The product is in specific operational state with RDPS connectivity configured.

2) Documentation describing the remote data processing solution authentication mechanism is available.

Assessment activities

1) Review documentation to identify the remote data processing solution authentication mechanism.

2) Substitute the remote data processing solution with an endpoint that does not satisfy authentication. Verify the product does not transmit data to the substituted endpoint.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the remote data processing solution authentication mechanism.

2) The product does not authenticate a remote data processing solution before transmitting data to it.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the remote data processing solution authentication mechanism.

2) The product authenticates a remote data processing solution before transmitting data to it.

Assessment evidence

1) Documentation describing the remote data processing solution authentication mechanism.

2) Test results showing the product authenticates a remote data processing solution before transmitting data to it.

[AC-RDPS-1-04] Verify that where the product communicates with a remote data processing solution, the product retries failed communications with the remote data processing solution as documented in the instructions to the user.

Assessment reference

Requirement [REQ-RDPS-1-04].

Assessment objective

Confirm that where the product communicates with a remote data processing solution, the product retries failed communications with the remote data processing solution as documented in the instructions to the user.

Assessment preparation

1) The product is in specific operational state with RDPS connectivity configured.

2) Instructions to the user describing the retry behaviour for failed communications with a remote data processing solution are available.

Assessment activities

1) Review the instructions to the user to identify the retry behaviour for failed communications with a remote data processing solution.

2) Block connectivity to the remote data processing solution and monitor the product retry attempts. Verify the product retries as documented in the instructions to the user.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) The instructions to the user do not describe the retry behaviour for failed communications with a remote data processing solution.

2) The product does not retry failed communications with a remote data processing solution as documented in the instructions to the user.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) The instructions to the user describe the retry behaviour for failed communications with a remote data processing solution.

2) The product retries failed communications with a remote data processing solution as documented in the instructions to the user.

Assessment evidence

1) Instructions to the user describing the retry behaviour for failed communications with a remote data processing solution.

2) Test results showing the product retries failed communications with a remote data processing solution as documented in the instructions to the user.

[AC-RDPS-1-05] Verify that the product generates audit events for communication failures with a remote data processing solution.

Assessment reference

Requirement [REQ-RDPS-1-05].

Assessment objective

Confirm that the product generates audit events for communication failures with a remote data processing solution.

Assessment preparation

1) The product is in specific operational state with RDPS connectivity configured.

2) Documentation describing the audit events generated for communication failures with a remote data processing solution is available.

Assessment activities

1) Review documentation to identify the audit events generated for communication failures with a remote data processing solution.

2) Trigger a communication failure with a remote data processing solution. Verify the product generates an audit event.

Assessment verdict

The verdict fail is assigned if any of the following conditions apply:

1) Documentation does not describe the audit events generated for communication failures with a remote data processing solution.

2) The product does not generate audit events for communication failures with a remote data processing solution.

The verdict pass is assigned if none of the above conditions apply and all of the following conditions are met:

1) Documentation describes the audit events generated for communication failures with a remote data processing solution.

2) The product generates audit events for communication failures with a remote data processing solution.

Assessment evidence

1) Documentation describing the audit events generated for communication failures with a remote data processing solution.

2) Test results showing the product generates audit events for communication failures with a remote data processing solution.

Annex A (informative): Relationship between the present document and the essential cybersecurity requirements of EU Regulation (EU) 2024/2847

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

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

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

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
Annex I, Part I, (1)	"Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks."	Clause 5 Clause 6	
Annex I, Part I, (2)(a)	"Products with digital elements shall be made available on the market without known exploitable vulnerabilities."	Clause 5.3 Clause 6.3	
Annex I, Part I, (2)(b)	"Products with digital elements shall be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state."	Clauses 5.4.1 and 5.4.2 Clauses 6.4.1 and 6.4.2	
Annex I, Part I, (2)(c)	"Products with digital elements shall ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them."	Clause 5.5.1 Clause 6.5.1	
Annex I, Part I, (2)(d)	"Products with digital elements shall ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access."	Clauses 5.6.1, 5.6.2, 5.6.3 and 5.6.4 Clauses 6.6.1, 6.6.2, 6.6.3 and 6.6.4	
Annex I, Part I, (2)(e)	"Products with digital elements shall protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by best practice mechanisms, and by using other technical means."	Clause 5.7 Clause 6.7	
Annex I, Part I, (2)(f)	"Products with digital elements shall protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions."	Clause 5.7 Clause 6.7	

Description	Essential Requirements of Regulation (EU) 2024/2847	Clause(s) of the present document	Remarks / Notes
Annex I, Part I, (2)(g)	"Products with digital elements shall process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation)."	Clause 5.7 Clause 6.7	
Annex I, Part I, (2)(h)	"Products with digital elements shall protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks."	Clause 5.8 Clause 6.8	
Annex I, Part I, (2)(i)	"Products with digital elements shall minimise the negative impact by the products themselves or connected products on the availability of services provided by other products or networks."	Clause 5.9 Clause 6.9	
Annex I, Part I, (2)(j)	"Products with digital elements shall be designed, developed and produced to limit attack surfaces, including external interfaces."	Clauses 5.10.2 and 5.10.3 Clauses 6.10.2 and 6.10.3	
Annex I, Part I, (2)(k)	"Products with digital elements shall be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques."	Clause 5.10.1 Clause 6.10.1	
Annex I, Part I, (2)(l)	"Products with digital elements shall provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user."	Clause 5.11 Clause 6.11	
Annex I, Part I, (2)(m)	"Products with digital elements shall provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner."	Clauses 5.4.2, 5.12.1 and 5.12.2 Clauses 6.4.2, 6.12.1 and 6.12.2	

Key to columns:

Description A textual reference to the requirement.

Essential Requirements of Regulation (EU) 2024/2847

Identification of point(s) defining the requirement in Regulation (EU) 2024/2847 - the Cyber Resilience Act.

Clause(s) of the present document

Identification of clause(s) addressing the requirement in the present document.

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

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

Annex B (informative): Security analysis

B.1 General

This clause provides the threat and vulnerability analysis that informed the risk factor-based security requirements defined in clause 5 of the present document.

First, threats are identified in relation to the product functions described in clause 4.2, the assets described in clause 4.3.2, and the capabilities described in clause 4.3.3 of the present document. These threats are listed in clause B.2. In this way, the threats described in clause B.2 can be connected to the product context within which they may arise.

Second, the relevance of threats is assessed based on risk factors. Given the informative nature of this annex, the assessment of threat relevance is provided in clause B.3. This framework is used to condition requirements, where applicable, on the presence of risk factors that affect the applicability and likelihood of the corresponding threats.

