ETSI TS 103 961 V1.1.1 (2023-12)

CYBER;
Optical Network and Device Security;
Security provisions for the management of
Optical Network devices and services

Reference
DTS/CYBER-0086

Keywords
cybersecurity, optical, optical network device,
security requirements

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 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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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 Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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 Optical Network Device Security (ONDS) suite of documents is developed as an interlinked collection, shown in figure 1.

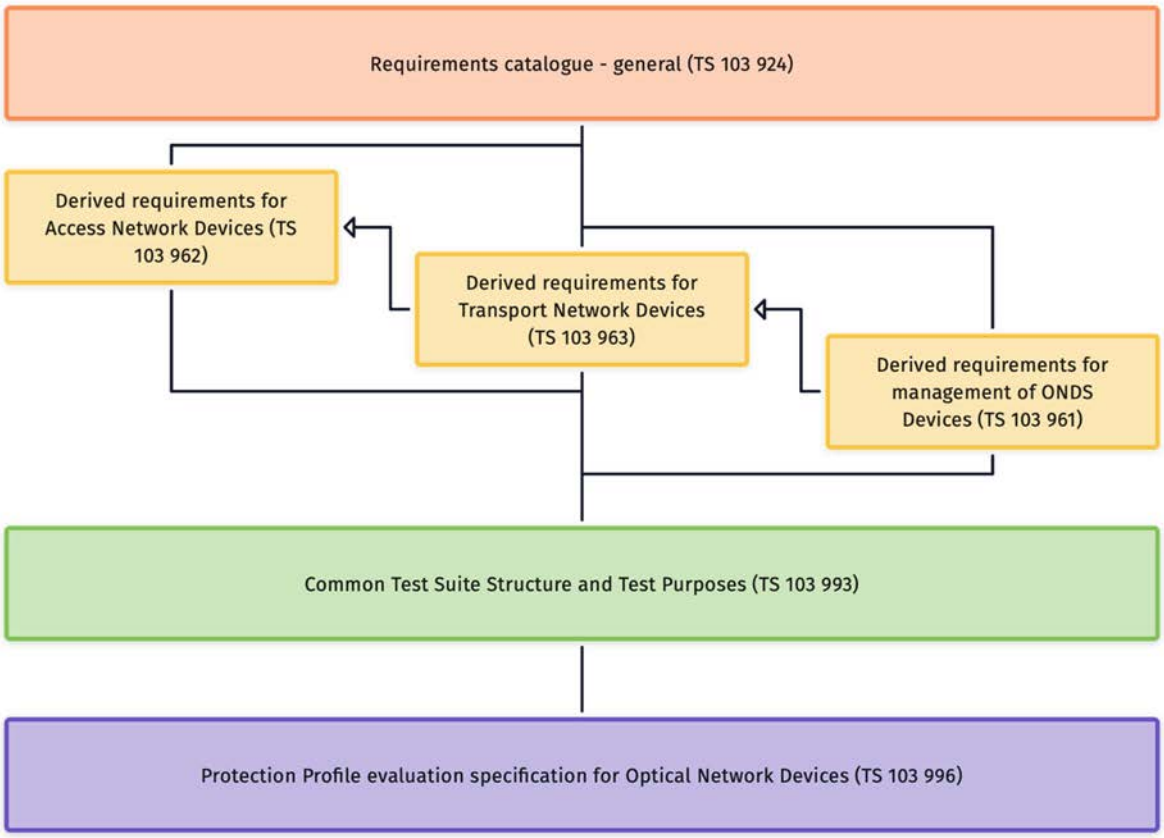

Figure 1: Document structure for Optical Network Device Security

Each of ETSI TS 103 962 [4], ETSI TS 103 963 [5] and ETSI TS 103 961 (the present document) expand upon the requirements identified in the common catalogue of ETSI TS 103 924 [1]. In the definition of detailed provisions ETSI TS 103 962 [4] acts as the master document with each of ETSI TS 103 963 [5] and the present document identifying further specializations.

To drive the evaluation and test of the ONDS suite a common Test Suite Structure and Test Purposes definition is proposed to be given in ETSI TS 103 993 [i.13], and from that will be derived a specification of the evaluation assessments to be applied for the present document, is to be given in the form of a partial protection profile in ETSI TS 103 996 [i.14].

