



CE CYBER SECURITY REPORT

Equipment : The Things Outdoor Gateway
Model No. : WAPS-232N LW-TN
Standard : EN 18031-1

Self-Declaration of Conformity :

This document serves as a declaration that the equipment described herein has been evaluated in accordance with the requirements of the CE Radio Equipment Directive — Essential Assessment (RED-EA) and has been found to be in compliance with all applicable essential requirements. The assessment has been carried out based on the decision trees, criteria, and procedures defined in the relevant RED-EA guidance documents. The results summarized in this report confirm that the equipment meets the applicable performance, safety, and security requirements, enabling its placement on the market within the European Economic Area (EEA) bearing the CE marking.

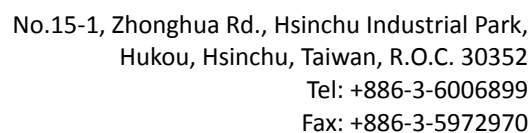
Contents

Contents.....	2
History of this test report.....	5
1. Summary of Test Procedure and Test Verdicts.....	6
1.1 Applicable Standards.....	6
2. Test Configuration of Device Under Test.....	9
2.1 Feature of Device Under Test.....	9
2.2 Test Software.....	12
2.3 Description of Test System.....	12
2.4 General Information of Test.....	12
3. The assessment.....	13
4. Test Verdict and Data.....	15
4.1 [ACM] Access control mechanism.....	15
[ACM-1] Applicability of access control mechanisms.....	15
[ACM-2] Appropriate access control mechanisms.....	19
4.2 [AUM]Authentication mechanism.....	21
[AUM-1] Applicability of authentication mechanisms.....	21
[AUM-1-1] Requirement network interface.....	21
[AUM-1-2] Requirement user interface.....	26
[AUM-2] Appropriate authentication mechanisms.....	29
[AUM-3] Authenticator validation.....	30
[AUM-4] Changing authenticators.....	32
[AUM-5] Password strength.....	35
[AUM-5-1] Requirement for factory default passwords.....	35
[AUM-5-2] Requirement for non-factory default passwords.....	38
[AUM-6] Brute force protection.....	40
4.3 [SUM]Secure update mechanism.....	43



[SUM-1] Applicability of update mechanisms.....	43
[SUM-2] Secure updates.....	47
[SUM-3] Automated updates.....	49
4.4 [SSM] Secure storage mechanism.....	52
[SSM-1] Applicability of secure storage mechanisms.....	52
[SSM-2] Appropriate integrity protection for secure storage mechanisms.....	56
[SSM-3] Appropriate confidentiality protection for secure storage mechanisms.	58
4.5 [SCM] Secure communication mechanism.....	60
[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms.....	63
[SCM-3] Appropriate confidentiality protection for secure communication mechanisms.....	65
[SCM-4] Appropriate replay protection for secure communication mechanisms.	67
4.6 [RLM] Resilience mechanism.....	70
[RLM-1] Applicability and appropriateness of resilience mechanisms.....	70
4.7 [NMM] Network monitoring mechanism.....	74
[NMM-1] Applicability and appropriateness of network monitoring mechanisms	74
4.8 [TCM] Traffic control mechanism.....	76
[TCM-1] Applicability of and appropriate traffic control mechanisms.....	76
4.9 [CCK] Confidential cryptographic keys.....	78
[CCK-1] Appropriate CCKs.....	78
[CCK-2] CCK generation mechanisms.....	83
[CCK-3] Preventing static default values for preinstalled CCKs.....	87
4.10 [GEC] General equipment capabilities.....	90
[GEC-1] Up-to-date software and hardware with no publicly known exploitable	

vulnerabilities.....	90
[GEC-2] Limit exposure of services via related network interfaces.....	94
[GEC-3] Configuration of optional services and the related exposed network interfaces.....	96
[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces.....	98
[GEC-5] No unnecessary external interfaces.....	101
[GEC-6] Input validation.....	104
4.11 [CRY] Cryptography.....	106
[CRY-1] Best practice cryptography.....	106

[illegible]

1. Summary of Test Procedure and Test Verdicts

1.1 Applicable Standards

The measurements shown in this test report were made in accordance with the procedures given in EUROPEAN COUNCIL DIRECTIVE 2014/53/EU.

EN 18031-1:2024, BS EN 18031-1:2024

Standard Section Reference		Test Item	Verdict
6.1 Access control mechanism	Provision 6.1.1	ACM-1	PASS
	Provision 6.1.2	ACM-2	PASS
6.2 Authentication mechanism	Provision 6.2.1.1	AUM-1-1	PASS
	Provision 6.2.1.2	AUM-1-2	PASS
	Provision 6.2.2	AUM-2	PASS
	Provision 6.2.3	AUM-3	PASS
	Provision 6.2.4	AUM-4	PASS
	Provision 6.2.5.1	AUM-5-1	PASS
	Provision 6.2.5.2	AUM-5-2	N/A
	Provision 6.2.6	AUM-6	PASS
6.3 Secure update mechanism	Provision 6.3.1	SUM-1	PASS
	Provision 6.3.2	SUM-2	PASS
	Provision 6.3.3	SUM-3	PASS
6.4 Secure storage mechanism	Provision 6.4.1	SSM-1	PASS
	Provision 6.4.2	SSM-2	PASS