This threat-driven approach intends to ensure that security requirements remain proportionate to actual risk while achieving the security objectives defined by the CRA.

B.2 Threat landscape

B.2.1 Threats related to vulnerability handling

Table B.1: Threats related to vulnerability handling

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-VH-01]	Exploitation of known vulnerabilities in security products	• [FN-G-01] Configuration and management • [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SP-01] Traffic access control and decision making • [FN-SM-01] Signature and intelligence management • [FN-NC-01] Network connectivity • [FN-SG-01] Traffic segmentation • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement
[T-VH-02]	Exploitation of inspection engine parsing vulnerabilities	• [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis
[T-VH-03]	State table exhaustion attacks	• [FN-TI-01] Traffic inspection and analysis • [FN-SP-01] Traffic access control and decision making • [AS-FW-03] Inspection engine state • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-04] Inline traffic enforcement

B.2.2 Threats related to access control and authentication

Table B.2: Threats related to access control and authentication

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-AC-01]	Access to management functions without authorisation	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [FN-SM-01] Signature and intelligence management • [FN-SG-01] Traffic segmentation • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence
[T-AC-02]	Credential compromise and brute force attacks	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets
[T-AC-03]	Session hijacking and replay attacks	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets
[T-AC-04]	Privilege escalation through management interfaces	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets
[T-AC-05]	Access through inspection interfaces without authorisation	• [FN-TI-01] Traffic inspection and analysis • [AS-FW-01] Security policies and rule sets • [CAP-FW-04] Inline traffic enforcement

B.2.3 Threats related to availability and inspection bypass

Table B.3: Threats related to availability and inspection bypass

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-AV-01]	Denial-of-service against security enforcement	• [FN-G-01] Configuration and management • [FN-TI-01] Traffic inspection and analysis • [FN-SP-01] Traffic access control and decision making • [FN-NC-01] Network connectivity • [FN-SG-01] Traffic segmentation • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-04] Inline traffic enforcement
[T-AV-02]	Inspection bypass through evasion techniques	• [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SG-01] Traffic segmentation • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection
[T-AV-03]	Fail-open exploitation during system failures	• [FN-TI-01] Traffic inspection and analysis • [FN-SP-01] Traffic access control and decision making • [FN-NC-01] Network connectivity • [FN-SG-01] Traffic segmentation • [AS-FW-03] Inspection engine state • [CAP-FW-04] Inline traffic enforcement

B.2.4 Threats related to integrity and tampering

Table B.4: Threats related to integrity and tampering

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-IT-01]	Firmware and boot process compromise	• [FN-G-01] Configuration and management • [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SP-01] Traffic access control and decision making • [FN-SM-01] Signature and intelligence management • [FN-NC-01] Network connectivity • [FN-LG-01] Logging • [FN-SG-01] Traffic segmentation • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement
[T-IT-02]	Security rule and configuration tampering	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [FN-SG-01] Traffic segmentation • [AS-FW-01] Security policies and rule sets
[T-IT-03]	Tampered update package installation	• [FN-G-01] Configuration and management • [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SP-01] Traffic access control and decision making • [FN-SM-01] Signature and intelligence management • [FN-NC-01] Network connectivity • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement

B.2.5 Threats related to signature and intelligence integrity

Table B.5: Threats related to signature and intelligence integrity

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-SI-01]	Malicious signature distribution through compromised updates	• [FN-TD-01] Threat detection and pattern matching • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-02]	Signature database integrity compromise	• [FN-TD-01] Threat detection and pattern matching • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-03]	Threat intelligence poisoning	• [FN-TD-01] Threat detection and pattern matching • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-04]	Signature rollback enabling detection bypass	• [FN-TD-01] Threat detection and pattern matching • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection
[T-SI-05]	Signature update disruption	• [FN-G-01] Configuration and management • [FN-SM-01] Signature and intelligence management • [AS-FW-02] Signature databases and threat intelligence • [CAP-FW-03] Signature-based threat detection

B.2.6 Threats related to data protection

Table B.6: Threats related to data protection

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-DP-01]	Credential and cryptographic material disclosure	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-04] Audit event records
[T-DP-02]	Data exfiltration through export functions	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-04] Audit event records
[T-DP-03]	Excessive data collection through inspection functions	• [FN-TI-01] Traffic inspection and analysis • [AS-FW-04] Audit event records • [CAP-FW-01] Deep packet inspection

B.2.7 Threats related to monitoring and visibility

Table B.7: Threats related to monitoring and visibility

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-MV-01]	Security event visibility elimination	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [FN-LG-01] Logging • [AS-FW-04] Audit event records
[T-MV-02]	Audit trail tampering	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [FN-LG-01] Logging • [AS-FW-04] Audit event records

B.2.8 Threats related to default configuration

Table B.8: Threats related to default configuration

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-DC-01]	Insecure default configuration exploitation	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement
[T-DC-02]	Lifecycle transition data exposure	• [FN-G-01] Configuration and management • [FN-SP-01] Traffic access control and decision making • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-04] Audit event records

B.2.9 Threats related to physical and deployment security

Table B.9: Threats related to physical and deployment security

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-PD-01]	Physical tampering of hardware appliance	• [FN-G-01] Configuration and management • [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SP-01] Traffic access control and decision making • [FN-NC-01] Network connectivity • [FN-LG-01] Logging • [FN-SG-01] Traffic segmentation • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement
[T-PD-02]	Hypervisor and infrastructure compromise of virtual deployment	• [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [FN-SP-01] Traffic access control and decision making • [FN-NC-01] Network connectivity • [FN-SG-01] Traffic segmentation • [AS-FW-01] Security policies and rule sets • [AS-FW-02] Signature databases and threat intelligence • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection • [CAP-FW-04] Inline traffic enforcement

B.2.10 Threats related to detection disruption

Table B.10: Threats related to detection disruption

Threat ID	Threat title	Primarily affected functions, assets and capabilities
[T-DD-01]	Disabling passive monitoring sensors	• [FN-TI-01] Traffic inspection and analysis • [FN-TD-01] Threat detection and pattern matching • [AS-FW-03] Inspection engine state • [CAP-FW-01] Deep packet inspection • [CAP-FW-02] Stateful traffic analysis • [CAP-FW-03] Signature-based threat detection

B.3 Threat assessment framework

B.3.1 Introduction

This clause establishes an assessment framework for the threats described in clause B.2. Products within scope differ widely, so not all threats apply equally to all products and deployments. Applicability depends on specific properties of the product and its operational environment.

Each threat in clause B.2 identifies the product functions, assets, and capabilities that contribute to the attack surface of that threat. This characterisation is informative. It describes which product properties make a threat relevant but does not directly govern requirement applicability. Requirement applicability is determined by the risk factors in clause B.3 and by feature-specific conditionals in clause 5.