NOTE: All of the documents identified in figure 1 act together to fully define the requirements, test and evaluation for placing an ONDS device on the market.

1 Scope

The present document defines security measures for the management of Optical Network devices and services as defined in ETSI TS 103 962 [4] and ETSI TS 103 963 [5].

The present document extends the provisions identified in the Catalogue of Requirements for Optical Network and Device Security from ETSI TS 103 924 [1].

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 at https://docbox.etsi.org/Reference.

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] ETSI TS 103 924: "Optical Network and Device Security; Catalogue of Requirements".

[2] Recommendation ITU-T G.7710: "Common equipment management function requirements".

[3] Recommendation ITU-T M.3700: "Common management services - Object management - Protocol neutral requirements and analysis".

[4] ETSI TS 103 962: "CYBER; Optical Network and Device Security; Security provisions in Optical Access Network Devices".

[5] ETSI TS 103 963: "CYBER; Optical Network and Device Security; Security provisions in transport network devices".

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

[i.1] IETF STD0062: "Simple Network Management Protocol".

NOTE: The RFCs cited for STD0062 are listed in the bibliography.

[i.2] Recommendations ITU-T M series: "Telecommunication management, including TMN and network maintenance".

[i.3] IETF RFC 5440: "Path Computation Element (PCE) Communication Protocol (PCEP)".

[i.4] IETF RFC 6241: "Network Configuration Protocol (NETCONF)".

[i.5] ETSI TS 102 165-2: "CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

NOTE: An update to the work item above is in development but the latest draft is publicly available.

[i.6] Trusting Computing Group: "TCG Roots of Trust Specification (draft)".

[i.7] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.8] FIPS PUB 202: "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions".

[i.9] NIST SP 800-171: "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations".

[i.10] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.11] Recommendation ITU-T X.200: "Information technology - Open Systems Interconnection - Basic Reference Model: The basic model".

[i.12] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

NOTE: This reference is in development in ETSI TC CYBER.

[i.13] ETSI TS 103 993: "Cyber Security (CYBER); ONDS; Test Suite Structure and Test Purposes".

[i.14] ETSI TS 103 996: "Cyber Security (CYBER); ONDS; Protection profile - Test cases".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

canonical identifier: structured identifier that is globally unique

crypto-agile: able to change or replace the existing suite of cryptographic algorithms or parameters with ease and without the rest of the infrastructure being significantly affected

delegated trust: trust arising where an entity A is unable to evaluate the appropriate level of trust for a relationship with another entity B, entity A chooses to delegate the decision to another entity C, which by having a direct relationship to entity B is in a position to make such a decision

NOTE 1: For delegated trust there is a precondition that there is a direct trust relationship from entity A to entity C.

NOTE 2: In this form of delegated trust entity C is aware of the relationship between entity A and entity B.

direct trust: trust decision by an entity A to trust entity B without any other party being involved

root identity: canonical identifier of the device that is attested to in the root identity certificate of the device

root of trust: component of a system that provides physical and cryptographic guarantees of securely providing processing and storage functions in a system

semantic identifier: formal representation of a property of an entity that describes one of the functions of the entity

EXAMPLE: In the sentence "Aristotle, the author of Politics, established the Lyceum" semantic identification means to identify Aristotle as a person (author is a person) and Politics as a written work of political philosophy (the Lyceum is an example of writing on political philosophy).

transitive trust: trust decision by an entity A to trust entity B because entity C asserts the trustworthiness of B

NOTE: Transitive trust differs from simple delegated trust (see above) as entity C does not know of the relationship between entity A and entity B.

trust domain: collection of entities between which there is either direct, delegated or transitive trust

3.2 Symbols

Void.

3.3 Abbreviations

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

AAT	Authority Attribute Tree
AES	Advanced Encryption System
CTR	CounTeR

NOTE: Mode of operation of a cryptographic algorithm.

ECDSA	Elliptic Curve Digital Signature Algorithm
EMS	Element Management System
FALCON	Fast Fourier Lattice-based Compact Signatures over NTRU
FCAPS	Fault Configuration Accounting Performance Security

NOTE: Or Fault management.

