

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

FINAL DRAFT
FprEN 18031-1

May 2024

ICS

English version

Common security requirements for radio equipment - Part
1: Internet connected radio equipment

Exigences de sécurité communes applicables aux
équipements radioélectriques - Partie 1 : Équipements
radioélectriques connectés à l'internet

Gemeinsame Sicherheitsanforderungen für
Funkanlagen - Teil 1: Funkanlagen mit
Internetanschluss

This draft European Standard is submitted to CEN members for formal vote. It has been drawn up by the Technical Committee CEN/CLC/JTC 13.

If this draft becomes a European Standard, CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CEN and CENELEC in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

Contents

	Page
European foreword	4
Introduction	5
1 Scope.....	6
2 Normative references.....	6
3 Terms and definitions.....	6
4 Abbreviations.....	11
5 Application of this document.....	12
6 Requirements.....	15
6.1 [ACM] Access control mechanism	15
6.1.1 [ACM-1] Applicability of access control mechanisms	15
6.1.2 [ACM-2] Appropriate access control mechanisms	20
6.2 [AUM] Authentication mechanism.....	25
6.2.1 [AUM-1] Applicability of authentication mechanisms	25
6.2.2 [AUM-2] Appropriate authentication mechanisms	34
6.2.3 [AUM-3] Authenticator validation	37
6.2.4 [AUM-4] Changing authenticators.....	41
6.2.5 [AUM-5] Password strength	44
6.2.6 [AUM-6] Brute force protection.....	52
6.3 [SUM] Secure update mechanism.....	56
6.3.1 [SUM-1] Applicability of update mechanisms.....	56
6.3.2 [SUM-2] Secure updates.....	59
6.3.3 [SUM-3] Automated updates.....	64
6.4 [SSM] Secure storage mechanism	68
6.4.1 [SSM-1] Applicability of secure storage mechanisms	68
6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms	72
6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms	77
6.5 [SCM] Secure communication mechanism.....	82
6.5.1 [SCM-1] Applicability of secure communication mechanisms	82
6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	88
6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms	94
6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms	99
6.6 [RLM] Resilience mechanism.....	104
6.6.1 [RLM-1] Applicability and appropriateness of resilience mechanisms	104
6.7 [NMM] Network monitoring mechanism.....	109
6.7.1 [NMM-1] Applicability and appropriateness of network monitoring mechanisms.	109
6.8 [TCM] Traffic control mechanism	113
6.8.1 [TCM-1] Applicability of and appropriate traffic control mechanisms	113
6.9 [CCK] Confidential cryptographic keys	116
6.9.1 [CCK-1] Appropriate CCKs	116
6.9.2 [CCK-2] CCK generation mechanisms	120
6.9.3 [CCK-3] Preventing static default values for preinstalled CCKs.....	125
6.10 [GEC] General equipment capabilities	129

6.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities.....	129
6.10.2 [GEC-2] Limit exposure of services via related network interfaces	134
6.10.3 [GEC-3] Configuration of optional services and the related exposed network interfaces.....	138
6.10.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces.....	141
6.10.5 [GEC-5] No unnecessary external interfaces.....	144
6.10.6 [GEC-6] Input validation.....	147
6.11 [CRY] Cryptography	152
6.11.1 [CRY-1] Best practice cryptography.....	152
Annex A (informative) Rationale	157
A.1 General	157
A.2 Rationale.....	157
A.2.1 Family of standards	157
A.2.2 Security by design.....	157
A.2.3 Threat modelling and security risk assessment	158
A.2.4 Functional sufficiency assessment.....	159
A.2.5 Implementation categories.....	159
A.2.6 Assets	160
A.2.7 Mechanisms	161
A.2.8 Assessment criteria	162
A.2.9 Interfaces.....	165
Annex B (informative) Mapping with EN IEC 62443-4-2: 2019.....	168
B.1 General	168
B.2 Mapping.....	168
Annex C (informative) Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements).....	171
C.1 General	171
C.2 Mapping.....	171
Annex D (informative) Mapping with Security Evaluation Standard for IoT Platforms (SESIP)	175
D.1 General	175
D.2 Mapping.....	175
Annex ZA (informative) Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered	178
Bibliography	179

European foreword

This document (FprEN 18031-1:2024) has been prepared by Technical Committee CEN/CENELEC JTC 13 “Cybersecurity and Data Protection”, the secretariat of which is held by DIN.

This document is currently submitted to the Formal Vote.

This document has been prepared under a mandate given to CEN/CENELEC by the European Commission and the European Free Trade Association and supports essential requirements of EU Directive(s) / Regulation(s).

For relationship with EU Directive(s) / Regulation(s), see informative Annex ZA, which is an integral part of this document.

Introduction

Vigilance is required from manufacturers to improve the overall resilience against cybersecurity threats caused by the increased connectivity of radio equipment [33] and the growing ability of malicious threat actors to cause harm to users, organizations, and society.

The security requirements presented in this baseline standard are developed to improve the ability of radio equipment to protect its security assets and network assets against common cybersecurity threats and to mitigate publicly known exploitable vulnerabilities.

It is important to note that to achieve the overall cybersecurity of radio equipment, defence in depth best practices will be needed by both the manufacturer and user. In particular, no single measure will suffice to achieve the given objectives, indeed achieving even a single security objective will usually require a suite of mechanisms and measures. Throughout this document, the guidance material includes lists of examples. These examples given are only indicative possibilities, as there are other possibilities that are not listed, and even using the examples given will not be sufficient unless the mechanisms and measures chosen are implemented in a coordinated fashion.

1 Scope

This document specifies common security requirements and related assessment criteria for internet-connected radio equipment [34] (hereinafter referred to as "equipment").

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp/>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1

access control mechanism

equipment functionality to grant, restrict or deny access to specific equipment's *resources*

Note 1 to entry: Access to specific equipment's resources can amongst others be:

- reading specific data; or
- writing specific data to equipment's persistent storage; or
- performing a specific equipment functionality such as recording audio.

3.2

authentication

provision of assurance that an *entity* is who or what it claims to be

Note 1 to entry: An entity can amongst others claim to be:

- a specific human, owner of a user account, device, or service; or
- a member of specific groups such as an authorized group to access a specific equipment's resource; or
- authorized by another entity to access a specific equipment's resource.

3.3

authentication mechanism

equipment functionality to verify that an *entity* is who or what it claims to be

Note 1 to entry: Typically, the verification is based on examining evidence from one or more elements of the categories:

- knowledge; and
- possession; and
- inherence.

**3.4
authenticator**

something known or possessed, and controlled by an *entity* that is used for *authentication*

Note 1 to entry: Typically, it is a physical device or a password.

EXAMPLE A password or token can be used as an authenticator.

**3.5
assessment objective**

statement, provided as part of the assessment input, which defines the reasons for performing the assessment

[SOURCE: ISO/IEC 33001:2015, 3.2.6 [27]]

**3.6
best practice**

measures that have been shown to provide appropriate security for the corresponding use case

**3.7
brute force attack**

attack on a cryptosystem that employs a trial-and-error search of a set of keys, *passwords* or other data

**3.8
communication mechanism**

equipment functionality that allows communication via a *machine interface*

**3.9
confidential cryptographic key**

confidential security parameter, excluding *passwords*, which is used in the operation of a cryptographic algorithm or cryptographic protocol

**3.10
confidential network function configuration**

network function configuration whose disclosure can harm the network or its functioning or can lead to misuse of network resources

**3.11
confidential security parameter**

security parameter whose disclosure can harm the network or its functioning or can lead to misuse of network resources

**3.12
denial of service**

prevention or interruption of authorized access to an equipment *resource* or the delaying of the equipment operations and functions

[SOURCE : IEC 62443-1-1 :2019, 3.2.42 [28]] modified

**3.13
device**

product external to the equipment

**3.14
entity**
user, *device*, equipment or service

3.15

entropy

measure of the disorder, randomness or variability in a closed system

3.16

external interface

interface of an equipment that is accessible from outside the equipment.

Note 1 to entry: Machine, network, and user interfaces are specific types of external interfaces.

3.17

factory default state

defined state where the configuration settings and configuration of the equipment is set to initial values

Note 1 to entry: A factory default state can include security updates, installed after the equipment being placed on the market.

3.18

hard-coded

software development practice of embedding data directly into the source code of a program or other executable object

3.19

initialization

process that configures the network connectivity of the equipment for operation

Note 1 to entry: Initialization can provide the possibility to configure authentication features for a user or for network access.

3.20

interface

shared boundary across which *entities* exchange information

3.21

justification

documented information providing evidence that a claim is true under the assumption of common expertise

Note 1 to entry: Such evidence can be supported for example by:

- a description of the intended equipment functionality; or
- a descriptions of equipment's operational environment of use; or
- a description of equipment's technical properties such as security measures; or
- an analysis of relevant risks related to the operation of the equipment within its reasonably foreseeable use and intended equipment functionality.

3.22

machine interface

external interface between the equipment and a service or *device*

3.23**network asset**

sensitive network function configuration or confidential network function configuration or network functions

3.24**network equipment**

equipment that exchanges data between different networks used to permanently connect directly other devices to the internet

3.25**network function**

equipment's functionality to provide or utilize network resources by itself

3.26**network function configuration**

data processed by the equipment that defines the behaviour of the equipment's *network function*

3.27**network interface**

external interface enabling the equipment to have or provide access to a network

Note 1 to entry: Examples for network interfaces are a LAN port (wired) or a wireless network interface enabling WLAN or short-range wireless communication, e.g., using a 2.4 GHz antenna.

3.28**operational state**

state in which the equipment is functioning normally according to the intended equipment functionality [35] and within its intended operational environment of use

3.29**optional service**

service which is not necessary to setup the equipment, and which is not part of the basic functionality but is still relevant for the intended equipment functionality [35] and is delivered as part of the factory default.

EXAMPLE An SSH service on the equipment is not required for basic functionality of the equipment, but it can be used to allow a remote access to the equipment.

3.30**password**

sequence of characters (letters, numbers, or other symbols) used to authenticate an *entity*

Note 1 to entry: Personal identification numbers (PINs) are also considered a form of password.

3.31**public security parameter**

sensitive security parameter that is not confidential

3.32**resilient**

able to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber *resources*.

[SOURCE: NIST SP 800-172 [29]]

3.33

risk

combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014 [30]]

3.34

resource

functional unit or data item needed to perform required operations

[SOURCE: IEC [31]]

3.35

security asset

sensitive security parameter or confidential security parameter or security function

3.36

security function

functionality on the equipment that is relevant to protect it from harming the network or its functioning or misusing network resources

3.37

security parameter

data processed by the equipment that defines the behaviour of the equipment's *security function*

3.38

security strength

number associated with the amount of work that is required to break a cryptographic algorithm or system

Note 1 to entry: The amount of work can for example be the number of operations required to break a cryptographic algorithm or system.

3.39

sensitive network function configuration

network function configuration whose manipulation can harm the network or its functioning or can lead to misuse of network resources

3.40

sensitive security parameter

security parameter whose manipulation can harm the network or its functioning or can lead to misuse of network resources

3.41

security update

software update that addresses security vulnerabilities through *software* patches or other mitigations

3.42

software

assembly of programs, procedures, rules, documentation, and data, pertaining to the operation of an equipment

Note 1 to entry: Software also includes firmware.

3.43

storage mechanism

equipment functionality that allows to store information

3.44**update mechanism**

equipment functionality that allows to change equipment's *software*

3.45**user interface**

external interface between the equipment and a user

3.46**vulnerability**

weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the equipment, network, application, or protocol involved

[SOURCE: (ITSEC) (definition given by ENISA, "computer system" has been replaced by "equipment") [32]]

4 Abbreviations

ACM access control mechanism

API application programming interface

AU assessment unit

AUM authentication mechanism

CCK confidential cryptographic key(s)

CRY cryptography

CSP confidential security parameter

CWE common weakness enumeration

DHCP dynamic host configuration protocol

DN decision node

DoS denial of service

DT decision tree

E evidence

E.Info evidence.information

E.Just evidence.justification

GEC general equipment capabilities

IC implementation category

ICMP Internet control message protocol

IP Internet protocol

LAN	local area network
OS	operating system
MitM	Man-in-the-Middle
NNM	network monitoring mechanism
OS	operating system
PIN	personal identification number
PKI	public key infrastructure
RLM	resilience mechanism
SCM	secure communication mechanism
SDO	standards developing organization
SQL	structured query language
SSM	secure storage mechanism
SSP	sensitive security parameter
SUM	secure update mechanism
TCM	traffic control mechanism
USB	universal serial bus
WLAN	wireless local area network

5 Application of this document

This document uses the concept of mechanisms to instruct the user of this document when to apply certain security measures. Mechanisms address the applicability and appropriateness through a set of requirements including assessment criteria. An applicable/non-applicable decision is taken for each of the items specified. If applicable it is followed by a pass/fail appropriateness decision for each of the items specified. For example, when checking the applicability of a requirement on external interfaces, then the decision whether the requirement needs to be fulfilled is determined for each external interface independently.

The mechanisms and their application are documented using the structure shown in the table below:

Table 1 — Requirements structure

Clause #	Title		Description on how to apply this document
6.x	XXX Mechanism		Mechanism for each specific item (e.g., external interface or security asset)
6.x.1	XXX-1 Applicability of mechanisms		Applicability of the mechanism
6.x.1.1	Requirement		For each specific item determine and assess if the mechanism is required.
6.x.1.2	Rationale		NOTE A mechanism might combine applicability and appropriateness in a single requirement.
6.x.1.3	Guidance		
6.x.1.4	Assessment criteria		
6.x.1.4.1		Assessment objective	
6.x.1.4.2		Implementation categories	
6.x.1.4.3		Required information	
6.x.1.4.4		Conceptual assessment	
6.x.1.4.5		Functional completeness assessment	
6.x.1.4.6		Functional sufficiency assessment	
6.x.2	XXX-2 Appropriate mechanisms		Appropriateness of the mechanism
6.x.2.1	Requirement		For each specific item for which the mechanism is required as determined by XXX-1, determine and assess whether the mechanism is implemented properly.
6.x.2.2	Rationale		NOTE A mechanism might have multiple appropriateness sub-clauses to focus on specific properties.
6.x.2.3	Guidance		
6.x.2.4	Assessment criteria		
6.x.2.4.1		Assessment objective	
6.x.2.4.2		Implementation categories	
6.x.2.4.3		Required information	
6.x.2.4.4		Conceptual assessment	
6.x.2.4.5		Functional completeness assessment	
6.x.2.4.6		Functional sufficiency assessment	
6.x.y	XXX-# Supporting Requirements		Applicability and appropriateness of supporting requirements for the mechanism
6.x.y.1	Requirement		For each specific item for which the mechanism is required as determined by XXX-1, determine and assess if the supporting requirement needs to be implemented (there might be specific conditions, for instance if the equipment is a toy) and if it needs to be implemented, whether it is implemented properly.
6.x.y.2	Rationale		
6.x.y.3	Guidance		
6.x.y.4	Assessment criteria		
6.x.y.4.1		Assessment objective	
6.x.y.4.2		Implementation categories	
6.x.y.4.3		Required information	

Clause #	Title	Description on how to apply this document
6.x.y.4.4	Conceptual assessment	NOTE Some chapters contain multiple requirements, which leads to slight deviations in terms of numbering.
6.x.y.4.5	Functional completeness assessment	
6.x.y.4.6	Functional sufficiency assessment	

The assessments are conducted by examining the documented assessment cases, not all assessment cases might be provided for every mechanism:

- Conceptual assessment

Examine if the provided documentation and rationale provide the required evidence (for example the rationale why a mechanism is not applicable for a specific network interface).

- Functional completeness assessment

Examine and test if the provided documentation is complete (for example use network scanners to verify that all external interfaces are properly identified, documented and assessed)

- Functional sufficiency assessment

Examine and test if the implementation is adequate (for example run fuzzing tools on a network interface to check if it is resilient to attacks with malformed data)

Each of the assessments is further divided into the following sub-clauses which might use a decision tree to guide the assessment:

- Assessment purpose
- Preconditions
- Assessment units
- Assignment of verdict

Required information lists the information to be provided through technical documentation. This document does not require each required information element to be provided as a separate document.

For the section assessment criteria, the following identifiers with the defined syntax are used to structure the elements which are needed to perform an assessment:

- Required information

E.<Type>.<MechanismAbbreviation-<Nr>>.<CategoryName>

Identifier for the category of the required information excluding DTs

- Required information for decision trees

E.<Type>.DT.<MechanismAbbreviation-<Nr>>

Identifier for the category of the required information in the context of DTs

- Implementation Category

- IC.<MechanismAbbreviation-<Nr>>.<ImplementationCategoryName>
 - Identifier for the implementation category
 - Assessment Unit
- AU.<MechanismAbbreviation-<Nr>>.<AssessmentUnitName>
 - Identifier for the assessment unit
- Decision Tree Nodes
- DT.<MechanismAbbreviation-<Nr>>.DN-<Number>
 - Identifier for a specific node inside the DT

The placeholders are used as follows:

- <Type>: “Info” or “Just” to indicate the kind of required documentation which could by “information” or justification.
- <CategoryName>: Name of the category for the required documentation. A <CategoryName> could contain additional Sub-Category-Names divided with “.”.
- <ImplementationCategoryName>: Name of the implementation category which describes the defined implementation.
- <AssessmentUnitName>: Name of the assessment unit for a specific implementation category.
- <MechanismAbbreviation-<Nr>>: Abbreviation of the name from the specific requirement which belongs to the assessment criteria.

6 Requirements

6.1 [ACM] Access control mechanism

6.1.1 [ACM-1] Applicability of access control mechanisms

6.1.1.1 Requirement

The equipment shall use access control mechanisms to manage entities' access to security assets and network assets, except for access to security assets or network assets where:

- public accessibility is the equipment's intended functionality; or
- physical or logical measures in the equipment's targeted operational environment limit their accessibility to authorized entities; or
- legal implications do not allow for access control mechanisms.

6.1.1.2 Rationale

Security assets and network assets might be exposed to unauthorized access attempts. Access control mechanisms limit the ability of any unauthorized entity to access these assets.

6.1.1.3 Guidance

The requirement does not demand access control mechanisms on assets that it does not cover (for example, the dispense button on a coffee machine). Further it does not demand access control mechanisms for security assets or network assets that are in principle covered, but where the intended equipment functionality [35] is to be generally accessible by the public or where the intended operational environment of use ensures that only authorized access is possible.

Radio interfaces might be accessible even if the equipment is in an environment preventing physical manipulation by an unauthorized entity, for instance a wireless network is often accessible from outside a user's home.

For example, depending on the equipment's technical properties, intended equipment functionality and intended operational environment of use access control mechanisms might not be necessary for relevant security assets or network assets where:

- all entities with access to the equipment (the equipment is intended to be operated in an area which has physical access control) are authorized to access these assets (for example, the WPS button on a home router);
- the equipment's functionality only provides information (on security assets or network assets) that is intended to be publicly accessible (for instance broadcasting Bluetooth advertising beacons).

Access control mechanisms need properties to tie access rights to. Such properties can amongst others be:

- verified claims of entities (for instance being owner of a user account, member of specific group, authorized by another entity);
- certain states of the equipment or the equipment's environment (for instance an electronic flight bag might have different access rights for a local user when it is operated in the air, than when it is stored at the ground);
- the external interface an access is performed from (for instance a local access, where physical access control is obviously in place, might have different access rights than a remote access);
- various combinations of the properties mentioned, as well as additional ones.

6.1.1.4 Assessment criteria

6.1.1.4.1 Assessment objective

The assessment addresses the requirement ACM-1.

6.1.1.4.2 Implementation categories

Not applicable.

6.1.1.4.3 Required information

[E.Info.ACM-1.SecurityAsset]: Description of each security asset that is accessible by entities, including:

- [E.Info.ACM-1.SecurityAsset.Access]: possible entities' accesses to the security asset on the equipment; and

- (if access control by the equipment is absent for public accessibility of the security asset is the equipment's intended functionality) [E.Info.ACM-1.SecurityAsset.PublicAccess]: Description of the equipment's intended functionality concerning the public accessibility of the security asset; and
- (if access control by the equipment is absent because physical or logical measures in the equipment's targeted operational environment exists, that limit accessibility to authorized entities) [E.Info.ACM-1.SecurityAsset.Environment]: Description of:
 - physical or logical access control measures in the equipment's targeted operational environment; and
 - how entities are authenticated/authorized in the equipment's targeted operational environment; and
- (if legal implications do not allow for access control mechanisms) [E.Info.ACM-1.SecurityAsset.Legal]: References to all corresponding paragraph(s) or passages in all relevant legal documents, including a description on how this is applicable for the equipment or affected asset; and
- (if access control mechanisms are claimed to be required for entities access to the security asset) [E.Info.ACM-1.SecurityAsset.ACM]: Description of each access control mechanism that manages entities' access to the security asset.

[E.Info.ACM-1.NetworkAsset]: Description of each network asset that is accessible by entities, including:

- [E.Info.ACM-1.NetworkAsset.Access]: possible entities' accesses to the network asset on the equipment; and
- (if access control by the equipment is absent for public accessibility of the network asset is the equipment's intended functionality) [E.Info.ACM-1.NetworkAsset.PublicAccess]: Description of the equipment's intended functionality concerning the public accessibility of the network asset; and
- (if access control by the equipment is absent because physical or logical measures in the equipment's targeted operational environment exists, that limit accessibility to authorized entities) [E.Info.ACM-1.NetworkAsset.Environment]: Description of:
 - physical or logical access control measures in the equipment's targeted operational environment; and
 - how entities are authenticated/authorized in the equipment's targeted operational environment; and
- (if legal implications do not allow for access control mechanisms) [E.Info.ACM-1.NetworkAsset.Legal]: References to all corresponding paragraph(s) or passages in all relevant legal documents, including a description on how this is applicable for the equipment or affected asset; and
- (if access control mechanisms are claimed to be required for entities access to the network asset) [E.Info.ACM-1.NetworkAsset.ACM]: Description of each access control mechanism that manages entities' access to the network asset.

[E.Info.DT.ACM-1]: Description of the selected path through the decision tree in Figure 1 for each security asset and network asset documented in [E.Info.ACM-1.SecurityAsset] and [E.Info.ACM-1.NetworkAsset] where paths to access the asset exists, respectively.

[E.Just.DT.ACM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.ACM-1], with the following properties:

- (if a decision from [DT.ACM-1.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.ACM-1.DN-1] is based on [E.Info.ACM-1.SecurityAsset.PublicAccess] or [E.Info.ACM-1.NetworkAsset.PublicAccess]; and
- (if a decision from [DT.ACM-1.DN-2] results in “NOT APPLICABLE”) the justification for the decision [DT.ACM-1.DN-2] is based on [E.Info.ACM-1.SecurityAsset.Environment] or [E.Info.ACM-1.NetworkAsset.Environment]; and
- (if a decision from [DT.ACM-1.DN-3] results in “NOT APPLICABLE”) the justification for the decision [DT.ACM-1.DN-3] is based on [E.Info.ACM-1.SecurityAsset.Legal] or [E.Info.ACM-1.NetworkAsset.Legal]; and
- the justification for the decision [DT.ACM-1.DN-4] is based on [E.Info.ACM-1.SecurityAsset.ACM] or [E.Info.ACM-1.NetworkAsset.ACM].

6.1.1.4.4 Conceptual assessment

6.1.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether access control mechanisms are implemented when they are required per ACM-1.

6.1.1.4.4.2 Preconditions

None.

6.1.1.4.4.3 Assessment units

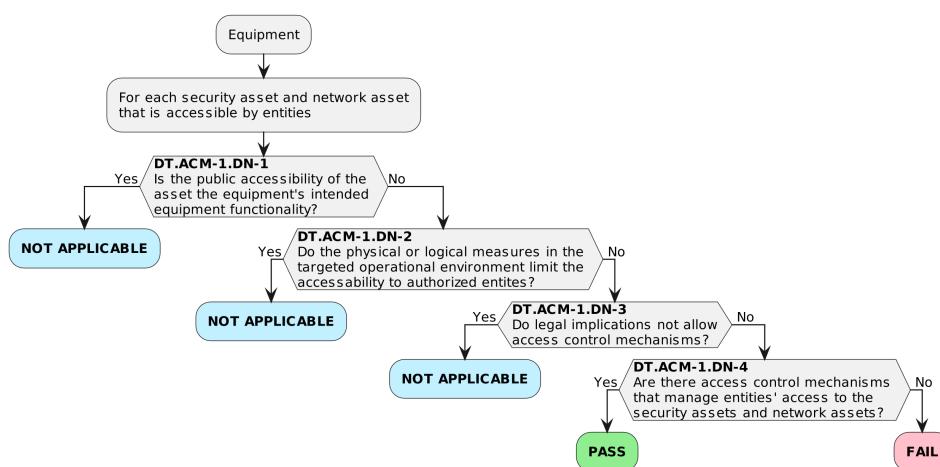


Figure 1 — Decision Tree for requirement ACM-1

For each security asset documented in [E.Info.ACM-1.SecurityAsset] and each network asset documented in [E.Info.ACM-1.NetworkAsset], check whether the path through the decision tree documented in [E.Info.DT.ACM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.ACM-1], examine its justification documented in [E.Just.DT.ACM-1].

6.1.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.ACM-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.ACM-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.ACM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACM-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.ACM-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.ACM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.ACM-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.1.4.5 Functional completeness assessment

6.1.1.4.5.1 Assessment purpose

The purpose of the functional assessment is to verify that all the security assets and network assets that are accessible by entities, are documented in [E.Info.ACM-1.NetworkAsset] or [E.Info.ACM-1.SecurityAsset].

6.1.1.4.5.2 Preconditions

The equipment is in an operational state.

6.1.1.4.5.3 Assessment units

Functionally assess whether there are security assets, that are accessible by entities, in the equipment, which are not documented in [E.Info.ACM-1.SecurityAsset] and whether there are network assets, that are accessible by entities, in the equipment, which are not documented in [E.Info.ACM-1.NetworkAsset], e.g. by inspecting all parts of the software such as built-in software, installed applications and interfaces for connected peripherals.

6.1.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all security assets found are documented in [E.Info.ACM-1.SecurityAsset] and all network assets found are documented in [E.Info.ACM-1.NetworkAsset].

The verdict FAIL for the assessment case is assigned if a security asset is found which is not documented in [E.Info.ACM-1.SecurityAsset] or a network asset is found which is not documented in [E.Info.ACM-1.NetworkAsset].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.1.4.6 Functional sufficiency assessment

6.1.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether access control mechanisms are implemented when required per ACM-1.

6.1.1.4.6.2 Preconditions

The equipment is in an operational state.

6.1.1.4.6.3 Assessment units

For each security asset documented in [E.Info.ACM-1.SecurityAsset] and each network asset documented in [E.Info.ACM-1.NetworkAsset] functionally confirm the existence of access control mechanisms according to [E.Info.ACM-1.SecurityAsset.ACML] or [E.Info.ACM-1.NetworkAsset.ACML] by accessing the assets following [E.Info.ACM-1.NetworkAsset.Access] and [E.Info.ACM-1.SecurityAsset.Access].

6.1.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an access control mechanism documented in [E.Info.ACM-1.SecurityAsset.ACML] or [E.Info.ACM-1.NetworkAsset.ACML] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that an access control mechanism documented in [E.Info.ACM-1.SecurityAsset.ACML] or [E.Info.ACM-1.NetworkAsset.ACML] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.2 [ACM-2] Appropriate access control mechanisms

6.1.2.1 Requirement

Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets.

6.1.2.2 Rationale

Security assets and network assets may be exposed by unauthorized access attempts. Appropriate access control mechanisms ensure these assets are protected from unauthorized access.

6.1.2.3 Guidance

This requirement is intended to ensure that the access control mechanisms used to protect the relevant security assets or network assets are chosen and configured such that unauthorized access is denied. With a variety of asset access methods and control mechanisms (for instance display on a wearable's screen), equipment use-cases and operational environments, it is difficult to specify a generic model for entities and associated access rights.

Whether an access control mechanism can deny unauthorized access, always depends on external assumptions that need to be fulfilled. For example, that the sharing of passwords or unauthorized physical access are not permitted.

Depending on the equipment's technical properties, intended operational environment of use, the access control mechanisms use appropriate properties to tie access rights to and that all involved entities are provided with authorization information.

When access control mechanisms rely on authentication mechanisms, see AUM, for example:

- an authorized entity, e.g., specific human, owner of a user account, device, or service, can after authentication access their security asset or network asset, such as changing security configuration; or
- a member of specific authorized groups can after authentication access a security asset or a network asset; or
- an entity, authorized by another entity to do so, can access a specific security asset or network asset.

For the determination of the appropriate access control mechanisms on security assets and network assets the following aspects are important:

- the risk associated with an entity's access to a security asset or network asset,
- the form of access an equipment's functionality allows to a security asset or network asset,
- the external interface the security asset or network asset is accessed through and
- the impact of access control provided by the intended operational environment of use.

For the determination of entities' access rights on security assets or network assets (authorized entities for certain access on assets), the following aspects are important:

- the risk associated with an entity's access to a security asset or network asset,
- the “need-to-know principle”: Does an entity need to obtain some information to a security asset or network asset,
- the “need-to-use principle”: Does an entity have a valid need to use a functionality based on a security asset or network asset,
- the “least privileges principle”: everything is forbidden unless permitted,
- the equipment's clearly advertised functionality e.g., concerning accessibility of security assets or network assets or interoperability with components of an existing infrastructure.

6.1.2.4 Assessment criteria

6.1.2.4.1 Assessment objective

The assessment addresses the requirement ACM-2.

6.1.2.4.2 Implementation categories

[IC.ACM-2.RBAC]: The methods to validate the appropriateness of the access control mechanism solely rely on role-based access control.

[IC.ACM-2.DAC]: The methods to validate the appropriateness of the access control mechanism solely rely on discretionary access control.

[IC.ACM-2.MAC]: The methods to validate the appropriateness of the access control mechanism solely rely on mandatory access control.

[IC.ACM-2.Generic]: The methods to validate the appropriateness of the access control mechanism do not solely rely on any of the methods described in ACM-2-RBAC, ACM-2-DAC or ACM-2-MAC.

6.1.2.4.3 Required information

[E.Info.ACM-2.SecurityAsset]: Description of each security asset for which ACM-1 requires access control mechanisms, including:

- [E.Info.ACM-2.SecurityAsset.ACM]: Description of each access control mechanism required per ACM-1 that manages entities' access to the security asset and of how the mechanisms ensure that only authorized entities have access to the security asset based on the implementation category.

[E.Info.ACM-2.NetworkAsset]: Description of each network asset for which ACM-1 requires access control mechanisms, including:

- [E.Info.ACM-2.NetworkAsset.ACM]: Description of each access control mechanism required per ACM-1 that manages entities' access to the network asset and of how the mechanisms ensure that only authorized entities have access to the network asset based on the implementation category.

[E.Info.DT.ACM-2]: Description of the selected path through the decision tree in Figure 2 for each security asset documented in [E.Info.ACM-2.SecurityAsset] and network asset documented in [E.Info.ACM-2.NetworkAsset].

[E.Just.DT.ACM-2]: Justification for the selected path through the decision tree documented in [E.Info.DT.ACM-2], with the following property:

- the justification for the decision [DT.ACM-2.DN-1] is based on [E.Info.ACM-2.NetworkAsset.ACM] or [E.Info.ACM-2.SecurityAsset.ACM].

NOTE A justification includes a description of the entities, their access rights on the respective security asset or network asset and means how the access control mechanisms ensure that only authorised access to the respective asset is granted.

6.1.2.4.4 Conceptual assessment

6.1.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the access control mechanisms that are required per ACM-1 are implemented as required per ACM-2.

6.1.2.4.4.2 Preconditions

None.

6.1.2.4.4.3 Assessment units

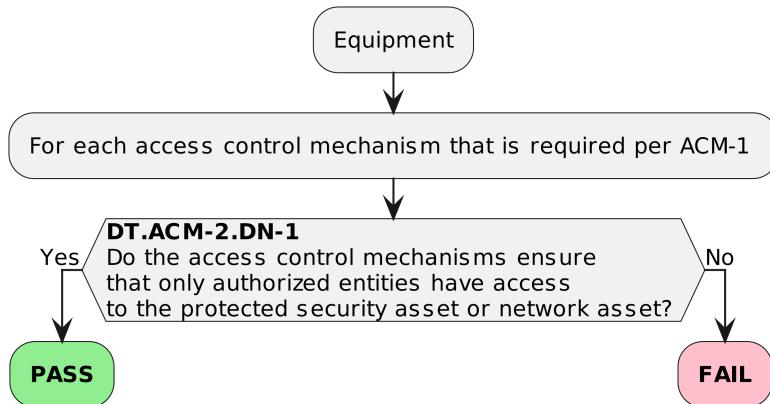


Figure 2 — Decision Tree for requirement ACM-2

For each security asset documented in [E.Info.ACm-2.SecurityAsset] and each network asset documented in [E.Info.ACm-2.NetworkAsset], check whether the path through the decision tree documented in [E.Info.DT.ACm-2] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.ACm-2], examine its justification documented in [E.Just.DT.ACm-2].

6.1.2.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.ACm-2] end with “PASS”; and
- the information provided in [E.Just.DT.ACm-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.ACm-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.ACm-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.ACm-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.ACm-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.1.2.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the access control mechanism’s applicability.

Therefore, the functional completeness assessment in ACM-2 is not necessary.

6.1.2.4.6 Functional sufficiency assessment

6.1.2.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the access control mechanisms are implemented as required per ACM-2.

6.1.2.4.6.2 Assessment units

For each security asset documented in [E.Info.ACM-2.SecurityAsset] and network asset documented in [E.Info.ACM-2.NetworkAsset]:

[AU.ACM-2.RBAC]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.NetworkAsset.ACM] belong to [IC.ACM-2.RBAC], functionally confirm that:

- roles are assigned to each user with associated authorization; and
- least privileges are associated with the roles; and
- the security asset or network asset is only accessible by authorized users given by their role; and
- changes in roles can only be performed by authorized users.

[AU.ACM-2.DAC]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.NetworkAsset.ACM] belong to [IC.ACM-2.DAC], functionally confirm that:

- identities are assigned to each user with associated authorization; and
- least privileges are associated with the identities; and
- the security asset or network asset is only accessible by authorized users given by their identity; and
- changes in identities can only be performed by authorized users.

[AU.ACM-2.MAC]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.NetworkAsset.ACM] belong to [IC.ACM-2.MAC], functionally confirm that:

- the security asset or network asset is only accessible by authorized users after clearance was issued by the operating system and/or system administrator; and
- the issuance of clearance is associated with the principle of least privileges; and
- changing the operating system and/or system administrator that is responsible for the issuance of clearance to the user can only be performed by the authorized system administrator.

[AU.ACM-2.Generic]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.NetworkAsset.ACM] belong to [IC.ACM-2.Generic], functionally confirm that:

- the security asset or network asset is only accessible by authorized users; and
- the principle of least privileges for users is followed; and
- changing settings related to the access control mechanism or changes of privileges of users are only allowed to be performed by authorized users.

6.1.2.4.6.3 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each security asset documented in [E.Info.ACM-2.SecurityAsset] and network asset documented in [E.Info.ACM-2.NetworkAsset] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for any security asset documented in [E.Info.ACM-2.SecurityAsset] or network asset documented in [E.Info.ACM-2.NetworkAsset] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2 [AUM] Authentication mechanism

6.2.1 [AUM-1] Applicability of authentication mechanisms

6.2.1.1 [AUM-1-1] Requirement network interface

Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to:

- read confidential network function configuration or confidential security parameters; or
- modify sensitive network function configuration or sensitive security parameters; or
- use network functions or security functions,

except for access:

- to network functions or network function configuration where the absence of authentication is required for the equipment's intended functionality; or
- via networks where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorised entities.

6.2.1.2 [AUM-1-2] Requirement user interface

Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to:

- read confidential network function configuration or confidential security parameters; or
- modify sensitive network function configuration or sensitive security parameters; or
- use network functions or security functions,

except for access:

- where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorized entities;

and except for read only access to network functions or network functions configuration where access without authentication is needed:

- to enable the intended equipment functionality; or
- because legal implications do not allow for authentication mechanisms.

6.2.1.3 Rationale

The equipment needs to provide an authentication mechanism such that the corresponding access control mechanism prevents unauthorized access from entities which are not who or what they claim to be that may harm the network or misuse network resources.

6.2.1.4 Guidance

Authentication mechanisms might use different layers (e.g., application or network layer) for verifying the validity of entities' claims. The management of associated access rights for entities are addressed by access control mechanisms. There are different kinds of entities that can interact with the equipment, e.g.:

- a specific human, owner of a user account, device, or service; or
- a member of specific groups such as an authorized group to access a specific equipment's resource; or
- authorised by another entity to access a specific equipment's resource.

Typically, the verification of an entity is based on examining evidence from one or more elements of the categories:

- knowledge (something you know); and
- possession (something you have); and
- inherence (something you are).

A trust relation to a network (e.g., an entity owns a shared secret like Wi-Fi credentials) could be used to authenticate an entity.

Authentication might not be needed for all accesses subject to ACM-1 via network interfaces, for instance for protocols that might provide access to security asset or network assets which are intended to be accessible without authentication such as but not limited to DHCP and ICMP messages.

Other examples of access where authentication might not be mandatory are amongst others:

- reading equipment's public IP configuration; or
- reading a public key; or
- reading equipment's public network state.

Examples of physical or logical measures in the targeted environment that provide confidence in the correctness of an entity's claim might be amongst others:

- physical access control that only allows authorized access to the inside of personal road vehicles or watercrafts; or
- physical access control that only allows authorized access e.g., to a WPS button of a home gateway to attach other devices to a Wi-Fi network within a private house.

6.2.1.5 Assessment criteria network interface

6.2.1.5.1 Assessment objective

The assessment addresses the requirement AUM-1-1.

6.2.1.5.2 Implementation categories

Not applicable.

6.2.1.5.3 Required information

[E.Info.AUM-1-1.ACML]: Description of each access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions, including:

- [E.Info.AUM-1-1.ACML.NetworkInterface]: Description of the network interfaces for the managed access; and
- [E.Info.AUM-1-1.ACML.ManagedAccessNetworkAsset]: Description of the managed access to network assets via network interfaces; and
- [E.Info.AUM-1-1.ACML.ManagedAccessSecurityAsset]: Description of the managed access to security assets via network interfaces; and
- (if absence of authentication for access to network functions or network functions configuration via network interfaces is required for the equipment's intended functionality) [E.Info.AUM-1-1.ACML.IntendedFunctionality]: Description of
 - the unauthenticated accessible network functions or network functions configuration; and
 - the equipment's intended functionality; and
 - its properties that require the absence of authentication for access to the network functions or network functions configuration; and
- (if authentication is absent for access via networks where access is limited to authorised entities) [E.Info.AUM-1-1.ACML.TrustedNetwork]: Description the networks and the physical or logical measures in the equipment's targeted operational environment that limit access to authorized entities; and
- (if authentication is required per AUM-1-1) [E.Info.AUM-1-1.ACML.AuthenticationMechanism]: Description of the implemented authentication mechanisms.

[E.Info.DT.AUM-1-1]: Description of the selected path through the decision tree in Figure 3 for each access control mechanism documented in [E.Info.AUM-1-1.ACML].

[E.Just.DT.AUM-1-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-1-1] with the following properties:

- (if a decision from [DT.AUM-1-1.DN-1] results in "NOT APPLICABLE") the justification for the decision [DT.AUM-1-1.DN-1] is based on [E.Info.AUM-1-1.ACML.IntendedFunctionality]; and
- (if a decision from [DT.AUM-1-1.DN-2] results in "NOT APPLICABLE") the justification for the decision [DT.AUM-1-1.DN-2] is based on [E.Info.AUM-1-1.ACML.TrustedNetwork]; and
- the justification for the decision [DT.AUM-1-1.DN-3] is based on [E.Info.AUM-1-1.ACML].

6.2.1.5.4 Conceptual assessment

6.2.1.5.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether an authentication mechanism is implemented when it is required per AUM-1-1.

6.2.1.5.4.2 Preconditions

None.

6.2.1.5.4.3 Assessment units

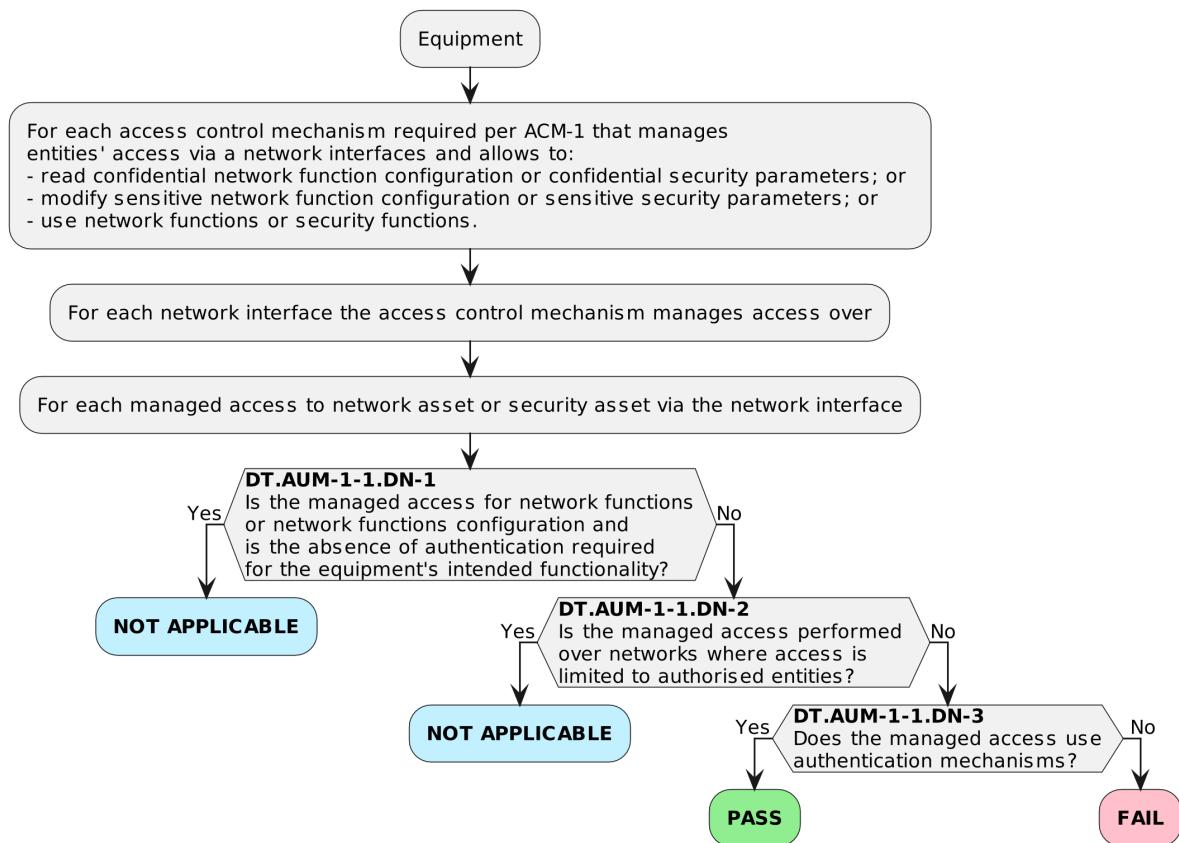


Figure 3 — Decision Tree for requirement AUM-1-1

For each access control mechanism documented in [E.Info.AUM-1-1.AC], check whether the path through the decision tree documented in [E.Info.DT.AUM-1-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-1-1], examine its justification documented in [E.Just.DT.AUM-1-1].