B.3.2 Risk factors

B.3.2.0 Introduction

The risk factors are organised into five categories:

- baseline risk factors;
- traffic inspection risk factors;
- update and intelligence risk factors;
- deployment architecture risk factors;
- data operations risk factors.

Where not explicitly stated otherwise, the risk factors apply equally to all use cases.

B.3.2.1 Baseline risk factors

The following risk factors arise from fundamental security properties required for all security products.

Table B.11: Baseline risk factors

ID	Title	Description
[RF-B-01]	Initial deployment risk factor	This risk factor applies to all products when first deployed as vulnerabilities identified in the timespan between the product being made available on the market and its initial deployment are still present when the product is put to service for the first time.
[RF-B-02]	Lifecycle transition risk factor	This risk factor applies when products undergo decommissioning, service returns, ownership transfers, or equipment recycling, as products retaining configuration data during lifecycle transitions can expose information such as credentials, cryptographic keys, network topology, and threat detection rules to parties without authorisation.
[RF-B-03]	Availability disruption risk factor	This risk factor applies to all products providing network security inspection or enforcement, as failure of the product cascades through dependent systems. The relevance of this risk factor increases when the product is deployed inline at network perimeters or segmentation boundaries.
[RF-B-04]	System integrity compromise risk factor	This risk factor applies to all products executing firmware and software, as in absence of trust anchors products cannot distinguish legitimate updates from malicious modifications.
[RF-B-05]	Packet processing risk factor	This risk factor applies to all products inspecting or forwarding network packets, as packets whose structures deviate from protocol specifications can impact the functionalities of the product by effects such as buffer overflows, memory corruption, or evasion of inspection.
[RF-B-06]	Attack surface exposure risk factor	This risk factor applies to all products with network interfaces, management functions, physical ports, and diagnostic capabilities, as every exposed interface potentially increases the attack surface of the product.
[RF-B-07]	Security event visibility risk factor	This risk factor applies to all products requiring breach detection, incident response, and compliance demonstration, as incomplete or missing audit logging reduces the ability to detect and investigate security incidents.

B.3.2.2 Traffic inspection risk factors

The following risk factors arise from how products access and process network traffic.

Table B.12: Traffic inspection risk factors

ID	Title	Description
[RF-TI-01]	Passive monitoring risk factor	This risk factor applies when products operate in traffic mirroring mode receiving packet copies without enforcement capability, as detected threats have already reached their destinations and response depends on human intervention.
[RF-TI-02]	Inline enforcement risk factor	This risk factor applies when products operate inline with network traffic flows, as the product creates a single point of failure where all traffic passes through inspection engines.

B.3.2.3 Update and intelligence risk factors

The following risk factors arise from security update and threat intelligence methods.

Table B.13: Update and intelligence risk factors

ID	Title	Description
[RF-UI-01]	Manual update risk factor	This risk factor applies when products receive security updates through manual processes requiring administrative action, as in this case updates depend on the availability of the necessary personnel and are prone to human error and delay.
[RF-UI-02]	Automated update risk factor	This risk factor applies when products implement automated security update mechanisms, as compromised update infrastructure can distribute malicious updates to entire product fleets.
[RF-UI-03]	Threat intelligence exposure risk factor	This risk factor applies when products participate in threat intelligence sharing networks, as products can reveal defensive capabilities through contributed data and automatically incorporate external threat indicators without validation.

B.3.2.4 Deployment architecture risk factors

The following risk factors arise from physical or virtual deployment forms.

Table B.14: Deployment architecture risk factors

ID	Title	Description
[RF-DA-01]	Physical appliance risk factor	This risk factor applies when products are delivered as physical appliances, as physical access to the hardware can enable modification of firmware, extraction of cryptographic keys, or installation of hardware implants.
[RF-DA-02]	Virtual deployment risk factor	This risk factor applies when products are delivered as software without dedicated hardware, as products depend on the security of the underlying infrastructure and cannot independently verify infrastructure integrity.

B.3.2.5 Data operations risk factors

The following risk factors arise from data import/export and transfer capabilities.

Table B.15: Data operations risk factors

ID	Title	Description
[RF-DO-01]	Data transfer risk factor	This risk factor applies when products implement data export, import, or exchange capabilities, as critical security parameters can be leaked or manipulated during transfer.

B.3.2.6 Remote data processing risk factors

The following risk factors arise from product dependencies on remote data processing solutions. Requirements specific to these risk factors are defined in clause 5.13.

Table B.16: Remote data processing risk factors

ID	Title	Description
[RF-RDPS-01]	Remote data processing dependency risk factor	This risk factor applies when the product depends on one or more remote data processing solutions for product functions, as compromise of the RDPS boundary can affect firewall, intrusion detection, or intrusion prevention operations across all connected product instances.

B.3.3 Threat justification and mitigation

Table B.17 lists, for each threat, the risk factors that contribute to its impact and likelihood, and the requirements of the present document that mitigate it.