	Provision 6.4.3	SSM-3	PASS
6.5 Secure communication mechanism	Provision 6.5.1	SCM-1	PASS
	Provision 6.5.2	SCM-2	PASS
	Provision 6.5.3	SCM-3	PASS
	Provision 6.5.4	SCM-4	PASS
6.6 Resilience mechanism	Provision 6.6.1	RLM-1	PASS
6.7 Network monitoring mechanism	Provision 6.7.1	NMM-1	PASS
6.8 Traffic control mechanism	Provision 6.8.1	TCM-1	PASS
6.9 Confidential cryptographic keys	Provision 6.9.1	CCK-1	PASS
	Provision 6.9.2	CCK-2	PASS
	Provision 6.9.3	CCK-3	PASS
6.10 General equipment capabilities	Provision 6.10.1	GEC-1	N/A
	Provision 6.10.2	GEC-2	N/A
	Provision 6.10.3	GEC-3	PASS
	Provision 6.10.4	GEC-4	PASS
	Provision 6.10.5	GEC-5	PASS
	Provision 6.10.6	GEC-6	PASS
6.11 Cryptography	Provision 6.11.1	CRY-1	PASS
<p>The support column following notations are used:</p> <p>PASS : Overall Conformance</p> <p>FAIL: Requirement Not Met</p> <p>N/A : The item verdict NOT APPLICABLE / NOT NECESSARY / NOT SUPPORT / NONE</p>			

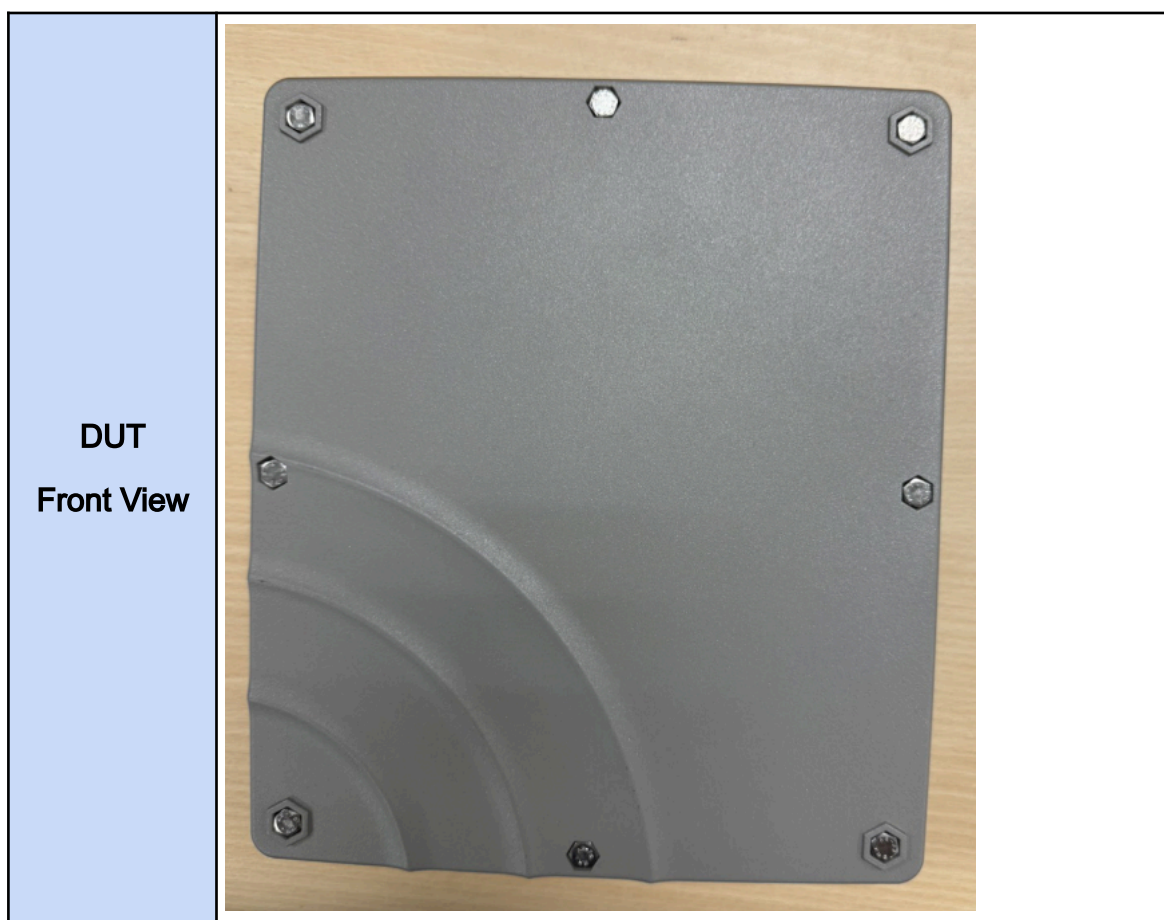


No.15-1, Zhonghua Rd., Hsinchu Industrial Park,
Hukou, Hsinchu, Taiwan, R.O.C. 30352
Tel: +886-3-6006899
Fax: +886-3-5972970

2. Test Configuration of Device Under Test

2.1 Feature of Device Under Test

Version	1.01.91
Communication interface	Ethernet/LTE
Connections	RJ45 x1
	SIM Card x1
IPv4 Address	192.168.11.172





BROWAN

No.15-1, Zhonghua Rd., Hsinchu Industrial Park,
Hukou, Hsinchu, Taiwan, R.O.C. 30352