6.2.1.5.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.AUM-1-1] ends with “PASS”; and

- no path through the decision tree documented in [E.Info.DT.AUM-1-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.AUM-1-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-1-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-1-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-1-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-1-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.5.5 Functional completeness assessment

6.2.1.5.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether there are access control mechanisms on the equipment for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions that are not described in [E.Info.AUM-1-1.AC].

6.2.1.5.5.2 Preconditions

The equipment is in an operational state.

6.2.1.5.5.3 Assessment units

Functionally assess whether there are access control mechanisms required per ACM-1 for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions that are not described in [E.Info.AUM-1-1.AC].

6.2.1.5.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions, is found that is not documented in [E.Info.AUM-1-1.AC].

The verdict FAIL for the assessment case is assigned if there is evidence that an access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions, is found that is not documented in [E.Info.AUM-1-1.AC].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.5.6 Functional sufficiency assessment

6.2.1.5.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1-1 are implemented.

6.2.1.5.6.2 Preconditions

The equipment is in an operational state.

6.2.1.5.6.3 Assessment units

For each access control mechanisms documented in [E.Info.AUM-1-1.ACM], each managed access via network interfaces to network assets documented in [E.Info.AUM-1-1.ACM.ManagedAccessNetworkAsset] and each managed access via network interfaces to security assets documented in [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset], access the corresponding security assets or network assets and check whether the authentication mechanism is implemented.

6.2.1.5.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism documented in [E.Info.AUM-1-1.ACM.AuthenticationMechanism] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism documented in [E.Info.AUM-1-1.ACM.AuthenticationMechanism] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.6 Assessment criteria user interface

6.2.1.6.1 Assessment objective

The assessment addresses the requirement AUM-1-2.

6.2.1.6.2 Implementation categories

Not applicable.

6.2.1.6.3 Required information

[E.Info.AUM-1-2.ACM]: Description of each access control mechanism required per ACM-1 for managing entities' access over user interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions, including:

- A description of the user interfaces for the managed access; and
- [E.Info.AUM-1-2.ACM.ManagedAccessNetworkAsset]: Description of the managed access to network assets via user interfaces; and
- [E.Info.AUM-1-2.ACM.ManagedAccessSecurityAsset]: Description of the managed access to security assets via user interfaces; and
- (if physical or logical measures in the targeted environment provide confidence in the correctness of an entity's claim) [E.Info.AUM-1-2.ACM.IntendedEnvironment]: Description of the physical or logical measures in the targeted environment; and

- (if authentication is required per AUM-1-2) [E.Info.AUM-1-2.ACML.AuthenticationMechanism]: Description of the implemented authentication mechanisms; and
- (if authentication is absent for read only access to network functions or network functions configuration where access without authentication is needed to enable the intended equipment functionality) [E.Info.AUM-1-2.ACML.ReadOnlyFunctionality]: Description of the equipment's intended functionality concerning the absence of authentication for read only access to affected assets via user interfaces; and
- (if authentication is absent for read only access to network functions or network functions configuration where legal implications do not allow for authentication mechanisms) [E.Info.AUM-1-2.ACML.ReadOnlyLegal]: References to all corresponding paragraph(s) or passages in all relevant legal documents, including a description on how this is applicable for the equipment or affected asset.

[E.Info.DT.AUM-1-2]: Description of the selected path through the decision tree in Figure 4 for each access control mechanism documented in [E.Info.AUM-1-2.ACML].

[E.Just.DT.AUM-1-2]: Justification for the path through the decision tree documented in [E.Info.DT.AUM-1-2] with the following properties:

- (if decision from [DT.AUM-1-2.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.AUM-1-2.DN-1] is based on [E.Info.AUM-1-2.ACML.IntendedEnvironment]; and
- (if decision from [DT.AUM-1-2.DN-2] results in “NOT APPLICABLE”) the justification for the decision [DT.AUM-1-2.DN-2] is based on [E.Info.AUM-1-2.ACML.ReadOnlyFunctionality]; and
- (if decision from [DT.AUM-1-2.DN-3] results in “NOT APPLICABLE”) the justification for the decision [DT.AUM-1-2.DN-3] is based on [E.Info.AUM-1-2.ACML.ReadOnlyLegal]; and
- the justification for the decision [DT.AUM-1-2.DN-4] is based on [E.Info.AUM-1-2.ACML].

6.2.1.6.4 Conceptual assessment

6.2.1.6.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether an authentication mechanism is implemented when it is required per AUM-1-2.

6.2.1.6.4.2 Preconditions

None.

6.2.1.6.4.3 Assessment units

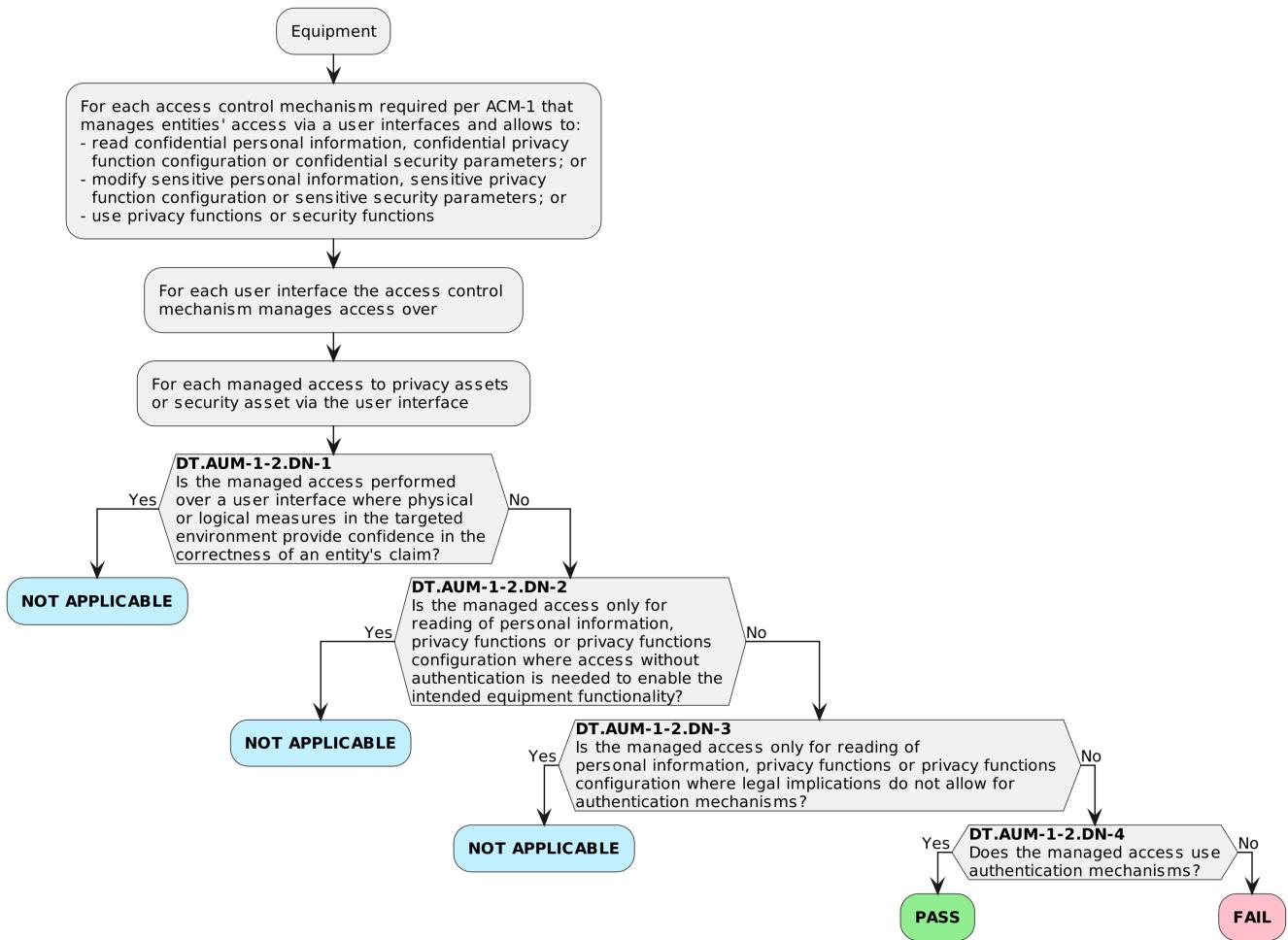


Figure 4 — Decision Tree for requirement AUM-1-2

For each access control mechanism documented in [E.Info.AUM-1-2.ACM], check whether the path through the decision tree documented in [E.Info.DT.AUM-1-2] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-1-2], examine its justification documented in [E.Just.DT.AUM-1-2].

6.2.1.6.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.AUM-1-2] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.AUM-1-2] ends with “FAIL”; and
- the information provided in [E.Just.DT.AUM-1-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-1-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-1-2] ends with “FAIL”; or

- a justification provided in [E.Just.DT.AUM-1-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-1-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.6.5 Functional completeness assessment

6.2.1.6.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether there are access control mechanisms on the equipment for managing entities' access over user interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions that are not described in [E.Info.AUM-1-2.AC].

6.2.1.6.5.2 Preconditions

The equipment is in an operational state.

6.2.1.6.5.3 Assessment units

Functionally assess whether there are access control mechanisms required per ACM-1 for managing entities' access over user interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions that are not described in [E.Info.AUM-1-2.AC].

6.2.1.6.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an access control mechanism required per ACM-1 for managing entities' access over user interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions, is found that is not documented in [E.Info.AUM-1-2.AC].

The verdict FAIL for the assessment case is assigned if there is evidence that an access control mechanism required per ACM-1 for managing entities' access over user interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions, is found that is not documented in [E.Info.AUM-1-2.AC].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.1.6.6 Functional sufficiency assessment

6.2.1.6.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1-2 are implemented.

6.2.1.6.6.2 Preconditions

The equipment is in an operational state.

6.2.1.6.6.3 Assessment units

For each access control mechanism documented in [E.Info.AUM-1-2.ACML], each managed access via user interfaces to network assets documented in [E.Info.AUM-1-2.ACML.ManagedAccessNetworkAsset] and each managed access via user interfaces to security assets documented in [E.Info.AUM-1-2.ACML.ManagedAccessSecurityAsset], access the corresponding security assets and network assets and check whether the authentication mechanism is implemented.

6.2.1.6.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism documented in [E.Info.AUM-1-2.ACML.AuthenticationMechanism] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism documented in [E.Info.AUM-1-2.ACML.AuthenticationMechanism] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.2 [AUM-2] Appropriate authentication mechanisms

6.2.2.1 Requirement

Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity's claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication).

6.2.2.2 Rationale

One factor authentication is suitable to protect the network resources of an equipment against misuse, e.g., as part of a DoS attack.

6.2.2.3 Guidance

Examples for a verification of an entity's claim based on examining evidence from one element of the categories, knowledge, possession, and inherence, are:

- PIN-Code used for user interface
- 1-Factor (e.g., password based) of each incoming connection on a user or network interface
- fingerprint biometrics or face recognition for a user interface
- verifying the possession of a private key that matches to a trusted certificate
- trust relation to a network (e.g., based on a common secret) established at on-boarding.

Considering possible constraints of human users with disabilities is an important aspect for implementing appropriate authentication mechanisms. Examples of considerations when selecting authentication mechanisms include:

- transferring the authentication information to and from a relevant assistive technology,
- enabling a dual or shared use when the equipment is in use by a user and a support worker (and/or parent and child),
- offering alternative authentication mechanisms so that they are useable by a user with specific learning impairments (including dyslexia) and do not trigger negative feelings (e.g.,

by avoiding specifying family or personal information which may be distressing or not relevant for the end user).

At the time of publishing the present document long passwords like "WeihnachtsmarkTElephanTCarpeT@Bon(n)" are considered stronger passwords than short passwords like "P@ssw0rd!" and more guidance on current best practice on passwords can be found in NIST Special Publication 800-63B [9], ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], IEC EN 62443-4-2 [2] and ETSI EN 303 645 [5].

6.2.2.4 Assessment criteria

6.2.2.4.1 Assessment objective

The assessment addresses the requirement AUM-2.

6.2.2.4.2 Implementation categories

Not applicable.

6.2.2.4.3 Required information

[E.Info.AUM-2.AuthenticationMechanism]: Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface) including:

- [E.Info.AUM-2.AuthenticationMechanism.AuthFactor]: Description of the authenticator.

[E.Info.DT.AUM-2]: Description of the selected path through the decision tree in Figure 5 for each authentication mechanism that is documented in [E.Info.AUM-2.AuthenticationMechanism].

[E.Just.DT.AUM-2]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-2] with the following property:

- the justification for the decision [DT.AUM-2.DN-1] is based on [E.Info.AUM-2.AuthenticationMechanism.AuthFactor].

6.2.2.4.4 Conceptual assessment

6.2.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) are implemented as required per AUM-2.

6.2.2.4.4.2 Preconditions

None.

6.2.2.4.4.3 Assessment units

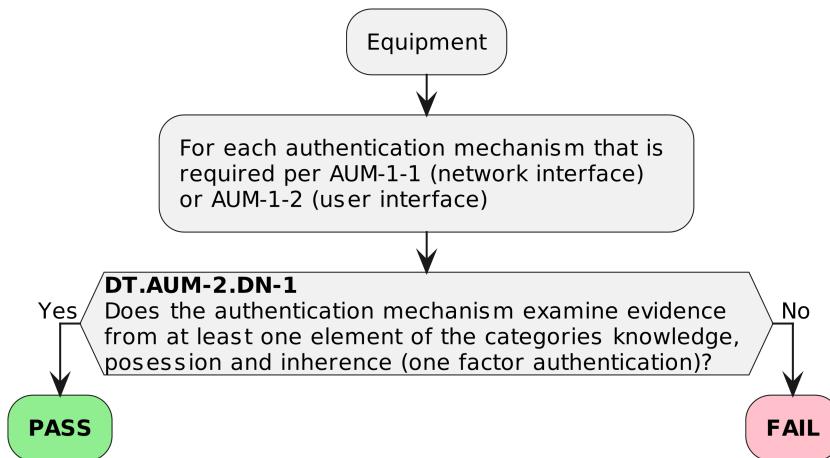


Figure 5 — Decision Tree for requirement AUM-2

For each authentication mechanism that is required per AUM-1-1 (network interface) or AUM-1-2 (user interface) documented in [E.Info.AUM-2.AuthenticationMechanism], check whether the path through the decision tree documented in [E.Info.DT.AUM-2] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-2], examine its justification documented in [E.Just.DT.AUM-2].

6.2.2.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-2] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.2.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.2.4.6 Functional sufficiency assessment

6.2.2.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) are implemented as documented.

6.2.2.4.6.2 Preconditions

The equipment is in an operational state.

6.2.2.4.6.3 Assessment units

For each authentication mechanism that is required per AUM-1-1 (network interface) or AUM-1-2 (user interface) documented in [E.Info.AUM-2.AuthenticationMechanism] perform an authentication and check whether the authentication mechanism is implemented as documented.

6.2.2.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an authentication mechanism's implementation deviates from [E.Info.AUM-2.AuthenticationMechanism].

The verdict FAIL for the assessment case is assigned if there is evidence that an authentication mechanism's implementation deviates from [E.Info.AUM-2.AuthenticationMechanism].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.3 [AUM-3] Authenticator validation

6.2.3.1 Requirement

Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use.

6.2.3.2 Rationale

Even when the equipment provides an authentication mechanism, the risk is given that an attacker uses typical design weaknesses to overcome it. The usage of forged or partially forged authenticators are often used for an attack against such a mechanism. Therefore, the security design of the mechanisms needs techniques to resist forged authenticators, for example manipulated PKI certificates.

6.2.3.3 Guidance

The authenticator and its attributes vary, depending on the authentication mechanism. For the validation of the authenticator, best practice ought to be applied for the corresponding authentication mechanism. This is necessary in order to detect and prevent the use of an authenticator that is invalid. For example, if the equipment only validates the common name of a PKI certificate without further validation of the complete certification information, then a correspondingly forged authenticator would be accepted. In this example, the relevant properties of the authenticator are the signatures and public keys of the trust chain, the revocation status and in many cases also the validity period of the certificate. The set of relevant properties can differ depending on whether the equipment is actually internet connected or not. For example, offline equipment probably does not have access to a reliable time source or to certificate revocation information.

Another example for insufficient validation of authenticators is, if only parts of the password is checked. This would weaken the strength of the password, facilitating brute force attacks on the corresponding authentication mechanism.

6.2.3.4 Assessment criteria

6.2.3.4.1 Assessment objective

The assessment addresses the requirement AUM-3.

6.2.3.4.2 Implementation categories

[IC.AUM-3.Password]: The authenticator is a password.

[IC.AUM-3.CertificatePrivateKey]: The authenticator is a private key associated to a certificate trusted by the equipment.

NOTE A certificate can be trusted by the equipment for example via a chain of trust to a preinstalled root certificate of a PKI or by certificate pinning.

[IC.AUM-3.Generic]: The authenticator is different from [IC.AUM-3.Password] or [IC.AUM-3.CertificatePrivateKey].

EXAMPLE Biometrics, Secure Shell (SSH) keys, symmetric keys

6.2.3.4.3 Required information

[E.Info.AUM-3.AUM]: Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface), including:

- [E.Info.AUM-3.AUM.AuthVal]: Description how the validation of the authenticator is performed including its implementation category and the relevant properties; and
- [E.Info.AUM-3.AUM.AuthEnv]: Description of the available information about the authenticator in the operational environment of use.

[E.Info.DT.AUM-3]: Description of the selected path through the decision tree in Figure 6 for each authentication mechanism that is documented in [E.Info.AUM-3.AUM].

[E.Just.DT.AUM-3]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-3] with the following property:

- the justification for the decision [DT.AUM-3.DN-1] is based on [E.Info.AUM-3.AUM.AuthVal] and [E.Info.AUM-3.AUM.AuthEnv].

6.2.3.4.4 Conceptual assessment

6.2.3.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms validate all relevant properties of the authenticator as documented in [E.Info.AUM-3.AUM]. This assessment is conducted on each path to security assets and/or network assets required by AUM-1-1 or AUM-1-2.

6.2.3.4.4.2 Preconditions

None.

6.2.3.4.4.3 Assessment units

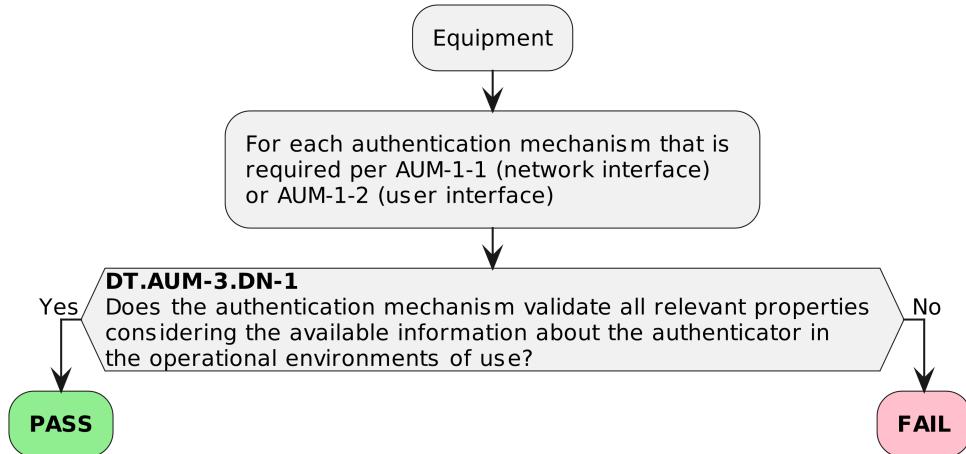


Figure 6 — Decision Tree for requirement AUM-3

For each authentication mechanism documented in [E.Info.AUM-3.AUM], check whether the path through the decision tree documented in [E.Info.DT.AUM-3] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-3], examine its justification documented in [E.Just.DT.AUM-3].

6.2.3.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-3] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.3.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.3.4.6 Functional sufficiency assessment

6.2.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the authentication mechanism required per AUM-1-1 or AUM-1-2 validates all required properties.

6.2.3.4.6.2 Preconditions

The equipment is in an operational state.

6.2.3.4.6.3 Assessment units

For each authentication mechanism documented in [E.Info.AUM-3.AUM]:

[AU.AUM-3.Password]: If the authenticator belongs to [IC.AUM-3.Password], functionally confirm the validation of the relevant properties of the authenticator documented in [E.Info.AUM-3.AUM.AuthVal] by examining whether:

- incorrect passwords can be used for successful authentication; and
- (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of an recorded successful authentication attempt can be used for successful authentication; and
- parts of the correct password can be used for authentication; and
- (if different user accounts exist or can be created) passwords of other entities can be used for authentication.

[AU.AUM-3.CertificatePrivateKey]: If the authenticator belongs to [IC.AUM-3.CertificatePrivateKey], functionally confirm the validation of the relevant properties of the authenticator documented in [E.Info.AUM-3.AUM.AuthVal] by examining whether:

- incorrect private keys to a trusted certificate can be used for successful authentication; and
- (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of an recorded successful authentication attempt can be used for successful authentication; and
- valid private keys to untrusted or invalid certificates can be used for successful authentication; and

NOTE untrusted or invalid certificates can be certificates revoked by the certificate authority, expired certificates, certificates with an invalid chain of trust e.g., generated by an untrusted entity containing an expected "Common Name" (CN) entry.

- (if different user accounts exist or can be created) private keys to a trusted certificate of other entities can be used for authentication.

[AU.AUM-3.Generic]: If the authenticator belongs to [IC.AUM-3.Generic], functionally confirm the validation of the relevant properties of the authenticator documented in [E.Info.AUM-3.AUM.AuthVal] by examining whether:

- incorrect authenticators can be used for successful authentication; and
- (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of an recorded successful authentication attempt can be used for successful authentication; and
- (if different user accounts exist or can be created) authenticators of other entities can be used for authentication.

6.2.3.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each authentication mechanism documented in [E.Info.AUM-3.AUM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for an authentication mechanism documented in [E.Info.AUM-3.AUM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.4 [AUM-4] Changing authenticators

6.2.4.1 Requirement

Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change.

6.2.4.2 Rationale

Static authenticators can be a security risk for the equipment, e.g., increased vulnerability to brute force and eavesdropping attacks. Therefore, the support for changing authenticators on the equipment is needed as a countermeasure.

6.2.4.3 Guidance

An authorised entity needs the possibility to change the authenticator. The procedure can vary depending on the authentication mechanism used:

- the equipment provides a functionality to the authorised entity, e.g., user, to change the authenticator on the equipment; or
- the authenticator, e.g., token, is renewed or changed by the manufacturer and the equipment accepts the changed authenticator because the trust chain is still valid; or
- the authenticator is updated using a secure update mechanism.

In case of machine interfaces new pairing can be necessary. The integration of the change of the authenticator in the normal workflow simplifies the procedure for the user. This procedure depends on the selected authenticator (e.g., fingerprint, password, or token)

There can be use cases, where a static authenticator is acceptable, such as a root of trust where the confidentiality of the corresponding cryptographic key is ensured by the manufacturer. In such an example the manufacturer typically provides tokens to authorized entities that are all linked to the same root of trust.

There can also be exceptions, where the overall risk of changing an authenticator, e.g., due to complexity, outweighs the risk associated with the security assets or network assets when using static authenticators. In such cases, it's important to consider best practice security design principles to minimize the risk associated with the static authenticator, for example, by avoiding the use of global authenticators.

Depending on the intended equipment functionality it might be needed to ensure the availability of the equipment functionality due a deferral option, e.g., not forcing the update of a password whilst driving a car.

6.2.4.4 Assessment criteria

6.2.4.4.1 Assessment objective

The assessment addresses the requirement AUM-4.

6.2.4.4.2 Implementation categories

Not applicable.

6.2.4.4.3 Required information

[E.Info.AUM-4.AUM]: Description of each authentication mechanism required by AUM-1-1 (network interface) or AUM-1-2 (user interface), including:

- (if conflicting security goals do not allow for a change) [E.Info.AUM-4.AUM.ConfSecGoals]: Description of the conflicting security goals from the security concept of the equipment concerning the change of the authenticator.[E.Info.AUM-4.AUM.AuthChange]: Description for each authentication mechanism documented in [E.Info.AUM-4.AUM] how the change of the authenticator is performed under consideration of the security concept of the equipment.

[E.Info.DT.AUM-4]: Description of the selected path through the decision tree in Figure 7 for each authenticator change functionality documented in [E.Info.AUM-4.AUM.AuthChange].

[E.Just.DT.AUM-4]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-4] with the following properties:

- the justification for the decision [DT.AUM-4.DN-1] is based on [E.Info.AUM-4.AUM.ConfSecGoals]; and
- the justification for the decision [DT.AUM-4.DN-2] is based on [E.Info.AUM-4.AUM.AuthChange].

6.2.4.4.4 Conceptual assessment

6.2.4.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authenticator used by the authentication mechanisms documented in [E.Info.AUM-4.AUM] can be changed.

6.2.4.4.4.2 Preconditions

None.

6.2.4.4.3 Assessment units

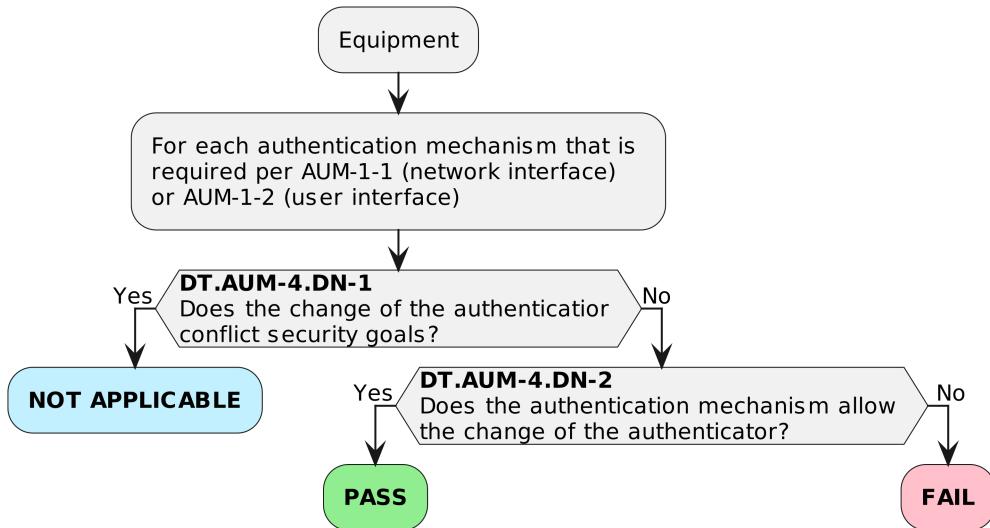


Figure 7 — Decision Tree for requirement AUM-4

For each authenticator change functionality documented in [E.Info.AUM-4.AUM], check whether the path through the decision tree documented in [E.Info.DT.AUM-4] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-4], examine its justification documented in [E.Just.DT.AUM-4].

6.2.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.AUM-4] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.AUM-4] ends with “FAIL”; and
- the information provided in [E.Just.DT.AUM-4] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-4].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-4] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-4] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-4].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.4.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.4.4.6 Functional sufficiency assessment

6.2.4.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) allow for changing the authenticator as documented in [E.Info.AUM-4.AUM.AuthChange].

6.2.4.4.6.2 Preconditions

The equipment is in an operational state.

6.2.4.4.6.3 Assessment units

For each authentication mechanism that is required per AUM-1-1 (network interface) or AUM-1-2 (user interface) documented in [E.Info.AUM-4.AUM], functionally confirm the ability to change authenticator as documented in [E.Info.AUM-4.AUM.AuthChange] by

- checking whether the newly assigned authenticator grants access on each path to security assets and/or network assets; and
- checking whether the previous authenticator does no longer grant access on any path to security assets and/or network assets

after changing the authenticator.

6.2.4.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an implementation of changing an authenticator deviates from [E.Info.AUM-4.AUM.AuthChange].

The verdict FAIL for the assessment case is assigned if there is evidence that an implementation of changing an authenticator deviates from [E.Info.AUM-4.AUM.AuthChange].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.5 [AUM-5] Password strength

6.2.5.1 [AUM-5-1] Requirement for factory default passwords

If factory default passwords are used by an authentication mechanism that is required per AUM-1-1 or AUM-1-2, they shall:

- be unique per equipment; and
- follow best practice concerning strength;

or

- be enforced to be changed by the user before or on first use.

NOTE The user may choose to not use any password.

6.2.5.2 [AUM-5-2] Requirement for non-factory default passwords

If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall:

- be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or
- be defined by an authorized entity within a network where access is limited to authorised entities; or
- be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.

NOTE The user may choose to not use any password.

6.2.5.3 Rationale

Weak passwords like universal passwords represent one of the most exploited attack vectors for equipment. There is a wide range of malware that uses such passwords to automatically compromise equipment. Hence, it is imperative to enforce distinct passwords when set at the factory or user/entity-defined passwords for each piece of equipment during their initial setup.

6.2.5.4 Guidance

There are a variety of techniques to avoid universal passwords, examples are:

- The equipment password for the factory default state is printed on a sticker under the equipment casing. The password is created by using a True Random Number Generator or another cryptographically secure pseudorandom number generator (CSPRNG) implementation.
- The equipment prompts a user to create a password on the first use.

It is highly recommended to follow well established standards for the secure generation of random numbers used to generate secure passwords. There are numerous well-recognised publicly available standards for random number generation mechanisms which have undergone peer review. Well established examples for such standards are NIST SP800-90A[11], NIST SP800-90B[12], NIST SP800-90C[13], BSI AIS31[19].

Guidance on best practice on passwords can be found in NIST Special Publication 800-63B [9], ISO/IEC EN 27002:2022 [3], ISO/IEC EN 24760 [4], IEC EN 62443-4-2 [2] and ETSI EN 303 645 [5]

Unique relates to not systematically reused or deducible for another equipment of the same product type and cannot be easily derived from equipment properties (e.g., manufacturer name, model name or Media Access Control (MAC) address). Established random generator can be used to generate practically unique passwords.

When enforcing a password change, safety aspects are also relevant, such as not forcing a password change while driving a car.

6.2.5.5 Assessment criteria for factory default passwords

6.2.5.5.1 Assessment objective

The assessment addresses the requirement AUM-5-1.

6.2.5.5.2 Implementation Categories

[IC.AUM-5-1.UniqueBestPractice]: The user is not enforced to change a factory default password on or before first use and a password is unique per equipment and follows best practice concerning strength.

[IC.AUM-5-1.EnforceSettingFirstUse]: The user is enforced to change a factory default password on or before first use.

6.2.5.5.3 Required information

[E.Info.AUM-5-1.AUM]: Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface) that uses factory default passwords, including:

- [E.Info.AUM-5-1.AUM.PwdProperty]: Description for each authentication mechanism's factory default password:
 - (if the implementation is based on [IC.AUM-5-1.UniqueBestPractice]) of how uniqueness and best practice concerning password strengths is implemented for the password with regard to the underlying use case of the authentication; and
 - (if the implementation is based on [IC.AUM-5-1.EnforceSettingFirstUse]) of how the change of the password is enforced on or before first use.

[E.Info.DT.AUM-5-1]: Description of the selected path through the decision tree in Figure 8 for each authentication mechanism that is documented in [E.Info.AUM-5-1.AUM].

[E.Just.DT.AUM-5-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-5-1] with the following properties:

- the justification for the decisions [DT.AUM-5-1.DN-1], [DT.AUM-5-1.DN-2] and [DT.AUM-5-1.DN-3] are based on [E.Info.AUM-5-1.AUM.PwdProperty].

6.2.5.5.4 Conceptual assessment

6.2.5.5.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 are implemented as required per AUM-5-1.

6.2.5.5.4.2 Preconditions

None.

6.2.5.5.4.3 Assessment units

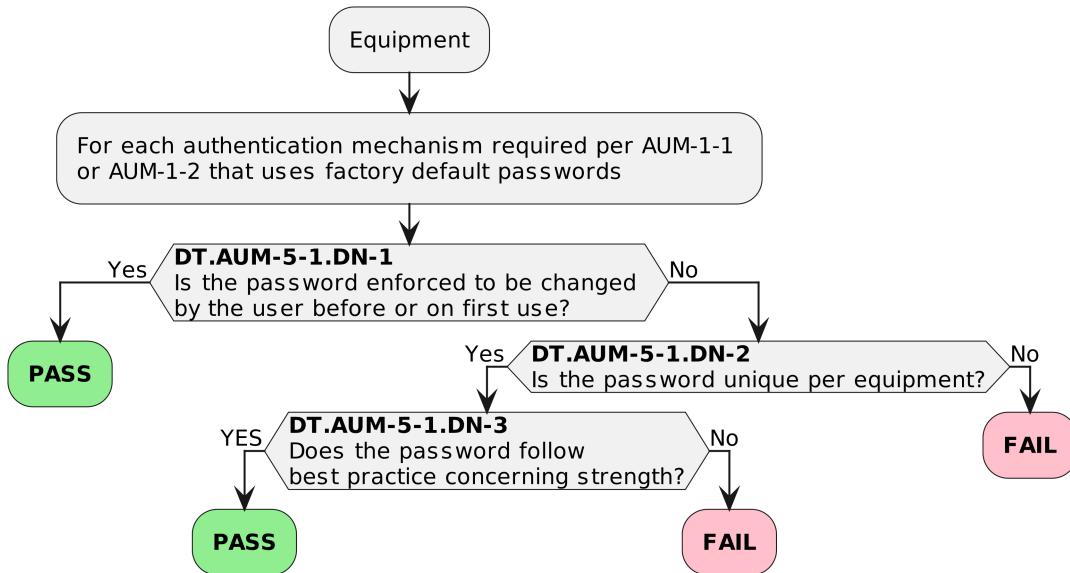


Figure 8 — Decision Tree for requirement AUM-5-1

For each authentication mechanism documented in [E.Info.AUM-5-1.AUM], check whether the path through the decision tree documented in [E.Info.DT.AUM-5-1] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-5-1], examine its justification documented in [E.Just.DT.AUM-5-1].

6.2.5.5.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-5-1] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-5-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-5-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-5-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-5-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-5-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.5.5.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.5.5.6 Functional sufficiency assessment

6.2.5.5.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 are implemented as required per AUM-5-1.

6.2.5.5.6.2 Preconditions

The equipment is in the factory default state and not commissioned.

(If the method documented in [E.Info.AUM-5-1.AUM.PwdProperty] belongs to [IC.AUM-5-1.UniqueBestPractice]) The equipment's actual factory default password is available.

6.2.5.5.6.3 Assessment units

For each authentication mechanism documented in [E.Info.AUM-5-1.AUM]:

[AU.AUM-5-1.UniqueBestPractice]:

If the method documented in [E.Info.AUM-5-1.AUM.PwdProperty] belongs to [IC.AUM-5-1.UniqueBestPractice], functionally confirm the implementation of the methods documented in [E.Info.AUM-5-1.AUM.PwdProperty] by:

- comparing the actual factory default passwords with the description of the implementation provided in [E.Info.AUM-5-1.AUM.PwdProperty]; and
- putting the equipment into service according to the installation instructions and verifying that the actual factory default passwords are valid.

[AU.AUM-5-1.EnforceSettingFirstUse]:

If the method documented in [E.Info.AUM-5-1.AUM.PwdProperty] belongs to [IC.AUM-5-1.EnforceSettingFirstUse]), functionally confirm the implementation of the methods documented in [E.Info.AUM-5-1.AUM.PwdProperty] by:

- putting the equipment into service according to the installation instructions; and
- using the factory default passwords.

6.2.5.5.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an implementation of an authentication mechanism's factory default password deviates from [E.Info.AUM-5-1.AUM.PwdProperty].

The verdict FAIL for the assessment case is assigned if there is evidence that an implementation of an authentication mechanism's factory default password deviates from [E.Info.AUM-5-1.AUM.PwdProperty].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.5.6 Assessment criteria for non-factory default passwords

6.2.5.6.1 Assessment objective

The assessment addresses the requirement AUM-5-2.

6.2.5.6.2 Implementation Categories

[IC.AUM-5-2.SettingFirstUse]: The user is enforced to set a non-factory default password on or before first use before the equipment is logically connected to a network.

[IC.AUM-5-2.DefinedAuthEntity]: An authorized entity defines a non-factory default password within a network where access is limited to authorised entities.

[IC.AUM-5-2.EquipmentGenerated]: A non-factory default password is generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.

6.2.5.6.3 Required information

[E.Info.AUM-5-2.AUM]: Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface) that uses non-factory default passwords, including:

- [E.Info.AUM-5-2.AUM.PwdProperty]: Description for each authentication mechanism's non-factory default password:
 - (if the implementation is based on [IC.AUM-5-2.SettingFirstUse]) of how the setting of the password is enforced and the means to prevent logical network connection before setting the password; and
 - (if the implementation is based on [IC.AUM-5-2.DefinedAuthEntity]) of how the definition of the password is restricted to authorized entities and the means to prevent their definition within a network where access is not limited to authorised entities; and
 - (if the implementation is based on [IC.AUM-5-2.EquipmentGenerated]) of how best practice concerning password strengths is implemented with regard to the underlying use case of the authentication and the means to prevent their communication to unauthorized entities or within a network where access is not limited to authorised entities.

[E.Info.DT.AUM-5-2]: Description of the selected path through the decision tree in Figure 9 for each authentication mechanism that is documented in [E.Info.AUM-5-2.AUM].

[E.Just.DT.AUM-5-2]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-5-2] with the following property:

- the justification for the decisions [DT.AUM-5-2.DN-1], [DT.AUM-5-2.DN-2] and [DT.AUM-5-2.DN-3] are based on [E.Info.AUM-5-2.AUM.PwdProperty].

6.2.5.6.4 Conceptual assessment

6.2.5.6.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 are implemented as required per AUM-5-2.

6.2.5.6.4.2 Preconditions

None.

6.2.5.6.4.3 Assessment units

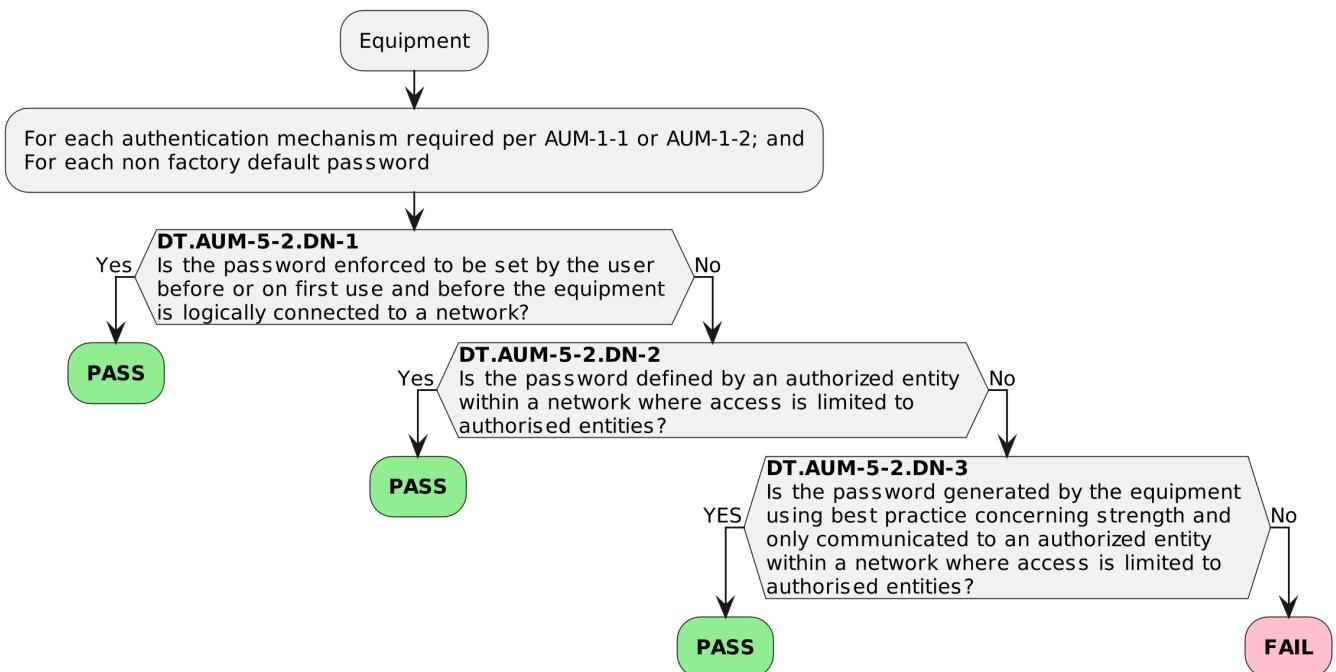


Figure 9 — Decision Tree for requirement AUM-5-2

For each authentication mechanism documented in [E.Info.AUM-5-2.AUM], check whether the path through the decision tree documented in [E.Info.DT.AUM-5-2] ends with "PASS".

For each path through the decision tree documented in [E.Info.DT.AUM-5-2], examine its justification documented in [E.Info.DT.AUM-5-2].