Table B.17: Threat justification and mitigation

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-VH-01]	Exploitation of known vulnerabilities in security products	[RF-B-01] [RF-B-05] [RF-UI-01]	[REQ-KEV-1-01] [REQ-KEV-1-02] [REQ-KEV-1-03] [REQ-UPDATE-1-01] [REQ-UPDATE-1-02] [REQ-DEFAULT-1-09] [REQ-AUTH-4-05] [REQ-EXPOSURE-1-01] [REQ-DEFAULT-1-12] [REQ-DEFAULT-1-07]
[T-VH-02]	Exploitation of inspection engine parsing vulnerabilities	[RF-B-05] [RF-TI-02]	[REQ-PACKET-1-01] [REQ-PACKET-1-03] [REQ-PACKET-1-05] [REQ-AVAIL-1-01] [REQ-DEFAULT-1-07]
[T-VH-03]	State table exhaustion attacks	[RF-B-03] [RF-TI-02]	[REQ-AVAIL-1-01] [REQ-AVAIL-1-02] [REQ-AVAIL-1-03] [REQ-PACKET-1-01] [REQ-PACKET-1-02] [REQ-DEFAULT-1-07] [REQ-IM-1-01]
[T-AC-01]	Access to management functions without authorisation	[RF-B-06] [RF-RDPS-01]	[REQ-AUTH-1-01] [REQ-AUTH-1-02] [REQ-AUTH-1-03] [REQ-AUTH-1-05] [REQ-AUTH-1-06] [REQ-AUTH-2-01] [REQ-AUTH-2-02] [REQ-AUTH-2-03] [REQ-AUTH-2-04] [REQ-AUTH-4-01] [REQ-AUTH-4-02] [REQ-AUTH-4-03] [REQ-DEFAULT-1-05] [REQ-DEFAULT-1-06] [REQ-DEFAULT-1-08] [REQ-RDPS-1-03] [REQ-DEFAULT-1-07]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-AC-02]	Credential compromise and brute force attacks	[RF-B-06]	[REQ-AUTH-1-02] [REQ-AUTH-1-03] [REQ-AUTH-1-04] [REQ-AUTH-1-05] [REQ-AUTH-1-06] [REQ-AUTH-1-07] [REQ-DEFAULT-1-07]
[T-AC-03]	Session hijacking and replay attacks	[RF-B-06]	[REQ-AUTH-3-01] [REQ-AUTH-3-02] [REQ-AUTH-3-03] [REQ-AUTH-3-04] [REQ-LOG-1-02] [REQ-DEFAULT-1-07]
[T-AC-04]	Privilege escalation through management interfaces	[RF-B-06]	[REQ-DEFAULT-1-03] [REQ-DEFAULT-1-04] [REQ-AUTH-2-01] [REQ-AUTH-2-02] [REQ-AUTH-2-03] [REQ-AUTH-2-04] [REQ-DEFAULT-1-07]
[T-AC-05]	Access through inspection interfaces without authorisation	[RF-B-06] [RF-TI-02]	[REQ-AUTH-4-01] [REQ-EXPOSURE-1-01] [REQ-EXPOSURE-1-02] [REQ-DEFAULT-1-07]
[T-AV-01]	Denial-of-service against security enforcement	[RF-B-03] [RF-TI-02]	[REQ-AVAIL-1-01] [REQ-AVAIL-1-02] [REQ-AVAIL-1-03] [REQ-PACKET-1-01] [REQ-PACKET-1-02] [REQ-DEFAULT-1-07] [REQ-IM-1-01]
[T-AV-02]	Inspection bypass through evasion techniques	[RF-B-05] [RF-TI-01] [RF-TI-02]	[REQ-PACKET-1-01] [REQ-PACKET-1-03] [REQ-PACKET-1-04] [REQ-PACKET-1-05] [REQ-DEFAULT-1-07]
[T-AV-03]	Fail-open exploitation during system failures	[RF-B-03] [RF-TI-02]	[REQ-PACKET-1-01] [REQ-PACKET-1-02] [REQ-PACKET-1-04] [REQ-AVAIL-1-01] [REQ-AVAIL-1-02] [REQ-DEFAULT-1-07] [REQ-IM-1-01]
[T-IT-01]	Firmware and boot process compromise	[RF-B-04] [RF-DA-01]	[REQ-INTEGRITY-1-01] [REQ-INTEGRITY-1-02] [REQ-INTEGRITY-1-03] [REQ-INTEGRITY-1-04] [REQ-DEFAULT-1-07]
[T-IT-02]	Security rule and configuration tampering	[RF-B-06] [RF-RDPS-01]	[REQ-AUTH-1-01] [REQ-AUTH-2-02] [REQ-AUTH-2-04] [REQ-AUTH-4-01] [REQ-DATA-1-03] [REQ-DEFAULT-1-05] [REQ-DEFAULT-1-06] [REQ-RDPS-1-02] [REQ-RDPS-1-03] [REQ-RDPS-1-05] [REQ-LOG-1-03] [REQ-DEFAULT-1-07]
[T-IT-03]	Tampered update package installation	[RF-B-04] [RF-UI-02]	[REQ-UPDATE-1-03] [REQ-UPDATE-1-04] [REQ-UPDATE-1-06] [REQ-DEFAULT-1-07] [REQ-UPDATE-1-07]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-SI-01]	Malicious signature distribution through compromised updates	[RF-UI-02] [RF-RDPS-01]	[REQ-SIGNATURE-1-01] [REQ-SIGNATURE-1-03] [REQ-SIGNATURE-1-02] [REQ-SIGNATURE-1-04] [REQ-RDPS-1-02] [REQ-RDPS-1-03] [REQ-DEFAULT-1-07] [REQ-UPDATE-1-07]
[T-SI-02]	Signature database integrity compromise	[RF-UI-02] [RF-UI-03]	[REQ-SIGNATURE-1-02] [REQ-SIGNATURE-1-04] [REQ-SIGNATURE-1-05] [REQ-DEFAULT-1-07]
[T-SI-03]	Threat intelligence poisoning	[RF-UI-03] [RF-RDPS-01]	[REQ-SIGNATURE-1-01] [REQ-SIGNATURE-1-05] [REQ-RDPS-1-02] [REQ-RDPS-1-03] [REQ-DEFAULT-1-07] [REQ-RDPS-1-05]
[T-SI-04]	Signature rollback enabling detection bypass	[RF-UI-02] [RF-UI-03]	[REQ-SIGNATURE-1-03] [REQ-SIGNATURE-1-02] [REQ-DEFAULT-1-07]
[T-SI-05]	Signature update disruption	[RF-UI-02] [RF-UI-01] [RF-RDPS-01]	[REQ-SIGNATURE-1-06] [REQ-SIGNATURE-1-07] [REQ-SIGNATURE-1-08] [REQ-SIGNATURE-1-09] [REQ-RDPS-1-04] [REQ-DEFAULT-1-07] [REQ-RDPS-1-05]
[T-DP-01]	Credential and cryptographic material disclosure	[RF-B-02] [RF-DO-01]	[REQ-AUTH-1-03] [REQ-AUTH-1-04] [REQ-AUTH-4-02] [REQ-AUTH-4-03] [REQ-DATA-1-02] [REQ-RESET-1-01] [REQ-DEFAULT-1-07]
[T-DP-02]	Data exfiltration through export functions	[RF-DO-01]	[REQ-TRANSFER-1-01] [REQ-TRANSFER-1-02] [REQ-TRANSFER-1-03] [REQ-TRANSFER-1-04] [REQ-DEFAULT-1-07]
[T-DP-03]	Excessive data collection through inspection functions	[RF-TI-01] [RF-TI-02]	[REQ-DATA-1-04] [REQ-DEFAULT-1-07]
[T-MV-01]	Security event visibility elimination	[RF-B-07]	[REQ-AUTH-4-05] [REQ-AVAIL-1-03] [REQ-INTEGRITY-1-03] [REQ-INTEGRITY-1-04] [REQ-LOG-1-01] [REQ-LOG-1-02] [REQ-LOG-1-03] [REQ-DEFAULT-1-07]
[T-MV-02]	Audit trail tampering	[RF-B-07]	[REQ-AUTH-2-04] [REQ-LOG-1-03] [REQ-DEFAULT-1-07]
[T-DC-01]	Insecure default configuration exploitation	[RF-B-01]	[REQ-DEFAULT-1-01] [REQ-DEFAULT-1-02] [REQ-DEFAULT-1-03] [REQ-DEFAULT-1-04] [REQ-DEFAULT-1-08] [REQ-DEFAULT-1-11] [REQ-DEFAULT-1-07] [REQ-DEFAULT-1-12]
[T-DC-02]	Lifecycle transition data exposure	[RF-B-02]	[REQ-RESET-1-01] [REQ-RESET-1-02] [REQ-RESET-1-03] [REQ-DEFAULT-1-07]