Tel: +886-3-6006899

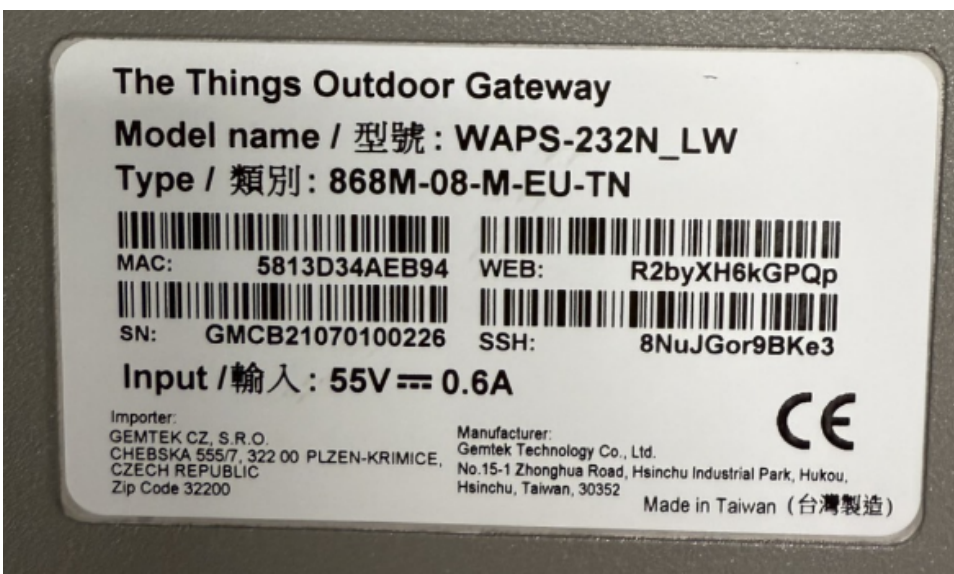
Fax: +886-3-5972970

DUT
Rear View



DUT
I/O ports



DUT Label No./ Serial No.	 <p>The Things Outdoor Gateway Model name / 型號: WAPS-232N_LW Type / 類別: 868M-08-M-EU-TN</p> <p>MAC: 5813D34AEB94 WEB: R2byXH6kGPQp SN: GMCB21070100226 SSH: 8NuJGor9BKe3</p> <p>Input / 輸入: 55V \equiv 0.6A</p> <p>Importer: GEMTEK CZ, S.R.O. CHEBSKA 555/7, 322 00 PLZEN-KRIMICE, CZECH REPUBLIC Zip Code 32200</p> <p>Manufacturer: Gemtek Technology Co., Ltd. No.15-1 Zhonghua Road, Hsinchu Industrial Park, Hukou, Hsinchu, Taiwan, 30352</p> <p>Made in Taiwan (台灣製造)</p> <p>CE</p>
--	--

2.2 Test Software

Tool	Version
WireShark	Version 4.0.7 (v4.0.7-0-g0ad1823cc090)
Zenmap	7.95
ssllcan	2.0.7

2.3 Description of Test System

Equipment	Brand	Model	Length/Type	Power cord/Length/Type
Notebook	Lenovo	T480	N/A	Adapter / 1.8m / B

2.4 General Information of Test

Test Site	Browan Communications Inc Address: No.15-1 Zhonghua Road, Hsinchu Industrial Park, Hukou, Hsinchu,Taiwan, 30352, Taiwan (R.O.C.) Tel:+886-3-6006-899
-----------	---

Test period	Tested By
2025/08/20 ~2025/08/31	Joey Ho

3. The assessment

【Conceptual assessment】

The verdict is established in accordance with the decision tree applied to each item.

【Functional Completeness Assessment】

Purpose: To conduct a functional verification that all aspects covered by the requirement's scope—including security assets, network interfaces, and vulnerabilities—are comprehensively and correctly documented.

Assessment Criteria:

PASS: Every relevant item discovered during functional verification is duly documented in compliance with the specified requirements.

FAIL: During functional verification, an item that falls within the required documentation scope is identified but not recorded in the provided information.

NOT APPLICABLE: An assessment is categorized as Not Necessary when the requirement is already encompassed by the Functional Sufficiency Assessment of the mechanism's applicability, or when the mechanism is mandated as compulsory.

Exceptions/Conditions: Requirements primarily addressing appropriateness rather than the mechanism's presence or applicability are typically classified as Not Necessary. Such requirements may include preconditions that demand a defined equipment state, such as factory default.

【Functional Sufficiency Assessment】

Purpose: The objective is to functionally assess the implemented security requirements and mechanisms to determine whether they are correctly operating, sufficiently robust, and effective in delivering the documented security properties.

Assessment Criteria:

PASS: Functional testing validates that the implementation performs in accordance with the documentation and effectively provides the required security, with no evidence of malfunction or deviation detected.

FAIL: Functional testing demonstrates that the implementation is inconsistent with the documentation or fails to provide the mandated security property, for instance, when a security control is ineffective.

NOT APPLICABLE: This designation is explicitly applied to certain requirements where conducting functional validation is impractical or outside the scope of the intended assessment—for example, in the validation of confidential key generation or in the assessment of specific physical interfaces.

Exceptions/Conditions: The assessment requires the equipment to be in an active operational state. It involves a series of functional tests, possibly supported by specialized tools, to evaluate both effectiveness and conformity with documentation. Depending on the technical implementation, customized test procedures may apply.

4. Test Verdict and Data

4.1 [ACM] Access control mechanism

[ACM-1] Applicability of access control mechanisms

【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.