6.2.5.6.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-5-2] end with "PASS"; and
- the information provided in [E.Just.DT.AUM-5-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-5-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-5-2] ends with "FAIL"; or
- a justification provided in [E.Just.DT.AUM-5-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-5-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.5.6.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.5.6.6 Functional sufficiency assessment

6.2.5.6.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 are implemented as required per AUM-5-2.

6.2.5.6.6.2 Preconditions

The equipment is in the factory default state and not commissioned.

6.2.5.6.6.3 Assessment units

For each authentication mechanism documented in [E.Info.AUM-5-2.AUM]:

[AU.AUM-5-2.SettingFirstUse]: If the method documented in [E.Info.AUM-5-2.AUM.PwdProperty] belongs to [IC.AUM-5-2.SettingFirstUse], functionally confirm the implementation of the methods documented in [E.Info.AUM-5-2.AUM.PwdProperty] by:

- observing the equipment's network's logical connectivity; and
- putting the equipment into service according to the installation instructions; and
- using non-factory default passwords.

[AU.AUM-5-2.DefinedAuthEntity]: If the method documented in [E.Info.AUM-5-2.AUM.PwdProperty] belongs to [IC.AUM-5-2.DefinedAuthEntity], functionally confirm the implementation of the methods documented in [E.Info.AUM-5-2.AUM.PwdProperty] by:

- putting the equipment into service according to the installation instructions; and
- (if the equipment can connect to network where access is not limited to authorised entities) defining the non-factory default passwords as an authorized entity via a network where access is not limited to authorised entities; and
- defining the non-factory default passwords as an unauthorized entity; and
- defining the non-factory default passwords as an authorized entity via a network where access is limited to authorised entities or via a non-network interface.

[AU.AUM-5-2.EquipmentGenerated]: If the method documented in [E.Info.AUM-5-2.AUM.PwdProperty] belongs to [IC.AUM-5-2.EquipmentGenerated], functionally confirm the implementation of the methods documented in [E.Info.AUM-5-2.AUM.PwdProperty] by:

- putting the equipment into service according to the installation instructions; and
- initialising the generation of passwords; and
- receiving the password as unauthorized entity; and
- (if the equipment can connect to network where access is not limited to authorised entities) receiving the password as authorized entity via a network where access is not limited to authorised entities; and
- defining the non-factory default passwords as an authorized entity via a network where access is limited to authorised entities or via a non-network interface; and

- comparing the generated passwords with the description of the implementation provided in [E.Info.AUM-5-2.AUM.PwdProperty].

6.2.5.6.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an implementation of an authentication mechanism's non-factory default password deviates from [E.Info.AUM-5-2.AUM.PwdProperty].

The verdict FAIL for the assessment case is assigned if there is evidence that an implementation of an authentication mechanism's non-factory default password deviates from [E.Info.AUM-5-2.AUM.PwdProperty].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.6 [AUM-6] Brute force protection

6.2.6.1 Requirement

Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks.

6.2.6.2 Rationale

An attacker can try to use mass authentication attempts to overcome an authentication mechanism or to impact equipment availability. Therefore, techniques are required to mitigate the impact of such an attack.

6.2.6.3 Guidance

Techniques for brute force protection of authentication mechanisms include e.g.:

- Time delays between consecutive failed attempts to authenticate;
- A limited number of failed authentication attempts followed by a suspension period where no login is allowed;
- Multi-factor authentication;
- Appropriate strength for authentication values based on best practice cryptography;
- Machine-to-machine authentication might implement mitigation measures such as:
 - long password (more than 16 characters and high complexity);
 - list of allowed IP addresses;
 - warning/logging mechanism in machine-to-machine interface.
- Depending on the implemented techniques, related risks concerning "resource exhaustion" and "denial of service" need to be considered.

Consideration is to be given to mitigating the impact of repeated attempts to gain illegitimate authentication and mitigate the blocking of legitimate access by triggering the preceding defence mechanism.

See NIST 800-63 series [8].

6.2.6.4 Assessment criteria

6.2.6.4.1 Assessment objective

The assessment addresses the requirement AUM-6.

6.2.6.4.2 Implementation Categories

[IC.AUM-6.TimeDelay]: The methods for resilience against brute force attacks rely on time delays between authentication attempts.

[IC.AUM-6.LimitedAttempts]: The methods for resilience against brute force attacks rely on a limited number of authentication attempts.

[IC.AUM-6.AuthenticatorComplexity]: The methods for resilience against brute force attacks rely on authenticator complexity.

EXAMPLE mandatory multi factor authentication, enforce CCKs with a minimum-security strength of 112-bits

[IC.AUM-6.Generic]: The methods for resilience against brute force attacks rely on methods other than [IC.AUM-6.TimeDelay], [IC.AUM-6.LimitedAttempts] or [IC.AUM-6.AuthenticatorComplexity].

6.2.6.4.3 Required information

[E.Info.AUM-6.AUM]: Description of each authentication mechanism required per AUM-1-1 (network interface) or AUM-1-2 (user interface), including:

- [E.Info.AUM-6.AUM.BFProtection]: Description how the resilience against brute force attacks is ensured, considering the implementation categories.

[E.Info.DT.AUM-6]: Description of the selected path through the decision tree in Figure 10 for each authentication mechanism that is documented in [E.Info.AUM-6.AUM].

[E.Just.DT.AUM-6]: Justification for the selected path through the decision tree documented in [E.Info.DT.AUM-6] with the following properties:

- the justification for the decision [DT.AUM-6.DN-1] is based on [E.Info.AUM-6.AUM.BFProtection].

6.2.6.4.4 Conceptual assessment

6.2.6.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 have the capability as required by AUM-6.

6.2.6.4.4.2 Preconditions

None.

6.2.6.4.3 Assessment units

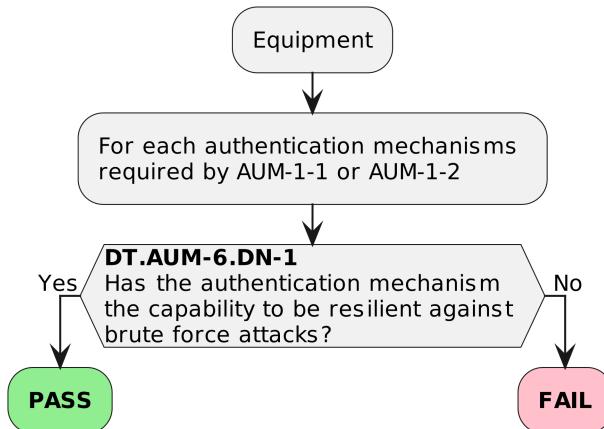


Figure 10 — Decision Tree for requirement AUM-6

For each authentication mechanism documented in [E.Info.AUM-6.AUM], check whether the path through the decision tree documented in [E.Info.DT.AUM-6] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.AUM-6], examine its justification documented in [E.Just.DT.AUM-6].

6.2.6.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.AUM-6] end with “PASS”; and
- the information provided in [E.Just.DT.AUM-6] are correct justifications for all paths through the decision tree documented in [E.Info.DT.AUM-6].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.AUM-6] ends with “FAIL”; or
- a justification provided in [E.Just.DT.AUM-6] is not correct or missing for a path through the decision tree documented in [E.Info.DT.AUM-6].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.2.6.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.2.6.4.6 Functional sufficiency assessment

6.2.6.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 comply with the requirement for AUM-6.

6.2.6.4.6.2 Preconditions

The equipment is in an operational state.

6.2.6.4.6.3 Assessment units

For each authentication mechanism documented in [E.Info.AUM-6.AUM]:

[AU.AUM-6.TimeDelay]: If the method documented in [E.Info.AUM-6.AUM.BFProtection] belongs to [IC.AUM-6.TimeDelay], functionally confirm the implementation of the methods documented in [E.Info.AUM-6.AUM.BFProtection] by:

- repeatedly performing authentication attempts using erroneous authenticators; and
- measuring the time delays enforced by the equipment between consecutive failed attempts.

[AU.AUM-6.LimitedAttempts]: If the method documented in [E.Info.AUM-6.AUM.BFProtection] belongs to [IC.AUM-6.LimitedAttempts], functionally confirm the implementation of the methods documented in [E.Info.AUM-6.AUM.BFProtection] by:

- repeatedly performing authentication attempts using erroneous authenticators; and
- counting the number consecutive failed attempts before the equipment prevents further attempts.

[AU.AUM-6.AuthenticatorComplexity]: If the method documented in [E.Info.AUM-6.AUM.BFProtection] belongs to [IC.AUM-6.AuthenticatorComplexity], functionally confirm the implementation of the methods documented in [E.Info.AUM-6.AUM.BFProtection] by:

- trying to assign an authenticator that does not meet the complexity criteria documented in [E.Info.AUM-6.AUM.BFProtection]; and
- performing a brute force attack on the authentication mechanism.

[AU.AUM-6.Generic]: If the method documented in [E.Info.AUM-6.AUM.BFProtection] belongs to [IC.AUM-6.Generic], functionally confirm the implementation of the methods documented in [E.Info.AUM-6.AUM.BFProtection] by:

- performing a brute force attack on the authentication mechanism.

6.2.6.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each authentication mechanism documented in [E.Info.AUM-6.AUM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for an authentication mechanism documented in [E.Info.AUM-6.AUM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.3 [SUM] Secure update mechanism

6.3.1 [SUM-1] Applicability of update mechanisms

6.3.1.1 Requirement

The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or network assets, except for software:

- where functional safety implications do not allow updatability; or
- which is immutable; or
- where alternative measures protect the affected security assets and/or network assets during the entire lifecycle of the equipment.

6.3.1.2 Rationale

Having the ability to provide and deploy software updates through an update mechanism is an essential capability. It helps in maintaining equipment, addressing security vulnerabilities, and preventing potential exploitation that could compromise the equipment. Such compromises can pose risks to the network, disrupt its functioning, or lead to the misuse of network resources, resulting in an unacceptable degradation of service.

However, some parts of the software might be immutable and therefore not updatable for technology reasons or functional safety implications do not allow their updatability. Vulnerabilities might also be mitigated by alternative measures, such as exchanging vulnerable equipment throughout the entire life cycle or being securely mitigated by other equipment that ensures the protection of the security assets and network assets.

6.3.1.3 Guidance

There might be more than one update mechanism for different parts of the software. However, this requirement demands at least one update mechanism for each software affecting security assets and/or network assets where no except criteria applies.

Not all software on the equipment can be updatable. This can include software stored in non-updatable memory due to the technology or to satisfy functional safety requirements or legal requirements.

There are cases where alternative measures exist to prevent harm from potential publicly known exploitable vulnerabilities in parts of the software or where an exploitable vulnerability in its software might not endanger the security assets and network assets to be protected. For instance:

- equipment having a replacement strategy, e.g., for equipment with limited resources such as sensors that would have to work on battery for many years; or
- equipment or parts of the software, which can and are foreseen to be securely isolated; or
- the system of which the equipment is part of mitigates the exploit of any vulnerability.

Where it is possible, it is good practice to implement a software update mechanism that allows for separate security related software updates and application software updates.

6.3.1.4 Assessment criteria

6.3.1.4.1 Assessment objective

The assessment addresses the requirement SUM-1.

6.3.1.4.2 Implementation categories

Not applicable.

6.3.1.4.3 Required information

[E.Info.SUM-1.PartOfSoftw]: Description of each parts of the software affecting the security assets and/or network assets including:

- (if the part of the software is not updatable for functional safety implications) [E.Info.SUM-1.PartOfSoftw.FuncSaftyImp]: Description of:
 - the functional safety requirements and their source; and
 - the software's function relation to the functional safety requirements; and
- (if the part of the software is not updatable because it is immutable) [E.Info.SUM-1.PartOfSoftw.Immutable]: Description of the methods that ensure that the part of the software is immutable; and
- (if the part of the software is not updatable because alternative measures exist) [E.Info.SUM-1.PartOfSoftw.AltMeasures]: Description of:
 - the security assets and/or network assets the part of the software affects; and
 - the alternative measures that protect the affected security assets and/or network assets esp. in case of a publicly known exploitable vulnerability affecting the security assets and/or network assets; and
 - the expected life cycle of the equipment; and
- (if the part of the software is updatable) [E.Info.SUM-1.PartOfSoftw.SUM]: Description of the update mechanisms that can update the part of the software.

NOTE The present document does not determine the granularity of the separation of the software into components. A suitable separation with respect to efforts in documentation considers the coverage of the parts of the software by certain update mechanisms.

[E.Info.DT.SUM-1]: Description of the selected path through the decision tree in Figure 11 for each part of the software documented in [E.Info.SUM-1.PartOfSoftw].

[E.Just.DT.SUM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.SUM-1] with the following properties:

- (if a decision from [DT.SUM-1.DN-1] results in "NOT APPLICABLE") the justification for the decision [DT.SUM-1.DN-1] is based on [E.Info.SUM-1.PartOfSoftw.FuncSaftyImp]; and
- (if a decision from [DT.SUM-1.DN-2] results in "NOT APPLICABLE") the justification for the decision [DT.SUM-1.DN-2] is based on [E.Info.SUM-1.PartOfSoftw.Immutable]; and

- (if a decision from [DT.SUM-1.DN-3] results in “NOT APPLICABLE”) the justification for the decision [DT.SUM-1.DN-3] is based on [E.Info.SUM-1.PartOfSoftw.AltMeasures].

6.3.1.4.4 Conceptual assessment

6.3.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether an update mechanism is implemented when it is required per SUM-1.

6.3.1.4.4.2 Preconditions

None.

6.3.1.4.4.3 Assessment units

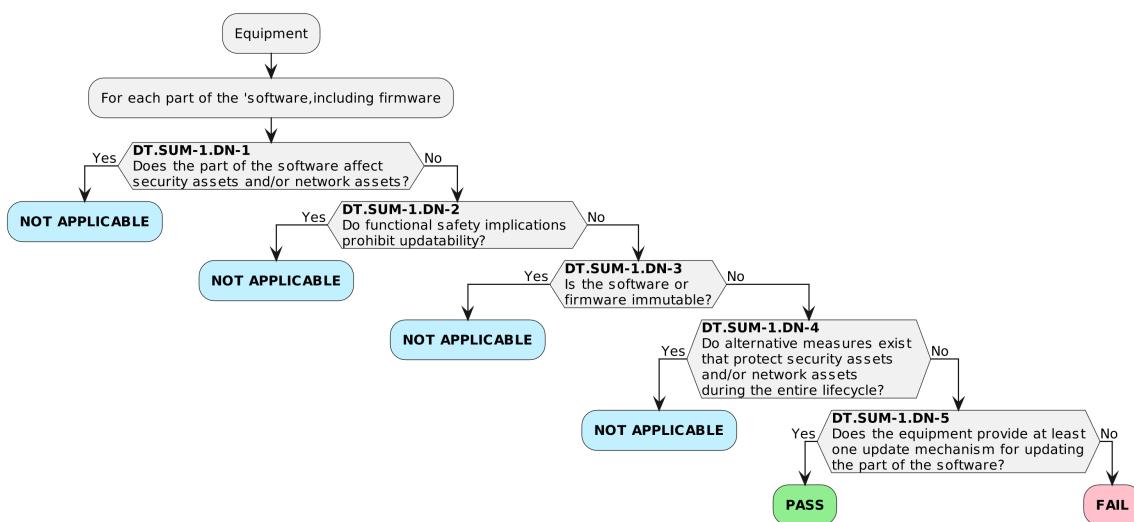


Figure 11 — Decision Tree for requirement SUM-1

For each part of the software documented in [E.Info.SUM-1.PartOfSoftw], check whether the path through the decision tree documented in [E.Info.DT.SUM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.SUM-1], check that its justification documented in [E.Just.DT.SUM-1] describes the security assets and/or network assets affected by the software as well as whether the software is updatable and, when not, the reasons.

6.3.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.SUM-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.SUM-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.SUM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SUM-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SUM-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SUM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SUM-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.3.1.4.5 Functional completeness assessment

None.

6.3.1.4.6 Functional sufficiency assessment

6.3.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the equipment supports update mechanisms for parts of the software affecting security assets and/or network assets as documented in [E.Info.SUM-1.PartOfSoftw.SUM].

6.3.1.4.6.2 Preconditions

The equipment is in an operational state.

For each update mechanism described in [E.Info.SUM-1.PartOfSoftw.SUM], the manufacturer provides updated software (in the following: SW-a) which is integrity-protected and authenticity-protected using a mechanism that the equipment natively supports.

6.3.1.4.6.3 Assessment units

For each update mechanism documented in [E.Info.SUM-1.PartOfSoftw.SUM] which ends with a PASS verdict in the SUM-1 conceptual assessment, install SW-a on the equipment.

6.3.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that an installation of SW-a is not successful for an update mechanism documented in [E.Info.SUM-1.PartOfSoftw.SUM].

The verdict FAIL for the assessment case is assigned if there is evidence that an installation of SW-a is not successful for an update mechanism documented in [E.Info.SUM-1.PartOfSoftw.SUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.3.2 [SUM-2] Secure updates

6.3.2.1 Requirement

Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.

6.3.2.2 Rationale

A secure software update mechanism ensures that the software that controls the equipment is not tampered via attacks on the update mechanism.

6.3.2.3 Guidance

A common approach for confirming that an update is valid is to verify, cryptographically, its integrity and authenticity based on a trust anchor. This can be done on the equipment or by another equipment that is trusted to perform this verification. For the latter the verified update is typically sent over a secure channel to the equipment, securely installed on the equipment.

NOTE A “Secure channel” typically preserves the security properties of the communicated information and can also include authorized and authenticated personnel providing the validated software update locally (example of technical or organisational measures).

A manufacturer can provide a secure method to install alternative software not provided by the manufacturer themselves, for example allowing a user to install alternative software on a home router.

It is a security best practice to prevent downgrading the software to an older version.

Due to some security update the product might return to default setting requiring to re-enter credentials and configuration data.

The use of SCM-3 is appropriate when a software update contains confidential cryptographic keys.

6.3.2.4 Assessment criteria

6.3.2.4.1 Assessment objective

The assessment addresses the requirement SUM-2.

6.3.2.4.2 Implementation categories

[IC.SUM-2.AuthIntVal.Sign]: The methods to validate the software’s integrity and authenticity solely rely on digital signatures for software updates by authorized entities.

[IC.SUM-2.AuthIntVal.SecChan]: The methods to validate the software’s integrity and authenticity solely rely on a secure communication mechanism to the authorized software update’s source as required per SCM-1 and SCM-2.

[IC.SUM-2.AuthIntVal.AccContMech]: The methods to validate the software’s integrity and authenticity solely rely on access control mechanisms that only allow updates by authorized entities as required per ACM-1 combined with hash-protected software update.

[IC.SUM-2.AuthIntVal.Generic]: The methods to validate the software’s integrity and authenticity are different from [IC.SUM-2.AuthIntVal.Sign], [IC.SUM-2.AuthIntVal.SecChan] or [IC.SUM-2.AuthIntVal.AccContMech].

6.3.2.4.3 Required information

[E.Info.SUM-2.SUM]: Description of each update mechanism that can update a part of the software documented in [E.Info.SUM-1.PartOfSoftw], including:

- (if the implementation is based on [IC.SUM-2.AuthIntVal.Sign]) [E.Info.SUM-2.SUM.Sign]: Description of the digital signature scheme used with a description of the underlying best practice cryptography as per [E.Info.CRY-1.Assets.Cryptography]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.SecChan]) [E.Info.SUM-2.SUM.SecChan]: Description of the secure communication mechanism referring to [E.Info.SCM-1.SCM] with a description of the underlying best practice cryptography as per [E.Info.CRY-1.Assets.Cryptography]; and

- (if the implementation is based on [IC.SUM-2.AuthIntVal.AccContMech]) [E.Info.SUM-2.SUM.AccContMech]: Description of the access control mechanism referring to [E.Info.ACM-2.SecurityAsset.ACM] and of the hash function referring to [E.Info.CRY-1.Assets.Cryptography]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.Generic]) [E.Info.SUM-2.SUM.Generic]: Description of the methods used to validate the software's integrity and authenticity.

[E.Info.DT.SUM-2]: Description of the selected path through the decision tree in Figure 12 for each update mechanism documented in [E.Info.SUM-2.SUM].

[E.Just.DT.SUM-2]: Justification for the selected path through the decision tree documented in [E.Info.DT.SUM-2] with the following properties:

- (if the implementation is based on [IC.SUM-2.AuthIntVal.Sign]) the justification for the decision [DT.SUM-2.DN-1] is based on [E.Info.SUM-2.SUM.Sign]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.SecChan]) the justification for the decision [DT.SUM-2.DN-1] is based on [E.Info.SUM-2.SUM.SecChan]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.AccContMech]) the justification for the decision [DT.SUM-2.DN-1] is based on [E.Info.SUM-2.SUM.AccContMech]; and
- (if the implementation is based on [IC.SUM-2.AuthIntVal.Generic]) the justification for the decision [DT.SUM-2.DN-1] is based on [E.Info.SUM-2.SUM.Generic].

6.3.2.4.4 Conceptual assessment

6.3.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the update mechanisms as required per SUM-1 only install software as required per SUM-2.

6.3.2.4.4.2 Preconditions

None.

6.3.2.4.4.3 Assessment units

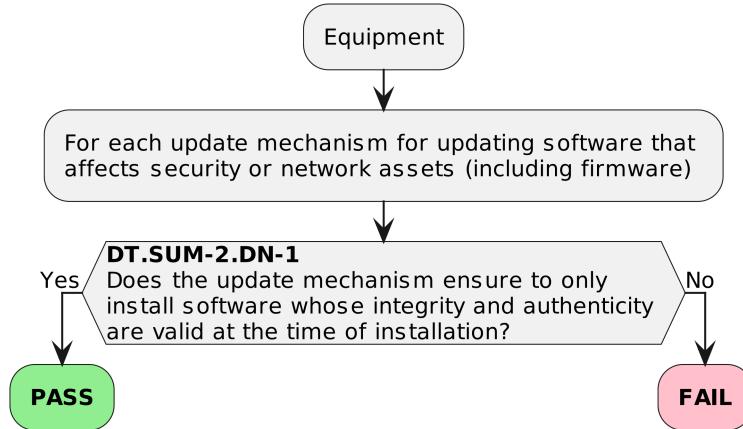


Figure 12 — Decision Tree for requirement SUM-2

For each update mechanism documented in [E.Info.SUM-2.SUM], check whether the path through the decision tree documented in [E.Just.DT.SUM-2] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.SUM-2], check that its justification documented in [E.Just.DT.SUM-2] describes, based on references to [E.Info.SUM-2.SUM.Generic], the methods to ensure the validity of the software’s integrity and authenticity at the time of installation.

6.3.2.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.SUM-2] end with “PASS”; and
- the information provided in [E.Just.DT.SUM-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SUM-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SUM-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SUM-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SUM-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.3.2.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the secure update mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.3.2.4.6 Functional sufficiency assessment

6.3.2.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the update mechanisms for parts of the software affecting security assets and/or network assets only install software whose integrity and authenticity are valid at the time of the installation as documented in [E.Info.SUM-2.SUM.Generic].

6.3.2.4.6.2 Preconditions

The equipment is in an operational state.

For any update mechanism, the manufacturer provides updated software.

6.3.2.4.6.3 Assessment units

For each update mechanism documented in [E.Info.SUM-2.SUM]:

[AU.SUM-2.Sign]: When the implementation is based on [IC.SUM-2.AuthIntVal.Sign], functionally confirm that:

- it is implemented using best practice cryptography according to CRY-1; and
- an unsigned software update is not installed; and
- a software update with a modified signature is not installed; and
- a modified software update with a valid signature for the unmodified software update is not installed; and
- a software update with a signature from an unauthorized entity is not installed.

[AU.SUM-2.SecChan]: When the implementation is based on [IC.SUM-2.AuthIntVal.SecChan], functionally confirm that:

- it is implemented using the secure communication mechanism according to SCM; and
- a software update from an unauthorized source is not installed; and
- the secure communication channel does not allow to impersonate the authorized software updates source via a man-in-the-middle attack; and
- a software update that is modified during communication is not installed.

[AU.SUM-2.AccContMech]: When the implementation is based on [IC.SUM-2.AuthIntVal.AccContMech], functionally confirm that:

- it is implemented using the access control mechanism according to ACM; and
- a modified software update with a valid hash for the unmodified software update is not installed; and
- a software update with a hash generated by an unsupported hash function is not installed; and
- a software update provided by an unauthorized entity is not installed.

[AU.SUM-2.Generic]: When the implementation is based on [IC.SUM-2.AuthIntVal.Generic], functionally confirm that:

- a software update whose integrity is not valid is not installed; and
- a software update whose authenticity is not valid is not installed.

6.3.2.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each update mechanism documented in [E.Info.SUM-2.SUM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for an update mechanism documented in [E.Info.SUM-2.SUM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.3.3 [SUM-3] Automated updates

6.3.3.1 Requirement

Each update mechanism that is required per SUM-1 shall be capable of updating the software:

- without human intervention at the equipment; or
- via scheduling the installation of an update under human approval; or
- via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment.

6.3.3.2 Rationale

In case of an existing publicly known exploitable vulnerability in the equipment, that can compromise security assets and network assets, an automated update mechanism can ensure that an available security update that addresses this vulnerability is applied without or with minimal human intervention preventing the vulnerability exploitation.

6.3.3.3 Guidance

This requirement demands at least one automated update mechanism for each part of the software where SUM-1 requires an update mechanism.

NOTE 1 One automated update mechanism can be used to update multiple parts of the software.

Automated updates are carried out by machines without needing or with minimal human control or intervention.

Automatic updates are a step further where the equipment makes decisions and executes updates on its own without human intervention.

In specific cases involving safety or time-critical aspects, or dependency on compatibility of the updates in a network, the update can require some precautions and/or on-site verifications before it is initiated and therefore cannot be performed in an automatic way so that the operation of the application is not affected. In such cases, human intervention to trigger or schedule the update is needed.

In case the installation of the new software version fails, e.g., validation of the software image(s) is unsuccessful, a best practice is to apply a roll-back policy to re-activate the previous software version, unless not enough memory is available to store the update.

Triggering the installation of an update under human approval can for example consist of displaying a notification that an update is available and prompting the user to install the update via a secure update mechanism.

Simple automated updates from a user's perspective improve the distribution rate of security updates.

NOTE 2 "Simple from a user's perspective" can include:

- simple configuration of notifications related to the secure update mechanism
- simple configuration of the update mechanism
- simple provision of consent to fully automatic updates

Where fully automatic update mechanisms are possible, asking for user's consent to activate it when putting the equipment into service, improves the distribution rate of security updates.

Checking the availability of new security updates after initialization and regularly improves the distribution rate of security updates.

6.3.3.4 Assessment criteria

6.3.3.4.1 Assessment objective

The assessment addresses the requirement SUM-3.

6.3.3.4.2 Implementation categories

Not applicable.

6.3.3.4.3 Required information

[E.Info.SUM-3.SUM]: Description of each update mechanism required per SUM-1, including:

- [E.Info.SUM-3.SUM.Automation]: Description of the means to automate the update mechanism.

[E.Info.DT.SUM-3]: Description of the selected path through the decision tree in Figure 13 for each update mechanism documented in [E.Info.SUM-3.SUM].

[E.Just.DT.SUM-3]: Justification for the selected path through the decision tree documented in [E.Info.DT.SUM-3] with the following properties:

- the justification for the decisions [DT.SUM-3.DN-1], [DT.SUM-3.DN-2] and [DT.SUM-3.DN-3] is based on [E.Info.SUM-3.SUM.Automation].

6.3.3.4.4 Conceptual assessment

6.3.3.4.4.1 Assessment purpose

The purpose of this assessment case is to determine whether each update mechanism supports automated updates as documented in [E.Info.SUM-3.SUM.Automation] as required per SUM-3.

6.3.3.4.4.2 Preconditions

None.

6.3.3.4.4.3 Assessment units

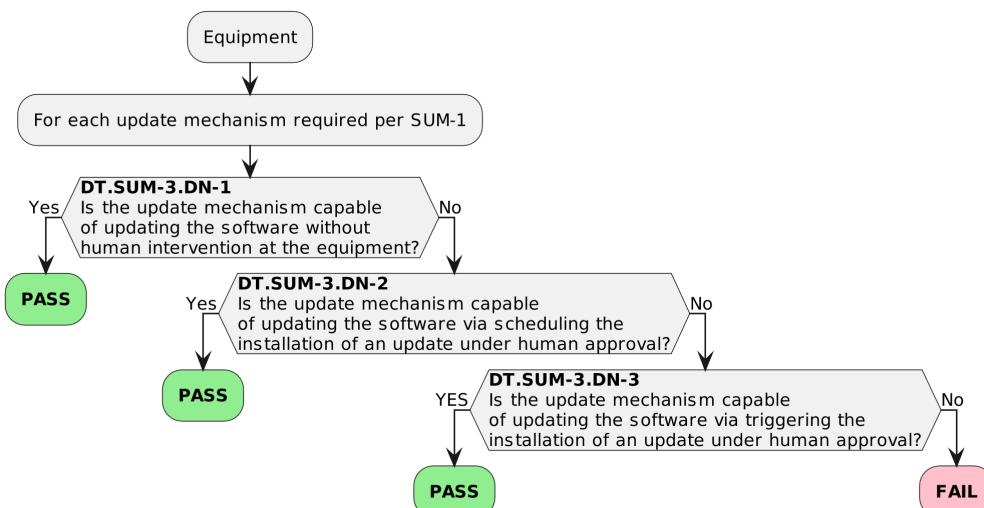


Figure 13 — Decision Tree for requirement SUM-3

For each update mechanism, check whether the path through the decision tree documented in [E.Info.DT.SUM-3] ends with “PASS” or “FAIL”.

For each path through the decision tree documented in [E.Info.DT.SUM-3], examine its justification documented in [E.Just.DT.SUM-3].

6.3.3.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.SUM-3] end with “PASS”; and
- the information provided in [E.Just.DT.SUM-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SUM-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SUM-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SUM-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SUM-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.3.3.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the secure update mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.3.3.4.6 Functional sufficiency assessment

6.3.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the update mechanisms for parts of the software affecting security assets and/or network assets are automated as documented in [E.Info.SUM-3.SUM.Automation].

6.3.3.4.6.2 Preconditions

The equipment is in an operational state.

The manufacturer provides the means to perform automated updates.

6.3.3.4.6.3 Assessment units

For each update mechanism documented in [E.Info.SUM-3.SUM] functionally assess whether the automation implementation deviates from [E.Info.SUM-3.SUM.Automation] by:

- checking the software version on the equipment; and
- making a software update available at the source holding security updates; and
- checking whether the equipment performs the software update:
 - without human intervention at the equipment; or

- via scheduling the installation of an update under human approval; or
- via triggering the installation of an update under human approval; and
- checking on the equipment that the software version has been updated to a new version number.

6.3.3.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that the implementation of an update mechanism required per SUM-1 deviates from [E.Info.SUM-3.SUM].

The verdict FAIL for the assessment case is assigned if there is evidence that the implementation of an update mechanism required per SUM-1 deviates from [E.Info.SUM-3.SUM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4 [SSM] Secure storage mechanism

6.4.1 [SSM-1] Applicability of secure storage mechanisms

6.4.1.1 Requirement

The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets where:

- the physical or logical measures in the target environment ensures the security asset or network asset stored on the equipment accessibility is limited to authorized entities.

6.4.1.2 Rationale

Secure storage mechanisms protect security assets and network assets from unauthorized access. If security assets or network assets are not appropriately secured, an attacker can access, tamper, or delete the assets and compromise the equipment, which might lead to the misuse of network resources.

6.4.1.3 Guidance

The security assets and network assets can be protected by e.g.:

- cryptographic measures like encryption to ensure confidentiality
- cryptographic measures like digital signatures to ensure integrity and authenticity
- access control using authentication or authorisation,
- hardware protection measures
- physical protection measures

The appropriate protection mechanism depends on the risks associated with the security assets or network assets to be stored and this might depend on:

- the criticality of the security assets or network assets;
- the amount of security assets or network assets;

- the duration for which the security assets or network assets need to be stored;
- the intended operational environment of use.

Removable storage that is not part of the equipment at the moment of placement on the market is not considered to be persistent storage but a storage that is meant to be used to move security assets or network assets between different equipment. Physical access to the equipment is required to remove such a storage from the equipment. This ensures access to the stored security assets or network assets is only available to authorized entities having physical access to the equipment.

Persistently stored data, not listed as security assets or network assets, may be protected by the secured storage mechanism but they are out of scope of this requirement.

6.4.1.4 Assessment criteria

6.4.1.4.1 Assessment objective

The assessment addresses the requirement SSM-1.

6.4.1.4.2 Implementation categories

Not applicable.

6.4.1.4.3 Required information

[E.Info.SSM-1.SecurityAsset]: Description of each security asset persistently stored on the equipment, including for each of its persistent storage:

- (if a secure storage mechanism is claimed to be not required because physical or logical measures in the environment's target operational environment ensure that the stored security asset's accessibility is limited to authorized entities) [E.Info.SSM-1.SecurityAsset.Environment]: Description of:
 - physical or logical measures in the equipment's targeted operational environment; and
 - how entities are authenticated/authorized in the equipment's targeted operational environment; and
- (if the persistent storage is provided by a secure storage mechanism) [E.Info.SSM-1.SecurityAsset.SSM]: Description of the secure storage mechanism.

[E.Info.SSM-1.NetworkAsset]: Description of each network asset persistently stored on the equipment, including for each of its persistent storage:

- (if a secure storage mechanism is claimed to be not required because physical or logical measures in the environment's target operational environment ensure that the stored network asset's accessibility is limited to authorized entities) [E.Info.SSM-1.NetworkAsset.Environment]: Description of:
 - physical or logical measures in the equipment's targeted operational environment; and
 - how entities are authenticated/authorized in the equipment's targeted operational environment; and

- (if the persistent storage is claimed to be required by a secure storage mechanism) [E.Info.SSM-1.NetworkAsset.SSM]: Description of the secure storage mechanism.

[E.Info.DT.SSM-1]: Description of the selected path through the decision tree in Figure 14 for each security asset and network asset documented in [E.Info.SSM-1.SecurityAsset] and [E.Info.SSM-1.NetworkAsset].

[E.Just.DT.SSM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.SSM-1] with the following properties:

- (if a decision from [DT.SSM-1.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.SSM-1.DN-1] is based on [E.Info.SSM-1.SecurityAsset.Environment] or [E.Info.SSM-1.NetworkAsset.Environment]; and
- the justification for the decision [DT.SSM-1.DN-2] is based on [E.Info.SSM-1.SecurityAsset.SSM] or [E.Info.SSM-1.NetworkAsset.SSM].

6.4.1.4.4 Conceptual assessment

6.4.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether secure storage mechanisms are implemented when it is required per SSM-1.

6.4.1.4.4.2 Preconditions

None.

6.4.1.4.4.3 Assessment units

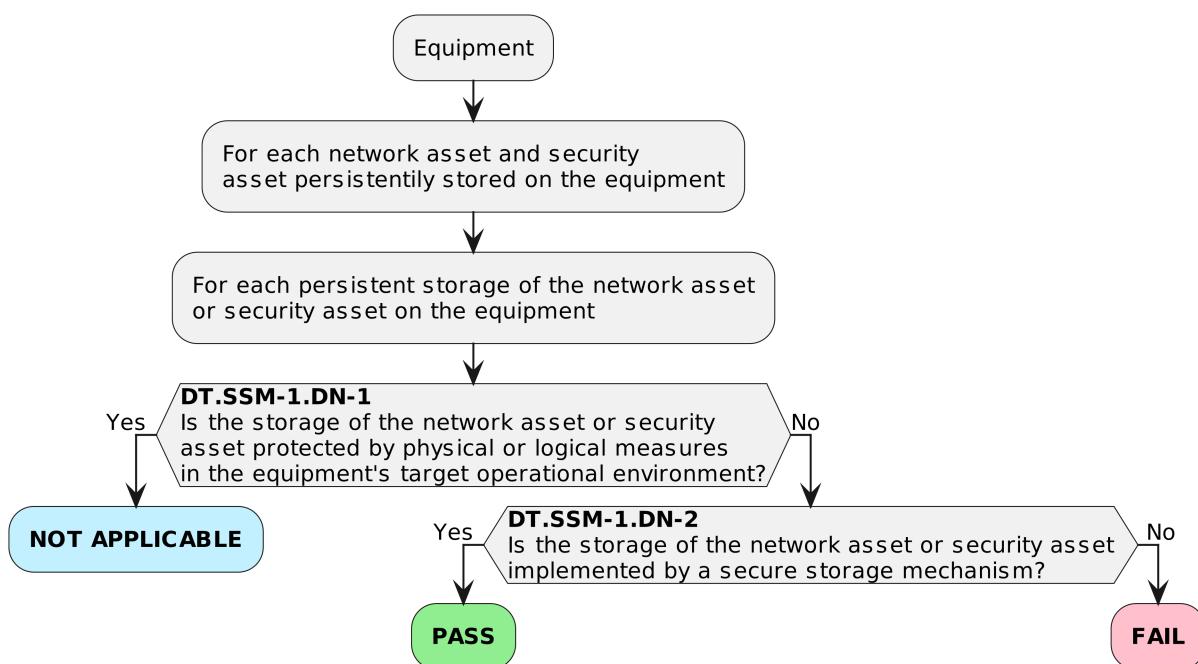


Figure 14 — Decision tree for requirement SSM-1

For each security asset documented in [E.Info.SSM-1.SecurityAsset] and for each network asset documented in [E.Info.SSM-1.NetworkAsset], check whether the path through the decision tree documented in [E.Info.DT.SSM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.SSM-1], examine its justification documented in [E.Just.DT.SSM-1].

6.4.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.SSM-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.SSM-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.SSM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SSM-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SSM-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SSM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SSM-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4.1.4.5 Functional completeness assessment

6.4.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether security assets documented in [E.Info.SSM-1.SecurityAsset] and network assets documented in [E.Info.SSM-1.NetworkAsset] are complete.

6.4.1.4.5.2 Preconditions

The equipment is in an operational state.

6.4.1.4.5.3 Assessment units

Functionally assess whether there are security assets persistently stored on the equipment, which are not listed in [E.Info.SSM-1.SecurityAsset].

Functionally assess whether there are network assets persistently stored on the equipment, which are not listed in [E.Info.SSM-1.NetworkAsset].

6.4.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all persistently stored security assets found are documented in [E.Info.SSM-1.SecurityAsset] and all network assets persistently stored found are documented in [E.Info.SSM-1.NetworkAsset].

The verdict FAIL for the assessment case is assigned if a persistently stored security asset is found which is not documented in [E.Info.SSM-1.SecurityAsset] or a persistently stored network asset is found which is not documented in [E.Info.SSM-1.NetworkAsset].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4.1.4.6 Functional sufficiency assessment

6.4.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether secure storage mechanisms are implemented when required per SSM-1.

6.4.1.4.6.2 Preconditions

The equipment is in an operational state.

6.4.1.4.6.3 Assessment units

For each security asset documented in [E.Info.SSM-1.SecurityAsset], functionally confirm it is persistently stored solely via secure storage mechanisms documented in [E.Info.SSM-1.SecurityAsset.SSM].

For each network asset documented in [E.Info.SSM-1.NetworkAsset], functionally confirm it is persistently stored solely via secure storage mechanisms documented in [E.Info.SSM-1.NetworkAsset.SSM].

6.4.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that:

- a security asset is persistently stored other than via secure storage mechanisms documented in [E.Info.SSM-1.SecurityAsset.SSM]; and
- a network asset is persistently stored other than via secure storage mechanisms documented in a [E.Info.SSM-1.NetworkAsset.SSM].

The verdict FAIL for the assessment case is assigned if there is evidence that:

- a security asset is persistently stored other than via secure storage mechanisms documented in [E.Info.SSM-1.SecurityAsset.SSM]; or
- a network asset is persistently stored other than via secure storage mechanisms documented in a [E.Info.SSM-1.NetworkAsset.SSM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms

6.4.2.1 Requirement

Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently.

6.4.2.2 Rationale

When stored, security assets and network assets require protection against tampering. If the integrity of the security assets or network assets stored is not appropriately secured, an attacker can manipulate those assets, which might endanger network resources.

The integrity protection applies for encrypted as well as for unencrypted storage.

6.4.2.3 Guidance

Data can be protected from tampering by for instance:

- cryptographic measures like digital signatures,
- access control,
- hardware protection measures,
- physical protection measures.

6.4.2.4 Assessment criteria

6.4.2.4.1 Assessment objective

The assessment addresses the requirement SSM-2.

6.4.2.4.2 Implementation categories

[IC.SSM-2.DigitalSignature]: The method to ensure the integrity of stored security assets or network assets using the digital signature derived using cryptography secret provisioned during manufacturing, commissioning, or normal operation of an equipment.

[IC.SSM-2.AccessControl]: The method to ensure the integrity of stored security assets or network assets is using access control mechanisms that deny unauthorized modification.

[IC.SSM-2.OTPProgrammable]: The method to ensure the integrity of stored security assets or network assets is based on one-time programmable memory.

[IC.SSM-2.HardwareProtection]: The method to ensure the integrity of stored security assets or network assets is based on hardware protecting the memory.

[IC.SSM-2.Generic]: The methods to ensure integrity and of stored security assets or network assets do not solely rely on [IC.SSM-2.DigitalSignature], [IC.SSM-2.AccessControl], [IC.SSM-2.OTPProgrammable] or [IC.SSM-2.HardwareProtection].

6.4.2.4.3 Required information

[E.Info.SSM-2.SSM]: Description of each secure storage mechanism, including

- a list of all security assets and network assets it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-2.DigitalSignature]) [E.Info.SSM-2.SSM.DigitalSignature]: Description of how integrity protection is realized using digital signature including:
 - a description of the digital signature mechanism and the cryptography for the security assets and network assets it stores persistently; and
 - a description of how the cryptographic secret used to derive the signature is provisioned onto or generated by the equipment; and
- (if the SSM implementation is based on [IC.SSM-2.AccessControl]) [E.Info.SSM-2.SSM.AccessControl]: Description of how integrity protection is realized using access control mechanisms, including:

- a description of the access control mechanisms and the corresponding access rights for the security assets and network assets it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-2.OTProgrammable]) [E.Info.SSM-2.SSM.OTProgrammable]: Description of how integrity protection is realized using one-time programmable memory, including:
 - a description of what type of one-time programmable memory is used for the security assets and network assets it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-2.HardwareProtection]) [[E.Info.SSM-2.SSM.HardwareProtection]]: Description of how integrity protection is realized using hardware protection including:
 - a description of what hardware protection is used for the security assets and network assets it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-2.Generic]) [E.Info.SSM-2.SSM.Generic]: Description of the integrity protection mechanism used to protect the security assets or network assets; and
- if it is claimed that the secure storage mechanism is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the secure storage mechanism complies to.