ID	Title	Contributing risk factor(s)	Requirement(s) for mitigation
[T-PD-01]	Physical tampering of hardware appliance	[RF-DA-01]	[REQ-DEFAULT-1-05] [REQ-DEFAULT-1-06] [REQ-DEFAULT-1-09] [REQ-INTEGRITY-1-01] [REQ-INTEGRITY-1-02] [REQ-EXPOSURE-1-01] [REQ-DEFAULT-1-07]
[T-PD-02]	Hypervisor and infrastructure compromise of virtual deployment	[RF-DA-02]	[REQ-INTEGRITY-1-01] [REQ-INTEGRITY-1-02] [REQ-DATA-1-03] [REQ-DEFAULT-1-07]
[T-DD-01]	Disabling passive monitoring sensors	[RF-TI-01]	[REQ-PACKET-1-01] [REQ-AVAIL-1-01] [REQ-AVAIL-1-03] [REQ-LOG-1-01] [REQ-DEFAULT-1-07]

Annexes C to J:
Void

Annex K (normative): Vertical specific state of the art cryptography

K.0 General

This annex provides additional vertical-specific generic requirements around the use of state of the art cryptography in firewalls, intrusion detection systems, and intrusion prevention systems. It lists, by reference to the relevant normative clauses elsewhere in the present document, the cryptographic algorithm primitives, schemes and protocols that are commonly deployed on the market for these product categories and that are classified as CRY-SOTA for the purposes of the present document.

K.1 Classification of cryptographic algorithms as CRY-SOTA

For the purposes of the present document, a cryptographic algorithm, scheme or protocol is classified as CRY-SOTA where it is admitted under one of the ACM-listed or ACM-extended routes defined in items i), ii) or iii) below. A cryptographic algorithm, scheme or protocol that is not CRY-SOTA may nonetheless be used where it is admitted under the interoperability-based route defined in item iv) below.

A cryptographic algorithm, scheme or protocol is CRY-SOTA where at least one of the following applies:

i) ACM-listed: it is listed as Recommended (or equivalent) in the European Cybersecurity Certification Group's Agreed Cryptographic Mechanisms catalogue (ACM) [1];

ii) ACM-extended (recognised catalogue): it is not listed in the ACM, and it is listed as Recommended (or equivalent), and is not marked as deprecated, legacy-only or disallowed at the time of the conformity assessment, in any of the following recognised public cryptographic catalogues:

- NIST publications in the Special Publication 800 series, the FIPS series, and the associated CAVP/ACVP test-vector programmes;
- BSI TR-02102 series [i.10];
- ANSSI Référentiel Général de Sécurité, Annex B2 [i.11];
- CCCS ITSP.40.062 [i.12];
- a sector-specific cryptographic algorithm catalogue maintained by a recognised standards-development organisation such as ETSI, 3GPP, ITU-T, IEEE and IETF (see EXAMPLE 2);

iii) ACM-extended (vertical content): it is listed in the normative cryptographic content of the present document for firewalls, intrusion detection systems, and intrusion prevention systems (see clauses K.3 through K.8).

A cryptographic algorithm, scheme or protocol that is not CRY-SOTA under items i), ii) or iii) may be used only as follows:

iv) Interoperability-based: it is required for a specific product function to comply with a well-defined external specification or external requirement, and its use meets all of the conditions for legacy interoperability set out in clause K.2.4 (2). Inclusion of a cryptographic algorithm, scheme or protocol under this route does not classify it as CRY-SOTA.

NOTE 1: Items i), ii) and iii) are listed as alternatives for classification as CRY-SOTA. A manufacturer is not required to demonstrate classification under more than one of these items for the same algorithm. Item iv) is not a CRY-SOTA classification; it admits a non-CRY-SOTA algorithm under controlled interoperability conditions.

NOTE 2: Where two recognised catalogues classify the same algorithm differently, the manufacturer should rely on whichever produces the more conservative (less permissive) classification.

NOTE 3: A cryptographic mechanism composed of more than one cryptographic primitive (for example a hybrid key-encapsulation mechanism or a hybrid signature scheme) inherits the most restrictive classification of its constituent primitives. A hybrid construction including a Legacy or Deprecated component is therefore classified as Legacy or Deprecated, regardless of the classification of the other components.

NOTE 4: In item iv), an external specification or external requirement means a specification or requirement that is imposed on the product and that requires the use of a specific cryptographic algorithm, scheme or protocol for the product to interoperate with an identified system, platform or operational context. An external requirement can be, for instance, a regulatory requirement, an operational constraint, a technical interoperability constraint, or a platform compatibility requirement.

NOTE 5: The routes in items i) to iv) correspond to the ACM-listed, ACM-extended and interoperability-based cryptographic mechanism routes of the cross-vertical Annex K framework. Items i) to iii) correspond to the ACM-listed and ACM-extended routes; item iv) corresponds to the interoperability-based route, the conditions of which are specified for the present document in clause K.2.4 (2).

K.2 Assessment criteria for compliance with cryptographic requirements

K.2.1 Assessment objective

The purpose of this assessment case is to verify that, for every cryptographic algorithm, scheme or protocol used by a security mechanism of the product, appropriate evidence is provided demonstrating classification as CRY-SOTA in accordance with clause K.1, by reference to one of paths i), ii) or iii) of that clause.

K.2.2 Assessment preparation

Preconditions for the assessment:

- where the product has a default configuration, that default configuration shall be used for the assessment;
- otherwise, the delivery-state configuration shall be used (i.e. the configuration of the product as made available on the market in accordance with Annex I, Part I, point (2)(b) of Regulation (EU) 2024/2847 [i.1]);
- the manufacturer shall make available a list identifying every security mechanism of the product, the cryptographic algorithm, scheme or protocol used by that mechanism, the parameters in use, and whether the algorithm forms part of the default or delivery-state configuration.