GCM	Gallios Counter Mode

NOTE: Mode of operation of a cryptographic algorithm.

HSM	Hardware Security Module
NMS	Network Management System
NTRU	Nth degree Truncated polynomial Ring Units
O&M	Operations and Management
OID	Object IDentifier
ON	Optical Network
OND	Optical Network Device
ONDS	Optical Network Device Security
OSI	Open Systems Interconnection
PCEP	Path Computation Element communication Protocol
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adleman
RtS	Root of trust for Storage
SNMP	Simple Network Management Protocol
TPM	Trusted Platfom Module

4 Overview of security of management function in Optical Networks (ONs)

4.1 General

As stated in ETSI TS 103 924 [1] the provisions for securing the management of the optical network should follow existing best practice for securing management data and protocols. The present document defines an abstract profile of existing best practice with specific mappings in informative annexes.

The network management manager manages and controls devices on optical networks, supports unified management, and offers control of networks. Thus, the network manager integrates functions including network management, service control, and network analysis. It is an enablement system for network resource pooling, network connection automation and self-optimization, and O&M automation. The Recommendation ITU-T M.3700 [3] series of Recommendations define the management functions applicable in the Network Management System-Element Management System (NMS-EMS) interface which includes object management, state management, notification management, performance management and fault management. More specifically, the common equipment management function requirements for an optical network are specified in Recommendation ITU-T G.7710 [2] The security requirements of the management plane are further defined in Recommendation ITU-T M.3016.0 [i.2], which in turn references Recommendation ITU-T M.3400 [i.2] for definition of the security management functions.

The overall approach for the security of managed objects of the ON is that the models of least persistence and least privilege shall apply (see NIST SP 800-171 [i.9]). Each managed object shall create an explicit security association with its managing entity where the security association shall give assurance of the following:

- the identity of participants in the security association;
- the integrity of data exchanged in the course of the security association; and
- the confidentiality of data.

NOTE 1: A device is expected to have at least one (1) and perhaps many managed objects and each managed object has an associated manager object.

NOTE 2: A single manager object can manage more than one object, in more than one device.

NOTE 3: A manager object can also be the managed object of another manager to create a hierarchy of managed objects.

NOTE 4: The present document does not distinguish between specific forms of managed object, thus applies equally to EMS (see Recommendation ITU-T M.3010 [i.2], clause 9.5.1.1) and NMS (see Recommendation ITU-T M.3010 [i.2], clause 9.5.1.2).

Within the overall structure the management functions shall be within the management plane and shall establish the primary trust domain for the entire network. The management plane shall act as the overall root of trust for the relevant operator and shall establish the trust domain of the operator. The managed object is considered independent of the OSI layering model [i.11] but may, by the nature of its function, be associated to a specific OSI layer.

EXAMPLE 1: The OSI layer 3 (network) entity has an associated network address specific to L3, or the L1 mapping has management and configuration data specific to the L1 mapping, thus the management object is associated to the OSI layer but the object being managed does not of itself have to have an OSI function.

Managed entities shall be entered into the trust domain by successfully proving their identity and by validation of the proof of attestation of function to the management plane. Where an entity/device supports multiple independent functions it shall establish a security and trust association to the primary trust domain for each function.

EXAMPLE 2: A device is likely to have a distinct trust association for (at least) device configuration (management plane to device), and for reporting (device to management plane).

EXAMPLE 3: Where a device supports multiple distinct capabilities (or attributes) each capability (or attribute) is attested to by a capability (or attribute) authority.

The management plane shall maintain the security policy for the primary trust domain. The security policy shall be driven from the management plane down to the Optical Network Devices (ONDs).

NOTE 5: The managed object to manager relationship acts as the trust domain.

The managed object should be initialized by the manager object. If the managed object detects either loss or corruption of the local configuration file or data it shall request a new set of configuration data from the associated manager. The manager shall ensure that all device configuration data for each managed object is always available.

EXAMPLE 4: The manager object enables a backup system that gives assurance of the required system availability.

4.2 Network management functional model

The optical network manager shall support the following functions:

- discovery and update of the network topology in real time;
- configuration of devices and services;
- FCAPS management (Fault Configuration Accounting Performance Security or Fault management, Configuration management, Accounting management, Performance management, Security management); and
- assurance of network resilience.