NOTE The information above may not always be available to the manufacturer when the secure storage mechanism provided by a supplier which will not disclose such information for security reasons while providing all necessary security instructions to use the secure storage mechanism.

[E.Info.DT.SSM-2]: Description of the selected path through the decision tree in Figure 15 for each secure storage mechanism described in [E.Info.SSM-2.SSM].

[E.Just.DT.SSM-2]: Justification for the selected path through the decision tree documented in [E.Info.DT.SSM-2] with the following properties:

- (if the implementation is based on [IC.SSM-2.DigitalSignature]) the justification for the decision [DT.SSM-2.DN-1] is based on [E.Info.SSM-2.SSM.DigitalSignature]; and
- (if the implementation is based on [IC.SSM-2.AccessControl]) the justification for the decision [DT.SSM-2.DN-1] is based on [E.Info.SSM-2.SSM.AccessControl]; and
- (if the implementation is based on [IC.SSM-2.OTProgrammable]) the justification for the decision [DT.SSM-2.DN-1] is based on [E.Info.SSM-2.SSM.OTProgrammable]; and
- (if the implementation is based on [IC.SSM-2.HardwareProtection]) the justification for the decision [DT.SSM-2.DN-1] is based on [E.Info.SSM-2.SSM.HardwareProtection]; and
- (if the implementation is based on [IC.SSM-2.Generic]) the justification for the decision [DT.SSM-2.DN-1] is based on [E.Info.SSM-2.SSM.Generic].

6.4.2.4.4 Conceptual assessment

6.4.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether secure storage mechanisms required by SSM-1 are implemented as required per SSM-2.

6.4.2.4.4.2 Preconditions

None.

6.4.2.4.4.3 Assessment units

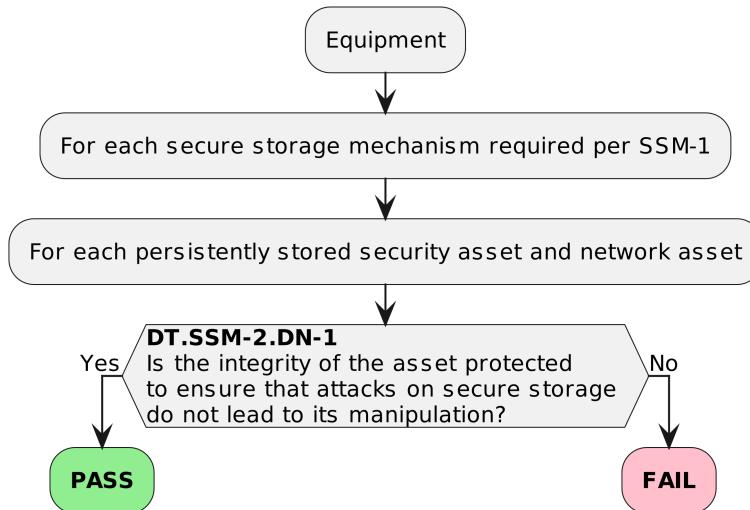


Figure 15 — Decision tree for requirement SSM-2

For each secure storage mechanism in [E.Info.SSM-2.SSM] check whether the path through the decision tree documented in [E.Info.DT.SSM-2] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.SSM-2], examine its justification documented in [E.Just.DT.SSM-2].

6.4.2.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.SSM-2] end with “PASS”; and
- the information provided in [E.Just.DT.SSM-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SSM-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SSM-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SSM-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SSM-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4.2.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the secure storage mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

6.4.2.4.6 Functional sufficiency assessment

6.4.2.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the secure storage mechanisms required per SSM-1 provide the required integrity protection.

6.4.2.4.6.2 Preconditions

The equipment is in an operational state.

6.4.2.4.6.3 Assessment units

For each secure storage mechanism documented in [E.Info.SSM-2.SSM]:

[AU.SSM-2.DigitalSignature]: if the secure storage mechanism's implementation is based on [IC.SSM-2.DigitalSignature], functionally confirm that:

- it is implemented according to [E.Info.SSM-2.SSM.DigitalSignature]; and
- the secret used to digitally sign the security assets or network assets cannot be intercepted, deduced, or extracted; and
- a modification of the security assets and network assets without valid signature is detected by the secure storage mechanism.

[AU.SSM-2.AccessControl]: if the secure storage mechanism's implementation is based on [IC.SSM-2.AccessControl], functionally confirm that:

- it is implemented according to [E.Info.SSM-2.SSM.AccessControl]; and
- an unauthorized modification of the stored security assets and network assets is denied.

[AU.SSM-2.OTPProgrammable]: if the secure storage mechanism's implementation is based on [IC.SSM-2.OTPProgrammable], functionally confirm that:

- it is implemented according to [E.Info.SSM-2.SSM.OTPProgrammable]; and
- a modification of the security assets and network assets is not possible.

[AU.SSM-2.HardwareProtection]: if the secure storage mechanism's implementation is based on [IC.SSM-2.HardwareProtection], functionally confirm that:

- it is implemented according to [E.Info.SSM-2.SSM.HardwareProtection]; and
- an unauthorized modification of the security assets and network assets is not possible or can be detected by the secure storage mechanism.

[AU.SSM-2.Generic]: if the secure storage mechanism's implementation is based on [IC.SSM-2.Generic], functionally confirm:

- it is implemented according to [E.Info.SSM-2.SSM.Generic]; and
- an unauthorized modification of the security assets or networks asset is not possible or can be detected by the secure storage mechanism.

6.4.2.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each secure storage mechanism documented in [E.Info.SSM-2.SSM] the confirmations in the implementation category dependent assessments units are successful.

The verdict FAIL for the assessment case is assigned if for any secure storage mechanism documented in [E.Info.SSM-2.SSM] a confirmation in the implementation category dependent assessment units is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms

6.4.3.1 Requirement

Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently.

6.4.3.2 Rationale

When stored, confidential security parameters and confidential network function configuration require protection from exposure. If such information is not appropriately secured, an attacker can access and misuse the equipment and stored data, which might lead to the misuse of network resources.

6.4.3.3 Guidance

Data can be protected from exposure by e.g.:

- cryptographic measures like encryption,
- access control,
- hardware protection measures.

6.4.3.4 Assessment criteria

6.4.3.4.1 Assessment objective

The assessment addresses the requirement SSM-3.

6.4.3.4.2 Implementation categories

[IC.SSM-3.Encryption]: The method to ensure the secrecy of stored confidential security parameters or confidential network function configuration is based on encryption using a secret provisioned during manufacturing, derived during commissioning or normal operation of an equipment.

[IC.SSM-3.AccessControl]: The method to ensure the secrecy of confidential security parameters or confidential network function configuration is using access control mechanisms that deny unauthorized reading.

[IC.SSM-3.HardwareProtection]: The method to ensure secrecy of stored confidential security parameters or confidential network function configuration based on hardware protection (e.g., scrambling, obfuscation, etc.).

[IC.SSM-3.Generic]: The methods to ensure the secrecy of stored confidential security parameters or confidential network function configuration do not solely rely on [IC.SSM-3.Encryption], [IC.SSM-3.AccessControl] or [IC.SSM-3.HardwareProtection].

6.4.3.4.3 Required information

[E.Info.SSM-3.SSM]: Description of each secure storage mechanism that persistently stores confidential security parameter or confidential network function configuration, including:

- [E.Info.SSM-3.SSM.Asset]: List of all confidential security parameter and confidential network function configuration it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-3.Encryption]) [E.Info.SSM-3.SSM.Encryption]: Description of how secrecy is realized using encryption including:
 - the encryption mechanism and the cryptography that are used to protect the secrecy of the confidential security parameter and confidential network function configuration it stores persistently; and
 - how the secret used to encrypt the asset was provisioned or derived; and
- (if the SSM implementation is based on [IC.SSM-3.AccessControl]) [E.Info.SSM-3.SSM.AccessControl]: Description of how secrecy is realized using access control mechanisms including:
 - a description of the access control mechanisms including the corresponding access rights for the confidential security parameter and confidential network function configuration it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-3.HardwareProtection]) [E.Info.SSM-3.SSM.HardwareProtection]: Description of how secrecy is realized using hardware protection including:
 - a description of what hardware protection is used for the confidential security parameter and confidential network function configuration it stores persistently; and
- (if the SSM implementation is based on [IC.SSM-3.Generic]) [E.Info.SSM-3.SSM.Generic]: Description of the confidentiality protection mechanism used to protect the secrecy of confidential security parameters and confidential network function configuration it stores persistently; and
- if it is claimed that the secure storage mechanism is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the secure storage mechanism complies to.

NOTE The information above may not always be available to the manufacturer when the secure storage mechanism provided by a supplier which will not disclose such information for security reasons while providing all necessary security instructions to use the secure storage mechanism.

[E.Info.DT.SSM-3]: Description of the selected path through the decision tree in Figure 16 for each secure storage mechanism described in [E.Info.SSM-3.SSM].

[E.Just.DT.SSM-3]: Justification for the selected path through the decision tree documented in [E.Info.DT.SSM-3] with the following properties:

- (if the implementation is based on [IC.SSM-3.Encryption]) the justification for the decision [DT.SSM-3.DN-1] is based on [E.Info.SSM-3.SSM.Encryption]; and
- (if the implementation is based on [IC.SSM-3.AccessControl]) the justification for the decision [DT.SSM-3.DN-1] is based on [E.Info.SSM-3.SSM.AccessControl]; and
- (if the implementation is based on [IC.SSM-3.HardwareProtection]) the justification for the decision [DT.SSM-3.DN-1] is based on [E.Info.SSM-3.SSM.HardwareProtection]; and
- (if the implementation is based on [IC.SSM-3.Generic]) the justification for the decision [DT.SSM-3.DN-1] is based on [E.Info.SSM-3.SSM.Generic].

6.4.3.4.4 Conceptual assessment

6.4.3.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether secure storage mechanisms required by SSM-1 that persistently store confidential security parameters or confidential network function configuration are implemented as required per SSM-3.

6.4.3.4.4.2 Preconditions

None.

6.4.3.4.4.3 Assessment units

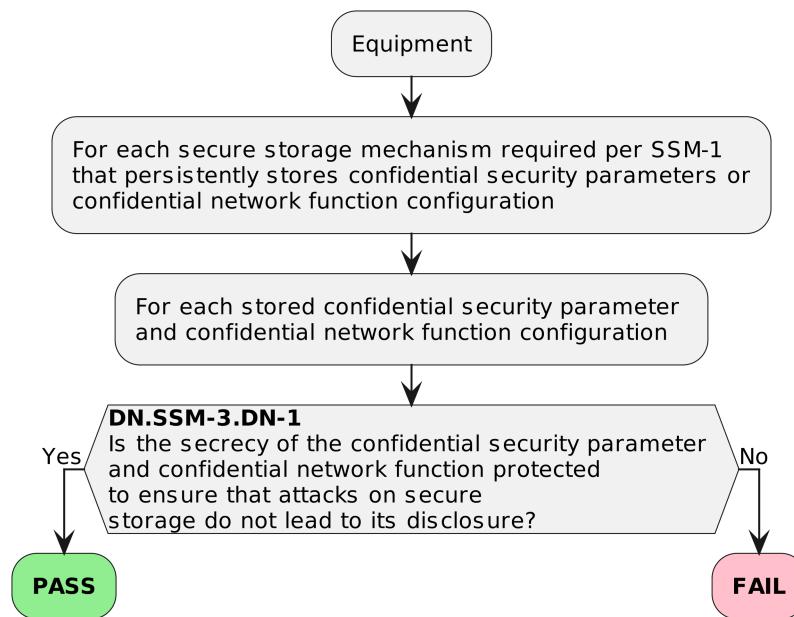


Figure 16 — Decision tree for requirement SSM-3

For each secure storage mechanism in [E.Info.SSM-3.SSM] check whether the path through the decision tree documented in [E.Info.DT.SSM-3] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.SSM-3], examine its justification documented in [E.Just.DT.SSM-3].

6.4.3.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.SSM-3] end with “PASS”; and
- the information provided in [E.Just.DT.SSM-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SSM-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SSM-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SSM-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SSM-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4.3.4.5 Functional completeness assessment

6.4.3.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the assets documented in [E.Info.SSM-3.SSM.Asset] are complete.

6.4.3.4.5.2 Preconditions

The equipment is in an operational state.

6.4.3.4.5.3 Assessment units

Functionally assess whether there are confidential security parameters or confidential network function configurations persistently stored on the equipment, which are not listed in [E.Info.SSM-3.SSM.Asset].

6.4.3.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all persistently stored confidential security parameters found and all confidential network function configurations persistently stored found are documented in [E.Info.SSM-3.SSM.Asset].

The verdict FAIL for the assessment case is assigned if a persistently stored confidential security parameter is found or a persistently stored confidential network function configuration is found which is not documented in [E.Info.SSM-3.SSM.Asset].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.4.3.4.6 Functional sufficiency assessment

6.4.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the secure storage mechanisms required per SSM-1 that persistently store confidential security parameters or confidential network function configuration provide the required confidentiality protection.

6.4.3.4.6.2 Preconditions

The equipment is in an operational state.

6.4.3.4.6.3 Assessment units

For each secure storage mechanism documented in [E.Info.SSM-3.SSM]:

[AU.SSM-3.Encryption]: if the secure storage mechanism's implementation is based on [IC.SSM-3.Encryption], functionally confirm that:

- it is implemented according to [E.Info.SSM-3.SSM.Encryption]; and
- the secret used to encrypt the confidential security parameters or confidential network function configuration cannot be intercepted, deducted, or extracted; and
- reading the confidential security parameters and confidential network function configuration without access to the secret used for decryption is not possible.

[AU.SSM-3.AccessControl]: if the secure storage mechanism's implementation is based on [IC.SSM-3.AccessControl], functionally confirm:

- it is implemented according to [E.Info.SSM-3.SSM.AccessControl]; and
- an unauthorized reading of the stored confidential security parameters and confidential network function configuration is denied.

[AU.SSM-3.HardwareProtection]: if the secure storage mechanism's implementation is based on [IC.SSM-3.HardwareProtection], functionally confirm:

- it is implemented according to [E.Info.SSM-3.SSM.HardwareProtection]; and
- the mechanism used to protect the confidentiality of the stored confidential security parameters and confidential network function configuration cannot be broken or bypassed; and
- an unauthorized reading of the stored confidential security parameters and confidential network function configuration is not possible.

[AU.SSM-3.Generic]: if the secure storage mechanism's implementation is based on [IC.SSM-3.Generic], functionally confirm:

- it is implemented according to [E.Info.SSM-3.SSM.Generic]; and
- an unauthorized reading of the stored confidential security parameters and confidential network function configuration is not possible.

6.4.3.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each secure storage mechanism documented in [E.Info.SSM-3.SSM] the confirmations in the implementation category dependent assessment units are successful.

The verdict FAIL for the assessment case is assigned if for any secure storage mechanism documented in [E.Info.SSM-3.SSM] a confirmation in the implementation category dependent assessment units is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5 [SCM] Secure communication mechanism

6.5.1 [SCM-1] Applicability of secure communication mechanisms

6.5.1.1 Requirement

The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces, except for:

- communicating security assets or network assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that network assets or security assets are not exposed to unauthorised entities; or
- communicating security assets or network assets whose exposure is part of establishing or managing a connection combined with additional measures to authenticate the connection or trust relation.

6.5.1.2 Rationale

The security assets or network assets of the equipment may be communicated to other communication partners for example when using web services. Ongoing communication potentially enables an attacker having access to the communication to eavesdrop, manipulate or replay the communication, especially when using wireless technologies. The equipment needs to ensure that the communication is protected against those attacks using secure communication mechanisms.

6.5.1.3 Guidance

There are various technologies that can be applied to secure the communication (see also CRY-1) of the equipment. Best practice communication protocols with corresponding configuration ought to be applied to protect the communication against eavesdropping, manipulation and replay. Typical measures therefore are a combination of authentication, integrity protection, encryption and replay protection. The measures can for example be applied to the communication channel or used for end-to-end protection. The equipment needs to offer best practice communication protocols to other communication partners by default. The way in which the initial relationship of trust is established between the equipment and another entity is crucial for the security of the subsequent communication.

It is strongly advised not to use protocols without or with weak security functionality for communication. In some cases, a deviation from this might be necessary especially for supporting interoperability. For the usage of such protocols, it needs to be foreseeable for the manufacturer that additional security measures are applied for example:

- The target environment of the equipment is an area which is only accessible for authorized persons and the radio communication range is short enough to render connection attempts from outside the building impractical. Typical examples for such areas are industrial sites or locked building service rooms in tenements.
- The target environment of the equipment is a specific network infrastructure using a virtual private network which tunnels the insecure protocol of the equipment.

Generally, it is recommended that the equipment notifies the user when an insecure communication is performed.

For equipment in local or personal networks (e.g., wearables) with limited user interface which does not allow to perform more complex pairing procedures, pairing protocols might be vulnerable to man-in-the-middle attacks. Here the attack vector needs to be reduced with additional measures (possession,

knowledge or inherence) for the establishment of a connection, e.g., a limited time slot for a user interaction which is necessary to complete the pairing.

6.5.1.4 Assessment criteria

6.5.1.4.1 Assessment objective

The assessment addresses the requirement SCM-1.

6.5.1.4.2 Implementation categories

Not applicable.

6.5.1.4.3 Required information

[E.Info.SCM-1.NetworkInterface]: Description of each network interface including:

- the description of the physical characteristics including:
 - (in case of a radio interface) [E.Info.SCM-1.NetworkInterface.Radio]: Technology used, the occupied radio spectrum, the transmission power used on the radio interface and the modes of operation that are implemented; or
 - (in case of a wired interface) [E.Info.SCM-1.NetworkInterface.Wired]: Electrical characteristics used on the wired interface and the modes of operation that are implemented; or
 - (in case of an optical interface) [E.Info.SCM-1.NetworkInterface.Optical]: Optical technology used on the interface and the modes of operation that are implemented; or
 - (in case of an acoustic interface) [E.Info.SCM-1.NetworkInterface.Acoustic]: Acoustic technology used on the interface and the modes of operation that are implemented; and
- the description of the logical characteristics including:
 - [E.Info.SCM-1.NetworkInterface.Protocol]: Description of all communication protocols implemented on the interface documented in [E.Info.SCM-1.NetworkInterface.Radio], [E.Info.SCM-1.NetworkInterface.Wired], [E.Info.SCM-1.NetworkInterface.Optical] or [E.Info.SCM-1.NetworkInterface.Acoustic] and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation; and
- the description of the configuration including
 - applied configuration for the equipment and the available options to change the interface's physical or logical behaviour.

[E.Info.SCM-1.SecurityAsset]: Description of each stored security asset that is communicated over network interfaces documented in [E.Info.SCM-1.NetworkInterface] and for which confidentiality, integrity or authenticity is needed in order to protect the equipment's network assets, including:

- (if a classification of the security assets is applicable) [E.Info.SCM-1.SecurityAsset.Class]: Security asset classification (e.g. root keys, master keys, wrapper keys or public keys) where

security assets may be listed in groups as a single category if they are part of the same use case and the same security level; and

- [E.Info.SCM-1.SecurityAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-1.NetworkInterface]; and
- [E.Info.SCM-1.SecurityAsset.NetworkInterface]: Network interface used for communication of the security asset (from [E.Info.SCM-1.NetworkInterface]); and
- (if transfer is protected by physical and logical measures in the targeted environment) [E.Info.SCM-1.SecurityAsset.TrustedEnv]: Description of the physical or logical measures in the equipment's targeted operational environment that ensure that the assets are not exposed to unauthorised entities; and
- (if the assets are part of establishing or managing the connection) [E.Info.SCM-1.SecurityAsset.AddMeasures]: Description of the implemented additional measures to authenticate the connection or trust relation.

[E.Info.SCM-1.NetworkAsset]: Description of each network asset that is communicated over network interfaces documented in [E.Info.SCM-1.NetworkInterface] and for which confidentiality, integrity or authenticity protection is needed, including

- (if a classification of the network assets is applicable) [E.Info.SCM-1.NetworkAsset.Class]: Network asset classification (e.g., network configuration, sensitive network access parameters); network assets may be grouped listed as a single category if they are part of the same use case and the same security level; and
- [E.Info.SCM-1.NetworkAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-1.NetworkInterface]; and
- [E.Info.SCM-1.NetworkAsset.NetInterface]: Network interface used for communication of the network asset (from [E.Info.SCM-1.NetworkInterface]); and
- (if transfer is protected by physical and logical measures in the targeted environment) [E.Info.SCM-1.NetworkAsset.TrustedEnv]: Description of the physical or logical measures in the equipment's targeted operational environment that ensures the assets are not exposed to unauthorised entities; and
- (if the assets are part of establishing or managing the connection) [E.Info.SCM-1.NetworkAssets.AddMeasures]: Description of the implemented additional measures to authenticate the connection or trust relation.

[E.Info.SCM-1.SCM]: Description of each secure communication mechanism that is used to communicate security assets documented in [E.Info.SCM-1.SecurityAsset] and network assets documented in [E.Info.SCM-1.NetworkAsset] over the network interfaces documented in [E.Info.SCM-1.NetworkInterface], including:

- [E.Info.SCM-1.SCM.Protocol]: Communication protocols where the mechanism is applied (from [E.Info.SCM-1.NetworkInterface.Protocol]); and
- [E.Info.SCM-1.SCM.States]: Equipment states where the communication of security assets documented in [E.Info.SCM-1.SecurityAsset] and network assets documented in [E.Info.SCM-1.NetworkAsset] occurs; and

- [E.Info.SCM-1.SCM.SecObjectives]: Security objectives considering the intended functionality of the equipment and the analysed threats and potentially successful attack scenarios (e.g., exposure of data, manipulation of data, unauthorised control of the equipment); and
- (if the equipment supports establishment or management of a connection) [E.Info.SCM-1.SCM.Manage]: Details of the establishment or management procedure.

[E.Info.DT.SCM-1]: Description of the selected path through the decision tree in Figure 17 for each of the relevant network interfaces documented in [E.Info.SCM-1.NetworkInterface].

NOTE Multiple valid paths may need to be documented due to the classification of security assets or network assets and the equipment states documented in [E.Info.SCM-1.SCM.States].

[E.Just.DT.SCM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.SCM-1] with the following properties:

- (if a decision from [DT.SCM-1.DN-2] results in “NOT APPLICABLE”) the justification for the decision [DT.SCM-1.DN-2] is based on [E.Info.SCM-1.SecurityAsset.TrustedEnv] and [E.Info.SCM-1.NetworkAsset.TrustedEnv]; and
- (if a decision from [DT.SCM-1.DN-3] results in “NOT APPLICABLE”) the justification for the decision [DT.SCM-1.DN-3] is based on [E.Info.SCM-1.SecurityAsset.AddMeasures] and [E.Info.SCM-1.NetworkAssets.AddMeasures].

6.5.1.4.4 Conceptual assessment

6.5.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether secure communication mechanisms are implemented when it is required to protect the security assets documented in [E.Info.SCM-1.SecurityAsset] or network assets documented in [E.Info.SCM-1.NetworkAsset] when communicated over network interfaces as required per SCM-1.

6.5.1.4.4.2 Preconditions

None.

6.5.1.4.4.3 Assessment units

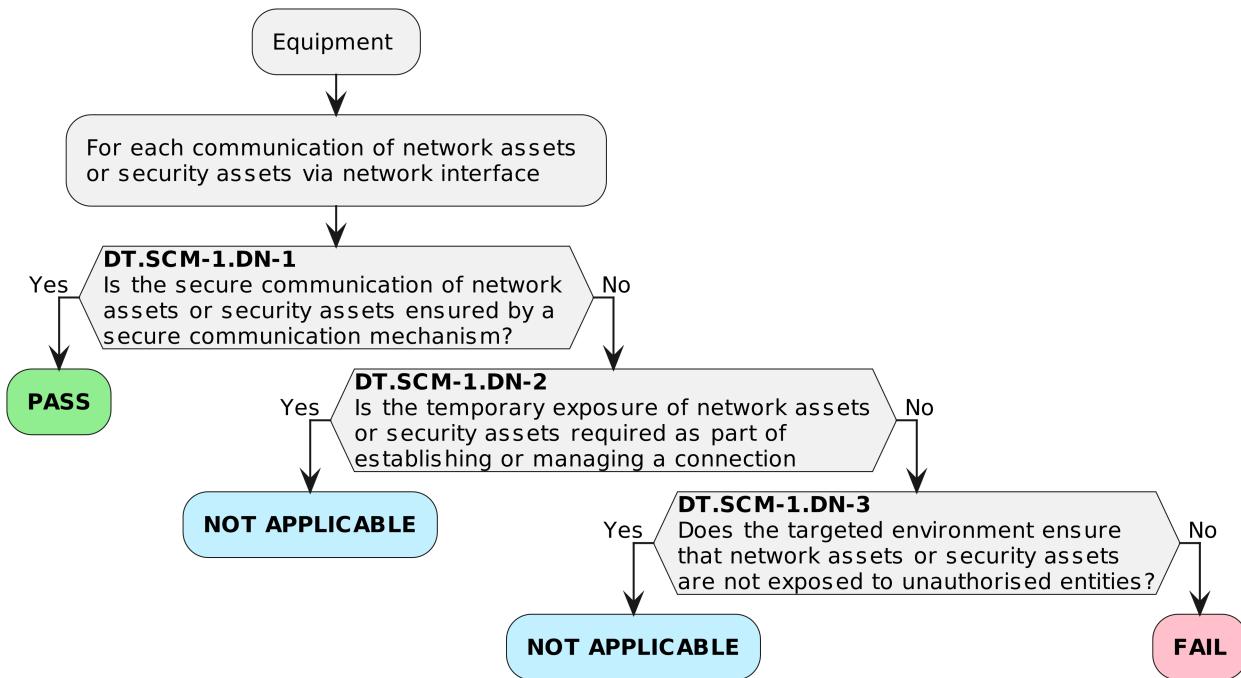


Figure 17 — Decision Tree for requirement SCM-1

For each network interface documented in [E.Info.SCM-1.NetworkInterface], check whether the path through the decision tree documented in [E.Info.DT.SCM-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.SCM-1], examine its justification documented in [E.Just.DT.SCM-1].

6.5.1.4.4.4 Assignment of verdict

The verdict **PASS** for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.SCM-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.SCM-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.SCM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SCM-1].

The verdict **FAIL** for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SCM-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SCM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SCM-1].

The verdict **NOT APPLICABLE** for the assessment case is assigned otherwise.

6.5.1.4.5 Functional completeness assessment

6.5.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation is complete.

6.5.1.4.5.2 Preconditions

The equipment is in an operational state.

6.5.1.4.5.3 Assessment units

Using up-to-date evaluation methods, functionally assess whether there are stored security assets communicated, which are not listed in [E.Info.SCM-1.SecurityAsset].

Using up-to-date evaluation methods, functionally assess whether there are network assets communicated, which are not listed in [E.Info.SCM-1.NetworkAsset].

6.5.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all communicated stored security assets found are documented in [E.Info.SCM-1.SecurityAsset] and all network assets found are documented in [E.Info.SCM-1.NetworkAsset].

The verdict FAIL for the assessment case is assigned if a communicated security asset is found which is not documented in [E.Info.SCM-1.SecurityAsset] or a network asset is found which is not documented in [E.Info.SCM-1.NetworkAsset].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5.1.4.6 Functional sufficiency assessment

6.5.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the secure communication mechanisms are implemented when they are required per SCM-1.

6.5.1.4.6.2 Preconditions

The equipment is in an operational state.

6.5.1.4.6.3 Assessment units

For each security asset documented in [E.Info.SCM-1.SecurityAsset] and for each network asset documented in [E.Info.SCM-1.NetworkAsset], functionally confirm, using up-to-date evaluation methods, the existence of secure communication mechanisms according to [E.Info.SCM-1.SCM] considering the equipment states documented.

6.5.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that a secure communication mechanism documented in [E.Info.SCM-1.SCM] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that a secure communication mechanism documented in [E.Info.SCM-1.SCM] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms

6.5.2.1 Requirement

Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and network assets communicated, except for communicating security assets or network assets where:

- a deviation from best practice for integrity or authenticity protection is required for interoperability reasons.

6.5.2.2 Rationale

During communication security assets and network assets require protection against manipulation. An attacker having gained access to the network might intercept and tamper the communication (man-in-the-middle attack). The equipment needs to ensure that the communication is protected against those attacks by using integrity and authenticity protection measures. The protection could be realized by the protocol used to communicate the security assets or network assets or by an additional protocol/additional measures.

The integrity and authenticity protection applies for encrypted as well as for unencrypted communications.

6.5.2.3 Guidance

In the context of secure communication, “best practice” addresses that approved protocols with corresponding configuration (see also CRY-1) are used and that the implementation of the protocol is regularly reviewed for vulnerabilities (see GEC-1).

The aim is to protect the communication against manipulation. Typical measures are a combination of authentication and integrity protection. The way in which the initial relationship of trust is established between the equipment and another entity is crucial for the security of the communication. The measures can for example be applied to the communication channel or used for “end-to-end” protection. Further, integrity and authenticity protection of communicated is typically realized by using Cipher-based Message Authentication Code (MAC) techniques.

A deviation from best practice is only possible for interoperability reasons within the intended equipment functionality. In this case compensating logical or physical measures need to be considered to ensure a comparable level of security.

The equipment needs to offer best practice protocols to other communication partners by default, even if other protocols might also be needed for interoperability reasons. Appropriate measures may differ between the underlying use cases of the communication to fulfil the equipment’s intended equipment functionality.

Examples for approved protocols which can be used to implement secure communication when best practice configuration (see also CRY-1) is applied are:

- Transport Layer Security (TLS)
- Wi-Fi Protected Access (WPA)
- Password Authenticated Connection Establishment (PACE)
- Symmetrical Cipher Methods (e.g., Advanced Encryption Standard - AES)

Insecure communication is often not caused by flaws in the protocol but by errors in its implementation. Therefore, requirement GEC-1 is important.

6.5.2.4 Assessment criteria

6.5.2.4.1 Assessment objective

The assessment addresses the requirement SCM-2.

6.5.2.4.2 Implementation categories

[IC.SCM-2.ManufSecret]: The method is to introduce the (initial) secret used to ensure integrity and authenticity of communicated network assets and security assets during the production of the equipment. The secret is individual for an equipment and is only used inside it. The protection of integrity and authenticity itself is realized as channel or message based with a message authentication code based on the secret.

[IC.SCM-2.SecChanExchange]: The method to exchange initial secrets relies on an independent channel: The (initial) secret used to ensure integrity and authenticity of communicated network assets and security assets is solely exchanged via a second channel which is independent from the communication mechanism. The protection of integrity and authenticity itself is realized as channel or message based with a message authentication code based on the secret.

EXAMPLE 1 Input of a shared key through a QR Code or manual entry of a secret

[IC.SCM-2.PKI-based]: The method to authenticate the certificate used to ensure integrity and authenticity of communicated network assets and security assets is solely based on the signature of the certificate issued by a trusted PKI. The protection of integrity and authenticity itself is realized channel or message based with a message authentication code based on the secret.

EXAMPLE 2 Usage of X.509 PKI-Certificates for TLS

[IC.SCM-2.ThirdPartyTrust]: The method to authenticate the (initial) secret used to ensure integrity and authenticity of communicated network assets and security assets solely based on an existing trust relation to a third party which confirms the authenticity of the secret. The protection of integrity and authenticity itself is realized channel or message based with a message authentication code based on the secret.

EXAMPLE 3 Kerberos protocol

[IC.SCM-2.Generic]: The methods to ensure integrity and authenticity of communicated network assets and security assets do not solely rely on any of the methods described before in this section.

6.5.2.4.3 Required information

[E.Info.SCM-2.SecurityAsset]: Description of each stored security asset that is communicated over network interfaces documented in [E.Info.SCM-2.NetworkInterface] and for which integrity or authenticity protection is needed in order to protect the equipment's network assets, including:

- [E.Info.SCM-2.SecurityAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-2.NetworkInterface].

NOTE 1 The information of [E.Info.SCM-2.SecurityAsset] is a subset of [E.Info.SCM-1.SecurityAsset].

[E.Info.SCM-2.NetworkAsset]: Description of each network asset that is communicated over network interfaces documented in [E.Info.SCM-2.NetworkInterface] and for which integrity or authenticity protection is needed, including:

- [E.Info.SCM-2.NetworkAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-2.NetworkInterface].

NOTE 2 This information of [E.Info.SCM-2.NetworkAsset] is a subset of [E.Info.SCM-1.NetworkAsset].

[E.Info.SCM-2.NetworkInterface]: Description of all network interfaces of the equipment, including

- [E.Info.SCM-2.NetworkInterface.Protocol]: All communication protocols implemented and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation.

[E.Info.SCM-2.SCM]: Description of each secure communication mechanism that is required per SCM-1 for the integrity and authenticity protection of communicated network assets documented in [E.Info.SCM-2.NetworkAsset] or security assets documented in [E.Info.SCM-2.SecurityAsset], including

- [E.Info.SCM-2.SCM.Capabilities]: Description of the security mechanisms and cryptographic modes that are used to protect the integrity and authenticity of security assets documented in [E.Info.SCM-2.SecurityAsset] or network assets documented in [E.Info.SCM-2.NetworkAsset] while communicated over network interfaces security; and
- (if the SCM implementation is based on [IC.SCM-2.ManufSecret]) [E.Info.SCM-2.SCM.ManufSecret]: Description of how the initial trust is achieved for integrity and authenticity protection and how it is implemented in the protocol documented in [E.Info.SCM-2.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-2.SecChanExchange]) [E.Info.SCM-2.SCM.SecChanExchange]: Description of how the second channel is realized and how the secret is used for integrity and authenticity protection and how it is implemented in the protocol documented in [E.Info.SCM-2.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-2.PKI-based]) [E.Info.SCM-2.SCM.PKI-based]: Description of how the PKI-certificates are validated and how this is implemented for integrity and authenticity protection in the protocol documented in [E.Info.SCM-2.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-2.ThirdPartyTrust]) [E.Info.SCM-2.SCM.ThirdPartyTrust]: Description of how the existing trust relation to a third party which confirms the authenticity of the secret is realized and how this is implemented for integrity and authenticity protection in the protocol documented in [E.Info.SCM-2.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-2.Generic]) [E.Info.SCM-2.SCM.Generic]: Description of how integrity and authenticity protection is realized in the protocol documented in [E.Info.SCM-2.NetworkInterface.Protocol]; and
- (if available) [E.Info.SCM-2.SCMImplDetail]: Refer to versioned standards or specifications where the selected implementation category is defined and, if applicable, the SW library that is used for the implementation; and

- [E.Info.SCM-2.SCM.CCK]: The description of the properties of the confidential cryptographic keys used for integrity and authenticity protection (see CRY-1); and
- [E.Info.SCM-2.SCM.ThreatProtection]: The description on how the mechanism protects against the following security threats:
 - Spoofing; and
 - Tampering.

[E.Info.DT.SCM-2]: Description of the selected path through the decision tree in Figure 18 for each secure communication mechanism documented in [E.Info.SCM-2.SCM].

NOTE 3 Multiple valid paths might need documentation due to the classification of security assets or network assets and the equipment states documented in [E.Info.SCM-2.SCM].

[E.Just.DT.SCM-2]: Justification for the selected path through the decision tree documented in [E.Info.DT.SCM-2] with the following property:

- the justification for the decision [DT.SCM-2.DN-1] is especially based on [E.Info.SCM-2.SecurityAsset.Com], [E.Info.SCM-2.NetworkAsset.Com], [E.Info.SCM-2.SCM.ThreatProtection] and [E.Info.SCM-2.SCM.Capabilities]; and
- (if a decision from [DT.SCM-2.DN-2] results in “NOT APPLICABLE”) the justification for the decision [DT.SCM-2.DN-2] is especially based on [E.Info.SCM-2.SecurityAsset.Com], [E.Info.SCM-2.PrivacyAsset.Com] and [E.Info.SCM-2.SCM.Capabilities].

6.5.2.4.4 Conceptual assessment

6.5.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure communication mechanism of the equipment is protecting the integrity and authenticity of security assets and network assets as required per SCM-2.

6.5.2.4.4.2 Preconditions

None.

6.5.2.4.4.3 Assessment units

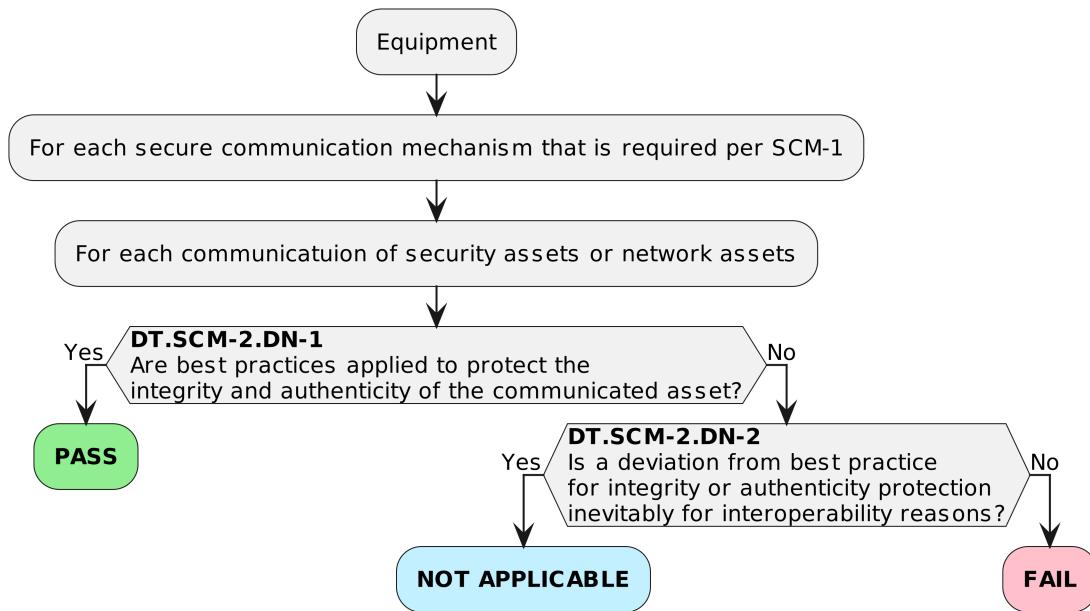


Figure 18 — Decision Tree for requirement SCM-2

For each secure communication mechanism in [E.Info.SCM-2.SCM], and for each equipment state documented, check whether the path through the decision tree documented in [E.Info.DT.SCM-2] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.SCM-2], examine its justification documented in [E.Just.DT.SCM-2].

6.5.2.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.SCM-2] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.SCM-2] ends with “FAIL”; and
- the information provided in [E.Just.DT.SCM-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SCM-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SCM-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SCM-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SCM-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5.2.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the secure communication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

6.5.2.4.6 Functional sufficiency assessment

6.5.2.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the security assets and network assets communicated are protected against unnoticed tampering.

6.5.2.4.6.2 Preconditions

The equipment is in an operational state.

6.5.2.4.6.3 Assessment units

For each security asset documented in [E.Info.SCM-2.SecurityAsset] and network asset documented in [E.Info.SCM-2.NetworkAsset], functionally confirm, using up-to-date evaluation methods, that integrity and authenticity protection is ensured by the communication mechanisms according to [E.Info.SCM-2.SCM] considering the equipment states documented, applying the documented implementation categories:

[AU.SCM-2.ManufSecret]: For [IC.SCM-2.ManufSecret], functionally confirm, as documented in [E.Info.SCM-2.SCM.ManufSecret], that:

- the secret introduced during production cannot be intercepted while the equipment is communicating via network; and
- a manipulated message is not accepted as being of integrity; and
- an unauthorized message is not accepted as authentic; and
- a successful MitM attack is not possible in case that channel-based communication is used.

[AU.SCM-2.SecChanExchange]: For [IC.SCM-2.SecChanExchange], functionally confirm, as documented in [E.Info.SCM-2.SCM.SecChanExchange], that:

- the secret cannot be intercepted using the assessed communication mechanism; and
- a manipulated message is not accepted as being of integrity; and
- an unauthorized message is not accepted as authentic; and
- a successful MitM attack is not possible in case that channel-based communication is used.

[AU.SCM-2.PKI-based]: For [IC.SCM-2.PKI-based], functionally confirm, as documented in [E.Info.SCM-2.SCM.PKI-based], that:

- a forged certificate is not accepted; and
- a manipulated message is not accepted as being of integrity; and
- an unauthorized message is not accepted as authentic; and

- a successful MitM attack is not possible in case that channel-based communication is used.

[AU.SCM-2.ThirdPartyTrust]: For [IC.SCM-2.ThirdPartyTrust], functionally confirm, as documented in [E.Info.SCM-2.SCM.ThirdPartyTrust], that:

- the response of the third party cannot be manipulated; and
- a manipulated message is not accepted as being of integrity; and
- an unauthorized message is not accepted as authentic; and
- a successful MitM attack is not possible in case that channel-based communication is used.

[AU.SCM-2.Generic]: For [IC.SCM-2.Generic], functionally confirm, as documented in [E.Info.SCM-2.SCM.Generic], that:

- secrets used for the protection of authenticity and integrity cannot be intercepted and misused; and
- a manipulated message is not accepted as being of integrity; and
- an unauthorized message is not accepted as authentic; and
- a successful MitM attack is not possible in case that channel-based communication is used.

6.5.2.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each secure communication mechanism documented in [E.Info.SCM-2.SCM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for a secure communication mechanism documented in [E.Info.SCM-2.SCM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms

6.5.3.1 Requirement

Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed, except for communicating security assets or network assets where:

- a deviation from best practice for protecting confidentiality is required for interoperability reasons.

6.5.3.2 Rationale

During communication, generally security assets and network assets require protection against eavesdropping. An attacker having gained access to the network over which the equipment communicates security assets or network assets might monitor the communication. The equipment needs to ensure that the communication is protected against those attacks by providing confidentiality.