K.2.3 Assessment activities

For every security mechanism identified under the preceding clause, the assessor shall:

1) review the documentation provided and confirm that, for each algorithm in use, the manufacturer has identified the path of clause K.1 (i), ii), or iii)) by which the algorithm is classified as CRY-SOTA, and the corresponding catalogue entry or clause reference;

2) verify that the catalogue entry or clause reference cited under (1) exists, is published, and is not marked as deprecated, legacy-only or disallowed at the time of the assessment;

3) inspect the product in the configuration identified under the preceding clause and confirm that the cryptographic algorithm and parameters in use match the documented configuration;

4) where the manufacturer has documented the use of an algorithm that is not classified as CRY-SOTA under any path of clause K.1, verify that the conditions for legacy interoperability are met.

K.2.4 Assessment evidence

1) For each cryptographic algorithm in use, a reference to a publicly available catalogue entry or to the relevant clause of the present document, in accordance with one of the paths of clause K.1. Acceptable references include:

   a) the entry in the ACM catalogue (path i);

   b) the entry in any of the recognised catalogues listed under K.1.1 (ii) (path ii); for example a national cryptographic catalogue published by a Member State authority, a sector-specific catalogue published by a recognised standards-development organisation, or an industry catalogue, where the catalogue is publicly available and is maintained under a documented revision and retirement process;

   c) the clause of the present document listing the algorithm as part of the vertical-specific cryptographic content for firewalls, intrusion detection systems, and intrusion prevention systems (path iii);

   d) where an algorithm is referenced under path ii) or path iii) but is not present in the ACM, the documentation shall in addition identify the publicly available specification (e.g. an IETF Request for Comments, an IEEE standard, an ETSI deliverable, a NIST publication) under which the algorithm is implemented.

2) Where a non-CRY-SOTA algorithm is offered by the product to support interoperability with a specifically identified legacy system, in accordance with recital (55) of Regulation (EU) 2024/2847 [i.1] and section 2.5 of the Commission Guidance on its application, the documentation shall demonstrate that all of the following conditions are met:

   a) the non-CRY-SOTA algorithm is not used in the default or delivery-state configuration;

   b) where the relevant security mechanism supports algorithm negotiation, a CRY-SOTA algorithm is offered and is preferred over the non-CRY-SOTA algorithm during negotiation;

   c) the documentation identifies the specific legacy system or systems for which the non-CRY-SOTA algorithm is required, and the legacy constraint that prevents use of a CRY-SOTA alternative;

   d) the documentation declares a sunset date for the non-CRY-SOTA algorithm that falls within the declared intended lifetime of the product;

   e) a user-facing indication (such as a log entry, a management-interface warning, or an equivalent mechanism) informs an administrator when the non-CRY-SOTA algorithm is in use.

3) As a supplemental verification, not sufficient on its own, the manufacturer shall identify whether any entry in the ENISA European Vulnerability Database (EUVD) [i.8], in the Single Reporting Platform (SRP) [i.9] established under Regulation (EU) 2024/2847 [i.1], or in equivalent publicly accessible cryptanalytic literature, identifies a fundamental cryptanalytic break of the algorithm in use (as distinct from an implementation defect in a specific product). Where such a break is identified, the algorithm shall not be classified as CRY-SOTA notwithstanding any catalogue listing.

4) Where the catalogue referenced under path ii) does not provide a lifecycle classification, the manufacturer shall document the algorithm's expected deprecation date based on the published cryptanalytic state of the art.

NOTE 1: The ACM catalogue references a number of cryptographic specifications published as ISO/IEC standards. Where such referenced specifications exist, technically equivalent specifications published in publicly available form (for example as IETF RFCs, as NIST Special Publications, or as IEEE standards) can also be cited as evidence under path ii) of clause K.1.

NOTE 2: The reference catalogues identified under K.1.1 (ii) use a range of lifecycle terminologies (for example "Recommended" / "Legacy" / "Deprecated" in the ACM; "Acceptable" / "Disallowed" in NIST SP 800-131A [i.13]; "Recommended" / "Legacy use" in BSI TR-02102-1 [i.10]).

NOTE 3: The supplemental check under (3) above is intended to capture the case where a cryptographic primitive listed in a catalogue is nevertheless subject to a fundamental break that has not yet been reflected in catalogue revisions. Vulnerability database entries typically catalogue implementation defects in specific products, which are not in themselves a basis for declassifying an algorithm.

K.2.5 Assessment verdict

The verdict pass shall be assigned where, for every cryptographic algorithm, scheme or protocol identified under the assessment preparation:

1) evidence has been provided classifying the algorithm as CRY-SOTA under one of the paths of clause K.1;
2) inspection has confirmed that the documented configuration is the active configuration of the product;
3) where applicable, the conditions for legacy interoperability have been verified; and
4) the supplemental cryptanalytic-status check has not identified a disqualifying entry.

The verdict fail shall be assigned otherwise.

EXAMPLE 1: A national cryptographic catalogue under K.1.1 (ii) is BSI TR-02102-1 [i.10], Cryptographic Mechanisms: Recommendations and Key Lengths, version 2026-01, 31 January 2026, published by the Federal Office for Information Security (Germany). It is also an example of a national catalogue referenced from the ACM.

EXAMPLE 2: Sector-specific cryptographic catalogues published by recognised standards-development organisations under K.1.1 (ii) include:

- ETSI TS 119 312 [2], Electronic Signatures and Trust Infrastructures (ESI); Cryptographic Suites;
- ETSI TS 133 210 [3], Network Domain Security (NDS); IP network layer security (relevant to operator-managed firewall, intrusion detection and intrusion prevention deployments);
- IETF cryptographic specifications published as Standards-Track or Best-Current-Practice RFCs, where the specification is referenced by a recognised national or sector catalogue.

EXAMPLE 3: An industry-relevant cryptographic catalogue example for firewalls, intrusion detection systems, and intrusion prevention systems is the Canadian Centre for Cyber Security ITSP.40.062 [i.12], Guidance on Securely Configuring Network Protocols, which provides parameter-level guidance for TLS, IPsec, SSH, and other protocols typical of the present document's product scope.

NOTE 1: Vertical-Standard-specific evidence for the appropriateness of a cryptographic algorithm can be added by the present document under path iii) of clause K.1. Examples of such evidence include a description and formal verification, a cryptographic security proof, a security analysis of a new algorithm, or a side-channel analysis.

NOTE 2: Formal verification, where used, employs mathematical proofs or rigorous methods to demonstrate that an algorithm meets its formal specification for all valid inputs, in contrast with testing, which samples specific cases.

NOTE 3: A hybrid cryptographic construction (for example a hybrid key-encapsulation mechanism or a hybrid signature scheme) inherits the most restrictive classification of its constituent primitives. Hybrid constructions are therefore not a general strategy for mitigating the deprecation of a constituent algorithm. Where a hybrid is used as part of the migration to post-quantum cryptography, the construction should be implemented in a way that allows the classical component to be cleanly removed once the post-quantum component is independently sufficient.