EXAMPLE: A number of available frameworks and standards support some or all of the identified functionalities including SNMP [i.1], ITU-T M series [i.2], PCEP [i.3], and Netconf [i.4].

4.3 Network management specificities

The specificities of managing network configuration and performance (e.g. Grade of Service, routing information to indicate where to address/send data, allocation of bandwidth to individual end-points) shall be managed through the configuration data elements.

EXAMPLE: The specificities include the management of network performance, routing information to indicate where to address/send data and allocation of bandwidth to individual end-points. This list is non-exhaustive.

4.4 Service control specificities

An ON may support multiple services (see Annex D of ETSI TS 103 962 [4]). Each service shall be managed as a discrete managed object (i.e. the service is the managed object).

4.5 Network analysis specificities

For the purposes of allowing the manager to make decisions the managed entity shall gather relevant metrics for each of fault management, security breach management, and performance management.

NOTE 1: The gather of metrics as defined above is distinct from the configuration of security attributes of any managed entity defined in previous clauses.

NOTE 2: The specific form of data processing used by the manager entities in the management plane to perform reactive or predictive interventions in network configurations is not addressed in the present document. However, where Artificial Intelligence or Machine Learning processes are used the guidance from ETSI ISG SAI applies.

5 Identification and authentication of ON management entities

ON managers and managed entities shall be identified with both a canonical identity and a semantic identifier. The semantic identifier shall be used to indicate the functional nature of the entity and the attestation of function shall be verifiable by a third party. This should be consistent with the Attribute Authority Tree (AAT) model described in ETSI TS 103 486 [i.12]. As with the AAT model it is not necessary to reveal all attributes of a managed entity, rather only those attributes relevant to the current situation should be made visible.

NOTE 1: Where the canonical identifier is attested to by the device in the root identity certificate it is termed the root identity of the device.

Managed entities can be either hardware or software entities.

All identities shall be cryptographically authenticated. Where asymmetric encryption is used the canonical identifier shall be asserted using an identity form of public-private key binding (e.g. X.509 identity certificate [i.10]), and any attribute shall be asserted using an attribute form of public-private key binding (e.g. X.509 attribute certificate [i.10]).

NOTE 2: Where the access control is based on a user role or user context these are treated as attributes and are asserted using attribute forms of public-private key binding.

Any public key carried in a PKC shall be checked to ensure that it is still valid and if the certificate has expired, or if the certificate and its key have been revoked, the verifier shall indicate a certificate verification error and shall not process any data associated to the key. If the PKC has been revoked or expired the managed object may request that the key chain is renewed or refreshed.

In case of failure of the authentication or identification, the time, location and reason for the failure shall be recorded in a log file. The log file shall only be accessible by the manager object as defined in clause 7.

Managed objects may be identified using Object IDentifiers (OIDs) as attributes of a device. The identity and any associated attributes shall be identified and authenticated within a PKI structure using attribute or identity certificates as appropriate.

EXAMPLE: Using X.509 [i.10] attribute certs support the use of OIDs.

6 Confidentiality and integrity protection of ON management protocols

Management functions enabled by a connection between the manager and the managed object should not have persistent security associations between the manager and the managed object. This is consistent with the principle of least persistence (see NIST SP 800-171 [i.9]).

NOTE 1: The principle of least persistence is that if a connection is not required it does not exist. Therefore, if a connection is established, it is removed as soon as possible after its function is fulfilled.

NOTE 2: Removal of connections after the function is fulfilled reduces the attack surface of the manager to managed object connection.

NOTE 3: A manager and managed object may pre-define a specific port for a function. Scanning for activity on the port does not imply a persistent connection at the port but may be used to instantiate a security association for the function.

The security association created during the identification and authentication phase should derive a session key used to protect the confidentiality of all data transferred between the manager and the managed object. The session key shall be used to encrypt the data using an algorithm agreed in the session establishment. To prevent replay the network management system shall support means to protect against replay attacks.

EXAMPLE: Any session keys are discarded after each use.

If a persistent shared secret is used as the basis of the session key it shall be randomized using a session-specific variable (e.g. nonce, counter, timestamp) in order to derive the session key. It shall not be feasible to determine the value of any shared secret by capture of the session-specific variable or the *en-clair* (plain text) content of the management message.