6.5.3.3 Guidance

In the context of secure communication, “best practice” addresses that approved protocols with corresponding configuration (especially concerning the integrated cryptography, see CRY-1) are used and that the implementation of the protocol is regularly reviewed for vulnerabilities (see GEC-1).

There are various security mechanisms that can be applied to secure the confidentiality of the communication (see also CRY-1). Best practice configuration ought to be applied to protect the communication from eavesdropping. This is typically achieved by symmetric encryption schemes. Those schemes can be applied to the communication channel or used for “end-to-end” protection. It is recommended to provide confidentiality by default between the communicating entities and to use best practice cryptography. If there is the necessity for deviating from best practices (e.g., due to interoperability reasons) the resulting risks towards “best practice security” ought to be assessed. Appropriate measures may differ between the underlying use cases of the communication to fulfil the equipment’s intended equipment functionality.

A deviation from best practice is only possible for interoperability reasons within the intended equipment functionality. In this case compensating logical or physical measures need to be considered to ensure a comparable level of security.

If confidentiality needs to be preserved for a long period of time it is recommended to use cryptography and cryptographic protocols best practices which enforce perfect forward secrecy for network assets and security assets communicated.

The cryptographic schemes used to protect the confidentiality of the data communicated is determined in the requirement CRY-1.

NOTE Authenticated encryption (AE) can be used to assure data confidentiality and authenticity in one cryptographic scheme. Those schemes can be used to address the requirement in SCM-2 as well.

6.5.3.4 Assessment criteria

6.5.3.4.1 Assessment objective

The assessment addresses the requirement SCM-3.

6.5.3.4.2 Implementation categories

[IC.SCM-3.MessageEnc]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the encryption. The method is that each message encapsulates the content-encryption key to decrypt the payload of the message. This key is encrypted symmetrically or asymmetrically with the existing secret. An authorized receiving entity can only decrypt the payload, if it holds the secret to decrypt the content-encryption key before.

[IC.SCM-3.ChannelEnc]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the encryption. The method is that the equipment and the receiving entity possess the same symmetric key which is used to decrypt and encrypt the payload of communicated messages.

[IC.SCM-3.Generic]: The methods to ensure the confidentiality of communicated network assets and security assets do not solely rely on any of the methods described before in this section.

6.5.3.4.3 Required information

[E.Info.SCM-3.SecurityAsset]: Description of each sored security asset that is communicated over network interfaces documented in [E.Info.SCM-3.NetworkInterface] and for which confidentiality is needed in order to protect the equipment’s network assets, including:

- [E.Info.SCM-3.SecurityAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-3.NetworkInterface].

NOTE 1 The information of [E.Info.SCM-3.SecurityAsset] is a subset of [E.Info.SCM-1.SecurityAsset].

[E.Info.SCM-3.NetworkAsset]: Description of all network assets that are communicated over network interfaces and for which confidentiality is needed, including

- [E.Info.SCM-3.NetworkAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-3.NetworkInterface].

NOTE 2 The information of [E.Info.SCM-3.NetworkAsset] is a subset of [E.Info.SCM-1.NetworkAsset].

[E.Info.SCM-3.NetworkInterface]: Description of all network interfaces of the equipment, including

- [E.Info.SCM-3.NetworkInterface.Protocol]: All communication protocols implemented and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation.

[E.Info.SCM-3.SCM]: Description of each secure communication mechanism that is required per SCM-1 for confidentiality protection of network assets documented in [E.Info.SCM-3.NetworkAsset] or security assets documented in [E.Info.SCM-3.SecurityAsset], including:

- [E.Info.SCM-3.SCM.Capabilities]: Description of the security mechanisms and cryptographic modes that are used to protect the confidentiality of security assets documented in [E.Info.SCM-3.SecurityAsset] or network assets documented in [E.Info.SCM-3.NetworkAsset] while communicated over network interfaces; and
- (if the SCM implementation is based on [IC.SCM-3.MessageEnc]) [E.Info.SCM-3.MessageEnc]: Description of how the content-encryption key is generated and encrypted for confidentiality protection and how it is implemented in the protocol documented in [E.Info.SCM-3.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-3.ChannelEnc]) [E.Info.SCM-3.ChannelEnc]: Description of how the session key is generated and used for confidentiality protection and how it is implemented in the protocol documented in [E.Info.SCM-3.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-3.Generic]) [E.Info.SCM-3.Generic]: Description of how confidentiality protection is realized in the protocol documented in [E.Info.SCM-3.NetworkInterface.Protocol]; and
- (if available) [E.Info.SCM-3.SCMImplDetail]: Refer to versioned standards or specifications where the selected implementation category is defined and, if applicable, the SW library that is used for the implementation; and
- [E.Info.SCM-3.SCM.CCK]: The properties of the confidential cryptographic keys used for confidentiality protection (see CRY-1); and
- [E.Info.SCM-3.SCM.ThreatProtection]: How the mechanism at least protects against the following security threats:
 - Information disclosure; and

- Elevation of privilege

[E.Info.DT.SCM-3]: Description of the selected path through the decision tree in Figure 191 for each secure communication mechanism documented in [E.Info.SCM-3.SCM].

NOTE 3 Multiple valid paths may need to be documented due to the classification of security assets or network assets and the equipment states documented in [E.Info.SCM-3.SCM].

[E.Just.DT.SCM-3]: Justification for the selected path through the decision tree documented in [E.Info.DT.SCM-3] with the following properties:

- The justification for the decision [DT.SCM-3.DN-1] is especially based on [E.Info.SCM-3.SecurityAsset.Com], [E.Info.SCM-3.NetworkAsset.Com], [E.Info.SCM-3.SCM.ThreatProtection] and [E.Info.SCM-3.SCM.Capabilities]; and
- (if a decision from [DT.SCM-3.DN-2] results in “NOT APPLICABLE”) The justification for the decision [DT.SCM-3.DN-2] is especially based on [E.Info.SCM-3.SecurityAsset.Com], [E.Info.SCM-3.NetworkAsset.Com] and [E.Info.SCM-3.SCM.Capabilities].

6.5.3.4.4 Conceptual assessment

6.5.3.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure communication mechanism of the equipment is protecting the confidentiality of network assets (documented in [E.Info.SCM-3.NetworkAsset]) and security assets (documented in [E.Info.SCM-3.SecurityAsset]) while communicated as required per SCM-3.

6.5.3.4.4.2 Preconditions

None.

6.5.3.4.4.3 Assessment units

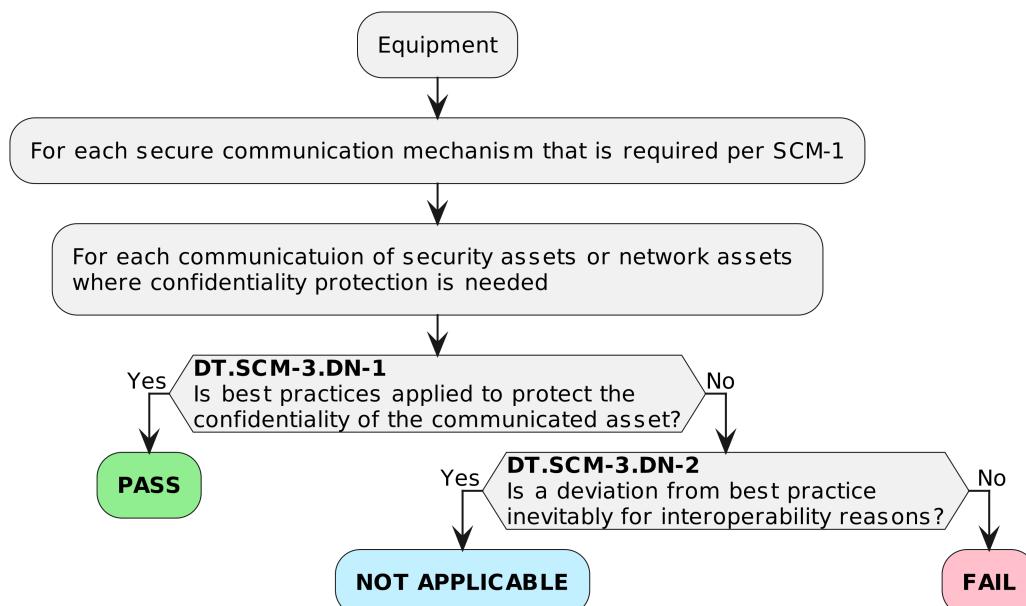


Figure 191 — Decision tree for requirement SCM-3

For each secure communication mechanism documented in [E.Info.SCM-3.SCM], and for each equipment state documented, check whether the path through the decision tree documented in [E.Info.DT.SCM-3] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.SCM-3], examine its justification documented in [E.Just.DT.SCM-3].

6.5.3.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.SCM-3] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.SCM-3] ends with “FAIL”; and
- the information provided in [E.Just.DT.SCM-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SCM-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SCM-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SCM-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SCM-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5.3.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the secure communication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.5.3.4.6 Functional sufficiency assessment

6.5.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the security assets or network assets communicated are protected against eavesdropping.

6.5.3.4.6.2 Preconditions

The equipment is in an operational state.

6.5.3.4.6.3 Assessment units

Perform a legitimate communication for each security asset documented in [E.Info.SCM-3.SecurityAsset] and network asset documented in [E.Info.SCM-3.NetworkAsset], between the equipment and an authorised communication endpoint. Functionally confirm, using up-to-date evaluation methods, that confidentiality protection is ensured by the communication mechanisms according to [E.Info.SCM-3.SCM] considering the equipment states documented, applying the documented implementation categories:

[AU.SCM-3.MessageEnc]: For [IC.SCM-3.MessageEnc], functionally confirm, as documented in [E.Info.SCM-3.MessageEnc], that:

- the key inside the message which is used to encrypt the payload cannot be disclosed; and

- the communicated security assets and network assets cannot be eavesdropped.

[AU.SCM-3.ChannelEnc]: For [IC.SCM-3.ChannelEnc], functionally confirm, as documented in [E.Info.SCM-3.ChannelEnc], that:

- the key which is used to encrypt the messages inside the communication channel cannot be intercepted; and
- the communicated security assets and network assets cannot be eavesdropped.

[AU.SCM-3.Generic]: For [IC.SCM-3.Generic], functionally confirm, as documented in [E.Info.SCM-3.Generic], that:

- the secret used to encrypt the message cannot be intercepted or eavesdropped; and
- the encrypted content of the message cannot be eavesdropped or disclosed.

6.5.3.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each secure communication mechanism documented in [E.Info.SCM-3.SCM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for a secure communication mechanism documented in [E.Info.SCM-3.SCM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms

6.5.4.1 Requirement

Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the network assets communicated against replay attacks, except for communicating security assets or network assets where:

- a duplicate transfer does not impose a threat of a replay attack; or
- a deviation from best practice for replay protection is required for interoperability reasons.

6.5.4.2 Rationale

A replay attack is a form of network attack in which valid data transmission is maliciously repeated. An attacker having gained access to the network might record the communication and replay it unchanged, causing undesired effects at the receiving entity. A replay attack poses a threat in particular if authentication can be undermined or unauthorized control commands can be submitted.

For example, if, during a login process of a user the password is communicated encrypted, but without replay protection (especially session hijacking protection), an attacker may be able to replay the encrypted login part of the communication, and thus gain maliciously authorized access to the system. A session hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. The equipment needs to protect the communication against that class of attacks.

Based on a risk assessment use cases might be identified for which a replay protection might not be needed, e.g., when the data communicated does not lead to a state change at the receiving entity. For example, the request to retrieve an X.509 certificate from a server might not pose a risk for a replay attack.

6.5.4.3 Guidance

Replay attacks can typically be prevented by tagging each message of a communication session with a session ID and a counter. The session ID prevents replay attacks of the complete communication, while the counter prevents the replay of a specific messages within a communication session. Further, timestamps or a one-time encryption technique can be used to prevent replay attacks. Nevertheless, the implementation of replay attack protection is complex. Therefore, the usage of approved protocols which provide already replay attack protection needs to be considered first. Examples for approved protocols which can be used to implement secure communication when best practice configuration (see also CRY-1) is applied are:

- Transport Layer Security (TLS)
- Secure Socket Shell (SSH)
- Internet Protocol Security (IPsec)

6.5.4.4 Assessment criteria

6.5.4.4.1 Assessment objective

The assessment addresses the requirement SCM-4.

6.5.4.4.2 Implementation categories

[IC.SCM-4.SeqNumb]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the message authentication code to ensure the integrity of the communication. The method is that a unique sequence number is assigned to each message transmitted. When the recipient receives a message, it checks the sequence number to ensure that it has not been received before. If the sequence number has already been seen, the message is discarded as a replay attack.

NOTE 1 To protect against MitM Attacks the authenticity of the sequence number can be ensured by using it as input to the function generating the message authentication code (MAC).

[IC.SCM-4.TimeStamp]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the message authentication code to ensure the integrity of the communication. The method is that the equipment integrates timestamps in messages to ensure that they are not being replayed at a later point in time. The recipient checks the timestamp to make sure that the message was not generated too far in the past or future.

NOTE 2 To protect against MitM Attacks the authenticity of the timestamp can be ensured by using it as input to the function generating the message authentication code (MAC).

[IC.SCM-4.OneTimeEncKey]: The sending entity and the receiving entity have already exchanged a secret via a trust relation which builds the basis for the encryption of the messages. The method is that the equipment and the receiver establish a completely random session key, which is a type of code that is only valid for one transaction and cannot be reused.

[IC.SCM-4.Generic]: The methods to avoid replay attacks concerning communicated network assets and security assets do not solely rely on any of the methods described before in this section.

6.5.4.4.3 Required information

[E.Info.SCM-4.SecurityAsset]: Description of each stored security asset that is communicated over network interfaces documented in [E.Info.SCM-4.NetworkInterface] and for which replay protection is needed in order to protect the equipment's network assets, including:

- [E.Info.SCM-4.SecurityAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-4.NetworkInterface].

NOTE 1 The information of [E.Info.SCM-4.SecurityAsset] is a subset of [E.Info.SCM-1.SecurityAsset].

[E.Info.SCM-4.NetworkAsset]: Description of each network asset that is communicated over network interfaces documented in [E.Info.SCM-4.NetworkInterface] and for which replay protection is needed, including:

- [E.Info.SCM-4.NetworkAsset.Com]: Description of the use case where the asset is communicated (e.g. pairing with base station) over a network interface documented in [E.Info.SCM-4.NetworkInterface].

NOTE 2 The information of [E.Info.SCM-4.NetworkAsset] is a subset of [E.Info.SCM-1.NetworkAsset].

[E.Info.SCM-4.NetworkInterface]: Description of each network interface of the equipment, including:

- [E.Info.SCM-4.NetworkInterface.Protocol]: All communication protocols implemented and the modes of operation that are implemented, the version of the protocol and, if applicable, the SW library that is used for the implementation.

[E.Info.SCM-4.SCM]: Description of each secure communication mechanism that is required per SCM-1 for replay protection of network assets documented in [E.Info.SCM-4.NetworkAsset] or security assets documented in [E.Info.SCM-4.SecurityAsset], including:

- [E.Info.SCM-4.SCM.Capabilities]: Description of the security mechanisms and cryptographic modes that are used to avoid replay attacks on communication containing security assets documented in [E.Info.SCM-4.SecurityAsset] or network assets documented in [E.Info.SCM-4.NetworkAsset]; and
- (if the SCM implementation is based on [IC.SCM-4.SeqNumb]) [E.Info.SCM-4.SCM.SeqNumb]: Description of how the sequence numbers are used and integrated in the message authentication code for replay protection and how it is implemented in the protocol documented in [E.Info.SCM-4.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-4.TimeStamp]) [E.Info.SCM-4.SCM.TimeStamp]: Description of how the time stamps are used and integrated in the message authentication code for replay protection and how it is implemented in the protocol documented in [E.Info.SCM-4.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-4.OneTimeEncKey]) [E.Info.SCM-4.SCM.OneTimeEncKey]: Description of how the one-time encryption key is generated and used for replay protection and how it is implemented in the protocol documented in [E.Info.SCM-4.NetworkInterface.Protocol]; and
- (if the SCM implementation is based on [IC.SCM-4.Generic]) [E.Info.SCM-4.SCM.Generic]: Description of how replay protection is realized in the protocol documented in [E.Info.SCM-4.NetworkInterface.Protocol]; and
- (if standards or specifications where the selected implementation category is defined are available) [E.Info.SCM-4.SCMImplDetail]: Reference to versioned standards or specifications where the selected implementation category is defined and, if applicable, the SW library that is used for the implementation; and

- [E.Info.SCM-4.SCM.Repudiation]: Description of how the mechanism at least protects against the security threat “Repudiation”.

[E.Info.DT.SCM-4]: Description of the selected path through the decision tree in Figure 20 for each secure communication mechanism documented in [E.Info.SCM-4.SCM].

NOTE 3 Multiple valid paths may need to be documented due to the classification of security assets or network assets and the equipment states documented in [E.Info.SCM-4.SCM].

[E.Just.DT.SCM-4]: Justification for the selected path through the decision tree documented in [E.Info.DT.SCM-4] with the following properties:

- (if a decision from [DT.SCM-4.DN-1] results in “NOT APPLICABLE”) The justification for the decision [DT.SCM-4.DN-1] is based on [E.Info.SCM-4.SecurityAsset.Com], [E.Info.SCM-4.NetworkAsset.Com], [E.Info.SCM-4.SCM.Capabilities] and [E.Info.SCM-4.SCM.Repudiation]; and
- (if a decision from [DT.SCM-4.DN-3] results in “NOT APPLICABLE”) The justification for the decision [DT.SCM-4.DN-3] is especially based on [E.Info.SCM-4.SecurityAsset.Com], [E.Info.SCM-4.NetworkAsset.Com] and [E.Info.SCM-4.SCM.Capabilities].

6.5.4.4.4 Conceptual assessment

6.5.4.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each secure communication mechanism of the equipment is protecting the communication of security assets and network assets communicated against replay attacks as required per SCM-4.

6.5.4.4.4.2 Preconditions

None.

6.5.4.4.4.3 Assessment units

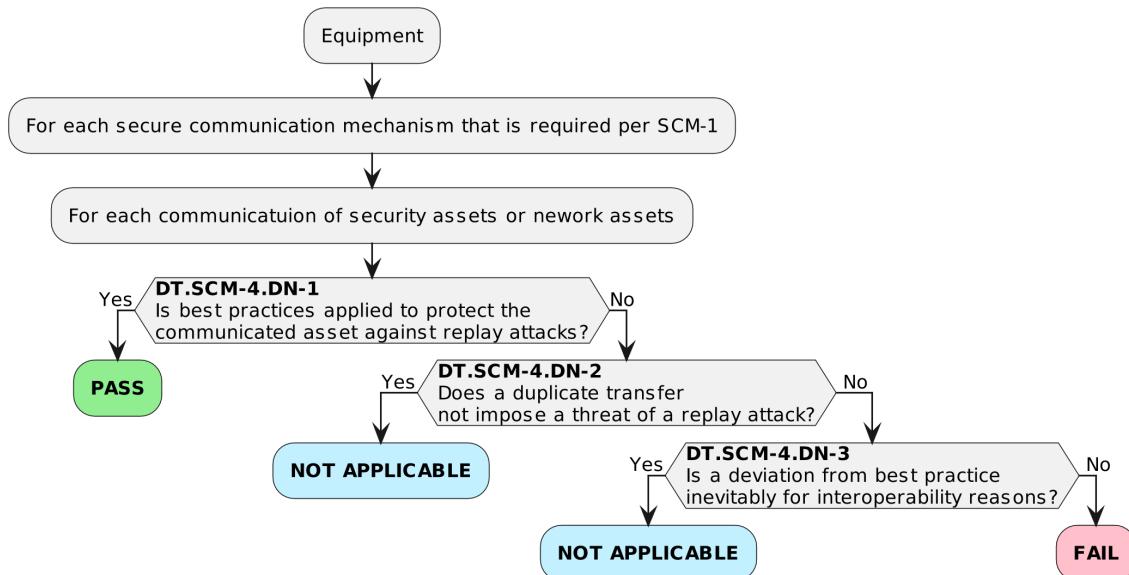


Figure 202 — Decision tree for requirement SCM-4

For each secure communication mechanism in [E.Info.SCM-4.SCM], and for each equipment state documented, check whether the path through the decision tree documented in [E.Info.DT.SCM-4] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.SCM-4], examine its justification documented in [E.Just.DT.SCM-4].

6.5.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.SCM-4] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.SCM-4] ends with “FAIL”; and
- the information provided in [E.Just.DT.SCM-4] are correct justifications for all paths through the decision tree documented in [E.Info.DT.SCM-4].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.SCM-4] ends with “FAIL”; or
- a justification provided in [E.Just.DT.SCM-4] is not correct or missing for a path through the decision tree documented in [E.Info.DT.SCM-4].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.5.4.5 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the secure communication mechanism’s applicability.

Therefore, this functional completeness assessment is not necessary.

6.5.4.6 Functional sufficiency assessment

6.5.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the security assets and network assets communicated are protected against replay attacks.

6.5.4.6.2 Preconditions

The equipment is in an operational state.

6.5.4.6.3 Assessment units

Perform a legitimate communication for each security asset documented in [E.Info.SCM-4.SecurityAsset] and network asset documented in [E.Info.SCM-4.NetworkAsset], between the equipment and an authorised communication endpoint. The communication sequences are recorded. Functionally confirm, using up-to-date evaluation methods, that replay protection is ensured by the communication mechanisms according to [E.Info.SCM-4.SCM] considering the equipment states documented, applying the documented implementation categories:

[AU.SCM-4.SeqNumb]: For [IC.SCM-4.SeqNumb], functionally confirm, as documented in [E.Info.SCM-4.SCM.SeqNumb], that:

- the incoming message (part of the communication of security assets and network assets) with a repeating sequence number is not accepted.

[AU.SCM-4.TimeStamp]: For [IC.SCM-4.TimeStamp], functionally confirm, as documented in [E.Info.SCM-4.SCM.TimeStamp], that:

- the incoming message (part of the communication of security assets and network assets) with an irregular timestamp is not accepted.

[AU.SCM-4.OneTimeEncKey]: For [IC.SCM-4.OneTimeEncKey], functionally confirm, as documented in [E.Info.SCM-4.SCM.OneTimeEncKey], that:

- the encryption key cannot be intercepted; and
- that the duplicate (binary copy) of an already accepted message (part of the communication of security assets and network assets) is not accepted again.

[AU.SCM-4.Generic]: For [IC.SCM-4.Generic], functionally confirm, as documented in [E.Info.SCM-4.SCM.Generic], that:

- that the duplicate (binary copy) of an already accepted message (part of the communication of security assets and network assets) is not accepted again.

6.5.4.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each secure communication mechanism documented in [E.Info.SCM-4.SCM] with the corresponding methods to ensure replay protection for the communication of security assets and network assets the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for any secure communication mechanism documented in [E.Info.SCM-4.SCM] with the corresponding methods to ensure replay protection for the communication of security assets and network assets a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.6 [RLM] Resilience mechanism

6.6.1 [RLM-1] Applicability and appropriateness of resilience mechanisms

6.6.1.1 Requirement

The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces and return to a defined state after the attack except for:

- network interfaces that are only used in a local network that do not interoperate with other networks; or
- network interfaces where other devices in the network provide sufficient protection against DoS attacks and loss of essential functions for network operations.

6.6.1.2 Rationale

Denial of Service attacks are disruptive to the availability of network resources and may cause permanent disruption in network operation if the attacked equipment is not recovering from a DoS attack properly.

Equipment that participates in the networking functions (e.g., a Mesh Networking node), needs to be able to recover from a DoS attack to be able to continue to support the networking functions.

Some industrial equipment requires very high availability to operate continuously. Mechanisms such as rate limiting could restrict authorized access to critical functions. Hence, resilience mechanisms on industrial equipment can be implemented in the environment of the equipment and not embedded in the equipment itself to avoid impact on its continuous operation.

6.6.1.3 Guidance

To reduce the effect of such attacks on the network interfaces, equipment ought to be designed in such a manner that it can employ functions that reduce the effect of such attacks on the network services and resources.

This means that when the network interfaces are subjected to Denial of Service attacks the equipment is designed so that it can recover to a defined state following the attack. The defined state is specified by the manufacturer of the equipment for the intended equipment functionality and may include resilience mechanisms enabling the equipment to maintain essential functions while being subjected to the effects of a Denial-of-Service attacks on one or more of its network interfaces.

The equipment enters a defined state during the attack and recovers to a defined operational state when the attack is finished. The aim is to ensure that the equipment continues to work during an ongoing attack on the network interfaces. Examples of resilience mechanisms that may be applicable depending on the intended equipment functionality are:

- Network storm protection
- Network packet filtering mechanisms
- Network traffic rate limiting techniques
- Strategies involving reservation of equipment internal resources (to limit use of resources and protect against exhaustion)

The selected resilience mechanisms need to avoid interfering with the intended equipment functionality or harm the availability of important and essential functions as documented by the manufacturer.

6.6.1.4 Assessment criteria

6.6.1.4.1 Assessment objective

The assessment addresses the requirement RLM-1.

6.6.1.4.2 Implementation categories

Not applicable.

6.6.1.4.3 Required information

(If the equipment communicates over network interfaces to the network) [E.Info.RLM-1.NetworkInterface]: Description of each network interface.

(If the equipment provides a resilience mechanism for mitigating the effects of DoS Attacks on the network interfaces) [E.Info.RLM-1.RLM]: Description of each resilience mechanism used for mitigating the effect of DoS Attacks on the network interfaces and returning the equipment to a defined state following the attack.

[E.Info.DT.RLM-1]: Description of the selected path through the decision tree in Figure 21 for each network interface that is documented in [E.Info.RLM-1.NetworkInterface].

[E.Just.DT.RLM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.RLM-1] including justifications for the decisions [DT.RLM-1.DN-1], [DT.RLM-1.DN-2] and [DT.RLM-1.DN-3] based on [E.Info.RLM-1.NetworkInterface] and [E.Info.RLM-1.RLM].

6.6.1.4.4 Conceptual assessment

6.6.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether a resilience mechanism is implemented when it is required per RLM-1.

6.6.1.4.4.2 Preconditions

None.

6.6.1.4.4.3 Assessment units

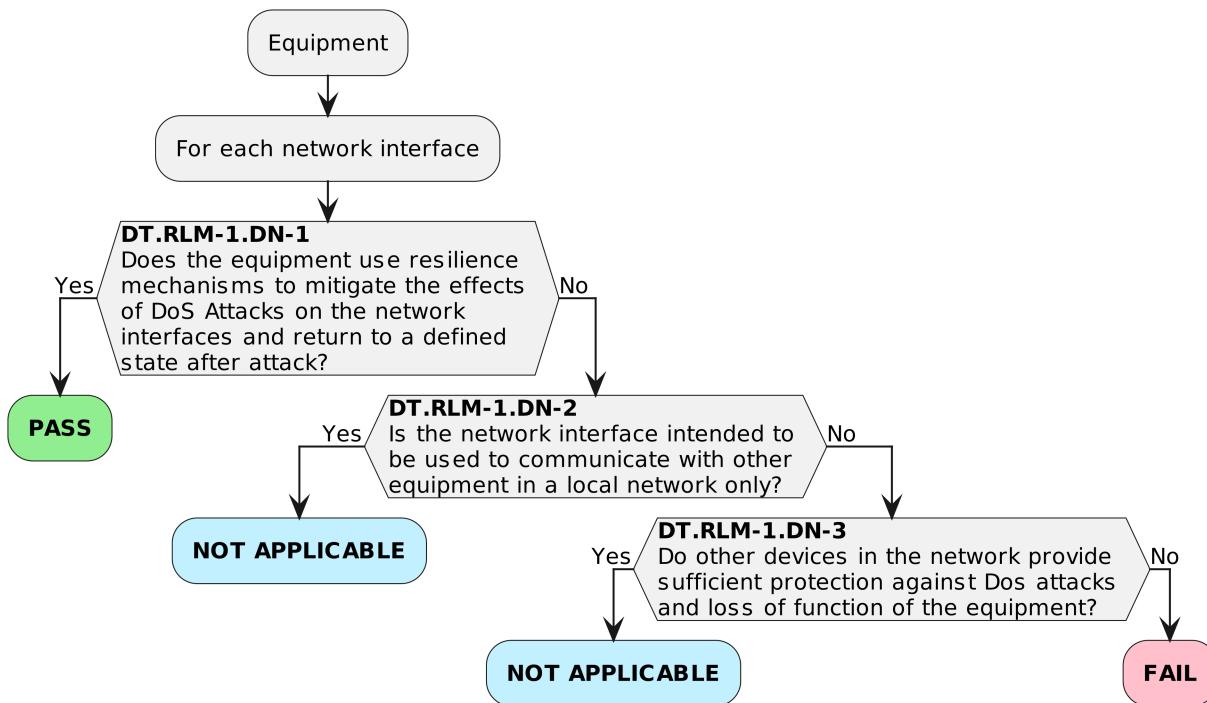


Figure 213 — Decision tree for requirement RLM-1

For each network interface documented in [E.Info.RLM-1.NetworkInterface], check whether the path through the decision tree documented in [E.Info.DT.RLM-1] ends with "NOT APPLICABLE" or "PASS".

For each path through the decision tree documented in [E.Info.DT.RLM-1], examine its justification documented in [E.Just.DT.RLM-1].

6.6.1.4.4 Assignment of verdict

The verdict **PASS** for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.RLM-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.RLM-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.RLM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.RLM-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.RLM-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.RLM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.RLM-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.6.1.4.5 Functional completeness assessment

6.6.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional validation whether the resilience mechanisms implemented mitigate the effects of DoS Attacks on the network interfaces and that the equipment returns to a defined state after an attack with regard to completeness of documentation of network interfaces and the correctness of implementation.

6.6.1.4.5.2 Preconditions

The equipment is in an operational state and each network interface documented in [E.Info.RLM-1.NetworkInterface] needs to either be enabled or configured so that each network interface can be tested.

Where [E.Info.RLM-1.RLM] are used, documentation is provided that specifies information on what to configure/ the required configuration of the RLM to be able to test the implemented mechanisms.

6.6.1.4.5.3 Assessment units

Functionally assess whether there are network interfaces, which are not listed in [E.Info.RLM-1.NetworkInterface].

Functionally assess if resilience mechanisms are implemented that are not documented in [E.Info.RLM-1.RLM].

6.6.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all network interfaces found are documented in [E.Info.RLM-1.NetworkInterface] and all resilience mechanisms found are documented in [E.Info.RLM-1.RLM].

The verdict FAIL for the assessment case is assigned if a network interface is found which is not documented in [E.Info.RLM-1.NetworkInterface] or a resilience mechanism is found which is not documented in [E.Info.RLM-1.RLM].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.6.1.4.6 Functional sufficiency assessment

6.6.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the resilience mechanisms are implemented when required per RLM-1.

6.6.1.4.6.2 Preconditions

The equipment is in an operational state and each [E.Info.RLM-1.NetworkInterface] is either enabled or configured.

Where [E.Info.RLM-1.RLM] are used the information on what to configure to be able to test the implemented mechanisms is provided.

6.6.1.4.6.3 Assessment units

Functionally confirm the usage of resilience mechanisms documented in [E.Info.RLM-1.RLM] and used in the justification [E.Just.DT.RLM-1].

Functionally assess whether the resilience mechanisms mitigate the effects of DoS attacks on the network interfaces and that the equipment returns to a defined state following an attack, considering the intended equipment functionality and its intended operational environment of use.

Commercial tools may be used in testing. The purpose of the test tools is to identify if the equipment when subjected to simulated DoS attacks on the network interfaces is capable of returning to a defined state following the simulated attack scenarios. Examples of tools are:

- network scanning tools,
- flooding test tools,
- application scanning tools to discover accessible services,
- and where applicable fuzzing tools such as:
 - protocol fuzzing tools,
 - application fuzzing tools.

6.6.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that a resilience mechanism documented in [E.Info.RLM-1.RLM] is not implemented.

The verdict FAIL for the assessment case is assigned if there is evidence that a resilience mechanism documented in [E.Info.RLM-1.RLM] is not implemented.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.7[NMM] Network monitoring mechanism

6.7.1 [NMM-1] Applicability and appropriateness of network monitoring mechanisms

6.7.1.1 Requirement

If the equipment is a network equipment, the equipment shall provide network monitoring mechanism(s) to detect for indicators of DoS attacks in the network traffic between networks which it processes.

6.7.1.2 Rationale

To increase cyber resilience of a system as a whole against unusual network traffic related to the intended equipment functionality which could lead to a Denial-of-Service (DoS). Each network equipment as a component of such a system needs to be able to detect implications for such DoS events. This requires the equipment to be able to detect unusual traffic and patterns which could be related to a DoS Attack.

6.7.1.3 Guidance

Unusual traffic which ought to be taken into account are network datagrams which can result in a partial or full Denial-of-Service of the network.

The origin of a DoS event can be an unintentional malfunction of an arbitrary network resource as well as an intentional attack.

Usually the network equipment which is implementing this requirement will not be the target of a DoS Attack. Probably it will route or forward the traffic directly or indirectly towards the target.

Detection of DoS events can be behaviour or pattern based, whichever method may be appropriate for the equipment, the intended equipment functionality and intended operational environment of use.

Examples of measures which could be implemented to monitor the network traffic with regard to possible DoS attacks are:

- monitoring of the number of datagrams in a defined timeframe,
- monitoring if there are datagrams which are originating from an unconfigured network or have a destination network which is outside of configured network of the network equipment,
- monitoring of malformed and modified datagrams.

6.7.1.4 Assessment criteria

6.7.1.4.1 Assessment objective

The assessment addresses the requirement NMM-1.

6.7.1.4.2 Implementation categories

[IC.NMM-1.GTPFiltering]: The network monitoring mechanisms are based on the monitoring and filtering of GPRS Tunnelling Protocols messages.

[IC.NMM-1.IPPacketFiltering]: The network monitoring mechanisms are based on the detection of specific internet protocol packets messages such as ICMP or ARP and their misuse to perform a DoS attack. The network equipment may also limit the functionalities related to such internet protocol packets to mitigate a DoS attack.

[IC.NMM-1.Generic]: The network monitoring mechanisms are different from [IC.NMM-1.GTPFiltering] or [IC.NMM-1.IPPacketFiltering].

NOTE Some network equipment may support both [IC.NMM-1.GTPFiltering] and [IC.NMM-1.IPPacketFiltering].

6.7.1.4.3 Required information

If the equipment is a network equipment:

- [E.Info.NMM-1.NMM]: Description of the implemented monitoring mechanism(s) to monitor and analyse the traffic between networks which is processed via the network interfaces of the network equipment including:
 - (if the NMM implementation is based on [IC.NMM-1.GTPFiltering]) [E.Info.NMM-1.NMM.GTPFiltering]: Description how the network monitoring mechanisms are implemented based on the monitoring and filtering of GPRS Tunnelling Protocols messages; and
 - (if the NMM implementation is based on [IC.NMM-1.IPPacketFiltering]) [E.Info.NMM-1.NMM.PacketFiltering]: Description how the network monitoring mechanisms are implemented based on the detection of specific internet protocol packets messages such as ICMP or ARP and their misuse to perform a DoS attack; and
 - [E.Info.NMM-1.NMM.NetworkEquipment]: Documented analysis, rationale and justification regarding the risks for the security assets and network assets which are processed, controlled or served by the network equipment between networks. This analysis is related to the protocol types which are processed by the network equipment for the traffic between networks, in the context of the intended equipment functionality and intended operational environment of use.

[E.Info.DT.NMM-1]: Description of the selected path through the decision tree in Figure 22 for each network monitoring mechanism documented in [E.Info.NMM-1.NMM]. This document needs to explain why the decision was taken under consideration of the content of [E.Info.NMM-1.NMM.NetworkEquipment].

[E.Just.DT.NMM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.NMM-1] with the following properties:

- (if a decision from [DT.NMM-1.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.NMM-1.DN-1] is based on [E.Info.NMM-1.NMM.NetworkEquipment].
- the justification for the decision [DT.NMM-1.DN-2] is based on [E.Info.NMM-1.NMM].

6.7.1.4.4 Conceptual assessment

6.7.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether a network monitoring mechanism is implemented in the network equipment as required per NMM-1.

6.7.1.4.4.2 Preconditions

None.

6.7.1.4.4.3 Assessment units

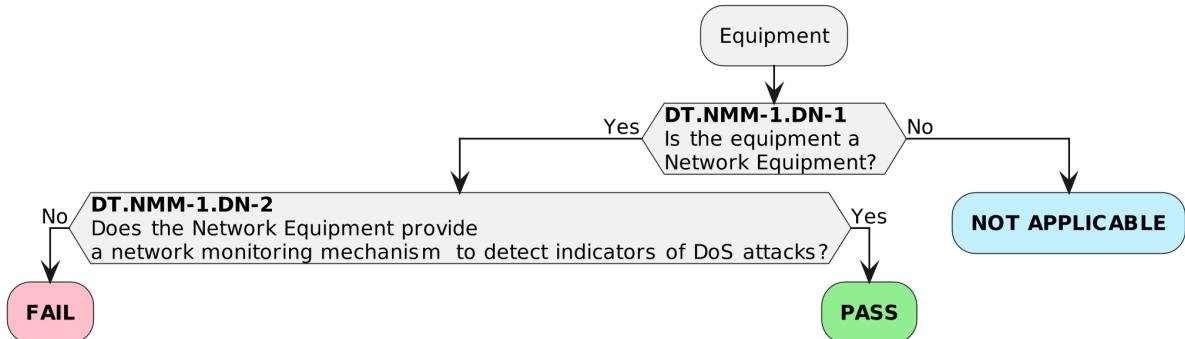


Figure 22 — Decision tree for requirement NMM-1

For each path through the decision tree documented in [E.Info.DT.NMM-1] examine its justification documented in [E.Just.DT.NMM-1].

Check whether the path through the decision tree documented in [E.Info.DT.NMM-1] ends with “NOT APPLICABLE” or “PASS”.

6.7.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.NMM-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.NMM-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.NMM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.NMM-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.NMM-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.NMM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.NMM-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.7.1.4.5 Functional completeness assessment

Functional completeness assessment is not necessary in this clause since the network monitoring mechanism is always mandatory for network equipment.

6.7.1.4.6 Functional sufficiency assessment

6.7.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional validation of the appropriateness of the Network Monitoring Mechanisms described in [E.Info.NMM-1.NMM]. The assessment verifies whether the traffic between networks (which is controlled or processed by the network equipment) is monitored and

analysed to mitigate the risk related to security assets and network assets in the networks documented in [E.Info.NMM-1.NMM.NetworkEquipment].

6.7.1.4.6.2 Preconditions

The equipment is operational and if available setup or configuration which is related to the traffic between networks did take place.

Physical network connection to communicate between networks is established.

6.7.1.4.6.3 Assessment units

For each network monitoring mechanism documented in [E.Info.NMM-1.NMM]:

[AU.NMM-1.GTPFiltering]: When the implementation is based on [IC.NMM-1.GTPFiltering] functionally confirm that:

- GTP messages are monitored by the network equipment; and
- GTP messages sender authorization is verified by the network equipment; and
- the network equipment is able to define and apply rules for the different GTP messages.

[AU.NMM-1.IPPacketFiltering]: When the implementation is based on [IC.NMM-1.IPPacketFiltering] functionally confirm that:

internet protocol packets such as ICMP and ARP are revealed and monitored by the network equipment; and

- a simulated ICMP based DoS attack is detected; and
- a simulated ARP based DoS attack is detected; and
- measure to limit the effect of such DoS attacks are put in place.

[AU.NMM-1.Generic]: When the implementation is based on [IC.NMM-1.Generic] functionally confirm that:

Assessment of traffic between networks processed, controlled, or served by the network equipment.

- Assess traffic between networks processed by the network equipment, to reveal processed protocol types via network analysing tools, use the information in [E.Info.NMM-1.NMM.NetworkEquipment] as a guidance; and
- assess if the revealed traffic and protocol types which are part of the traffic between networks processed by the network equipment are documented in [E.Info.NMM-1.NMM.NetworkEquipment], in relation to the risk for security assets and network assets processed, controlled or served by the network equipment between networks.

Simulate the in [E.Info.NMM-1.NMM] described conditions to trigger the related monitoring e.g., via generating malformed messages or messages in a very high cadence (e.g., via fuzzing), use [E.Info.NMM-1.NMM] as guidance.

Assess if the in [E.Info.NMM-1.NMM] described behaviour or output is generated as documented, use network equipment manual or design documentation as guidance.

6.7.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each network monitoring mechanism documented in [E.Info.NMM-1.NMM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for a network monitoring mechanism documented in [E.Info.NMM-1.NMM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.8[TCM] Traffic control mechanism

6.8.1 [TCM-1] Applicability of and appropriate traffic control mechanisms

6.8.1.1 Requirement

If the equipment is a network equipment, the equipment shall provide network traffic control mechanism(s).

6.8.1.2 Rationale

Malicious data traffic may be generated by a compromised equipment. While operators' networks may implement measures to mitigate the effects of malicious traffic based on a datagram's header information, their knowledge of the network's properties might hinder an effective treatment. Network equipment can have sufficient information to detect malicious traffic and a traffic control mechanism allows to prevent the network from corresponding harm. By implementing these security traffic control mechanisms, network equipment can establish a robust defence against anomalous traffic, protect sensitive data, and maintain the integrity and availability of the intended equipment functionality through its applications and networks.

6.8.1.3 Guidance

Typical equipment, whose intended purpose includes forwarding datagrams and/or routing packets to a network are for example home routers that connect private IP networks to the internet or mobile network access points (i.e., base stations), which enable public mobile network access for other equipment.

Controlling data traffic on network layer based on network addresses includes the network equipment's ability to block or redirect certain datagrams based on their source or destination address.

Traffic control mechanisms refer to the set of mechanisms that can be combined with policies, and procedures designed to monitor, manage, and secure the flow of data and communications. These mechanisms aim to protect the availability and reliability of critical services.

6.8.1.4 Assessment criteria

6.8.1.4.1 Assessment objective

The assessment addresses the requirement TCM-1.

6.8.1.4.2 Implementation Categories

[IC.TCM-1.DatagramRules]: The traffic control mechanism is based on monitoring the IP datagrams and identify for example anomalous patterns, malicious traffic, source or address destination and to define rules such as discard or block such datagrams.

[IC.TCM-1.TrafficSeparation]: The traffic control mechanism is based on full physical or logical separation of traffic belonging to different network domains (e.g. data/forwarding plane, control plane). A full separation means that traffic forwarding between different networks domains is not allowed.