K.3 Symmetric atomic primitives

K.3.1 Block ciphers

The additional block ciphers included in Table K.1 are agreed as state of the art.

Table K.1: State of the art block ciphers

Primitive	Parameter's sizes	Notes
QARMA-64 (Arm CCA Security Model [i.14])	64 bit (block), 128 bit (key), 64 bit (tweak)	Tweakable block cipher used for Pointer Authentication (PAC) and memory tagging in Armv8.3 and later architectures.
QARMA-128 (Arm CCA Security Model [i.14])	128 bit (block), 256 bit (key), 128 bit (tweak)	Tweakable block cipher used in Arm Confidential Compute Architecture (CCA) for granule protection of confidential memory.

K.3.2 Stream ciphers

Block ciphers can be configured to behave like stream ciphers using counter (CTR) mode, as described in the ACM catalogue clause 3.1. In addition, the stream ciphers included in Table K.2 are agreed as state of the art.

Table K.2: State of the art stream ciphers

Primitive	Parameter's sizes	Notes
ChaCha20 (IRTF RFC 8439 [i.15])	256 bit (key)	A modern stream cipher used in VPNs and TLS 1.3. Preferred for devices without AES hardware acceleration. Extending ChaCha20 with a larger 24-byte nonce (XChaCha20) to mitigate nonce collisions is included in this primitive.

K.3.3 Hash functions

No additional primitives.

K.4 Symmetric constructions

K.4.1 Confidentiality modes of operation: encryption/decryption modes

No additional schemes.

K.4.2 Specific confidentiality modes: disk encryption

No additional schemes.

K.4.3 Integrity modes: message authentication codes

The additional message authentication codes included in Table K.3 are agreed as state of the art.

Table K.3: State of the art message authentication codes

Scheme	Parameter's sizes	Notes
Poly1305 (IRTF RFC 8439 [i.15])	128 (tag)	Paired with ChaCha20 in TLS 1.3.
UMAC (IETF RFC 4418 [i.16])	128	Used in SSH configurations for managing firewalls, intrusion detection systems, and intrusion prevention systems.

K.4.4 Symmetric entity authentication schemes

No additional schemes.

K.4.5 Authenticated encryption

The additional authentication encryption schemes included in Table K.4 are agreed as state of the art.

Table K.4: State of the art authentication encryption schemes

Scheme	Parameter's sizes	Notes
ChaCha20-Poly1305 (IRTF RFC 8439 [i.15])	256 bit (key)	Standard AEAD for TLS 1.3. Extending ChaCha20 with a larger 24-byte nonce (XChaCha20) to mitigate nonce collisions is included in this primitive.

K.4.6 Key protection

No additional schemes.

K.4.7 Key derivation functions

No additional functions.

K.4.8 Password protection/password hashing mechanisms

The additional password protection / password hashing mechanisms included in Table K.5 are agreed as state of the art.

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

Table K.5: State of the art password protection / password hashing mechanisms

Primitive	Parameter's sizes	Notes
Argon2id (IETF RFC 9106 [i.17])	Output: 32 bytes, OpsLimit: 2, Memory: 19 MiB, Threads: 1 (or higher)	A resource intensive hash function to protect passwords. Can also be used as a KDF to derive secret keys from passwords. Generated entropy depends on the entropy of the password.
Scrypt (IETF RFC 7914 [i.18])	Cost: 2^{17}, block size 1024 bytes, parallelisation 1 (or higher)	A resource intensive hash function to protect passwords. Can also be used as a KDF to derive secret keys from passwords. Generated entropy depends on the entropy of the password.

K.4.9 Key combiners

No additional schemes.

K.5 Asymmetric atomic primitives

K.5.1 RSA/Integer factorisation

No additional primitives.

K.5.2 Discrete logarithm in finite fields

No additional primitives.

K.5.3 Discrete logarithm in elliptic curves

The additional elliptic curve parameters included in Table K.6 are agreed as state of the art.

Table K.6: Additional elliptic curve parameters agreed as state of the art

Scheme	Curve	Notes
X25519 / Ed25519 (IETF RFC 8410 [i.19])	Curve25519	Standard for TLS 1.3, and SSH.
X448 / Ed448 (IETF RFC 8410 [i.19])	Curve448	High-security (224-bit security) IETF standard.

K.5.4 Learning with errors in (structured) lattices

No additional LWE mechanisms.

K.5.5 Hash function preimage resistance

No additional schemes.

K.5.6 Other intractable problems

No additional schemes.

K.6 Asymmetric constructions

K.6.1 Asymmetric encryption scheme

No additional schemes.

K.6.2 Digital signature

The additional digital signature schemes included in Table K.7 are agreed as state of the art.

Table K.7: State of the art digital signature schemes

Scheme	Parameter's sizes	Notes
Ed25519 (IRTF RFC 8032 [i.20])	256 bit key	Used for TLS and formally known as EdDSA.

K.6.3 Asymmetric entity authentication schemes

The additional asymmetric entity authentication schemes included in Table K.8 are agreed as state of the art.

Table K.8: State of the art entity authentication schemes

Scheme	Parameter's sizes	Notes
Ed25519-256 with Curve25519 (IETF RFC 8420 [i.21])	256 bit	
EAP-TLS (IEEE 802.11 [i.31])	ECDSA: 255-bit / RSA: 2048-bit	

K.6.4 Key establishment and key encapsulation

No additional schemes.

K.7 Cryptographic protocols

K.7.1 QUIC

The QUIC protocol included in Table K.9 is agreed as state of the art.

Table K.9: Additional QUIC protocol agreed as state of the art

QUIC Protocol Version
QUIC version 1 (IETF RFC 9000 [i.22])

The QUIC cipher suites included in Table K.10 are agreed as state of the art.

Table K.10: QUIC cipher suites agreed as state of the art

Hex Code	Cipher Suite	Notes
0x1301	TLS_AES_128_GCM_SHA256	
0x1302	TLS_AES_256_GCM_SHA384	
0x1303	TLS_CHACHA20_POLY1305_SHA256	
0x1304	TLS_AES_128_CCM_SHA256	

K.7.2 SNMP

The SNMP protocols included in Table K.11 are agreed as state of the art.

Table K.11: SNMP protocol agreed as state of the art

SNMP Protocol Version
SNMPv3 (IETF RFC 3411 [i.23], IETF RFC 5590 [i.24])

The SNMPv3 cipher suites included in Table K.12 are agreed as state of the art.

Table K.12: SNMPv3 cipher suites agreed as state of the art

Algorithm Name	Notes
AES-256-CFB	
AES-128-CFB	

K.7.3 Secure device identity

The secure device identity protocols included in Table K.13 are agreed as state of the art.