【ACM-1 Assets】

Asset No.	Assets	Type	Access Mechanism
ACMA-A	administrator password	Security	Web GUI
ACMA-B	TLS certificate	Security	Web GUI
ACMA-C	private key for the HTTPS web interface	Security	Web GUI
ACMA-D	SSH	Security	SSH
ACMA-E	IP configuration	Network	Web GUI
ACMA-F	DNS settings	Network	Web GUI
ACMA-G	HTTPS service	Network	Web GUI



【ACM-1 Conceptual assessment】

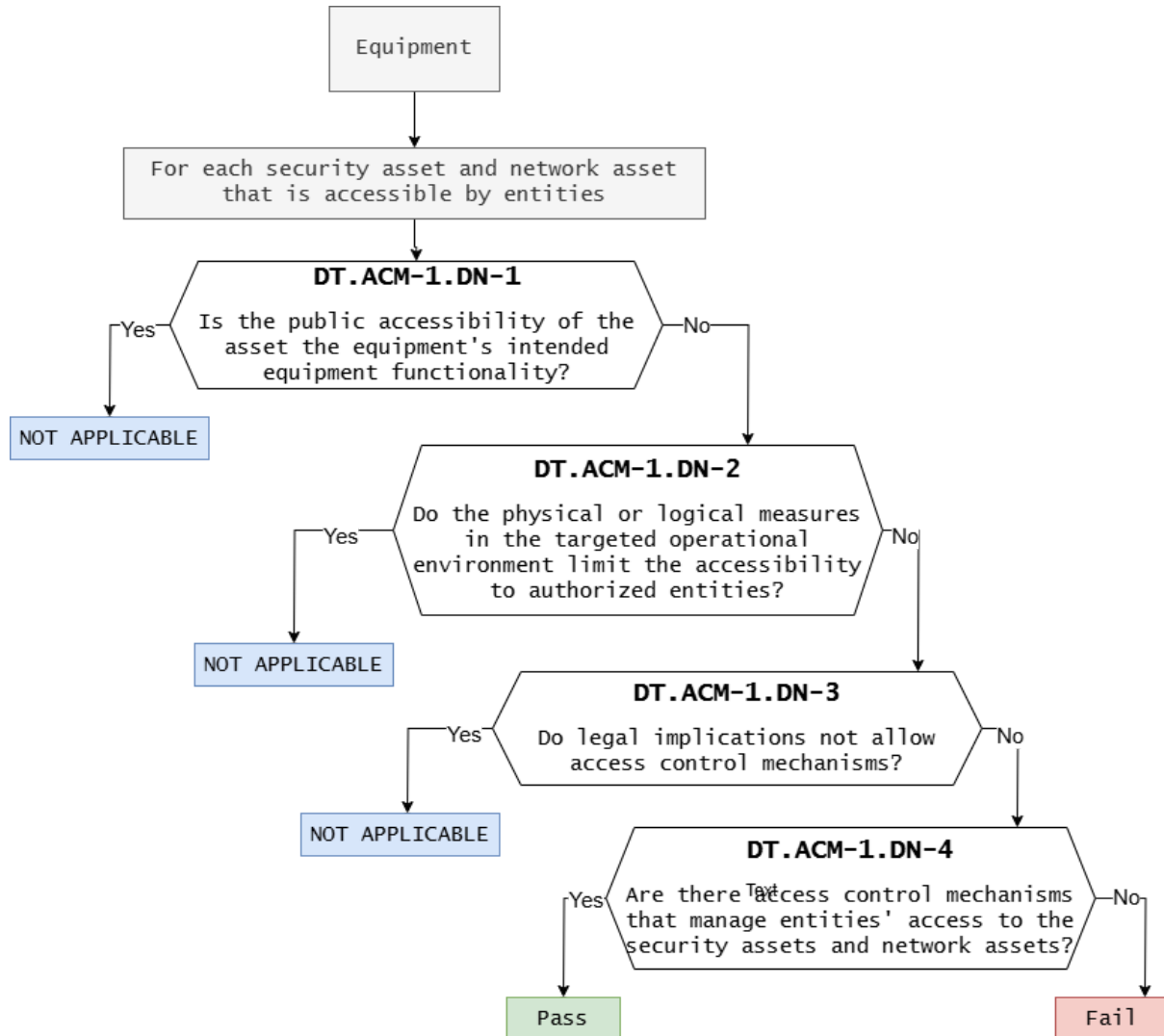


Figure 1 – Decision Tree for requirement ACM-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.ACM-1)
ACMA-A	DT.ACM-1.DN-1	No	The DUT cannot be accessed publicly.
ACMA-B	DT.ACM-1.DN-2	No	The DUT does not implement logical or physical controls to ensure access is limited to authorized entities.
ACMA-C			
ACMA-D			
ACMA-E	DT.ACM-1.DN-3	No	Legally, the implementation of access control mechanisms is allowed.
ACMA-F	DT.ACM-1.DN-4	Yes	Access to the DUT requires user authentication.
ACMA-G			

Verdict : PASS
【ACM-1 Functional completeness assessment】

Asset No.	Document Verification
ACMA-A	Y
ACMA-B	Y
ACMA-C	Y
ACMA-D	Y
ACMA-E	Y
ACMA-F	Y
ACMA-G	Y

Verdict : PASS

【ACM-1 Functional sufficiency assessment】

Asset No.	Implemented
ACMA-A	Y
ACMA-B	Y
ACMA-C	Y
ACMA-D	Y
ACMA-E	Y
ACMA-F	Y
ACMA-G	Y

Verdict : PASS

【Supporting Evidence】

The DUT is accessible only after user authentication

Outdoor-LBT

Authorization Required

Please enter your username and password.

Username

Password

ACM-1 Summary Assessment	Verdict
--------------------------	---------



Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

[ACM-2] Appropriate access control mechanisms

【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.