[IC.TCM-1.Generic]: The traffic control mechanism is different from [IC.TCM-1 DatagramRules] and [IC.TCM-1.TrafficSeparation]

NOTE Some network equipment may support both [IC.TCM-1 DatagramRules] and [IC.TCM-1.TrafficSeparation].

6.8.1.4.3 Required information

[E.Info.TCM-1.TCM]: Description of each traffic control mechanism implemented by the network equipment including:

- (if the TCM implementation is based on [IC.TCM-1 DatagramRules]) [E.Info.TCM-1.TCM DatagramRules]: Description how the traffic control mechanisms are implemented based on monitoring the IP datagrams.
- (if the TCM implementation is based on [IC.TCM-1.TrafficSeparation]) [E.Info.TCM-1.TCM TrafficSeparation]: Description how the traffic control mechanisms are implemented based on the physical or logical separation of traffic belonging to different network domains.
- [E.Info.TCM-1.TCM.NetworkEquipment]: Documented analysis, rationale and justification regarding the risk for the security assets and network assets which are processed, controlled or served by the network equipment between networks. This analysis is related to the protocol types which are processed by the network equipment for the traffic between networks, in the context of the intended equipment functionality and intended operational environment of use.

[E.Info.DT.TCM-1]: Description of the selected path through the decision tree in Figure 23 for each traffic control mechanism documented in [E.Info.TCM-1.TCM]. This document needs to explain why the decision was taken under consideration of the content of [E.Info.TCM-1.TCM.NetworkEquipment].

[E.Just.DT.TCM-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.TCM-1] with the following properties:

- (if a decision from [DT.TCM-1.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.TCM-1.DN-1] is based on [E.Info.TCM-1.TCM.NetworkEquipment],
- the justification for the decision [DT.TCM-1.DN-2] is based on [E.Info.TCM-1.TCM].

6.8.1.4.4 Conceptual assessment

6.8.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether a traffic control mechanism is implemented in the network equipment as required per TCM-1.

6.8.1.4.4.2 Preconditions

None.

6.8.1.4.4.3 Assessment units

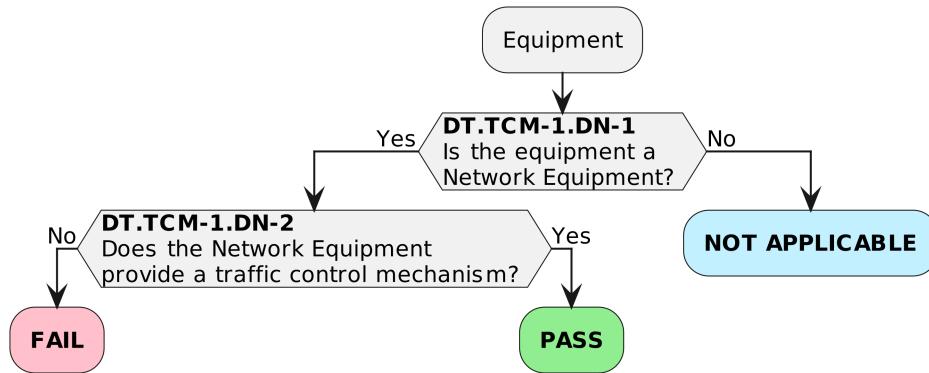


Figure 234 — Decision Tree for requirement TCM-1

For each path through the decision tree documented in [E.Info.DT.TCM-1] examine its justification documented in [E.Just.DT.TCM-1].

Check whether the path through the decision tree documented in [E.Info.DT.TCM-1] ends with "NOT APPLICABLE" or "PASS".

6.8.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.TCM-1] ends with "PASS"; and
- no path through the decision tree documented in [E.Info.DT.TCM-1] ends with "FAIL"; and
- the information provided in [E.Just.DT.TCM-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.TCM-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.TCM-1] ends with "FAIL"; or
- a justification provided in [E.Just.DT.TCM-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.TCM-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.8.1.4.5 Functional completeness assessment

Functional completeness assessment is not necessary in this clause since the traffic control mechanism is always mandatory for network equipment.

6.8.1.4.6 Functional sufficiency assessment

6.8.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional validation of the appropriateness of the Traffic Control Mechanisms described in [E.Info.TCM-1.TCM]. The assessment verifies whether the traffic forwarded by the network equipment to a network is controlled to avoid compromising or harm the

network assets and security assets in the networks which are controlled or served by the network equipment.

6.8.1.4.6.2 Preconditions

The equipment is in an operational state and if available setup or configuration did take place which is related to the traffic between networks.

6.8.1.4.6.3 Assessment units

For each traffic control mechanism documented in [E.Info.TCM-1.TCM]:

[AU.TCM-1.DatagramRules]: If the implementation is based on [IC.TCM-1.DatagramRules], functionally confirm that:

- datagrams are monitored by the network equipment; and
- a simulated anomalous patterns and malicious traffic is detected and discarded or blocked; and
- datagrams with not authorized source or address destination are detected and discarded or blocked.

[AU.TCM-1.TrafficSeparation]: If the implementation is based on [IC.TCM-1.TrafficSeparation], functionally confirm that:

- for each different network domain, traffic forwarding between the network domains is not allowed by the network equipment.

[AU.TCM-1.Generic]: If the implementation is based on [IC.TCM-1.Generic], functionally confirm that:

- the traffic forwarded by the network equipment is controlled and the controls are implemented as described in [E.Info.TCM-1.TCM].

6.8.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if for each traffic control mechanism documented in [E.Info.TCM-1.TCM] the confirmations in the implementation category dependent assessment unit are successful.

The verdict FAIL for the assessment case is assigned if for a traffic control mechanism documented in [E.Info.TCM-1.TCM] a confirmation in the implementation category dependent assessment unit is not successful.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.9 [CCK] Confidential cryptographic keys

6.9.1 [CCK-1] Appropriate CCKs

6.9.1.1 Requirement

Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits, except for:

- CCKs that are solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.

NOTE 1 Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.

NOTE 2 The requirement refers to all confidential cryptographic keys chosen by the equipment manufacturer either directly or imposed by a protocol. For instance, the manufacturer directly chooses/configures the cipher suite of TLS protocol to be used by the device, other protocols may impose one single option for cryptographic algorithms and their respective keys.

6.9.1.2 Rationale

The equipment can use cryptography and therefore CCKs for many and different purposes like for authentication to enforce access control to security assets or network assets, for protecting the confidentiality or integrity of security assets or network assets at rest or when communicated to another entity or for the derivation of other CCKs. If the confidentiality of a CCK is compromised the security assets and network assets protected by the CCK can get compromised too. A CCK of an equipment generated for an algorithm used for cryptographic protection is appropriate when a successful attack on it does not affect other CCKs used or generated by this equipment or by other equipment and the algorithm has an adequate security strength using this CCK to resist attacks proportionate to its use and targeting to break its confidentiality.

6.9.1.3 Guidance

The security strength supported by a CCK depends mainly on 3 parameters:

- the entropy of the RNG used for their generation; and
- its effective length (see BSI TR-02102-1 [19]); and
- on the cryptographic algorithm with which it is used.

Another important aspect which is related to the needed security strength supported by a CCK is the lifetime of the CCK. Long term CCKs which are stored and used repeatedly for a long period of time would need a longer in time resistance against attacks compared to short term CCKs which are usually generated on the equipment and only used for a short time. For instance, session keys used for a single communication session to encrypt the transferred security assets or network assets are a typical example for short term keys. However perfect forward secrecy is an aspect that usually is taken into account for the security of session keys and so these are usually generated/derived with adequate cryptographic mechanisms so that session keys of past sessions cannot be compromised.

Refer to CRY-1 for guidance on best practice.

Additional good security practices need also to be taken into account. For instance, it is a good security practice to use one CCK for a single purpose. Special care is to be taken for CCKs which are not used anymore, for instance these are to be deleted. It is recommended to follow recognised best practices for that, see CRY-1 requirement. It is also recommended that the same CCK is not replicated and used on the different specimens/units of this equipment.

There may be cases where deviations from the minimum security strength of 112 bits of CCKs is justified. For instance CCKs which are derived from human generated passwords may not provide 112 bits of security strength. Password key derivation is used in applications and protocols because they are practical and provide adequate security for their use case. There might be also cases where for interoperability reasons security measures dictates the deviation of the minimum security strength of 112 bits to be provided by CCKs. This can be due to the need for “interoperability support” (e.g., see SCM-1) or the need for usage of standardized and widely used communication protocols that deviate from the best practices.

For such deviations the resulting risks towards “the protection of the network assets and/or security assets” needs to be assessed.

6.9.1.4 Assessment criteria

6.9.1.4.1 Assessment objective

The assessment addresses the requirement CCK-1.

6.9.1.4.2 Implementation categories

Not applicable.

6.9.1.4.3 Required information

[E.Info.CCK-1.CCK]: For each confidential cryptographic key (whether preinstalled or generated by the equipment during its use), describe:

- The cryptographic algorithm for the confidential cryptographic key and the key length of confidential cryptographic key's implementation; and
- (if the confidential cryptographic key is solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM)[E.Info.CCK-1.CCK.Deviation]: Reference to the corresponding justification and to the required information the justification is based on; and
- [E.Info.CCK-1.CCK.SecurityStrength]: The security strength and the reference of the lookup tables used in the assessment.

NOTE for example, with reference to security strength definitions in SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [22] or NIST Special Publications 800-57 [7] or 800-131A [14].

[E.Info.DT.CCK-1]: Description of the selected path through the decision tree in Figure 24 for each confidential cryptographic key documented in [E.Info.CCK-1.CCK].

[E.Just.DT.CCK-1]: Justification for each selected path through the decision tree documented in [E.Info.DT.CCK-1] with the following properties:

- (if a decision from [DT.CCK-1.DN-2] results in “NOT APPLICABLE”) the justification for the decision [DT.CCK-1.DN-2] is based on [E.Info.CCK-1.CCK.Deviation]; and
- the justification for the decision [DT.CCK-1.DN-1] is based on [E.Info.CCK-1.CCK] and [E.Info.CCK-1.CCK.SecurityStrength].

6.9.1.4.4 Conceptual Assessment

6.9.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether confidential cryptographic keys are implemented as required per CCK-1.

6.9.1.4.4.2 Preconditions

None.

6.9.1.4.4.3 Assessment units

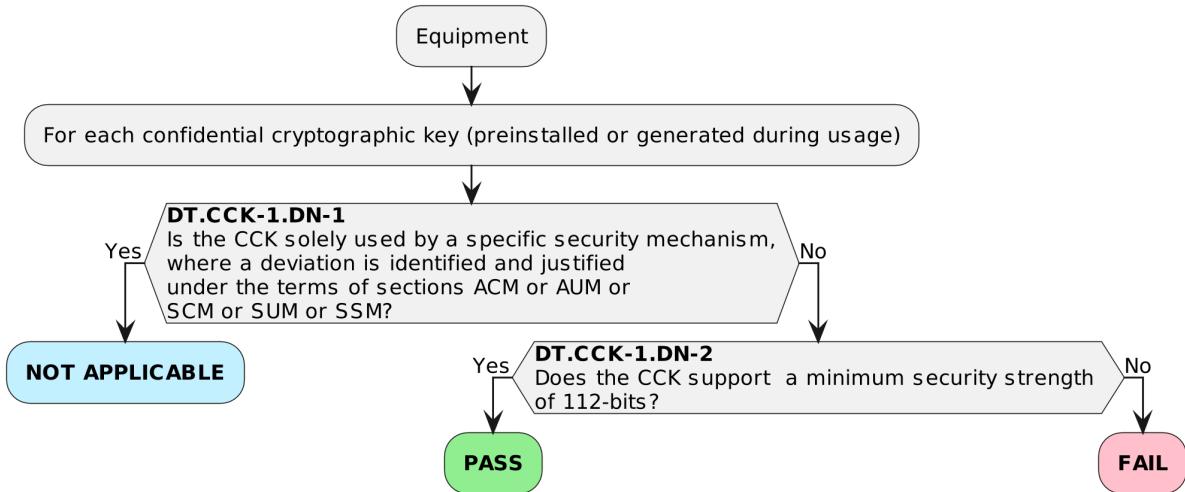


Figure 24 5— Decision Tree for requirement CCK-1

For each confidential cryptographic key documented in [E.Info.CCK-1.CCK], check whether the path through the decision tree documented in [E.Info.DT.CCK-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.CCK-1], examine its justification documented in [E.Just.DT.CCK-1].

6.9.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.CCK-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.CCK-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.CCK-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.CCK-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.CCK-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.CCK-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.CCK-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.9.1.4.5 Functional completeness assessment

6.9.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation of CCKs is complete.

6.9.1.4.5.2 Preconditions

The equipment is in an operational state.

6.9.1.4.5.3 Assessment units

Functionally assess whether there are CCK preinstalled or generated by the equipment, which are not documented in [E.Info.CCK-1.CCK].

6.9.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all CCKs found are documented in [E.Info.CCK-1.CCK].

The verdict FAIL for the assessment case is assigned if a CCK is found which is not documented in [E.Info.CCK-1.CCK].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.9.1.4.6 Functional sufficiency assessment

6.9.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the confidential cryptographic keys documented [E.Info.CCK-1.CCK] are implemented as documented.

NOTE The assessment of the bit length is only a necessary condition and does not constitute a complete functional sufficiency assessment for security strength.

6.9.1.4.6.2 Preconditions

The equipment is in an operational state.

6.9.1.4.6.3 Assessment units

For each confidential cryptographic key documented in [E.Info.CCK-1.CCK] functionally assess whether the CCK's length as documented in [E.Info.CCK-1.CCK] is implemented in accordance with [E.Info.CCK-1.CCK.SecurityStrength].

6.9.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that any CCK's length documented in [E.Info.CCK-1.CCK] deviates from their documentation.

The verdict FAIL for the assessment case is assigned if there is evidence that a CCK's length documented in [E.Info.CCK-1.CCK] deviates from the documentation.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.9.2 [CCK-2] CCK generation mechanisms

6.9.2.1 Requirement

The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for:

- the generation of CCKs for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.

NOTE Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.

6.9.2.2 Rationale

CCKs that are generated by the equipment and used to protect security assets or network assets, need to be generated appropriately in order to prevent successful attacks based on CCKs with insufficient security strength. An appropriate CCK generation mechanism ensures that CCKs have the necessary properties based on the associated risks and the operational conditions of the equipment.

6.9.2.3 Guidance

The security strength of a CCK is largely determined by the random number source (the main source of entropy) and the random number generator and the key generation/derivation algorithm which generate it.

Risks related to poor choices of random source, random number generators and key derivation can make a CCKs subject to attacks like

- guessing a CCK; or
- brute forcing a CCK; or
- reconstructing a CCK based on accessible information.

It is therefore essential that the CCK generation mechanism will not generate CCKs with insufficient security strength. A robust CCK generation mechanism relies on a secure RNG providing random numbers with sufficient entropy. It is a very complex task to create a securely robust CCK generation mechanism and the underlying RNG. It is highly recommended to follow well recognised standards for this purpose.

NOTE 1 There are various well-recognised standards for key generation mechanisms. For instance, recognised best practices for Random Number Generators are NIST SP800-90A[10], NIST SP800-90B[11], NIST SP800-90C[12], BSI AIS20 [37], BSI AIS31[18], ISO/IEC 18031 [38].

NOTE 2 Examples for well recognised best practices for key derivation are for instance described at SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms [22]. Alternatives are available here: ISO/IEC 11770 [26], NIST SP 800-108r1[13], NIST SP 800-132[15].

6.9.2.4 Assessment criteria

6.9.2.4.1 Assessment objective

The assessment addresses the requirement CCK-2.

6.9.2.4.2 Implementation categories

Not applicable.

6.9.2.4.3 Required information

[E.Info.CCK-2.Generation]: Description of each generation mechanism for confidential cryptographic keys, including the following details:

- [E.Info.CCK-2.Generation.CCK]: Specification of the confidential cryptographic keys the mechanism generates and whether their generation adheres to best practice cryptography; and
- (if the generation mechanism for CCK relies on a random number source and is used for the generation of confidential cryptographic key that adhere to best practice cryptography)
 - specify the best practices followed by the random number source; and
 - explain why the random number source provides sufficient security strength; and
 - explain how the random number source is configured and initialised; and
 - if it is claimed that the CCK is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the CCK complies to; and
- (if the generation mechanism for CCK relies on a random number generator and is used for the generation of confidential cryptographic key that adhere to best practice cryptography):
 - specify whether it is a deterministic or a non-deterministic random number generator; and
 - specify the best practices followed by the random number generator; and
 - specify why the random number generator provides sufficient security strength; and
 - explain how the random number generator is configured and initialised; and
 - if it is claimed that the CCK is compliant with recognised security standards or certification schemes, provide evidence to the recognised security standard or certification schemes the CCK complies to; and
- (if the generation mechanism for CCK relies on a derivation mechanism/ establishment mechanism and is used for the generation of confidential cryptographic key that adhere to best practice cryptography):
 - specify the best practices followed by the derivation mechanism/ establishment mechanism; and
 - specify the key derivation/generation algorithm used for that; and
- (if the generation mechanism generates confidential cryptographic keys used solely by a specific security mechanism, where a deviation from best practice cryptography is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM)[E.Info.CCK-2.Generation.Deviation]:
 - reference the corresponding justification and to the required information the justification is based on.

NOTE The information above may not always be available to the manufacturer when the generation mechanism is provided by a supplier which will not disclose such information for security reasons while providing all necessary security instructions to use the generation mechanism.

[E.Info.DT.CCK-2]: Description of the selected path through the decision tree in Figure 25 for each generation mechanism for confidential cryptographic keys documented in [E.Info.CCK-2.Generation].

[E.Just.DT.CCK-2]: Justification for the selected path through the decision tree documented in [E.Info.DT.CCK-2] with the following properties:

- (if a decision from [DT.CCK-2.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.CCK-2.DN-1] is based on [E.Info.CCK-2.Generation.Deviation]; and
- the justification for the decision [DT.CCK-2.DN-2] is based on [E.Info.CCK-2.Generation].

6.9.2.4.4 Conceptual assessment

6.9.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether all confidential cryptographic key generation mechanisms listed in [E.Info.CCK-2.Generation] are as required per CCK-2.

6.9.2.4.4.2 Preconditions

None.

6.9.2.4.4.3 Assessment units

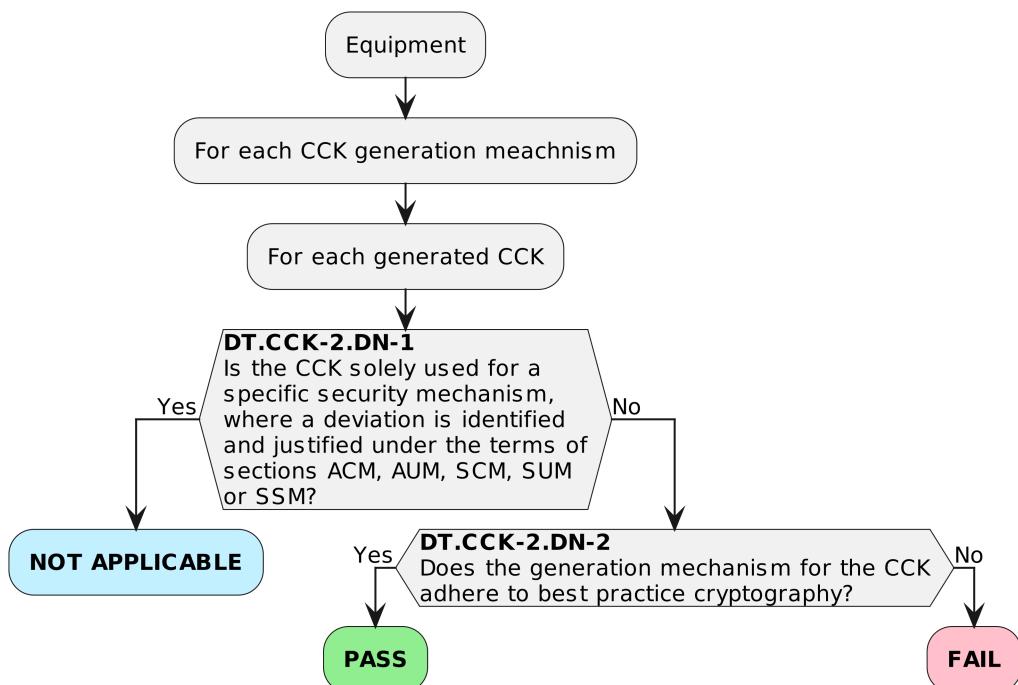


Figure 25— Decision Tree for requirement CCK-2

For each generation mechanism of confidential cryptographic keys on the equipment documented in [E.Info.CCK-2.Generation], check whether the path through the decision tree documented in [E.Info.DT.CCK-2] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.CCK-2], examine its justification documented in [E.Just.DT.CCK-2].

6.9.2.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.CCK-2] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.CCK-2] ends with “FAIL”; and
- the information provided in [E.Just.DT.CCK-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.CCK-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree end with “FAIL”; or
- a justifications provided in [E.Just.DT.CCK-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.CCK-2].

The verdict NOT APPLICABLE is assigned otherwise.

6.9.2.4.5 Conceptual completeness assessment of documentation

6.9.2.4.5.1 Assessment purpose

The purpose of this assessment case is to conceptually assess whether all generation mechanisms for confidential cryptographic keys on the equipment are documented in [E.Info.CCK-2.Generation].

6.9.2.4.5.2 Preconditions

None.

6.9.2.4.5.3 Assessment units

Check that there is no evidence for generation mechanisms for confidential cryptographic keys on the equipment that are not documented in [E.Info.CCK-2.Generation] through a consistency check with [E.Info.CCK-1.CCK].

6.9.2.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that there are generation mechanisms for confidential cryptographic keys that are not documented in [E.Info.CCK-2.Generation].

The verdict FAIL for the assessment case is assigned if there is any evidence that there are generation mechanisms for confidential cryptographic keys that are not documented in [E.Info.CCK-2.Generation].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.9.2.4.6 Functional sufficiency assessment

There is significant complexity surrounding the validation of cryptographic key generation mechanisms and typically they will be implemented by a third party with significant cryptographic expertise, who is unlikely to share details of such key generation processes. Given these considerations, no functional sufficiency assessment is provided for this requirement.

6.9.3 [CCK-3] Preventing static default values for preinstalled CCKs

6.9.3.1 Requirement

Preinstalled confidential cryptographic keys shall be practically unique per equipment, except for:

- CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or
- CCKS key are shared parameters required for the equipment's intended functionality.

NOTE Confidential cryptographic key is a defined term. Other secrets, whose disclosure cannot be used to harm the network or its functioning or for the misuse of network resources, such as secrets solely protecting intellectual property are not covered by the definition of confidential cryptographic key.

6.9.3.2 Rationale

Equipment can use cryptography and therefore CCKs to protect the security assets and network assets on the equipment. The CCKs are sometimes predefined, e.g. in the manufacturing process. CCKs used for the above-mentioned purpose need to be appropriate to prevent successful attacks based on CCKs with insufficient strength, especially when preinstalled.

6.9.3.3 Guidance

CCKs can be preinstalled on the equipment during manufacturing. Preinstalled CCKs that are unique per equipment instance and resist brute force attacks can mitigate cyber security risk associated with the specific use of the CCK.

Unique relates to not systematically reused or deducible for another equipment of the same product type and cannot be easily derived from equipment properties (e.g., manufacturer name, model name or Media Access Control (MAC) address). Established random generator can be used to generate practically unique cryptographic keys.

In some cases, keys are only used for establishing initial trust relationships under conditions controlled by an authorized entity or the key as shared parameter is essential to the equipment's operation, e.g., software updates or configuration of the migration for network equipment. In such cases the use of static keys can be applicable.

6.9.3.4 Assessment criteria

6.9.3.4.1 Assessment objective

The assessment addresses the requirement CCK-3.

6.9.3.4.2 Implementation categories

Not applicable.

6.9.3.4.3 Required information

[E.Info.CCK-3.CCK]: Description of each preinstalled confidential cryptographic key on the equipment, including:

- (if practically uniqueness of the confidential cryptographic key is claimed to be not required because it is only used for establishing initial trust relationships under conditions controlled by an authorized entity)[E.Info.CCK-3.CCK.Controlled]: Description of:

- the initial trust relationship to be established by the confidential cryptographic key; and
- the conditions controlled by an authorized entity; and
- (if practically uniqueness of the confidential cryptographic key is claimed to be not required because it is a shared parameter required for the equipment's intended functionality)[E.Info.CCK-3.CCK.Shared]: Description of the equipment's functionalities that require the confidential cryptographic key being a shared parameter; and
- (if the CCK is claimed to be practically unique per equipment) [E.Info.CCK-3.CCK.Unique]: Description of the methods that result in the CCK being practically unique per equipment.

[E.Info.DT.CCK-3]: Description of the selected path through the decision tree shown in Figure 26 for each preinstalled CCK documented in [E.Info.CCK-3.CCK].

[E.Just.DT.CCK-3]: Justification for the selected path through the decision tree documented in [E.Info.DT.CCK-3] with the following properties:

- (if a decision from [DT.CCK-3.DN-2] results in "NOT APPLICABLE") the justification for the decision [DT.CCK-3.DN-2] is based on [E.Info.CCK-3.CCK.Controlled]; and
- (if a decision from [DT.CCK-3.DN-3] results in "NOT APPLICABLE") the justification for the decision [DT.CCK-3.DN-3] is based on [E.Info.CCK-3.CCK.Shared]; and
- the justification for the decision [DT.CCK-3.DN-1] is based on [E.Info.CCK-3.CCK.Unique].

6.9.3.4.4 Conceptual assessment

6.9.3.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether preinstalled confidential cryptographic keys are implemented as required per CCK-3.

6.9.3.4.4.2 Preconditions

None.

6.9.3.4.4.3 Assessment units

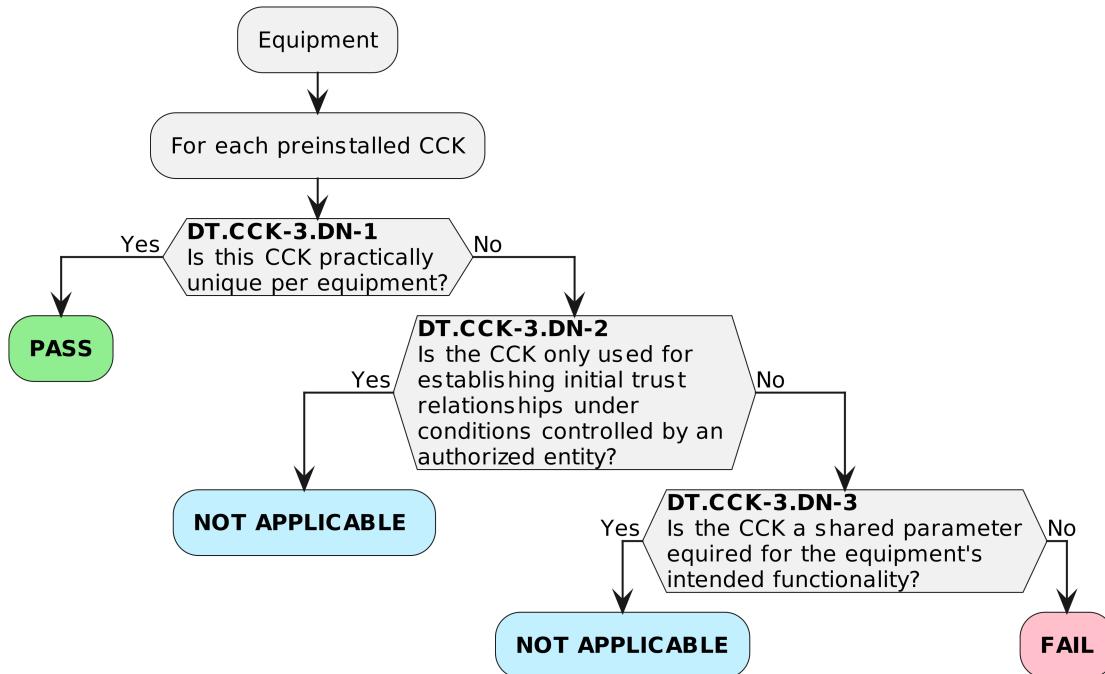


Figure 26 — Decision Tree for requirement CCK-3

For each confidential cryptographic key documented in [E.Info.CCK-3.CCK], check whether the path through the decision tree documented in [E.Info.DT.CCK-3] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.CCK-3], examine its justification documented in [E.Just.DT.CCK-3].

6.9.3.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.CCK-3] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.CCK-3] ends with “FAIL”; and
- the information provided in [E.Just.DT.CCK-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.CCK-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.CCK-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.CCK-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.CCK-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.9.3.4.5 Functional completeness assessment

6.9.3.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether all preinstalled CCKs are documented.

6.9.3.4.5.2 Preconditions

The equipment is in the factory default state.

6.9.3.4.5.3 Assessment units

Functionally assess whether there are preinstalled CCKs on the equipment which are not documented in [E.Info.CCK-3.CCK].

6.9.3.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all preinstalled CCK found are documented in [E.Info.CCK-3.CCK].

The verdict FAIL for the assessment case is assigned if a preinstalled CCK found is not documented in [E.Info.CCK-3.CCK].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.9.3.4.6 Functional sufficiency assessment

6.9.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether preinstalled CCKs that are claimed to be practically unique per equipment are sufficiently independent from each other.

6.9.3.4.6.2 Preconditions

Two instances of the equipment are in a factory default state.

6.9.3.4.6.3 Assessment units

For each CCK documented in [E.Info.CCK-3.CCK], where [E.Info.CCK-3.CCK.Unique] indicates that the CCK is claimed to be practically unique per equipment, functionally assess that the respective CCKs of the two equipments are practically unique by:

- (if the CCKs are accessible) comparing the CCKs and confirming that they are not the same and there is no obvious way to derive one from the other; and
- (if the CCKs are not accessible but come together with associated accessible public cryptographic keys, e.g. private/public key pairs, comparing the associated public cryptographic keys and confirming that they are not the same.

NOTE The specific functional test may not always be possible for each CCK as usually not all CCKs will be accessible or have an associated accessible public cryptographic key.

6.9.3.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that a CCK documented in [E.Info.CCK-3.CCK], where [E.Info.CCK-3.CCK.Unique] indicates that the CCK is claimed to be practically unique per equipment is not practically unique per equipment.

The verdict FAIL for the assessment case is assigned if there is evidence that a CCK documented in [E.Info.CCK-3.CCK], where [E.Info.CCK-3.CCK.Unique] indicates that the CCK is claimed to be practically unique per equipment is not practically unique per equipment.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10 [GEC] General equipment capabilities

6.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

6.10.1.1 Requirement

The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and network assets, except for vulnerabilities:

- that cannot be exploited in the specific conditions of the equipment; or
- that have been mitigated to an acceptable residual risk; or
- that have been accepted on a risk basis.

6.10.1.2 Rationale

Equipment can consist of hardware and software provided by different providers and the manufacturer might have insufficient visibility into the security practices of these providers.

It is essential that the manufacturer can identify publicly known exploitable vulnerabilities in the hardware and in the software, both commercial and open-source software, used in the equipment and can handle these vulnerabilities.

6.10.1.3 Guidance

To facilitate software vulnerability monitoring, the manufacturer of the equipment keeps technical documentation of the software of the equipment, including both open-source software and commercial off the shelf components. Likewise, technical documentation of hardware can assist in the identification of the hardware vulnerabilities.

To identify the publicly known exploitable vulnerabilities in the hardware and software of the equipment, the manufacturer consults a public vulnerability database (e.g. NIST National Vulnerabilities Database <https://nvd.nist.gov/> and existing National European Vulnerabilities Databases).

Different factors the manufacturer considers when assessing the publicly known exploitable vulnerabilities, include, but are not limited to:

- attack surface of the equipment and vectors/paths by which an attacker can gain access to the equipment to exploit the vulnerability;
- the evidence that the vulnerability has been actively exploited or it already has documented proof-of-concept or code exploits;

- the security capabilities and mechanisms implemented in the equipment which can mitigate the exploitation of the vulnerability;
- the “intended equipment functionality”;
- the equipment’s “intended operational environment of use” including the threat environment and the security capabilities and additional countermeasures provided by the environment which can mitigate or remediate the exploitation of the vulnerability.

6.10.1.4 Assessment criteria

6.10.1.4.1 Assessment objective

The assessment addresses the requirement GEC-1.

6.10.1.4.2 Implementation categories

Not applicable.

6.10.1.4.3 Required information

[E.Info.GEC-1.SecurityAsset]: Description of each security asset.

[E.Info.GEC-1.NetworkAsset]: Description of each network asset.

[E.Info.GEC-1.SoftwareDocumentation]: Description of the software of the equipment, including their versions, that affect the security assets and the network assets documented in [E.Info.GEC-1.SecurityAsset] and [E.Info.GEC-1.NetworkAsset].

[E.Info.GEC-1.HardwareDocumentation]: Description of the hardware of the equipment that affect the security assets and the network assets documented in [E.Info.GEC-1.SecurityAsset] and [E.Info.GEC-1.NetworkAsset].

[E.Info.GEC-1.ListOfVulnerabilities]: Description of all publicly known exploitable vulnerabilities in the hardware and software that affect the security assets and the network assets documented in [E.Info.GEC-1.SecurityAsset] and [E.Info.GEC-1.NetworkAsset]. The document includes also the source of the vulnerabilities’ information. Further a justification is given for each vulnerability that affects network assets and security assets about the remediation, mitigation and non-exploitation of the listed hardware or software publicly known exploitable vulnerabilities including:

- (if the vulnerability is remediated) [E.Info.GEC-1.ListOfVulnerabilities.Remediated]: The measures implemented to remediate the vulnerability; and
- (if the vulnerability cannot be exploited in the specific conditions of the equipment) [E.Info.GEC-1.ListOfVulnerabilities.SpecificCondition]: The description of specific conditions in which the vulnerability cannot be exploited ; and
- (if the vulnerability is mitigated) [E.Info.GEC-1.ListOfVulnerabilities.Mitigated]: The description of the measures for the mitigation; and
- (if the vulnerability is accepted) [E.Info.GEC-1.ListOfVulnerabilities.Accepted]: The description of the acceptance of the vulnerability on a risk basis.

[E.Info.DT.GEC-1]: Description of the selected path through the decision tree in Figure 27 for each software and hardware documented in [E.Info.GEC-1.SoftwareDocumentation] and [E.Info.GEC-1.HardwareDocumentation] where publicly known exploitable vulnerabilities exist.

[E.Just.DT.GEC-1]: Justification for the selected path through the decision tree documented in [E.Info.DT.GEC-1] with the following properties:

- the justification for the decision [DT.GEC-1.DN-1] is based on [E.Info.GEC-1.ListOfVulnerabilities];
- (if a decision from [DT.GEC-1.DN-2] results in “NOT APPLICABLE”) the justification for the decision [DT.GEC-1.DN-2] is based on [E.Info.GEC-1.ListOfVulnerabilities] and [E.Info.GEC-1.ListOfVulnerabilities.Remediated];
- (if a decision from [DT.GEC-1.DN-3] results in “NOT APPLICABLE”) the justification for the decision [DT.GEC-1.DN-3] is based on [E.Info.GEC-1.ListOfVulnerabilities.SpecificCondition];
- (if a decision from [DT.GEC-1.DN-4] results in “NOT APPLICABLE”) the justification for the decision [DT.GEC-1.DN-4] is based on [E.Info.GEC-1.ListOfVulnerabilities.Mitigated]; and
- the justification for the decision [DT.GEC-1.DN-5] is based on [E.Info.GEC-1.ListOfVulnerabilities.Accepted].

6.10.1.4.4 Conceptual assessment

6.10.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the hardware or software publicly known exploitable vulnerabilities present in the hardware and software of the equipment under test, in factory default state, are not able to affect security assets or network assets, if exploited as required per GEC-1.

6.10.1.4.4.2 Preconditions

None.

6.10.1.4.4.3 Assessment units

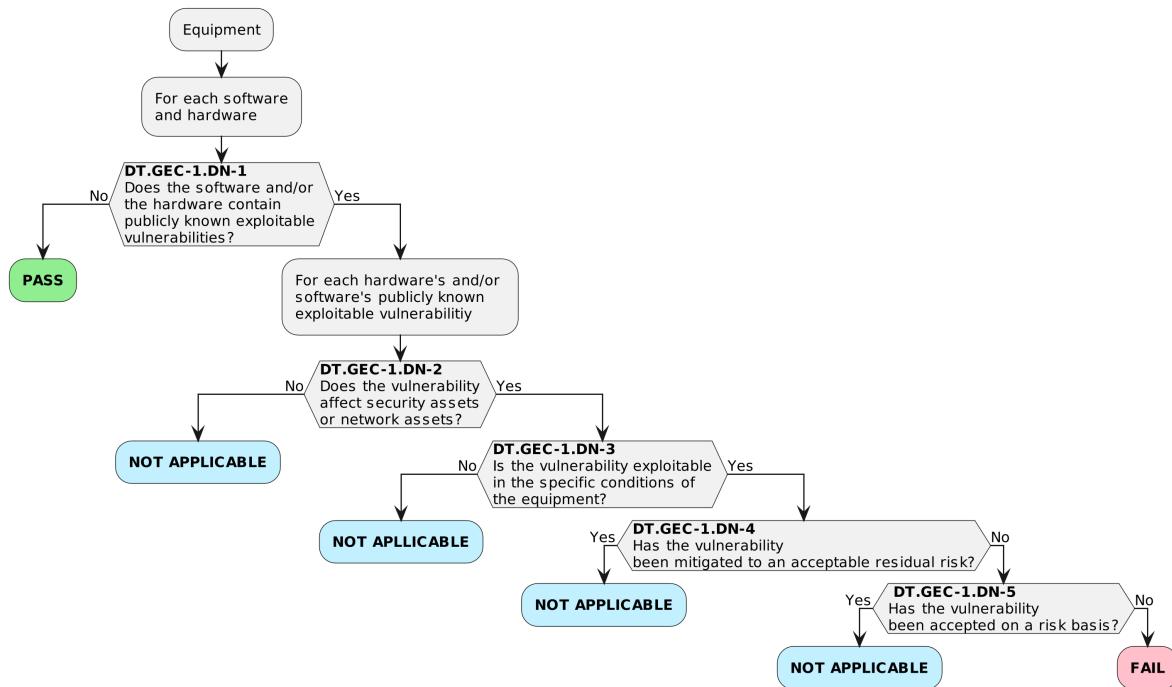


Figure 27 — Decision tree for requirement GEC-1

For each software in [E.Info.GEC-1.SoftwareDocumentation] and hardware documented in [E.Info.GEC-1.HardwareDocumentation], check whether the path through the decision tree documented in [E.Info.DT.GEC-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.GEC-1], examine its justification documented in [E.Just.DT.GEC-1].

6.10.1.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.GEC-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.GEC-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.GEC-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.GEC-1].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.GEC-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.GEC-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.GEC-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.1.4.5 Functional completeness assessment

6.10.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment of the equipment under test to verify the completeness of the documentation: that the vulnerabilities present in the equipment which affect security assets or network assets are only those listed in [E.Info.GEC-1.ListOfVulnerabilities].

6.10.1.4.5.2 Preconditions

The equipment is in an operational state.

The date for the source of the vulnerabilities to be used in the assessment of the list of publicly known exploitable vulnerabilities is recent.

6.10.1.4.5.3 Assessment units

Using up-to-date evaluation methods, functionally assess whether there are publicly known hardware vulnerabilities that affect the security assets and the network assets, which are not listed in [E.Info.GEC-1.ListOfVulnerabilities].

Using up-to-date evaluation methods, functionally assess whether there are publicly known software vulnerabilities that affect the security assets and the network assets, which are not listed in [E.Info.GEC-1.ListOfVulnerabilities].

NOTE Various software tools and measuring devices are available to automatically search for software and hardware vulnerabilities.

6.10.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all found publicly known software and hardware vulnerabilities that affect the security assets and the network assets are documented in [E.Info.GEC-1.ListOfVulnerabilities].

The verdict FAIL for the assessment case is assigned if a publicly known software or hardware vulnerability that affects a security asset or a network asset is not documented in [E.Info.GEC-1.ListOfVulnerabilities].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.1.4.6 Functional sufficiency assessment

6.10.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment if the vulnerabilities present in the equipment which are listed in [E.Info.GEC-1.ListOfVulnerabilities] are not able to affect security assets or network assets, if exploited.

6.10.1.4.6.2 Preconditions

The equipment is in an operational state.

The date for the source of the vulnerabilities to be used in the assessment of the list of publicly known exploitable vulnerabilities is recent.

6.10.1.4.6.3 Assessment units

Functionally assess whether the measures described in [E.Info.GEC-1.ListOfVulnerabilities] are implemented considering also the specific conditions for the exploitability defined in [E.Info.GEC-1.ListOfVulnerabilities] to ensure that the vulnerabilities are not able to affect security assets and network assets, if exploited.

NOTE For a lot of vulnerabilities Pentest tools are available to verify their exploitability.

6.10.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that measures to ensure that vulnerabilities are not able to affect security assets and network assets, if exploited, have not been implemented as described in [E.Info.GEC-1.ListOfVulnerabilities] considering also the specific conditions for the exploitability defined in [E.Info.GEC-1.ListOfVulnerabilities].

The verdict FAIL is assigned if there is evidence that measures to ensure that vulnerabilities are not able to affect security assets and network assets, if exploited, have not been implemented as described in [E.Info.GEC-1.ListOfVulnerabilities] considering also the specific conditions for the exploitability defined in [E.Info.GEC-1.ListOfVulnerabilities].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.2 [GEC-2] Limit exposure of services via related network interfaces

6.10.2.1 Requirement

In factory default state the equipment shall only expose

- network interfaces; and
- services via network interfaces

affecting security assets or network assets which are necessary for equipment setup or for basic operation of the equipment.

6.10.2.2 Rationale

An important factor for reducing the potential risk that the network resource of the equipment becomes compromised for instance to harm the network, are exposed services. Therefore, these exposed services need to be limited to those that are necessary for equipment setup and to operate the equipment in the intended operational environment of use.

6.10.2.3 Guidance

The configuration of the equipment can vary depending on the purpose of the equipment.