NOTE 4: Advice on the selection of algorithms is given in Annex A.

7 Secure storage of management data

7.1 General provisions

The managed object shall have means to ensure that data in the secure storage area is stored in a form that maintains confidentiality.

EXAMPLE: A TPM [i.6] may provide means to give a guarantee of tamper resistance that assures the confidentiality of data without requiring the data to be in encrypted form.

The managed object shall have means to ensure that any data manipulation that leads to loss of data integrity is prevented.

The following characteristics shall be met by the secure storage element:

- Tamper resistant.
- Tamper evident.
- Persistent.

If the management system detects any loss of data integrity a security alarm should be raised from the managed object to the associated manager.

NOTE: A general overview of the Roots of Trust in security modules can be found in the cited TCG publication [i.6].

7.2 Access control

In like manner to ETSI TS 103 962 [4] and ETSI TS 103 963 [5] the management system shall implement an access control policy in which the right to access any protected element (referred to as objects) shall be made by evaluation of the rules contained in the policy (see also ETSI TS 102 165-2 [i.5]). The principles of least privilege and least persistence shall apply at all times.

EXAMPLE 1: The principle of least privilege requires that the subject, after being authenticated, receives only those rights required of the role that is associated. Similarly, the principle of least persistence is to ensure that once access is granted to an object it is closed at the earliest opportunity. Least privilege may prevent escalation of privilege.

If the manager entity for any managed object changes over time this shall be captured as a policy rule (see ETSI TS 102 165-2 [i.5]) and should be applied with contextual constraints.

EXAMPLE 2: A configuration file is managed by one logical entity, but that logical entity may legitimately change location over time (this may be cyclical).In such cases the permission to access the configuration file is evaluated based on time, location and role of the managing entity.

If more than one subject (e.g. employee and their manager) is required to authorize a change to a managed object, this shall be addressed in the policy by enforcing at least 2 rules (employee and manager), one for each role, both of which have to pass.

EXAMPLE 3: Roles that may be supported include a security administrator (for changing security parameters), device administrator (for changing device operational characteristics), user (no access to change configuration data).

NOTE 1: The term security administrator may also be referred to as security manager.

NOTE 2: The term device administrator may also be referred to as device manager.

7.3 Logging requirements

As stated in clause 7.1 any change in configuration shall be recorded and the record of changes shall be maintained and stored in a secure storage area (where the key for the secure storage area is managed by an RtS). The present clause provides additional requirements for the content of such records.

NOTE 1: The general terms logging applies to the creation and maintenance of change records on the managed object.

NOTE 2: The RtS may act as the gatekeeper for an arbitrary sized secure data storage element.

Read access to log files related to a specific managed object shall be restricted to the related manager and its hierarchy and access control shall be granted as per the roles in the access control policy (additional contextual, identity or role attributes may be added as rules to the policy for evaluation) (see also ETSI TS 102 165-2 [i.5] for examples of the application of rules in access control policies).

Log files (or records) may be stored locally to the managed object (e.g. OND). Log files (or records) may be stored remotely from the managed object (e.g. OND). Irrespectively of where log files are stored the storage shall provide the following security services, where enabled by the manager:

- proof of integrity of the contents;
- confidentiality protection of all or part of the content (e.g. in encrypted form).

NOTE 3: The services above are therefore always available but are only used when configured to be used by the manager of the managed object.

NOTE 4: If the device supports all disk or all memory encryption no additional functionality is required.

NOTE 5: In some cases, there may be no added value in encrypting all of the log file but national or regional legislation may determine the scope of encryption.

If log files are stored remotely, they shall be transferred in a channel that shall provide the following security services, where enabled by the manager:

- proof of integrity of the contents;
- confidentiality protection of the content; and
- mutual authentication of the end-points prior to establishment of the transfer channel.

The period for which log records are to be retained shall be configurable by the manager.

Annex A (normative): Cryptographic provisions for ON security

A.1 Crypto-agility

Any cryptographic provision for ONs shall be crypto-agile. In particular cryptographic provisions should be designed in such a manner that they are able to support a Quantum Safe approach to both asymmetric and symmetric security.