【ACM-2 Conceptual assessment】

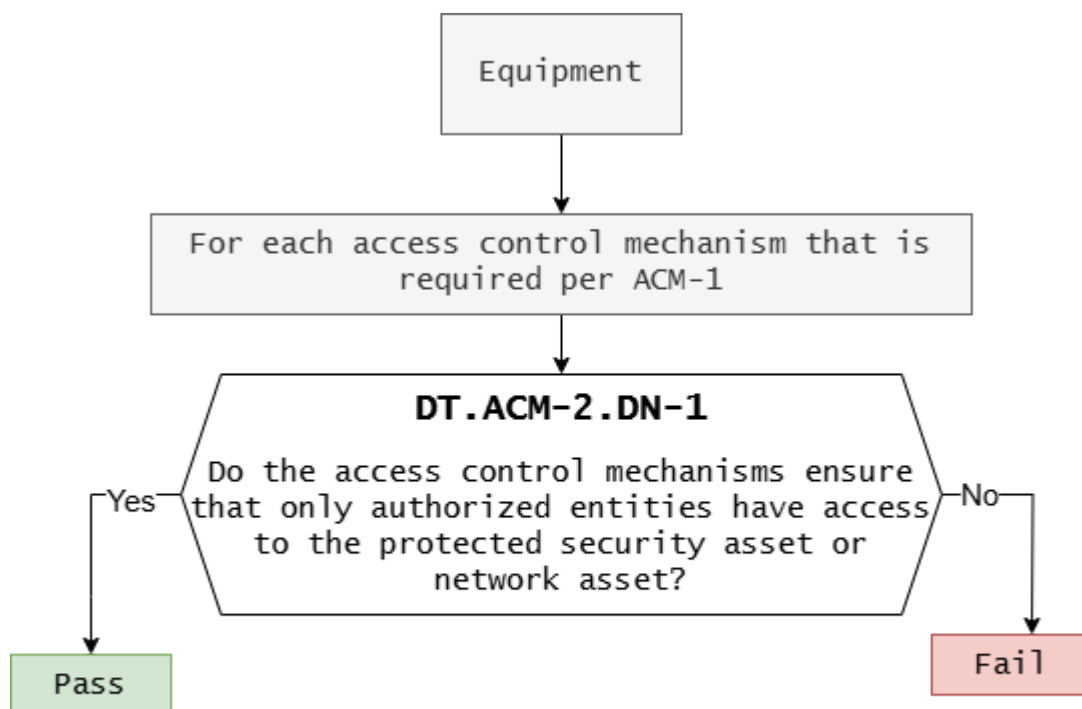


Figure 2 – Decision Tree for requirement ACM-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.ACM-2)
ACMA-A ACMA-B ACMA-C ACMA-D ACMA-E ACMA-F ACMA-G	DT.ACM-2.DN-1	Yes	Secure and network assets are accessed via password authentication.

Verdict : PASS

【ACM-2 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.

Verdict : NOT NECESSARY

【ACM-2 Functional sufficiency assessment】

Asset No.	Implemented
ACMA-A	Y
ACMA-B	Y
ACMA-C	Y
ACMA-D	Y
ACMA-E	Y



ACMA-F	Y
ACMA-G	Y

Verdict : PASS

【Supporting Evidence】

Follow ACM-1

ACM-2 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

4.2 [AUM]Authentication mechanism

[AUM-1] Applicability of authentication mechanisms

[AUM-1-1] Requirement network interface

【Requirement】

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 authorized entities.

【AUM-1-1 Assets】

Asset No.	Assets	Type	Access Mechanism
AUMA-A	Web GUI	Security	Network/User interface
AUMA-B	SSH	Security	Network/User interface