Generally, a differentiation is to be made between two types of equipment:

- Multipurpose equipment, e.g., smartphones, laptops: Offered services and functionality of multipurpose equipment are only under the control of the manufacturer until the equipment is placed on the market; and
- Equipment with a controlled fixed functionality, e.g., sensors, routers: Offered services and functionality of the equipment are embedded in an equipment-specific software which is provided by the manufacturer.

In case of equipment with a controlled fixed functionality only network interfaces or services (via network interfaces) are allowed in factory default state to be exposed which are essential to setup or use this functionality.

A multipurpose equipment has no specific intended use but is typically delivered by the manufacturer with a defined set of pre-installed applications. Further, the equipment provides an operational system for the following typical use cases in the factory default state:

- Manage/control the hardware of the equipment,
- Usage of the pre-installed applications,
- Installation of additional applications,
- Installation of software update.

These use cases define the permitted scope for the exposed network interfaces and services (via network interfaces).

Affecting security assets means that if the network interface or service (via network interfaces) is compromised it can have an impact on the security of the equipment.

6.10.2.4 Assessment criteria

6.10.2.4.1 Assessment objective

The assessment addresses the requirement GEC-2.

6.10.2.4.2 Implementation categories

Not applicable.

6.10.2.4.3 Required information

[E.Info.GEC-2.NetworkInterface.Exposure]: Description of each network interface and exposed service (via network interfaces) in factory default state of the equipment, including information if they are required for the basic operation or for the setup of the equipment or if they are optional.

(if the equipment implements a setup process) [E.Info.GEC-2.Setup]: Documentation how to setup the equipment.

[E.Info.GEC-2.SecurityAsset]: Documentation of each security asset that is accessible via network interfaces.

[E.Info.GEC-2.NetworkAsset]: Documentation of each network asset that is accessible via network interfaces.

[E.Info.DT.GEC-2]: Description of the selected path through the decision tree in Figure 28 for each network interface and service (via network interfaces) as documented in [E.Info.GEC-2.NetworkInterface.Exposure].

[E.Just.DT.GEC-2]: Justification for each selected path through the decision tree documented in [E.Info.DT.GEC-2] with the following properties:

- (if a decision from [DT.GEC-2.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.GEC-2.DN-1] is based on [E.Info.GEC-2.NetworkInterface.Exposure]; and
- (if a decision from [DT.GEC-2.DN-2] results in “NOT APPLICABLE”) the justification for the decision [DT.GEC-2.DN-2] is based on [E.Info.GEC-2.SecurityAsset] and [E.Info.GEC-2.NetworkAsset]; and
- the justification for the decision [DT.GEC-2.DN-3] is based on [E.Info.GEC-2.NetworkInterface.Exposure].

6.10.2.4.4 Conceptual assessment

6.10.2.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each exposure of network interfaces and services (via network interfaces) which are affecting security assets or network assets in factory default state documented in [E.Info.GEC-2.NetworkInterface.Exposure] is restricted to the ones which are necessary for equipment setup or for the basic operation of the equipment as required per GEC-2.

6.10.2.4.4.2 Preconditions

None.

6.10.2.4.4.3 Assessment units

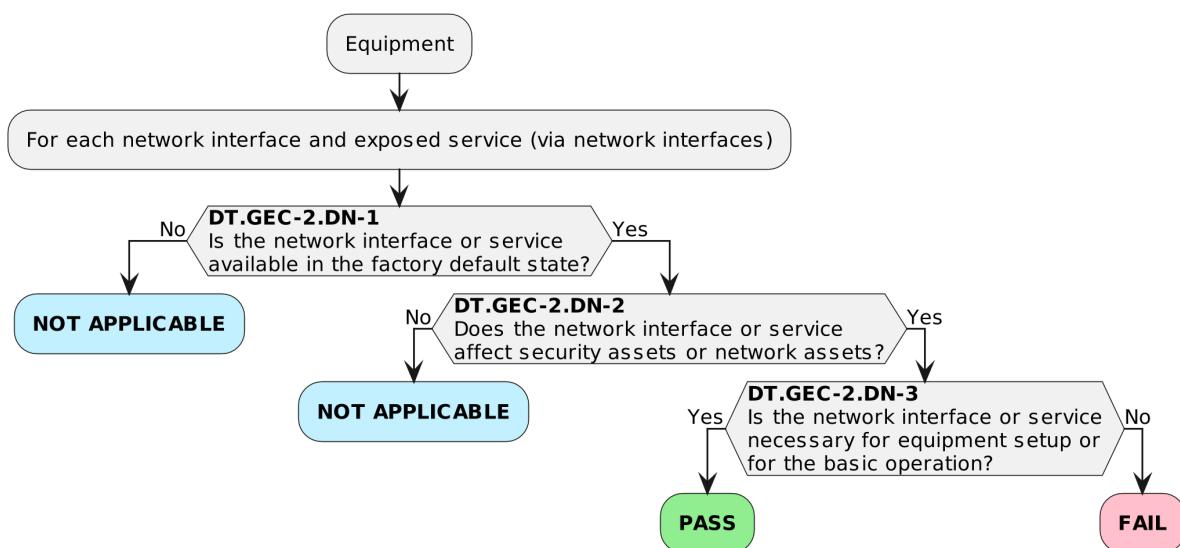


Figure 28 — Decision Tree for requirement GEC-2

For each network interface and exposed service (via network interfaces) documented in [E.Info.GEC-2.NetworkInterface.Exposure] check whether the path through the decision tree documented in [E.Info.DT.GEC-2] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.GEC-2], examine its justification documented in [E.Just.DT.GEC-2].

6.10.2.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.GEC-2] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.GEC-2] ends with “FAIL”; and
- the information provided in [E.Just.DT.GEC-2] are correct justifications for all paths through the decision tree documented in [E.Info.DT.GEC-2].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.GEC-2] ends with “FAIL”; or
- a justification provided in [E.Just.DT.GEC-2] is not correct or missing for a path through the decision tree documented in [E.Info.DT.GEC-2].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.2.4.5 Functional completeness assessment

6.10.2.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether in the factory default state only network interfaces or exposed services (via network interfaces) which are required for setup or for the basic operation of the equipment are exposed.

6.10.2.4.5.2 Preconditions

The equipment is in the factory default state and if available setup or another configuration did not take place until now.

Physical network connections to check the exposure of services (via network interfaces) are established.

6.10.2.4.5.3 Assessment units

Functionally assess whether there are further network interfaces or services (via network interfaces) exposed in factory default state, which are not listed in [E.Info.GEC-2.NetworkInterface.Exposure] or which are not required for setup according to [E.Info.GEC-2.Setup] or to operate the equipment in basic operation.

NOTE Various software tools and measuring devices are available to automatically search for exposed network interfaces or services which are accessible via network interface.

6.10.2.4.5.4 Assignment of verdict

The verdict PASS is assigned if every discovered network interface or service (via network interfaces) exposed in factory default state, is listed in [E.Info.GEC-2.NetworkInterface.Exposure] and is required for setup according to [E.Info.GEC-2.Setup] or for basic operation of the equipment.

The verdict FAIL is assigned if a network interface or a service (via network interface) exposed in factory default state is discovered that is not listed in [E.Info.GEC-2.NetworkInterface.Exposure] or not required for setup according to [E.Info.GEC-2.Setup] or for basic operation of the equipment.

The verdict NOT APPLICABLE is assigned otherwise.

6.10.2.4.6 Functional sufficiency assessment

Not applicable.

6.10.3 [GEC-3] Configuration of optional services and the related exposed network interfaces

6.10.3.1 Requirement

Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service.

6.10.3.2 Rationale

This will reduce the attack surface related to network interfaces and to the services exposed via these.

6.10.3.3 Guidance

The equipment provides a functionality for an authorized user to configure (enable/disable) the exposed optional services and the related network interfaces which are part the factory default state.

The configuration of network related services ought to be protected according to access control mechanism (ACM) and authentication mechanism (AUM).

6.10.3.4 Assessment criteria

6.10.3.4.1 Assessment objective

The assessment addresses the requirement GEC-3.

6.10.3.4.2 Implementation categories

Not applicable.

6.10.3.4.3 Required information

[E.Info.GEC-3.NetworkInterface.Exposure]: Description of each network interface and exposed service (via network interfaces) in factory default state of the equipment, including information if there is an option for an authorized user to enable and disable the network interface or service.

[E.Info.GEC-3.SecurityAsset]: Documentation of each security asset that is accessible via network interfaces.

[E.Info.GEC-3.NetworkAsset]: Documentation of each network asset that is accessible via network interfaces.

[E.Info.DT.GEC-3]: Description of the selected path through the decision tree in Figure 29 for each network interface and exposed optional service (via network interfaces) as documented in [E.Info.GEC-3.NetworkInterface.Exposure].

[E.Just.DT.GEC-3]: Justification for each selected path through the decision tree documented in [E.Info.DT.GEC-3] with the following properties:

- (if a decision from [DT.GEC-3.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.GEC-3.DN-1] is based on [E.Info.GEC-3.SecurityAsset] and [E.Info.GEC-3.NetworkAsset]; and
- the justification for the decision [DT.GEC-3.DN-2] is based on [E.Info.GEC-3.NetworkInterface.Exposure].

6.10.3.4.4 Conceptual assessment

6.10.3.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each optional network interface and each exposed optional service (via network interfaces) which is part of the factory default state of the equipment is configurable, at least with the option to enable and disable the service as required per GEC-3.

6.10.3.4.4.2 Preconditions

None.

6.10.3.4.4.3 Assessment units

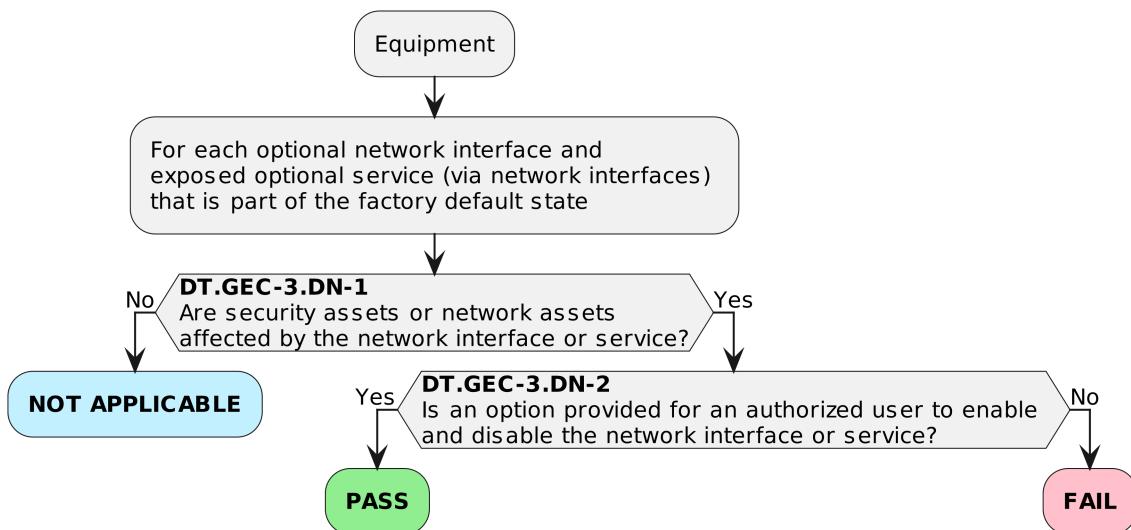


Figure 29 — Decision Tree for requirement GEC-3

For each optional network interface and exposed optional service (via network interfaces) documented in [E.Info.GEC-3.NetworkInterface.Exposure] that is part of the factory default state check whether the path through the decision tree documented in [E.Info.DT.GEC-3] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.GEC-3], examine its justification documented in [E.Just.DT.GEC-3].

6.10.3.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.GEC-3] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.GEC-3] ends with “FAIL”; and
- the information provided in [E.Just.DT.GEC-3] are correct justifications for all paths through the decision tree documented in [E.Info.DT.GEC-3].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.GEC-3] ends with “FAIL”; or
- a justification provided in [E.Just.DT.GEC-3] is not correct or missing for a path through the decision tree documented in [E.Info.DT.GEC-3].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.3.4.5 Functional completeness assessment

6.10.3.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether all optional network interfaces and exposed optional services (via network interfaces) which are part of the factory default state are configurable, at least with the option to enable and disable the service. Therefore, the completeness of documentation needs to be examined.

6.10.3.4.5.2 Preconditions

The equipment is in an operational state and if available the setup is done.

The necessary privileges are available for the configuration of the settings of the optional network interfaces or optional services (exposed via network interfaces).

6.10.3.4.5.3 Assessment units

Functionally assess whether there are optional network interfaces or exposed optional services (via network interfaces), which are not listed in [E.Info.GEC-3.NetworkInterface.Exposure].

6.10.3.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there are no optional network interfaces or optional services (via network interfaces) exposed, which are not listed in [E.Info.GEC-3.NetworkInterface.Exposure].

The verdict FAIL for the assessment case is assigned if there are optional network interfaces or optional services (via network interfaces) exposed, which are not listed in [E.Info.GEC-3.NetworkInterface.Exposure].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.3.4.6 Functional sufficiency assessment

6.10.3.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether all optional network interfaces and optional services (via network interfaces) exposed which are part of the factory default state are configurable, at least with the option to enable and disable the service.

6.10.3.4.6.2 Preconditions

The equipment is in an operational state and if available the setup is done.

The necessary privileges are available for the configuration of the settings of the optional network interfaces or optional services (via network interfaces).

6.10.3.4.6.3 Assessment units

For each optional network interface and optional service (via network interface) exposed that is part of the factory default state:

- Functionally assess whether the optional network interfaces and exposed optional services (via network interfaces) which are part of the factory default state and documented in [E.Info.GEC-3.NetworkInterface.Exposure] are configurable; and
- functionally assess if it is possible to at least change the status of the optional network interfaces and exposed optional services (via network interfaces) to enabled and disabled; and
- functionally assess whether the configuration of the settings of the optional network interfaces and exposed optional services (via network interfaces) which are part of the factory default state and listed in [E.Info.GEC-3.NetworkInterface.Exposure] is only possible by authorized users.

6.10.3.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is evidence that all optional network interfaces or exposed optional services (via network interfaces) are configurable at least with the option to enable and disable the network interface or service or changing the status of the optional network interfaces or exposed optional services (via network interfaces) to enabled or disabled is only possible by an authorized user as described in [E.Info.GEC-3.NetworkInterface.Exposure].

The verdict FAIL for the assessment case is assigned if there is no evidence that all optional network interfaces or exposed optional services (via network interfaces) are configurable at least with the option to enable and disable the network interface or service or changing the status of the optional network interface or exposed optional service (via network interfaces) to enabled or disabled is only possible by an authorized user as described in [E.Info.GEC-3.NetworkInterface.Exposure].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces

6.10.4.1 Requirement

The equipment's user documentation shall contain a description of

- all exposed network interfaces; and

- all services exposed via network interfaces,

which are delivered as part of the factory default state.

6.10.4.2 Rationale

The equipment itself and the surrounding network needs to be configured properly to assure the functionality of the equipment and to support the security of the network. Therefore, it is important to provide user information regarding the exposed network interfaces and exposed services (via network interfaces) and the intended operational environment of use.

6.10.4.3 Guidance

All network interfaces and exposed services (via network interfaces) in factory default state are to be listed in the documentation. For each service, its purpose could be provided as well. The aim is to provide transparency to the user about the connectivity of the equipment. Furthermore, the documentation serves to assess whether the commissioning of the equipment creates potential attack surfaces to the user's intended environment of use.

6.10.4.4 Assessment criteria

6.10.4.4.1 Assessment objective

The assessment addresses the requirement GEC-4.

6.10.4.4.2 Implementation categories

Not applicable.

6.10.4.4.3 Required information

[E.Info.GEC-4.UserDoc.NetworkInterface.Exposure]: User documentation of each exposed network interface and exposed service (via network interfaces) in factory default state of the equipment.

[E.Info.GEC-4.NetworkInterface.Exposure]: Description of each exposed network interface and exposed service (via network interfaces) in factory default state of the equipment.

[E.Info.DT.GEC-4]: Description of the selected path through the decision tree in Figure 30 for each exposed network interface and exposed service (via network interfaces) as documented in [E.Info.GEC-4.NetworkInterface.Exposure].

[E.Just.DT.GEC-4]: Justification for each selected path through the decision tree documented in [E.Info.DT.GEC-4] with the following properties:

- (if a decision from [DT.GEC-4.DN-1] results in "NOT APPLICABLE") the justification for the decision [DT.GEC-4.DN-1] is based on [E.Info.GEC-4.NetworkInterface.Exposure]; and
- the justification for the decision [DT.GEC-4.DN-2] is based on [E.Info.GEC-4.UserDoc.NetworkInterface.Exposure].

6.10.4.4.4 Conceptual assessment

6.10.4.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether all network interfaces and services which are exposed via network interfaces and are delivered as part of the factory default state are described in the user documentation as required per GEC-4.

6.10.4.4.2 Preconditions

None.

6.10.4.4.3 Assessment units

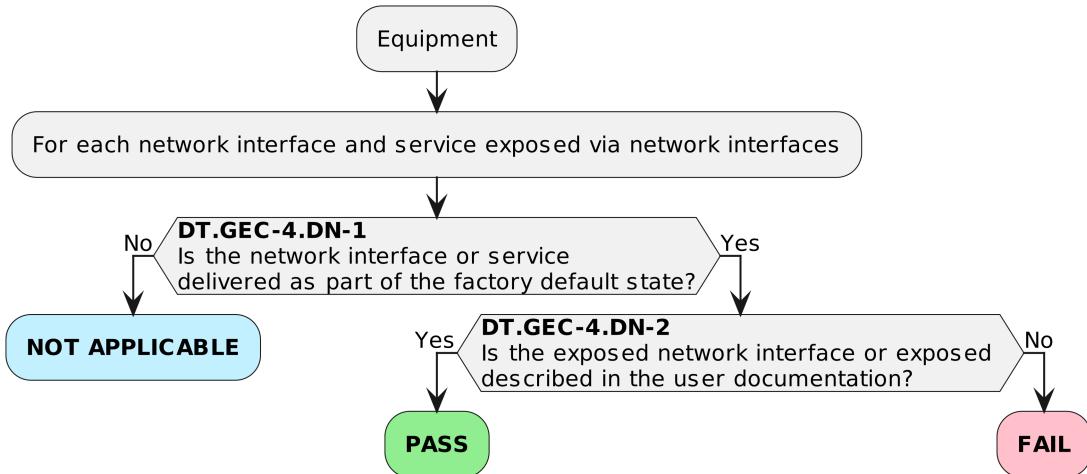


Figure 30 — Decision Tree for requirement GEC-4

For each network interface and exposed service (via network interfaces) in [E.Info.GEC-4.NetworkInterface.Exposure] check whether the path through the decision tree documented in [E.Info.DT.GEC-4] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.GEC-4], examine its justification documented in [E.Just.DT.GEC-4].

6.10.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.GEC-4] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.GEC-4] ends with “FAIL”; and
- the information provided in [E.Just.DT.GEC-4] are correct justifications for all paths through the decision tree documented in [E.Info.DT.GEC-4].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.GEC-4] ends with “FAIL”; or
- a justification provided in [E.Just.DT.GEC-4] is not correct or missing for a path through the decision tree documented in [E.Info.DT.GEC-4].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.4.4.5 Functional completeness assessment

6.10.4.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the user documentation describes every network interface and exposed service (via network interfaces) which are delivered as part of the factory default state.

6.10.4.4.5.2 Preconditions

The equipment is in a factory default state.

Network connections to check the exposure of network interfaces and services (via network interfaces) are established.

6.10.4.4.5.3 Assessment unit

To assess if the documentation of network interfaces and exposed services (via network interfaces) is complete:

- functionally assess whether there are further network interfaces that are exposed in the factory default state which are not documented in [E.Info.GEC-4.UserDoc.NetworkInterface.Exposure]; and
- functionally assess whether there are further exposed services (via network interfaces) that are not documented in [E.Info.GEC-4.UserDoc.NetworkInterface.Exposure].

NOTE Exposed network interfaces and services can be found with network scanning tools and service scanning tools.

6.10.4.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all network interfaces or exposed services (via network interfaces) in factory default state found are documented in [E.Info.GEC-4.NetworkInterface.Exposure].

The verdict FAIL for the assessment case is assigned if a network interface or an exposed service (via network interfaces) in factory default state is found which is not documented in [E.Info.GEC-4.NetworkInterface.Exposure].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.4.4.6 Functional sufficiency assessment

None.

6.10.5 [GEC-5] No unnecessary external interfaces

6.10.5.1 Requirement

The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.

6.10.5.2 Rationale

Physical external interfaces need to be kept to the minimum in order to minimise the potential attack surface.

6.10.5.3 Guidance

In cases where an unnecessary physical external interface is physically protected by its intended operational environment of use, this external interface is considered as not exposed by the equipment. External interfaces that are disabled or blocked are considered as not exposed by the equipment as well.

Physical external interfaces might include external interfaces that are intentionally used for internal system communication as well as user interfaces and machine interfaces.

The intended functionality can cover multiple use-cases and the physical external interfaces exposed need to serve a purpose in at least one of the use-cases.

6.10.5.4 Assessment criteria

6.10.5.4.1 Assessment objective

The assessment addresses the requirement GEC-5.

6.10.5.4.2 Implementation categories

Not applicable.

6.10.5.4.3 Required information

[E.Info.GEC-5.PhysicalExternalInterface]: Description of each physical external interface including:

- [E.Info.GEC-5.PhysicalExternalInterface.Purpose]: The purpose of the interface; and
- [E.Info.GEC-5.PhysicalExternalInterface.Type]: Description of the interface type (e.g. USB-C).

[E.Info.GEC-5.IntFunc]: Description of the intended functionality of the equipment.

[E.Info.DT.GEC-5]: Description of the selected path through the decision tree in Figure 31 for each physical external interface documented in [E.Info.GEC-5.PhysicalExternalInterface].

[E.Just.DT.GEC-5]: Justification for the selected path through the decision tree documented in [E.Info.DT.GEC-5], with the following property:

- the justification for the decision [DT.GEC-5.DN-1] is based on [E.Info.GEC-5.PhysicalExternalInterface].

6.10.5.4.4 Conceptual assessment

6.10.5.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether each exposure of physical external interfaces is restricted to the ones which are necessary for its intended functionality as required per GEC-5.

6.10.5.4.4.2 Preconditions

None.

6.10.5.4.4.3 Assessment units

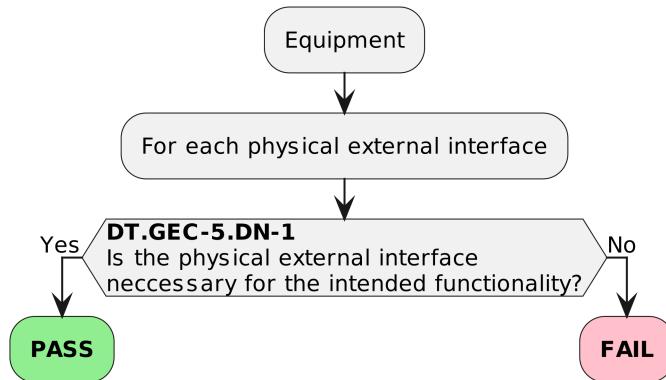


Figure 31 — Decision Tree for requirement GEC-5

For each physical external interface documented in [E.Info.GEC-5.PhysicalExternalInterface] check whether the path through the decision tree documented in [E.Info.DT.GEC-5] ends with “PASS”.

For each path through the decision tree documented in [E.Info.DT.GEC-5], examine its justification documented in [E.Just.DT.GEC-5].

6.10.5.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- all paths through the decision tree documented in [E.Info.DT.GEC-5] end with “PASS”; and
- the information provided in [E.Just.DT.GEC-5] are correct justifications for all paths through the decision tree documented in [E.Info.DT.GEC-5].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.GEC-5] ends with “FAIL”; or
- a justification provided in [E.Just.DT.GEC-5] is not correct or missing for a path through the decision tree documented in [E.Info.DT.GEC-5].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.5.4.5 Functional completeness assessment

6.10.5.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether only physical external interfaces are exposed, which are required for the intended functionality as documented in [E.Info.GEC-5.PhysicalExternalInterface].

6.10.5.4.5.2 Preconditions

The equipment is in an operational state.

6.10.5.4.3 Assessment units

Attempt to reveal any via the equipment exposed physical external interfaces even if the related function is not enabled or documented in [E.Info.GEC-5.PhysicalExternalInterface]:

- Examine equipment documentation such as design documentation, use case documentation and user manual; and
- examine which physical external interfaces are present on the equipment such as microphones, screens, buttons or slots for extension cards.

For each revealed physical external interface during the examination of documentation and also the examination of the equipment assess the documentation in [E.Info.GEC-5.PhysicalExternalInterface].

6.10.5.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all physical external interfaces found are documented in [E.Info.GEC-5.PhysicalExternalInterface].

The verdict FAIL for the assessment case is assigned if a physical external interface is found that is not documented in [E.Info.GEC-5.PhysicalExternalInterface].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.5.4.6 Functional sufficiency assessment

Not applicable.

6.10.6 [GEC-6] Input validation

6.10.6.1 Requirement

The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets.

6.10.6.2 Rationale

The equipment needs to validate any input which has potential impact to security assets or network assets to mitigate potential misuse, corruption, or unauthorized extraction of data on security assets and network assets.

Input validation is necessary to validate for instance the syntax, length and content of any input data that is provided as expected input and has the properties that are required to process the data correctly.

Improper input validation is regarded as one of the most common and dangerous software weaknesses which also contributes to several other software weaknesses like out-of-bounds write, and improper neutralization which can lead to various injection vulnerabilities (e.g., SQL injection, OS command injection and path traversal).

Especially data from potentially untrusted sources like any input received via network interfaces, need to be subject to input validation by checking the input for both syntax and semantics correctness. These checks ought to be done as early as possible when processing any input to avoid propagating invalid and perhaps even malicious input.

6.10.6.3 Guidance

Improper input validation is one of the root causes for many security vulnerabilities, input can only be successfully processed when it has been established that the input is valid by checking the syntax and semantics of the input, both on the raw data and metadata.

Syntax validation is checking that the input is delivered in the correct structure, for instance:

- the format of a date entry (e.g., dd-mm-yyyy or mm-dd-yyyy);
- the use of a decimal point or comma in a numeric input;
- the length of input;
- correct headers and structures for various file types (e.g., validate a .ZIP., .BMP or .JPEG file structure);
- a valid json, xml or html file.

Semantics validation is checking that the input is delivered with correct values, for instance:

- a value that is outside the expected range (e.g., a number that is too small or too large, a birthday in the future);
- special characters which are not allowed in a text input, e.g., special escape characters used for SQL injection;
- incorrect data size and offset values in a structure (e.g., an incorrect size might cause a buffer overrun when data is copied without checks, or a negative offset might copy incorrect data from the stack);
- inclusive listing (also known as “allow listing”) is a method which only permits defined input (e.g., specified values or expressions), everything else will be rejected as input.

Using parsers and/or regular expressions are methods to validate for instance text input. A developer could also consider other techniques to ensure an input can be successfully processed such as filtering and encoding.

Further guidance to be considered:

- Common Weakness Enumeration: Improper input validation (CWE-20), encoding/escaping (CWE-116), Improper Neutralization of Special Elements (CWE-138) and filtering (CWE-790); <https://cwe.mitre.org/data/index.html>
- Open Web Application Security Project (OWASP) Input Validation Cheat Sheet – https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
- IEC EN 62443-4-2[2] CR 3.5 (Input validation) and
- ETSI EN 303 645[5] 5.13 (Validate input data).

6.10.6.4 Assessment criteria

6.10.6.4.1 Assessment objective

The assessment addresses the requirement GEC-6.

6.10.6.4.2 Implementation categories

Not applicable.

6.10.6.4.3 Required information

[E.Info.GEC-6.ExternalInterface]: Description of each external interface including:

- [E.Info.GEC-6.ExternalInterface.Capabilities]: Description of any used APIs, protocols, input data types, file formats; and
- [E.Info.GEC-6.ExternalInterface.Validation]: Description how the input for instance via checking syntactic and semantic correctness is validated.

[E.Info.GEC-6.SecurityAsset]: Description of each security asset that is potentially impacted via external interfaces.

[E.Info.GEC-6.NetworkAsset]: Description of each network asset that is potentially impacted via external interfaces.

[E.Info.DT.GEC-6]: Description of the selected path through the decision tree in Figure 32 for each of the external interfaces documented in [E.Info.GEC-6.ExternalInterface].

[E.Just.DT.GEC-6]: Justification for the selected path through the decision tree documented in [E.Info.DT.GEC-6] with the following properties:

- (if a decision from [DT.GEC-6.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.GEC-6.DN-1] is based on [E.Info.GEC-6.ExternalInterface] and [E.Info.GEC-6.ExternalInterface.Capabilities]; and
- the justification for the decision [DT.GEC-6.DN-2] is especially based on [E.Info.GEC-6.ExternalInterface], [E.Info.GEC-6.ExternalInterface.Validation] and [E.Info.GEC-6.ExternalInterface.Capabilities].

6.10.6.4.4 Conceptual assessment

6.10.6.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the input validation functionality of the equipment is applied to the external interfaces and provides appropriate protection of security assets and/or network assets against common attacks considering the intended functionality of the equipment as required per GEC-6.

6.10.6.4.4.2 Preconditions

None.

6.10.6.4.4.3 Assessment units

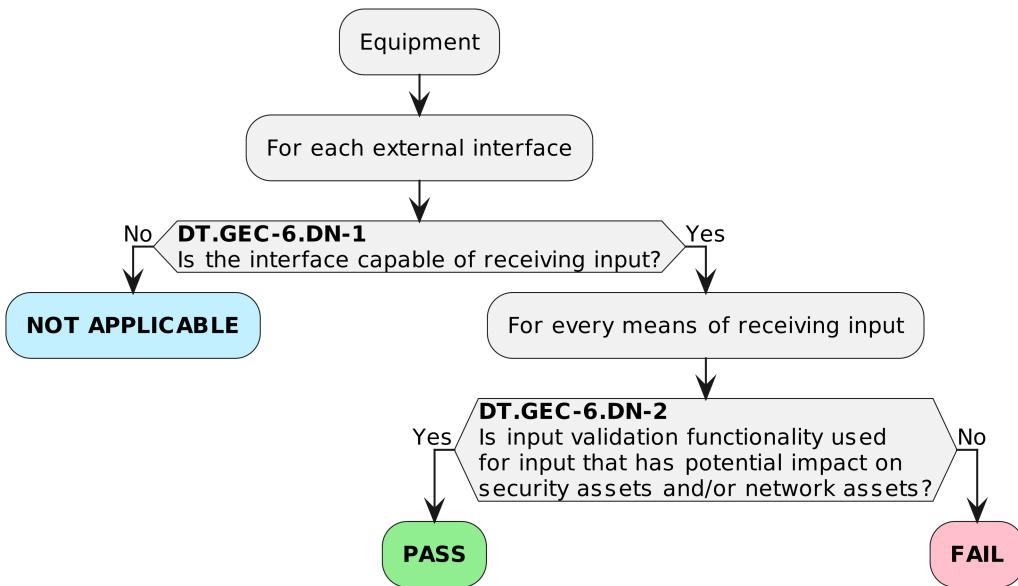


Figure 32 — Decision Tree for requirement GEC-6

For each external interface documented in [E.Info.GEC-6.ExternalInterface], check whether the path through the decision tree documented in [E.Info.DT.GEC-6] ends with “PASS” or “NOT APPLICABLE”.

For each path through the decision tree documented in [E.Info.DT.GEC-6], examine its justification documented in [E.Just.DT.GEC-6].

6.10.6.4.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.GEC-6] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.GEC-6] ends with “FAIL”; and
- the information provided in [E.Just.DT.GEC-6] are correct justifications for all paths through the decision tree documented in [E.Info.DT.GEC-6].

The verdict FAIL for the assessment case is assigned if:

- a path through the decision tree documented in [E.Info.DT.GEC-6] ends with “FAIL”; or
- a justification provided in [E.Just.DT.GEC-6] is not correct or missing for a path through the decision tree documented in [E.Info.DT.GEC-6].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.6.4.5 Functional completeness assessment

6.10.6.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment of the external interfaces of the equipment and the related input mechanisms regarding the completeness of the documentation.

6.10.6.4.5.2 Preconditions

The equipment is in an operational state and all external interfaces, which are part of the intended functionality, are either enabled or configurable to be enabled, so that each external interface can be tested.

Where authentication is necessary to access an external interface, a means is provided to be able to test the interface.

6.10.6.4.5.3 Assessment units

Functionally assess whether there are input methods that are not documented in [E.Info.GEC-6.ExternalInterface] by:

- functionally assessing traffic of network interfaces to reveal input methods, e.g. via network analysing tools; use the information in [E.Info.GEC-6.ExternalInterface] as a guidance; and
- functionally assessing equipment to reveal input methods of external interfaces which are no network interfaces via visual inspection, user manual and design-documentation; and
- following the description in [E.Info.GEC-6.ExternalInterface.Capabilities] to trigger the related input methods, e.g. via generating the described messages (e.g., via a web interface or generic message generating tools, or fuzzing tools).

6.10.6.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if all external interfaces found are documented in [E.Info.GEC-6.ExternalInterface].

The verdict FAIL for the assessment case is assigned if an external interface is found that is not documented in [E.Info.GEC-6.ExternalInterface].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.10.6.4.6 Functional sufficiency assessment

6.10.6.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment of the techniques to verify the implementation of the documented techniques.

6.10.6.4.6.2 Preconditions

The equipment is in an operational state and all external interfaces, which are part of the intended functionality, are either enabled or configurable to be enabled, so that each external interface can be tested.

Where authentication is necessary to access an external interface, a means is provided to be able to test the interface.

6.10.6.4.6.3 Assessment units

Functionally assess whether each external interface is resilient against common input attacks considering their functionality and the intended functionality of the equipment by:

- following the description in [E.Info.GEC-6.ExternalInterface] as guidance to test the related input methods e.g., via generating malformed or invalid messages (e.g., via a web interface or generic message generating tools, or fuzzing tools): Attempt to corrupt, extract or misuse the security assets described in [E.Info.GEC-6.SecurityAsset] and network assets described in [E.Info.GEC-6.NetworkAsset] by executing specific attacks related to the input mechanisms like SQL injection, Ajax injection, OS command injection or path traversal as well; and
- functionally assessing if the behaviour or output described in [E.Info.GEC-6.ExternalInterface] is generated as documented, use equipment manual or design-documentation as guidance.

6.10.6.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if there is no evidence that any input validation testing was successful to corrupt, extract or misuse any security asset as described in [E.Info.GEC-6.SecurityAsset] or network asset as described in [E.Info.GEC-6.NetworkAsset].

The verdict FAIL for the assessment case is assigned if there is evidence that an input validation testing was successful to corrupt, extract or misuse any security asset as described in [E.Info.GEC-6.SecurityAsset] or network asset as described in [E.Info.GEC-6.NetworkAsset].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.11 [CRY] Cryptography

6.11.1 [CRY-1] Best practice cryptography

6.11.1.1 Requirement

The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets, except for:

- cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.

6.11.1.2 Rationale

Cryptography that is not strong enough for a use case, e.g., because it is not suitable or broken and used for the protection of security assets or network assets poses a security risk to these assets. Using best practices or even more advanced, evidently suitable cryptography supports trust in the cryptographic protection of these assets.

If a cryptographic algorithm is cracked or cryptographic primitives are compromised, it may be necessary to update the equipment accordingly (see requirement SUM) in order to preserve the protection of the security assets and network assets the cryptography protects. While there is no absolute guarantee that this does not happen to any cryptography that is considered as best practice, it is more likely that cryptography becomes unsuitable for a certain use case, when there is already evidence that such cryptography might become deprecated within the intended lifetime of the equipment.

However, e.g., if the equipment can itself communicate over the internet and contains a hardware based crypto accelerator, it might not be prepared to update cryptography. In these cases, it is important that there is no evidence that the cryptography will not be best practice within the intended lifetime.

6.11.1.3 Guidance

There is various security guidance that can be used to identify best practices for cryptography, see respective ISO/IEC standards, publicly available crypto catalogues provided by SDOs and public authorities such as [sogis.eu](#), "SOGIS agreed Cryptographic Mechanisms" [22], ETSI TS 119 312 Electronic Signatures and Infrastructures; Cryptographic Suites [25] and guidance provided by ENISA and national agencies as the NIST SP 800 series [7]- [17] and BSI TR-02102-1[19]

A commonly used cryptographic method for a certain use case, with the lack of evidence for a feasible attack with current readily available techniques, can be considered as best practice.

However, it is also possible to provide evidence, that new cryptography is suitable for a certain use case and can therefore be considered as best practice for cryptography.

Cryptography is often used for protecting the relevant security assets and network assets, for example:

- Authentication (see AUM),
- Secure update (see SUM),
- Secure storage (see SSM),
- Secure communication (see SCM),
- Confidential Cryptographic key Generation (see CCK-2).

Cryptographic protection might not be compliant with best practice cryptography if interoperability is required. Legacy mechanism, that are deployed on a large scale are considered to provide an acceptable short – term security and suffer from some security assurance limitations as compared with the identified best practice mechanism in the above referenced crypto- catalogues (see e.g., [sogis.eu](#)). For up-to date lists of legacy mechanism and their validity period given by a deprecation deadline, the crypto catalogues are updated on a regular short-term basis (e.g., annually).

If reviewed or evaluated implementations according to the best practice are publicly available, these may be preferable used to deliver network and security functionalities, particularly in the field of cryptography.

To maintain best practices for cryptography within the intended lifetime of the equipment concepts to consider are crypto agility additional to the capability of updating cryptography on the equipment in accordance to SUM to respond to new attacks and new technological developments.

Elements to observe for the preparation of updating cryptography are amongst others:

- cryptographic schemes, protocols, algorithms, constructors and primes,
- the form of sensitive security parameters being used, and
- specific SSPs, such as roots of trust.

For equipment that cannot have their cryptographic algorithms or primitives updated for example if the implementation or part uses a hardware-based root of trust, it is important that the intended lifetime of the equipment does not exceed the recommended usage lifetime of the cryptographic algorithms and primitives used by the equipment.

6.11.1.4 Assessment criteria

6.11.1.4.1 Assessment objective

The assessment addresses the requirement CRY-1.

6.11.1.4.2 Implementation categories

Not applicable.

6.11.1.4.3 Required information

[E.Info.CRY-1.Assets]: List of all security assets and network assets on the equipment protected by cryptography, including for each cryptography used for cryptographic protection:

- [E.Info.CRY-1.Assets.Cryptography]: Description of the cryptography used for cryptographic protection, including:
 - description of each cryptographic protection goal; and
 - evidence to justify that the cryptography is best practice for the cryptographic protection goals

or;

- (if a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM)[E.Info.CRY-1.Assets.Deviation]: Reference to the corresponding justification and to the required information the justification is based on.

NOTE 1 The documentation of a cryptographic protection goal includes the security objectives provided by cryptography.

NOTE 2 Cryptography used for cryptographic protection can amongst others include cryptographic schemes, algorithms, constructors and primes.

NOTE 3 Evidence to justify that the cryptography is best practice for the cryptographic protection goals can be based a reference catalogues, e.g., SOGIS Agreed Cryptographic Mechanisms (<https://www.sogis.eu>) [22], or other evidence, e.g., by cryptoanalysis.

[E.Info.DT.CRY-1]: Description of the selected path through the decision tree in Figure 33 for each security asset and network asset described in [E.Info.CRY-1.Assets].

[E.Just.DT.CRY-1]: Justification for each selected path through the decision tree documented in [E.Info.DT.CRY-1] with the following properties:

- (if a decision from [DT.CRY-1.DN-1] results in “NOT APPLICABLE”) the justification for the decision [DT.CRY-1.DN-1] is based on [E.Info.CRY-1.Assets.Deviation]; and
- the justification for the decision [DT.CRY-1.DN-2] is based on [E.Info.CRY-1.Assets.Cryptography].

6.11.1.4.4 Conceptual assessment

6.11.1.4.4.1 Assessment purpose

The purpose of this assessment case is the conceptual assessment whether the implemented cryptography for protecting security asset or network assets is considered as best practice as required per CRY-1.

6.11.1.4.4.2 Preconditions

None.

6.11.1.4.4.3 Assessment units

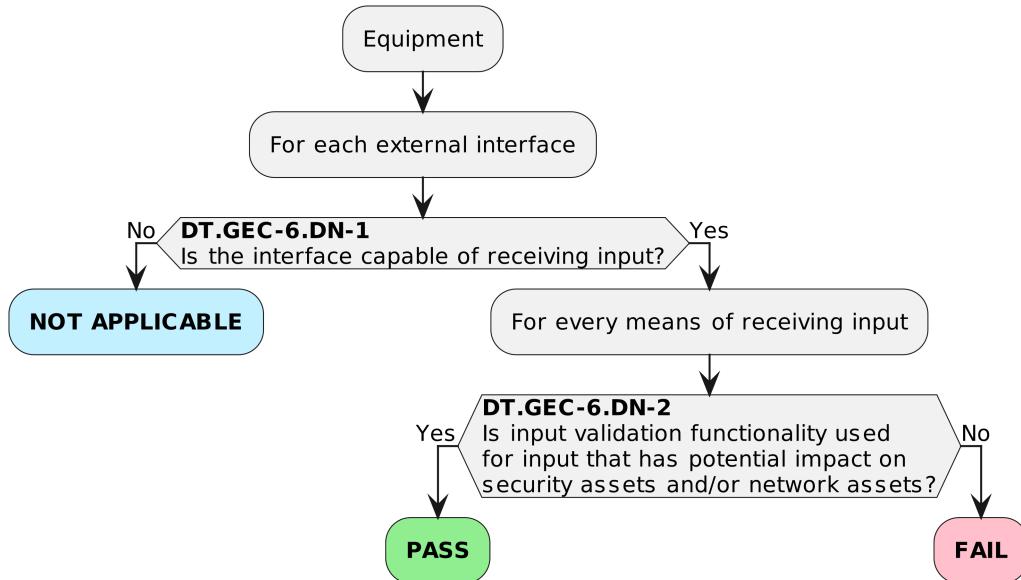


Figure 33 — Decision Tree for requirement CRY-1

For each security asset and network asset documented in [E.Info.CRY-1.Assets], check whether the path through the decision tree documented in [E.Info.DT.CRY-1] ends with “NOT APPLICABLE” or “PASS”.