All devices in the ON with a cryptographic function shall ensure that the cryptographic facility is "crypto agile" both within the same class of algorithms, and to allow for migration to an alternative class of algorithm.

NOTE: Crypto-agility in a single class of algorithms addresses the use of alternative curves in ECDSA, or alternative key sizes, as well as changing modes of operation in block ciphers (e.g. moving between CTR mode and GCM mode for AES). In the wider application of crypto-agility to move between algorithm classes this includes moving from conventional asymmetric modes (e.g. RSA, ECDSA) to modes based on, for example, codes, hashes, lattices and so forth (e.g. NTRU, FALCON).

A.2 Quantum safe

There is a general threat arising from the development of quantum computers to the security offered by cryptographic algorithms. As described in ETSI EG 203 310 [i.7] quantum computers are an existential threat to many common forms of asymmetric cryptography, and a critical threat to common forms of symmetric cryptography, and a substantial threat to many key management and distribution algorithms.

All algorithms used in ONs should be provisioned as quantum safe, or the underlying mechanisms should be designed as crypto-agile to support a quantum safe algorithm during the life of the equipment and its services.

NOTE 1: As of the time of preparation of the present document a small set of algorithms has been selected by NIST for further analysis but there is no consensus on the selection of quantum safe algorithms suited to ONs.

NOTE 2: It is acknowledged that some quantum safe cryptographic operations, for asymmetric cryptography, require substantially more processing and longer keys, resulting in larger signature sizes, than more conventional cryptographic measures. This may impact the physical elements of an HSM and appropriate provisions for crypto-agility may not be realisable.

A.3 Use of passwords

If passwords are used for authentication the password shall not be stored on the system. The system shall store a cryptographic hash of the password only. (Therefore, if the hash is accessed by an adversary, the adversary will not be able to retrieve the password).

EXAMPLE: The password may be converted to a hash using SHA-3 as defined in NIST FIPS 202 [i.8] and only the resultant hash stored in the system. To verify the password the hash of the entered password is compared to the stored value thus the password is never available to the system in plain text.

NOTE: Requirements which a hashing algorithm have to meet are summarized in Annex E of ETSI TS 102 165-2 [i.5].

A.4 Security parameter negotiation

In order to give assurance of a secure connection between 2 entities the entities shall negotiate to support a shared set of algorithms. If an algorithm proposed by the manager is not supported by the managed object, the manager object should raise an exception report indicating the algorithms are unmatched.

If a decision is made to change the algorithm to one of lower perceived cryptographic strength this should be logged as a potential bid-down attack by the managed object. Bid-down attacks should be avoided and if the managed object is not able to support the preferred algorithms of the manager object steps should be taken to update the managed object to support the stronger set of algorithms.

Annex B (informative): Lifecycle management

In addition to the provisions of the main body of the present document the following requirements are placed on the development of the management system.

Table B.1: Lifecycle management recommendations

Requirement	Liable party
The developer should check, assess and fix public-known security vulnerabilities of all software (including open-source software) used, before releasing any software package.	Developer
The manufacturer should publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, severity of vulnerabilities and information helping users to remediate the vulnerabilities.	Manufacturer
The manufacturer should use the general steps of ETSI TR 103 838 [i.10] in developing their vulnerability management process.	Manufacturer
The managed object should include a capability to allow it to be updated in response to a fixed vulnerability.	Developer
The managed object should be able to declare any limitations on its update and maintenance lifetime.	Manufacturer
A managed device should not be placed on the market, or supplied to the market, if any components (software or hardware) are no longer supported, or have reached end-of-life or end-of-support by their vendor, producer or developer.	Manufacturer
Any updates of software (in any form) should be signed and the signature verified to be true before installation.	Developer

Annex C (informative): Bibliography

- IETF RFC 3411: "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, December 2002.
- IETF RFC 3412: "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, December 2002.
- IETF RFC 3413: "Simple Network Management Protocol (SNMP) Applications", STD 62, December 2002.
- IETF RFC 3414: "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, December 2002.
- IETF RFC 3415: "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, December 2002.
- IETF RFC 3416: "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, December 2002.
- IETF RFC 3417: "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, December 2002.
- IETF RFC 3418: "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, December 2002.

History

Document history		
V1.1.1	December 2023	Publication