【AUM-1-1 Conceptual assessment】

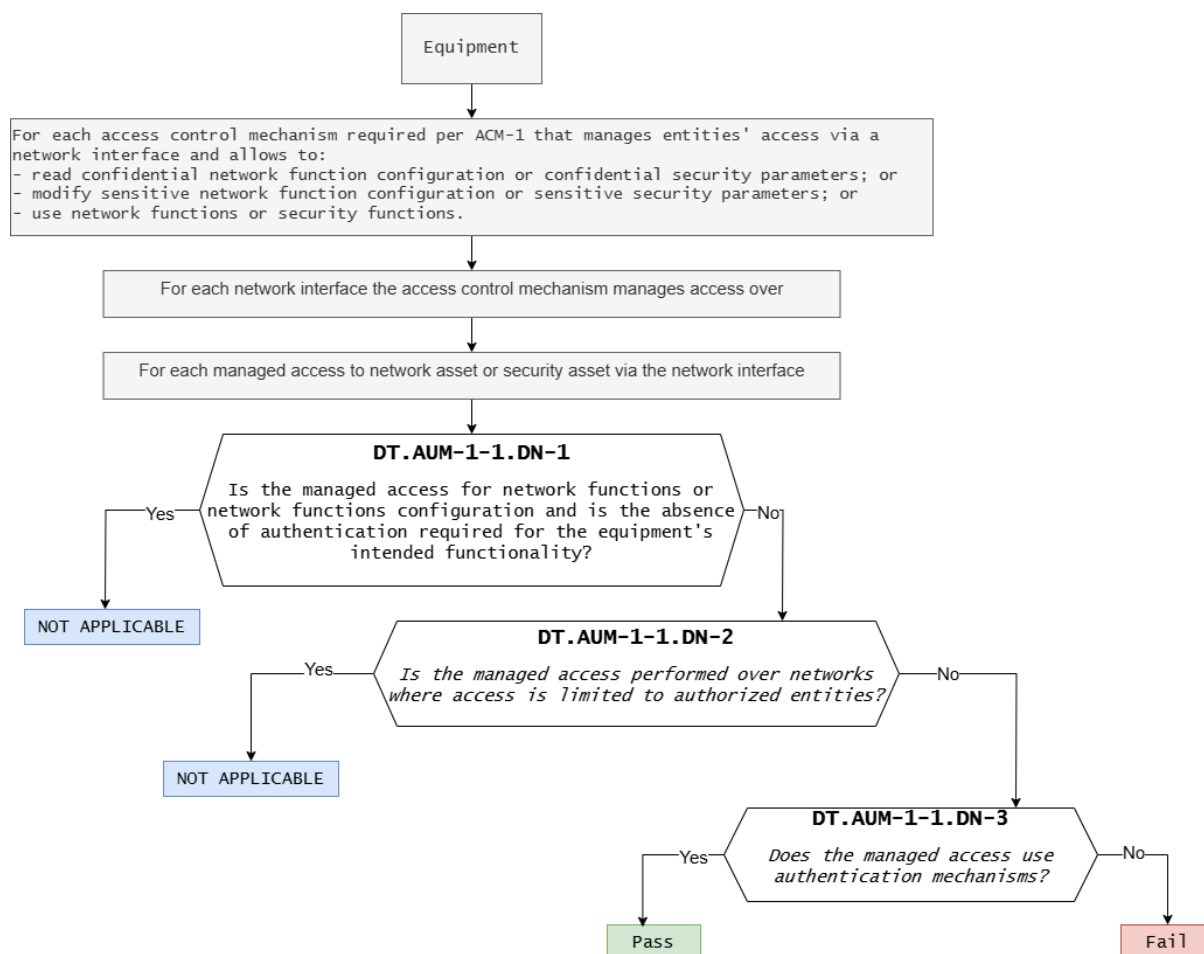


Figure 3 — Decision Tree for requirement AUM-1-1

【Assessment】

Asset	Decision Node	Decision	Justification (E.just.DT.AUM-1-1)
AUMA-A AUMA-B	DT.AUM-1-1.DN-1	No	The system requires user authentication through a password or equivalent credentials.
	DT.AUM-1-1.DN-2	No	No logical or physical safeguards have been implemented.
	DT.AUM-1-1.DN-3	Yes	The system includes an



			authentication mechanism.
--	--	--	---------------------------

Verdict: PASS

【AUM-1-1 Functional completeness assessment】

Asset No.	Document Verification
AUMA-A	Y
AUMA-B	Y

Verdict: PASS

【AUM-1-1 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	Y
AUMA-B	Y

Verdict: PASS



【Supporting Evidence】

Web GUI

Outdoor-LBT

Authorization Required

Please enter your username and password.

Username

Password

LOGIN

SSH

```
root@Joey-T480:~#  
root@Joey-T480:~# ssh root@192.168.11.172  
root@192.168.11.172's password: █
```

AUM-1-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

[AUM-1-2] Requirement user interface

【Requirement】

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.