For each path through the decision tree documented in [E.Info.DT.CRY-1], examine its justifications documented in [E.Just.DT.CRY-1].

6.11.1.4.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if:

- at least one path through the decision tree documented in [E.Info.DT.CRY-1] ends with “PASS”; and
- no path through the decision tree documented in [E.Info.DT.CRY-1] ends with “FAIL”; and
- the information provided in [E.Just.DT.CRY-1] are correct justifications for all paths through the decision tree documented in [E.Info.DT.CRY-1].

The verdict FAIL for the assessment case is assigned if:

- all path through the decision tree documented in [E.Info.DT.CRY-1] ends with “FAIL”; or
- a justification provided in [E.Just.DT.CRY-1] is not correct or missing for a path through the decision tree documented in [E.Info.DT.CRY-1].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.11.1.4.5 Functional completeness assessment

6.11.1.4.5.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the documentation in [E.Info.CRY-1.Assets.Cryptography] is complete.

6.11.1.4.5.2 Preconditions

The equipment is in an operational state.

6.11.1.4.5.3 Assessment units

Check whether there is evidence of cryptography used on the equipment for the protection of the security assets or network assets that is not documented in [E.Info.CRY-1.Assets.Cryptography].

NOTE Differences due to software updates to mitigate vulnerabilities or raise the security level are not to be considered as deviations from the documentation.

6.11.1.4.5.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if no evidence for cryptography used on the equipment is found that is not documented in [E.Info.CRY-1.Assets.Cryptography].

The verdict FAIL for the assessment case is assigned if any evidence for cryptography used on the equipment is found that is not documented in [E.Info.CRY-1.Assets.Cryptography].

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

6.11.1.4.6 Functional sufficiency assessment

6.11.1.4.6.1 Assessment purpose

The purpose of this assessment case is the functional assessment whether the cryptography documentation in [E.Info.CRY-1.Assets.Cryptography] is implemented as it is documented.

6.11.1.4.6.2 Preconditions

The equipment is in an operational state.

6.11.1.4.6.3 Assessment units

For each cryptographic protection documented in [E.Info.CRY-1.Assets.Cryptography] check whether there is evidence that the implementation deviates from its documentation.

NOTE Differences due to software updates to mitigate vulnerabilities or raise the security level are not to be considered as deviations from the documentation.

6.11.1.4.6.4 Assignment of verdict

The verdict PASS for the assessment case is assigned if no evidence for the deviation of cryptography from its documentation in [E.Info.CRY-1.Assets.Cryptography] is found.

The verdict FAIL for the assessment case is assigned if any evidence for the deviation of cryptography from its documentation in [E.Info.CRY-1.Assets.Cryptography] is found.

The verdict NOT APPLICABLE for the assessment case is assigned otherwise.

Annex A (informative)

Rationale

A.1 General

This annex provides a rationale for terms and concepts related to this document.

A.2 Rationale

A.2.1 Family of standards

This document belongs to a set of three standards to address the essential requirements defined in articles 3.3.d, 3.3e and 3.3.f of Directive 2014/53/EU [33] and activated by the Commission Delegated Regulation (EU) 2022/30 [34]. By using the Radio Equipment Directive, a first step has been made to start to enforce cybersecurity requirements for placing radio equipment on the European market, because a lack of security was and is an increasing concern for society, especially for consumer IoT equipment.

While the three standards focus on different essential requirements (harm to the network, personal data and privacy and protection from (financial) fraud) there are both unique and overlapping requirements in each of them that will require the implementation an increasing number of stronger security controls to protect the network, privacy, and financial assets operating within a developing threat landscape.

Whether one or multiple standards need to be applied to a specific radio equipment is a consideration that is made through a product-relevant risk assessment [35] by the economic operator in order to identify threats and assess risks on the need to fulfil the essential requirements of the Radio Equipment Directive. The RED [36] and Blue guides [35] of the European Commission can provide more guidance on this topic.

A.2.2 Security by design

Effective security management requires established security by design processes, which is not covered by this document which defines common security requirements for the equipment. Examples of security by design process standards which would aid in the ability to satisfy the security requirements include:

- IEC 62443-4-1[1]: Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements
- NIST 800-160[16]: Systems Security Engineering; Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- NIST 800-218[17]: Secure Software Development Framework (SSDF)
- Microsoft Security Development Lifecycle (SDL)
- SAFECode Fundamental Practices for Secure Software Development
- GSMA FS.16 NESAS Development and Lifecycle Security Requirements

A.2.3 Threat modelling and security risk assessment

STRIDE is an example of a classification scheme, useful for system decomposition, for characterizing identified threats according to the kinds of exploit that are used by the attacker. The STRIDE acronym is formed from the first letter of each of the following threat categories:

Table A.1 — STRIDE

Threat	Desired property	Description
Spoofing	Authenticity	Illegally accessing assets by pretending you are someone else (credentials, network address)
Tampering	Integrity	Prevent malicious modification of data (including system configuration)
Repudiation	Non-repudiability	Ability to proof an action between two parties took place (and do not allow repetition)
Information disclosure	Confidentiality	Do not disclose any information to unauthorized users (personal data, system configuration)
Denial of Service	Availability	Making a system or data unavailable to authorized users by overloading the system
Elevation of Privilege	Authorization	An unprivileged user gains privileged access and could compromise the entire system

Each security property has primary mitigation techniques to address the threats that could be identified by a risk management process. Table A.2 provides the list of mitigations provided as security requirements in this document, grouped into the following categories defined by ISO/IEC TR 27103 [39] and the NIST cybersecurity framework [40]:

- Identify: Process of recognizing the attributes that identify the object.
- Protect: The ability to limit or contain the impact of a potential cybersecurity event.
 - Prevent: Measures that avoid or preclude a cybersecurity event.
 - Limit: Measures intended to reduce the impact of a cybersecurity event.
- Detect: Security controls intended to detect a cybersecurity event.
- Respond: Appropriate activities to execute regarding a detected cybersecurity event.
- Recover: Appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Table A.2 is a visualisation of the mapping of the threats for each STRIDE category to the mitigations achieved by the individual security requirements. The mitigation techniques can be assessed and implemented to help ensure it will address the threats identified based on the radio equipment use case and intended function.

Table A.2 — security requirements, capabilities, mitigation techniques and design principles

Mitigation category		Security requirement / capability / mitigation technique / design principle	S	T	R	I	D	E	
Identify		Authentication mechanism (AUM)	X	X			X		
		Confidential cryptographic keys (CCK)	X	X	X				
Protect	Prevent	Access control mechanism (ACM)		X		X	X	X	
		Secure storage mechanism (SSM)	X	X		X		X	
		Secure communication mechanism (SCM)	X	X	X	X		X	
		Encryption (CRY)		X		X			
		Up-to-date software and hardware (GEC-1)	X	X	X	X	X	X	
		Configuration of optional services (GEC-3)				X	X	X	
		User documentation (GEC-4)				X			
	Limit	Limit exposure (GEC-2 and GEC-5)				X		X	
		Input validation (GEC-6)		X		X			
Detect		Network monitoring mechanism (NMM)	X			X	X		
Respond		Traffic control mechanism (TCM)	X	X		X	X		
Recover		Secure update mechanism (SUM)	X	X	X	X	X	X	
		Resilience mechanism (RLM)						X	

The identified threats are used by the manufacturer as one of the inputs for security risk assessment, to determine impact and the appropriateness of the selected mitigations.

A.2.4 Functional sufficiency assessment

Functional sufficiency assessments, where examining and testing for the adequacy of the implementation is performed, use different, requirements dependent approaches to facilitate an effective assessment.

In one approach the assessment units define actions to be performed to identify deviations between the documentation within required information and the actual implementation of the equipment under test.

NOTE The conceptual assessment already covers the assessment of the documentation provided with the required information with respect to the requirement.

In another approach the assessment units define actions to be performed to directly assess the equipment's implementation of a requirement to identify potentially deviations e.g., from an attackers perspective.

A.2.5 Implementation categories

In general, the requirements and assessment criteria are formulated such that different technical implementations can be covered. However, certain functional sufficiency assessment units provide, in addition to generic assessment units, implementation specific assessment units suitable for common technical solutions, referred to as "implementation categories".

A.2.6 Assets

To ensure requirements can be aligned across the three horizontal standards - each addressing a specific scope - assets have been introduced as the main targets against which to apply the requirements. The different types of assets are summarised in Table A.3:

Table A.3 — Assets and essential requirements

Essential requirement	3.3.d	3.3.e	3.3.f
Security asset	✓	✓	✓
Network asset	✓		
Privacy asset		✓	
Financial asset			✓

Protecting an asset is not just about the protection of the specific data stored and communicated or otherwise processed by the equipment, but also includes the protection of the functions and the configuration of these functions as used by the equipment.

This correlation is reflected in the definitions for the assets as shown below.

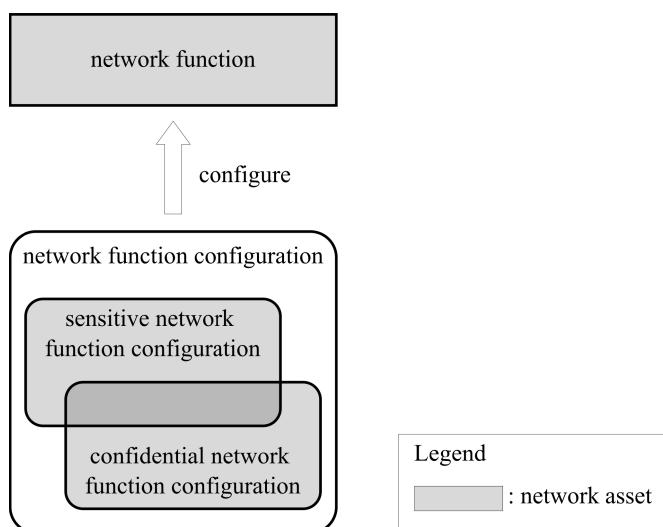


Figure A.1 — Equipment's network asset

Examples of network functions are:

- A network stack, like a TCP/IP implementation,
- a DNS service implementation providing network address resolution services to other devices.

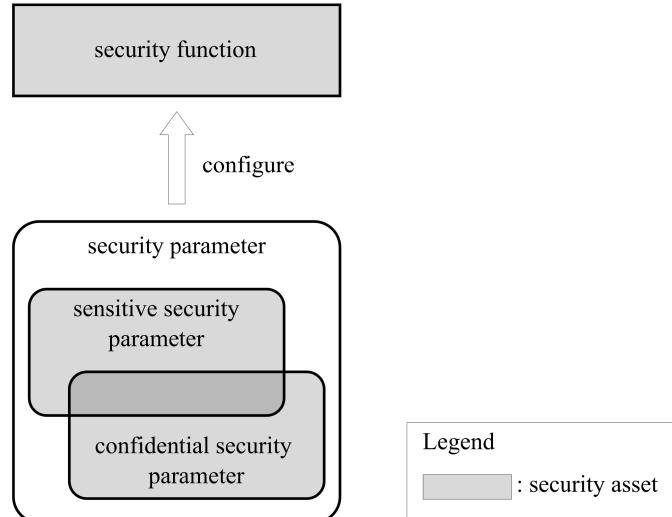


Figure A.2 — Equipment's security asset

A security parameter is information used in security functions to protect assets:

- Per definition, a confidential security parameter (CSP) is secret security related information whose disclosure can compromise the security of an asset. Typical examples are PINs and passwords, symmetric cryptographic keys or private asymmetric cryptographic keys.
- A sensitive security parameter (SSP) is security related information whose manipulation can compromise the security of an asset. Typical examples are symmetric and asymmetric cryptographic keys or access rights.
- A public security parameter is a sensitive security parameter that is not confidential. Typical examples are public asymmetric keys.
- A security parameter can be both sensitive and confidential, and according to the examples given above a private symmetric cryptographic key typically falls into this category.

Security functions are used to protect network assets or other security assets. For example, the implementation of an access control mechanism is a security function.

In some cases, security functions protect even their own security parameters, e.g., access control might be in place before granting access to sensitive or confidential access control security parameters.

The present document does not determine the granularity of the documentation concerning security assets and network assets. A suitable granularity with respect to efforts in documentation can consider common access paths to and access control mechanisms of (groups of) specific assets. For example, sensitive security parameters, which are only accessible via a specific API that makes use of a specific access control mechanism can be grouped together.

A.2.7 Mechanisms

This document uses the concept of mechanisms to address specific security requirements to facilitate the applicability and appropriateness of the requirements to different types of equipment implementation and use. As this document is a horizontal standard it needs to cover a wide range of products and use cases.

If and how generic security objectives are to be achieved depends on the intended equipment functionality and the intended operational environment of use. They influence the actual required

implementation of security measures and the strength of those controls in a specific equipment. A specific security measure might be appropriate for a product but might be too weak or strong for other products or the same product when used in another environment.

This document provides specific constraints and assessment questions to guide and avoid the full dependence on a manufacturer's scrutiny towards the necessary security measures to address the security concerns related to the intended equipment functionality and the intended operational environment of use.

To guide the user of this document as to when to apply a certain mechanism, the first requirement addresses the applicability of the mechanism. These requirements may have an 'except' component that lists the potential conditions for which the mechanism is not required. If it is determined that the mechanism is not applicable, then all further requirements in that specific clause are no longer mandatory.

When a mechanism is needed, the sufficiency is determined by evaluating the appropriateness type of the requirement and assessment criteria. Any supporting requirements in the clause are applicable as well.

This decision is made for each of the items specified, for example when checking the applicability of a requirement on external interfaces, then the decision whether the requirement and all further requirements need to be fulfilled is determined for each external interface independently.

A.2.8 Assessment criteria

The security mechanisms, functionality or other obligations imposed on the equipment have been defined in terms as precise and objective as possible, without compromising the technology-agnostic spirit of this document. How the manufacturer fulfils each will be documented by providing the inputs for the compliance test of the equipment.

A.2.8.1 Decision trees

Whether a mechanism or requirement is applicable and or appropriate is dependent on the intended use and intended operational environment of use. This document uses decision trees to aid in the decision making and assessment to provide clear direction. An example is shown below.

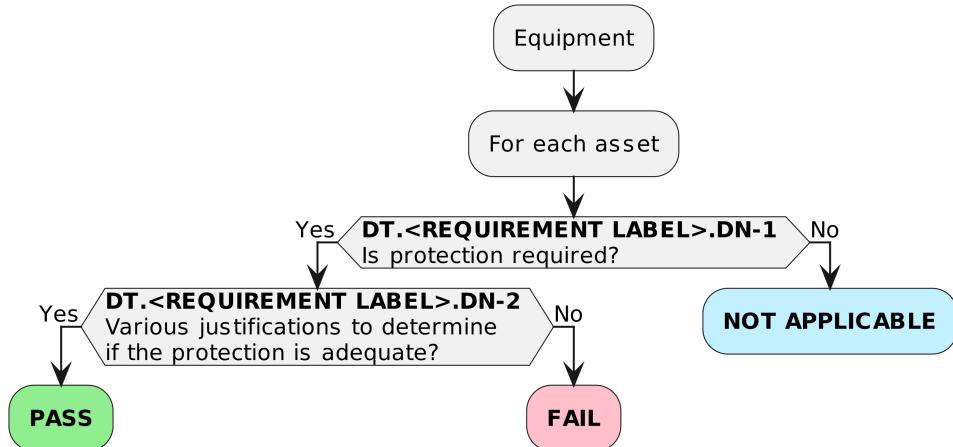


Figure A.3 — Example decision tree

Most decision trees start with the equipment followed by an element to iterate over (e.g., assets above). For each of those element's questions are answered on the characteristics of the equipment or related environmental factors. Each decision tree will have at least one or more PASS and FAIL paths and can optionally have one or more NOT APPLICABLE paths. A justification for each selected path will have to be documented.

A.2.8.2 Technical documentation

The assessments depend on the information to be provided as part of the manufacturer's technical documentation and the results of the applied test methodology prescribed for the respective implementation category where present. The specific information elements that need to be included in the manufacturers technical documentation for an assessment are indicated as [E.Info.xxxxx] where xxxx indicates the specific desired set of information, for instance [E.Info.ACm-1.ACm] is the identification of some of the access control mechanisms' information to be provided for the assessments for the requirement ACM-1 or [E.Info.AUm-1-1.ACm.NetworkInterface] includes a description of network interfaces for the assessment for the requirement AUM-1-1.

Some of the expected general information is:

- information on the intended equipment functionality
- equipment's technical information
- declared best practice considering the specific use case
- specific details such as a list of external interfaces
- security risk assessment

The assessment of a requirement could require the same or similar information as other requirements (e.g., interface information) in this case a reference could be used inside the documentation.

As input for the assessment the paths through the decision trees are indicated as [E.Info.DT.xxxxxx] and the justification is indicated as [E.Just.DT.xxxxxx]. Not all information elements that are indicated might be required depending on the selected implementation category and path through the decision tree. The table below is just an example of how this could be achieved for a conceptual assessment.

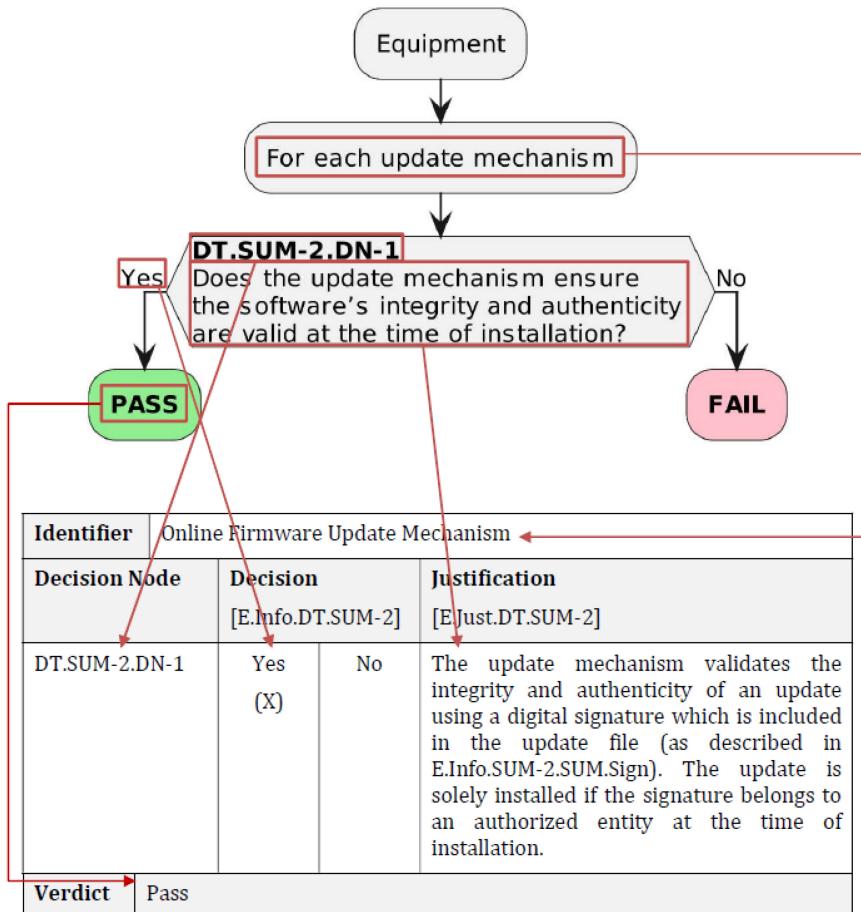


Figure A.4 — Example: Decision Tree Evidence

A.2.8.3 Security testing

The adequacy of most security controls is not quantifiable measurable, as there are no equivalents to a thermometer or frequency meter to measure the equipment's security posture or strict definitions to determine when good is good enough.

The outcome therefore is dependent on the evaluator's knowledge and view of the threat landscape and what is appropriate for a specific equipment in a specific environment, thereby further contributing to the fact that it is difficult to define verifiable, objective, and reproducible test criteria, because even two evaluators might have subtly different views and/or opinions.

Security test tools often use negative testing, demonstrating that certain weaknesses are not manifest, but because security tools are continuously updated, new issues might be found with updated information or when run for a more extensive period - as such this will also not lead to reproducible test results.

The approach taken in this document, therefore, improves the assessment outcome but cannot resolve this issue. Most of the assessments are based on the fact that sufficient information is provided.

A.2.9 Interfaces

Interfaces are an essential concept to describe the communication relationship between entities. The definitions for the interfaces are structured in a hierarchical manner:

Table A.4 — Interfaces

Definition		Note
interface		Abstract base definition
	external interface	Definition scoped to the equipment
	user interface	Specific interface types scoped to the equipment
	machine interface	
	network interface	

The hierarchical structure can be described by the following relationships:

- An “external interface” is an “interface”.
- A “user interface”, a “machine interface” and a “network interface” are all “external interfaces”.

This document only defines specific interface types that are in the scope of this document.

For the communication between the equipment and an entity a layered communication model is applied. Depending on the use case per communication layer different types of interfaces might be used.

For example, a web service on the equipment might provide a web page to a device to interact with the device’s user. While from the application point of view this is a user interface, the web page is transmitted over the network using a network interface.

The following examples illustrate the approach.

A.2.9.1 Example: Laptop with a built-in keyboard

In this example the keyboard is an integral part of the equipment. The equipment communicates with the user through a user interface.

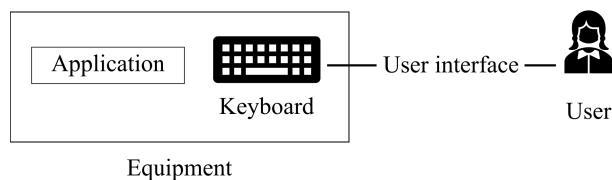


Figure A.5 — Example: Laptop with a built-in keyboard

A.2.9.2 Example: Equipment with a USB-keyboard

In this example the keyboard is not part of the equipment but is connected via USB. From the perspective of the equipment the keyboard is an external device, to which it communicates through a machine interface. However, from the application point of view the communication with the user takes place through a user interface.

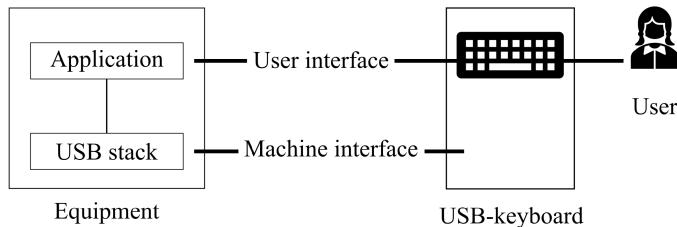


Figure A.6 — Example: Equipment with a USB-keyboard

A.2.9.3 Example: User interface over a network

A user is using a device to communicate with the equipment over the network using a keyboard. For this example, it is irrelevant, if the keyboard is built-in into the device, or if it is connected by other means to the device.

The equipment is using the network stack to communicate with the user's device, thus on this layer the communication takes place through a network interface. From the application point of view a user interface is used between the equipment's application and the user.

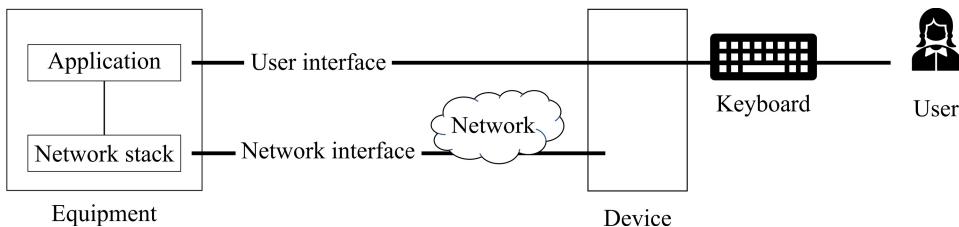


Figure A.7 — Example: User interface over the network

A.2.9.4 Example: USB-printer

A printer is connected to the equipment via USB. The example is like the USB-keyboard with the only difference that from application point of view the communication takes place through a machine interface.

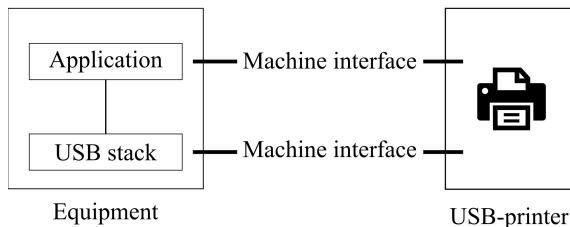


Figure A.8 — Example: USB-printer

A.2.9.5 Example: Network printer

In this example the equipment is communicating with a printer reachable over the network. Like for the user interface over the network example, it does not matter how the printer is connected to the network. On application layer the communication takes place through a machine interface, while from the network layer point of view a network interface is used for communication.

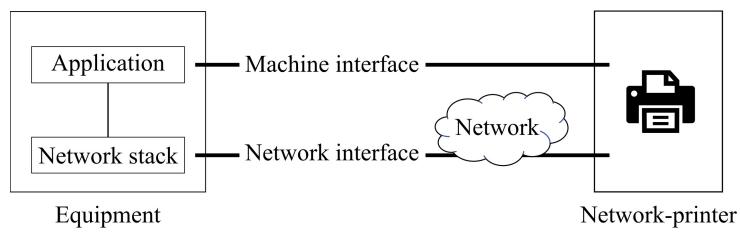


Figure A.9 — Example: Network-printer

Annex B (informative)

Mapping with EN IEC 62443-4-2: 2019

B.1 General

The intention of this informative annex is to provide a mapping between the requirements in this document and the Component Requirements (CRs) specified in EN IEC 62443-4-2: 2019 [2] in order to support manufacturers who are also applying EN IEC 62443-4-2: 2019 [2].

The required security level and applicable requirements are identified as a result of the risk assessment performed by the manufacturer.

Secure product development lifecycle related requirements are specified in EN IEC 62443-4-1:2018 and are not addressed in this annex.

Fulfilment of the EN IEC 62443-4-2: 2019 requirements (e.g., documented by a certificate) in itself does not provide conformance to the requirements in this document.

B.2 Mapping

Req.ID	EN IEC 62443-4-2:2019 Req.ID
ACM-1	FR1: CR 1.1 – CR 1.14 CR 2.1 CR 2.2 CR 2.3
ACM-2	FR1: CR 1.1 – CR 1.14 CR 2.1 CR 2.2 CR 2.3
AUM-1	FR1: CR 1.1 – CR 1.14
AUM-2	FR1: CR 1.1 – CR 1.14
AUM-3	CR 1.5 CR 1.10
AUM-4	CR 1.5
AUM-5	CR 1.7
AUM-6	CR 1.11 CR 1.7
SUM-1	CR 3.10
SUM-2	CR 3.10

Req.ID	EN IEC 62443-4-2:2019 Req.ID
SUM-3	CR 3.10
SSM-1	CR 3.1 CR 4.1
SSM-2	CR 3.1
SSM-3	CR 4.1
SCM-1	CR 3.1 CR 3.8 CR 4.1
SCM-2	CR 3.1 CR 3.8 CR 4.1
SCM-3	CR 4.1
SCM-4	CR 3.1 CR 3.8
RLM-1	CR 7.1 CR 7.2 CR 7.4
NMM-1	CR 5.2 CR 6.1 CR 6.2
TCM-1	CR 5.2
CCK-1	CR 4.3 CR 1.9 CR 1.14
CCK-2	CR 4.3
CCK-3	CR 4.3
GEC-1	Not covered by a CR in EN IEC 62443-4-2:2019
GEC-2	CR 7.6 CR 7.7 CR 5.2
GEC-3	CR 2.1 CR 7.6 CR 5.2
GEC-4	CR 7.6
GEC-5	CR 7.7

Req.ID	EN IEC 62443-4-2:2019 Req.ID
GEC-6	CR 3.5
CRY-1	CR 4.3

Annex C (informative)

Mapping with ETSI EN 303 645 (Cyber Security for Consumer Internet of Things: Baseline Requirements)

C.1 General

This annex provides a mapping illustrating what provisions of the ETSI EN 303 645 [5] can be used to support radio equipment compliance demonstration to the requirements from the present document.

C.2 Mapping

Req.ID	ETSI EN 303 645 [5] Provision: rationale
ACM-1	<p>Provision 5.5-4. The provision concerns device functionality, which includes security assets and network assets.</p> <p>Provision 5.5-5. The provision focuses on security configuration, which is also part of security assets.</p>
ACM-2	<p>Provision 5.5-5. Security assets include security configuration, which is covered by the provision.</p> <p>Provision 5.6-7. Least privilege principle as in the guidance section is ensured.</p>
AUM-1	<p>Provision 5.5-4. The provision concerns only an initial state.</p> <p>Provision 5.5-5. Security assets include security configuration, which is covered by the provision.</p>
AUM-2 and CRY-1	<p>Provision 5.1-3: The authentication against the device can be assumed to include protection of network assets and security assets by requiring best practice cryptography, incl. authentication mechanisms (which may include PKI-based authentication)</p>
AUM-3	Not covered in EN 303 645 [5]
AUM-4	<p>Provision 5.1-4. The provision covers a change of the authentication mechanisms, which includes authenticator tokens.</p>
AUM-5	<p>Provision 5.1-1. Uniqueness of passwords of different devices is enforced.</p>

Req.ID	ETSI EN 303 645 [5] Provision: rationale
	<p>Provision 5.1-2.</p> <p>Default passwords should be generated by a CSPRNG and therefore not be attackable by automated attacks.</p> <p>Provision 5.1-3.</p> <p>The provision covers the requirement regarding "best practice concerning strength" as it demands use of best practice cryptography.</p>
AUM-6	<p>Provision 5.1-5.</p> <p>Both the provision and requirement demand the protection / mitigation against brute force attacks (incl. mass authentication attacks)</p>
SUM-1	<p>Provision 5.3-1:</p> <p>The provision requires secure updates for each component.</p> <p>Provision 5.3-2.</p> <p>Secure Updates are required if there are no other reasons not to do them (e.g., constrained devices)</p> <p>Provision 5.3-15.</p> <p>The guidance includes a replacement strategy for equipment.</p>
SUM-2	<p>Provision 5.3-9.</p> <p>The provision guarantees the authenticity and integrity of updates.</p> <p>Provision 5.3-10.</p> <p>The provision guarantees the authenticity and integrity of updates, especially via network.</p>
SUM-3	<p>Provision 5.3-3.</p> <p>The guidance includes the simple updatability from a user's perspective.</p> <p>Provision 5.3-4.</p> <p>The provision includes automatic updates without human interaction.</p> <p>Provision 5.3-5.</p> <p>The guidance includes checking for updates after init and periodically.</p> <p>Provision 5.3-6.</p> <p>Primarily, "asking user for consent to activate autoupdates" and "checking for updates after init and periodically" are included in the guidance section.</p>
SSM-1	<p>Provision 5.4-1.</p> <p>Secure storage mechanisms are demanded for security assets (which include security parameters).</p> <p>Provision 5.6-3.</p> <p>The provision only covers physical protection, but "hardware and physical protection" are included in the guidance section.</p>
SSM-2	<p>Provision 5.4-1.</p> <p>The provision also protects security assets (which includes security parameters).</p> <p>Provision 5.4-2.</p>

Req.ID	ETSI EN 303 645 [5] Provision: rationale
	The provision aims to provide protection against integrity loss, such as tampering. The rationale of the prEN includes protection against tampering, but the provision only focuses on hard-coded identity cases.
SSM-3	Provision 5.4-1. Secure storage mechanisms are demanded for security assets (which include security parameters).
SCM-1	Provision 5.5-6. Critical security parameters are protected by the provision, but network assets are not necessarily covered. Provision 5.5-7. The provision focuses on confidentiality of security parameters.
SCM-2	Not covered in EN 303 645 [5]
SCM-3	Provision 5.5-6. The provision demands encryption of transmitted critical security parameters. Provision 5.5-7. The provision demands encryption of transmitted critical security parameters.
SCM-4	Provision 5.5-1. Best practice cryptography includes resiliency against replay attacks (see terms section).
RLM-1	Provision 5.9-1. DoS attacks are not explicitly mentioned in the provision but with focus on resiliency the outcome can be considered as a "data network outage".
NMM-1	Not covered in EN 303 645 [5]
TCM-1	Not covered in EN 303 645 [5]
CCK-1	Not covered in EN 303 645 [5]
CCK-2	Provision 5.1-3. Methods for protecting access to security assets shall use best practice cryptography.
CCK-3	Provision 5.1-1. The guidance section includes "security credentials", which includes passwords. Provision 5.4-4. Security params are required to be unique by both.

Req.ID	ETSI EN 303 645 [5] Provision: rationale
GEC-1	This requirement is not covered at the level of product requirement. However a manufacturer that complies with the processes Provisions 5.2-1, 5.2-2 and 5.2-3 will be facilitated to fulfil GEC-1 requirement.
GEC-2	Provision 5.6-1. Security params are required to be unique by both. Provision 5.6-5. Only services for operation and the setup of the device are allowed for both.
GEC-3	Not covered in EN 303 645 [5]
GEC-4	Not covered in EN 303 645 [5]
GEC-5	Provision 5.6-1. Not intended equipment functionality can be considered as unused. Provision 5.6-3. Only physical interfaces are covered by the EN.
GEC-6	Provision 5.13-1. Both the provision and the requirement demand input validation.
CRY-1	Provision 5.1-3. The provision concerns authentication mechanisms, which is a part of the requirement. Provision 5.3-7. The provision concerns Secure Updates, which is a part of the requirement. Provision 5.5-1. The provision concerns Secure Communications, which is a part of the requirement. Provision 5.5-2. Reviewed or evaluated cryptography is preferred in the guidance section. Provision 5.5-3. The provision concerns crypto agility, which is considered in the guidance section.

Annex D
 (informative)
**Mapping with Security Evaluation Standard for IoT Platforms
 (SESIP)**

D.1 General

This annex provides a mapping illustrating how the results of a SESIP (EN17927:2023) evaluation of connected platforms on which radio equipment are based, can be used as evidence to support radio equipment compliance demonstration to the requirements from the present document.

D.2 Mapping

Req.ID	EN17927:2023 SESIP support - evidence of implementation and assessment at equipment element/subcomponent level
ACM-1 to ACM-2	<p>Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore and/or Cryptographic Random Number Generation: those SESIP security claims assess the implementation of secure cryptographic services, which ones can be used by the equipment to implement an access control mechanism.</p> <p>Authenticated access control: this SESIP security claim assesses the implementation of a secure access control mechanism based on authentication, which one can be used directly by the equipment for access control purposes.</p>
AUM-1 to AUM-6	<p>Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore and/or Cryptographic Random number Generation: those SESIP security claims assess the implementation of secure cryptographic services, which ones can be used by the equipment to implement an authentication mechanism.</p> <p>Authenticated access control: this SESIP security claim assesses the implementation of a secure access control mechanism based on authentication, which one can be used directly by the equipment for authentication purposes.</p> <p>An explicit refinement of the requirement can require the validation of authenticator, the ability to change the authenticator, the preventing of static and default values. Protection against brute force and other cryptographic attack is part of the SESIP vulnerability analysis (AVA_VAN.SESIP) evaluation activity.</p>
SUM-1 to SUM-3	<p>Secure Update of platform, Secure Update of Application: this SESIP security claims assess the implementation of a secure update mechanism of the mutable part of the equipment element under evaluation, including the integrity and authenticity verification of the image to be installed/loaded.</p> <p>ALC_FLR: this SESIP evaluation activity assesses that for the equipment element under evaluation a process of flaw remediation is in place to allow</p>

	<p>the monitoring, the reporting and the correction of security issues which could be found in the field, and which would trigger the use of the secure update mechanism to mitigate the security issue.</p>
SSM-1 to SSM-3	<p>Secure Trusted Storage, Secure Confidential Storage, Secure Encrypted Storage and/or Secure Data Serialization: those SESIP security claims assess the implementation of secure storage mechanisms, including authenticity, integrity and/or confidentiality protections depending on the related stored assets protection needed.</p> <p>Cryptographic KeyStore: This SESIP security claim assesses that the element under evaluation implements a secure storage service for cryptographic material, which one can be used by the radio equipment to store confidential cryptographic keys.</p>
SCM-1 to SCM-4	<p>Secure Communication Support and Secure Communication Enforcement: those SESIP security claims assess the implementation of a secure communication mechanism, including authenticity, integrity, confidentiality and/or replay protections depending on the related transiting assets protection needed.</p>
RLM-1	<p>Constrained demands on the environment capability: This SESIP security claim assesses that the element under evaluation limits its demand to its environment according to a list of rules to not make undue demands on the environment, then supporting the final radio equipment to mitigate the effects of ongoing denial of services attacks.</p> <p>Availability Support: this SESIP security claim assesses the implementation of mechanisms supporting the availability of a determined list of its operations, which then supports the final equipment to mitigate the effects of ongoing denial of services attacks.</p>
NMM-1	<p>Generic Security Platform Feature: this SESIP security claim assesses the implementation of a mechanism very specific to an element under evaluation, which could be any support for a network monitoring mechanism at the equipment level.</p> <p>Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore and/or Cryptographic Random Number Generation: those SESIP security claims assess the implementation of secure cryptographic services, which ones could be needed by the equipment to support or implement a network monitoring mechanism.</p>
TCM-1	<p>Generic Security Platform Feature: this SESIP security claim assesses a mechanism very specific to an element under evaluation, which could be a support for a traffic control mechanism at the equipment level.</p> <p>Cryptographic Operation, Cryptographic Key Generation, Cryptographic KeyStore and/or Cryptographic Random Number Generation: those SESIP security claims assess the implementation of secure cryptographic services, which ones could be needed by the equipment to support or implement a traffic control mechanism.</p>

CCK-1 to CCK-3	<p>Cryptographic key generation: this SESIP security claim assesses the implementation of cryptographic key generation which can be used by the radio equipment to address CCK-2.</p> <p>All SESIP security services claim involving cryptographic keys (cryptographic services, secure initialization, secure update, secure communication, secure storage, etc.) are assessed to verify that those keys are securely handled and adhere to best practice cryptography.</p> <p>Explicit refinement of such security services claim can require that no static defaults values are used for confidential cryptographic keys.</p>
GEC-1 to GEC-6	<p>AVA_VAN.SESIP: this SESIP security evaluation activity requires the vulnerability analysis of the claimed security services implementation, during which:</p> <ul style="list-style-type: none"> - it is verified that the implementation under evaluation does not include publicly known exploitable vulnerabilities and that only needed interfaces are exposed for each life-cycle state. - it is checked that necessary input validation is performed. <p>Secure development: This SESIP security claim assesses that the element under evaluation has been developed following secure development rules, which could include the verification of the exposed attack surfaces. Note that the Radio Equipment Directive only covers product-specific requirements and not process requirements, hence making this activity a complementary action.</p> <p>AGD_OPE/PRE: these SESIP security evaluation activities require the documentation of security services exposed to the users.</p>
CRY-1	<p>All SESIP security services claim assessment involving cryptographic keys (cryptographic services, secure initialization, secure update, secure communication, secure storage, etc.) verify that those keys are securely handled and adhere to best practice cryptography.</p>

Annex ZA
 (informative)

Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2022) 5637 and its amendment C(2023) 5624 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3).

In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail.

Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153]

Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
3.3.(d)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11	
3.3.(e)		
3.3.(f)		

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Bibliography

- [1] IEC EN 62443-4-1, Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements
- [2] IEC EN 62443-4-2, Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
- [3] ISO/IEC EN 27002:2022, Information security, cybersecurity and privacy protection - Information security controls
- [4] ISO/IEC EN 24760 series, IT Security and Privacy - A framework for identity management
- [5] ETSI EN 303 645, Cyber Security for Consumer Internet of Things - Baseline Requirements
- [6] ETSI TS 103 701, Cyber Security for Consumer Internet of Things - Conformance Assessment of Baseline Requirements
- [7] NIST SP 800-57, Recommendation for Key Management, Part 1 Rev.5
- [8] NIST SP 800-63 series, Digital Identity Guidelines
- [9] NIST SP 800-63B, Digital Identity Guidelines - Authentication and Lifecycle Management
- [10] NIST SP 800-90A Rev.1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators
- [11] NIST SP 800-90B, Recommendation for the Entropy Sources Used for Random Bit Generation
- [12] NIST SP 800-90C, Recommendation for Random Bit Generator (RBG) Constructions
- [13] NIST SP 800-108r1, Recommendation for Key Derivation Using Pseudorandom Functions
- [14] NIST SP 800-131A Rev.2, Transitioning the Use of Cryptographic Algorithms and Key Lengths
- [15] NIST SP 800-132, Recommendation for Password-Based Key Derivation: Part 1: Storage Applications
- [16] NIST SP 800-160, Engineering Trustworthy Secure Systems
- [17] NIST SP 800-218, Secure Software Development Framework (SSDF) - Recommendations for Mitigating the Risk of Software Vulnerabilities
- [18] BSI AIS 31, A Proposal for Functionality Classes for Random Number Generators
- [19] BSI TR-02102 series, Cryptographic Mechanisms: Recommendations and Key Length, Version 2023-1
- [20] FIPS 140-2, Security Requirements for Cryptographic Modules
- [21] FIPS 140-3, Security Requirements for Cryptographic Modules

- [22] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms
- [23] ANSSI PA-79, guide de sélection d'algorithmes cryptographiques
- [24] EPC 342-08, Guidelines on cryptographic algorithms usage and key management / Version 9.0 / PSSG European Payments Council publication
- [25] ETSI TS 119 312 Electronic Signatures and Infrastructures; Cryptographic Suites
- [26] ISO/IEC 11770:2010 series Information technology, Security techniques, Key management
- [27] ISO/IEC 33001:2015 Information technology, Process assessment, Concepts and terminology
- [28] IEC EN 62443-1-1:2019, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models
- [29] NIST SP 800-172, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- [30] ISO/IEC Guide 51:2014, Safety aspects, Guidelines for their inclusion in standards
- [31] IEC Electropedia, <https://www.electropedia.org/>
- [32] ENISA Glossary, <https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary>
- [33] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC
- [34] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive
- [35] EU Commission 'Blue Guide' on the implementation of EU product rules, 2022
- [36] EU Commission 'RED guide' Guide to radio Equipment Directive 2014/53/EU, 2018
- [37] BSI AIS 20, Functionality classes and evaluation methodology for deterministic random number generators
- [38] ISO/IEC 18031, Information technology, Security techniques, Random bit generation
- [39] ISO/IEC TR 27103:2018, Information technology, Security techniques, Cybersecurity and ISO and IEC Standards
- [40] The NIST Cybersecurity Framework (CSF) 2.0