Table K.13: Secure device identity protocols agreed as state of the art

Secure Device Identity
IEEE 802.1AR [i.25]

The cipher suites used with secure device identity protocols included in Table K.14 are agreed as state of the art.

Table K.14: Secure device identity cipher suites agreed as state of the art

Algorithm Name	Notes
P-256	
P-384	

K.7.4 Time Protocols

The time protocols included in Table K.15 are agreed as state of the art.

Table K.15: Time protocol agreed as state of the art

Time Protocol
IEEE 1588-2019 [i.26]
NTS-Authenticated NTP (IETF RFC 8915 [i.27])

The cipher suites included in Table K.16 are agreed as state of the art for use with the time protocols.

Table K.16: Time protocol cipher suites agreed as state of the art

Group	Algorithm Name	Notes
IEEE 1588 PTP AUTHENTICATION TLV (Annex P of IEEE 1588 [i.26])	HMAC-SHA256-128	
IEEE 1588 PTP AUTHENTICATION TLV	AES-GMAC	
IEEE 1588 PTP AUTHENTICATION TLV	HMAC-SHA256	
IEEE 1588 PTP AUTHENTICATION TLV	HMAC-SHA512	

Group	Algorithm Name	Notes
NTS AEAD Integrity Algorithm	AES-SIV	Mandatory AEAD for Secure Network Time (IETF RFC 8915 [i.27]).

K.8 Cryptographic industry standards

The following industry standards serve as a baseline for approved cryptographic algorithms and are considered approved as CRY-SOTA. The standards listed in Table K.17 are agreed as state of the art.

Table K.17: National catalogues defined as CRY-SOTA

Cryptographic Mechanisms	Version	Notes
BSI TR-02102-1 [i.10]	2026-01	
BSI TR-02102-2 [i.28]	2026-01	
BSI TR-02102-3 [i.29]	2026-01	
BSI TR-02102-4 [i.30]	2026-01	

K.9 Crypto agility

K.9.1 Requirement

Where the product's default configuration uses a cryptographic mechanism for which the ACM catalogue, or the present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product, the product shall provide means for addressing the affected cryptographic mechanism by one or more of the following:

a) updating the cryptographic mechanism;

b) using another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation;

c) disabling the use of the affected cryptographic mechanism; or

d) limiting the use of the affected product functions accordingly.

EXAMPLE 1: Where a security mechanism uses a hybrid cryptographic construction, for example a hybrid key-encapsulation mechanism combining a classical and a post-quantum primitive, the lifecycle status of each constituent primitive is relevant to the lifecycle status of the construction. Hybridisation can be used as part of a planned migration strategy where permitted by the ACM catalogue or by the present document. However, hybridisation does not, by itself, extend the recommended usage lifetime of a constituent primitive that has been deprecated.

NOTE 1: Where a hybrid cryptographic construction includes multiple cryptographic primitives, the lifecycle status of each constituent primitive is relevant to the lifecycle status of the construction. Hybridisation is not assumed to mitigate the deprecation of a constituent primitive unless the ACM catalogue or the present document classifies the hybrid construction as suitable for the corresponding product function.

NOTE 2: Crypto agility supports maintaining appropriate cryptographic protection within the intended lifetime of the product, in addition to the capability of updating cryptographic mechanisms on the product in accordance with secure update and secure communication mechanisms.

NOTE 3: Deprecation information from sources other than the ACM catalogue or the present document can be considered as input to vulnerability management or security risk assessment but does not by itself trigger the requirement in clause K.9.1.

NOTE 4: Where the product provides cryptographic capabilities for use by other products, components or layers, the mechanism required by clause K.9.1 can consist of update, configuration, disabling, deprecation or limitation capabilities usable by the integrating product, system operator or user, where applicable.

NOTE 5: The applicability condition of this requirement can express exceptions based on product characteristics, e.g. cryptographic implementation based on immutable hardware co-processor(s) or hardware-based root of trust, or long-lived silicon used in a long-lived non-updateable environment.

K.9.2 Assessment of crypto-agility

K.9.2.1 Assessment objective

The purpose of this assessment case is to verify whether, where the product's default configuration uses a cryptographic mechanism for which the ACM catalogue, or the present document, specifies a deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product, the product provides means to address the affected cryptographic mechanism in accordance with clause K.9.1.

K.9.2.2 Assessment preparation

- Preconditions for the assessment: The product's default configuration shall be used for the assessment.
- The documentation shall identify:

  a) the intended lifetime of the product;

  b) the cryptographic mechanisms used in the product's default configuration;

  c) the related product function(s) for each cryptographic mechanism;

  d) the lifecycle information applicable to each cryptographic mechanism, where specified by the ACM catalogue or the present document, including any deprecation date, expiry date, migration condition or usage limitation.

K.9.2.3 Assessment activities

The assessment shall include verification that:

a) for each cryptographic mechanism used in the product's default configuration, the lifecycle information specified by the ACM catalogue or the present document has been identified, where such information is specified;

b) where the ACM catalogue or the present document specifies a deprecation date, expiry date, migration condition or usage limitation for a cryptographic mechanism, this information is reflected in the documentation;

c) where a deprecation date, expiry date, migration condition or usage limitation falls within the intended lifetime of the product, the product provides an applicable mechanism for updating the cryptographic mechanism, using another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation, disabling the use of the affected cryptographic mechanism, or limiting the use of the affected product functions accordingly;

d) where another cryptographic mechanism is used, that cryptographic mechanism complies with clause K.1.1 and is not subject to the relevant deprecation date, expiry date, migration condition or usage limitation.

K.9.2.4 Assessment evidence

The assessment evidence shall include, as applicable:

a) documentation of the intended lifetime of the product;

b) list of cryptographic mechanisms used in the product's default configuration;

c) identification of the related product function(s) for each cryptographic mechanism;

d) references to the ACM catalogue entry or to the provision of the present document used to determine lifecycle information, where applicable;

e) identification of any deprecation date, expiry date, migration condition or usage limitation falling within the intended lifetime of the product;

f) description of the means provided by the product, such as update of the cryptographic mechanism, use of another cryptographic mechanism that complies with clause K.1.1 and is not subject to the relevant lifecycle constraint, disabling the use of the affected cryptographic mechanism, or limitation of the use of the affected product functions.

K.9.2.5 Assessment verdict

- The verdict PASS shall be assigned if the required evidence has been provided, is complete, is applicable to the assessed configuration, and demonstrates compliance.

History

Version	Date	Status
V1.0.0	July 2026	SRdAP process EV 20261005: 2026-07-13 to 2026-10-05