【AUM-1-2 Conceptual assessment】

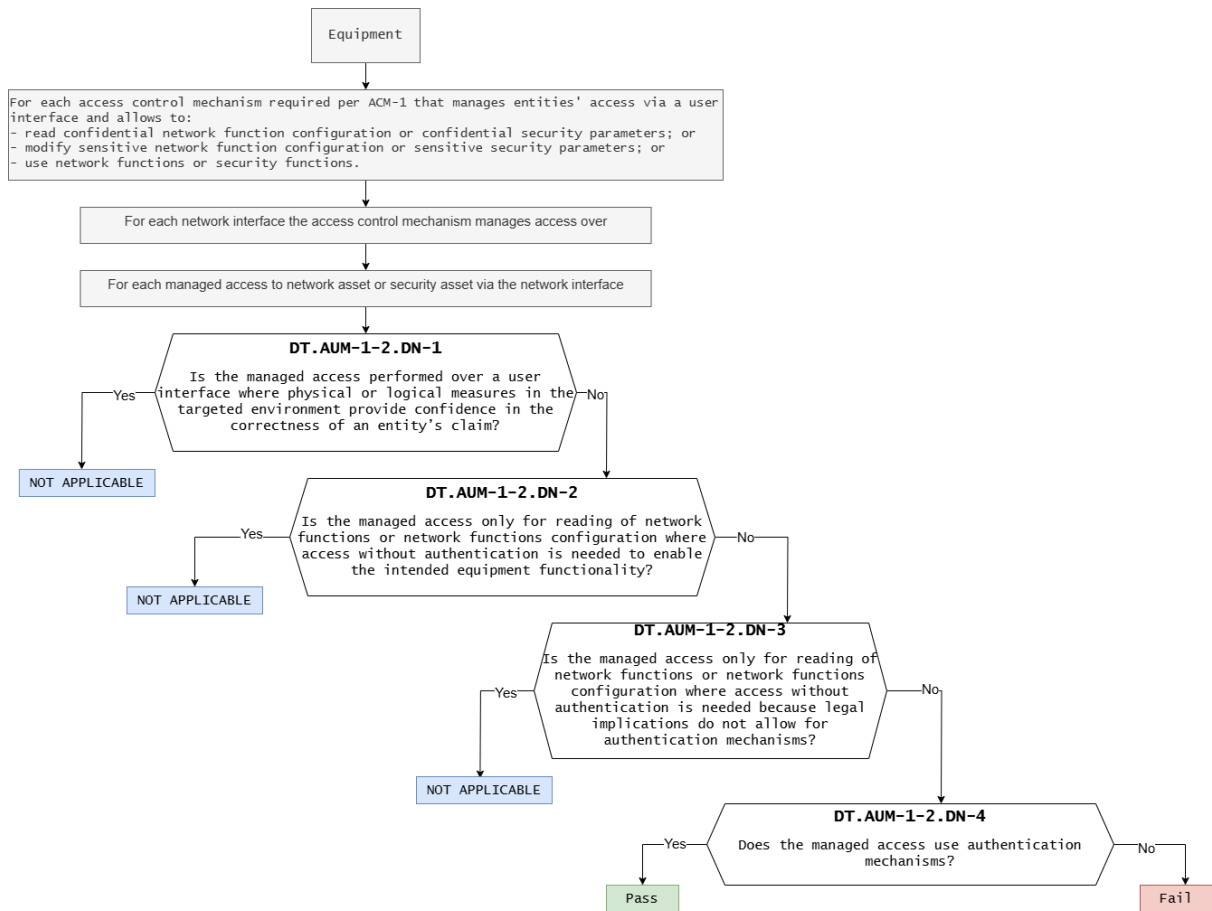


Figure 4 — Decision Tree for requirement AUM-1-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.AUM-1-2)
AUMA-A AUMA-B	DT.AUM-1-2.DN-1	No	Authentication is required to access the DUT.
	DT.AUM-1-2.DN-2	No	Authentication is required to access network functions.
	DT.AUM-1-2.DN-3	No	Network access requires authentication as a security

			measure, not a legal one.
	DT.AUM-1-2.DN-4	Yes	Apply authentication for access.

Verdict: PASS

【AUM-1-2 Functional completeness assessment】

Asset No.	Document Verification
AUMA-A	Y
AUMA-B	Y

Verdict: PASS

【AUM-1-2 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	Y
AUMA-B	Y

Verdict: PASS

【Supporting Evidence】

Follow AUM-1-1

AUM-1-2 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

[AUM-2] Appropriate authentication mechanisms

【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 inheritance (one factor authentication).

【AUM-2 Conceptual assessment】

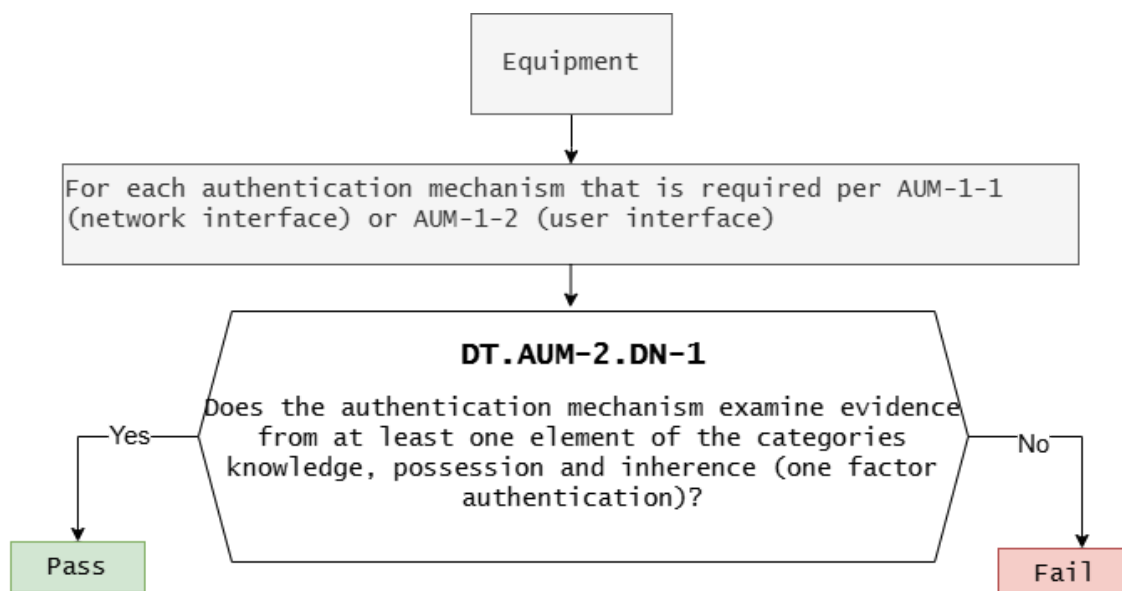


Figure 5 – Decision Tree for requirement AUM-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.AUM-2)
AUMA-A AUMA-B	DT.AUM-2.DN-1	Yes	Authentication is performed using a password.

Verdict: PASS

【AUM-2 Functional completeness assessment】

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 according to the sources.

Verdict: NOT NECESSARY

【AUM-2 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	Y
AUMA-B	Y

Verdict: PASS

【Supporting Evidence】

Follow AUM-1-1

AUM-2 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

【AUM-3] Authenticator validation

【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.

【AUM-3 Conceptual assessment】

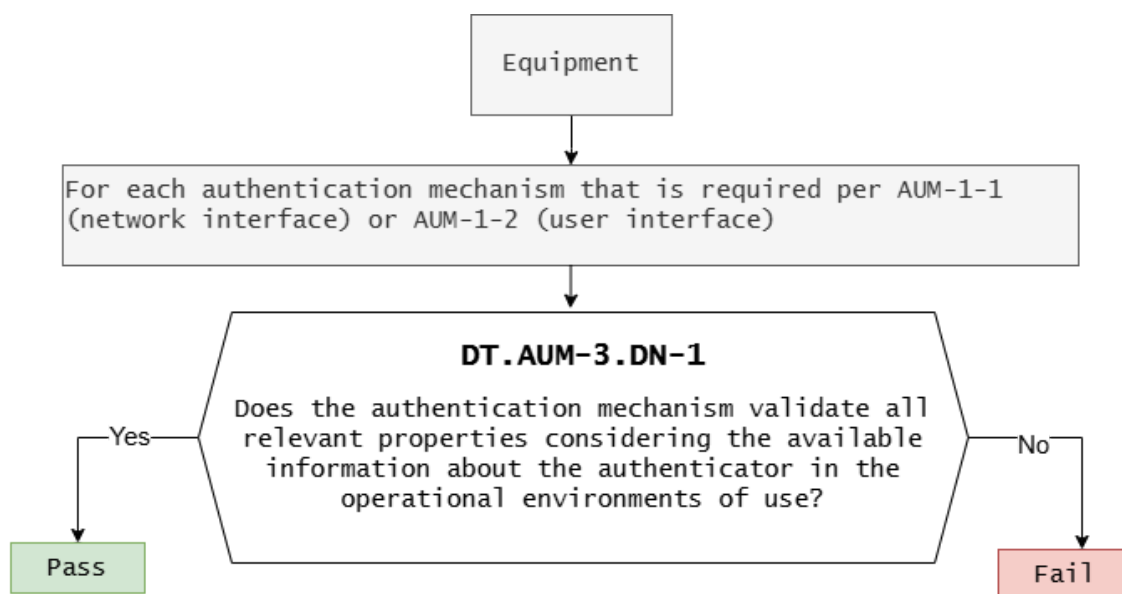


Figure 6 — Decision Tree for requirement AUM-3

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.AUM-3)
AUMA-A AUMA-B	DT.AUM-3.DN-1	Yes	Authentication is performed using a password.

Verdict: PASS

【AUM-3 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.

Verdict : NOT NECESSARY

【AUM-3 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	Y
AUMA-B	Y

Verdict: PASS

【Supporting Evidence】

Follow AUM-1-1

AUM-3 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

【AUM-4】 Changing authenticators

【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.



【AUM-4 Conceptual assessment】

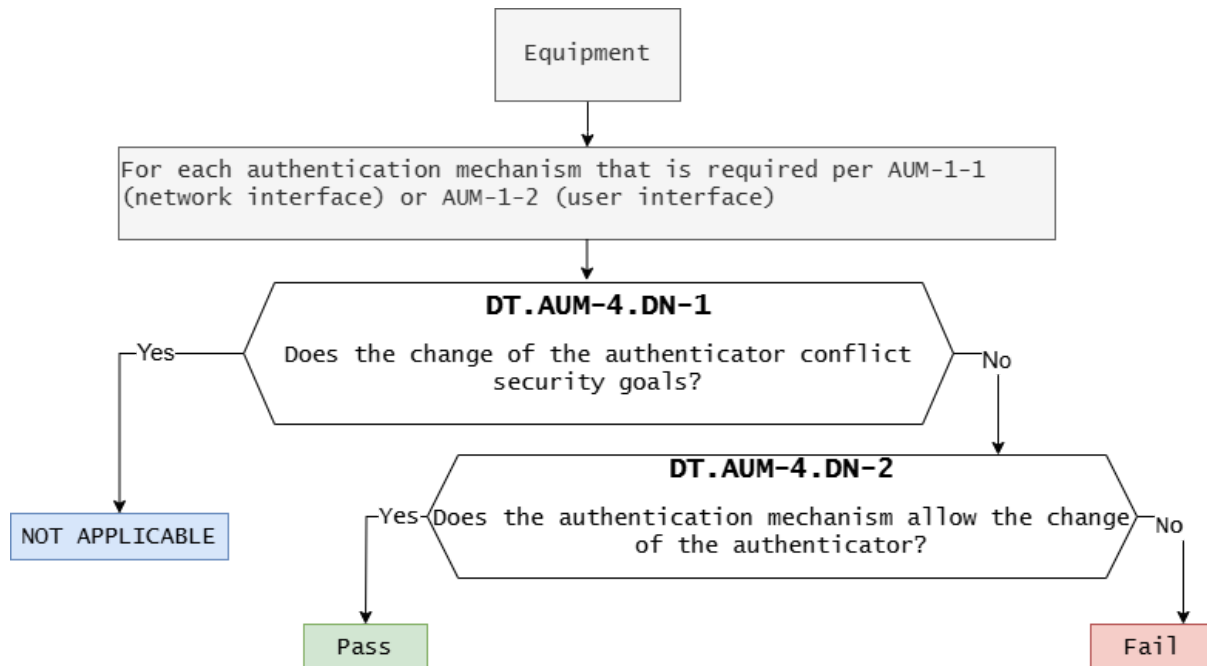


Figure 7 — Decision Tree for requirement AUM-4

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.AUM-4)
AUMA-A	DT.AUM-4.DN-1	No	Since no conflicting security requirements are present, modification of the authenticator is allowed.
	DT.AUM-4.DN-2	Yes	Modification of the authenticator is permitted.

Verdict: PASS



【AUM-4 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.

Verdict : NOT NECESSARY

【AUM-4 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	Y

Verdict: PASS

【Supporting Evidence】

← → ↻ Not secure https://192.168.11.172/cgi-bin/admin.cgi ☆ ⬇ Incognito (3)

GlOT opdk-1.01.91

System

- Administration
- Restore
- System Firmware

LoRa

Network

Firewall

[Logout](#)

Admin Password

Changes the administrator password for accessing the device

Password ✓

Confirmation ✓

Password Policy

- ✗ Minimum password length: 8 characters
- ✗ Must include at least one uppercase letter (A-Z)
- ✗ Must include at least one lowercase letter (a-z)
- ✗ Must include at least one digit (0-9)
- ✗ Must include at least one or more allowed special characters (@, #, !, &, ^, *, (,), <, >, -, _, +, =, ?)

APPLY CANCEL



AUM-4 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

[AUM-5] Password strength

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

【Requirement】

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 can choose to not use any password



【AUM-5-1 Conceptual assessment】

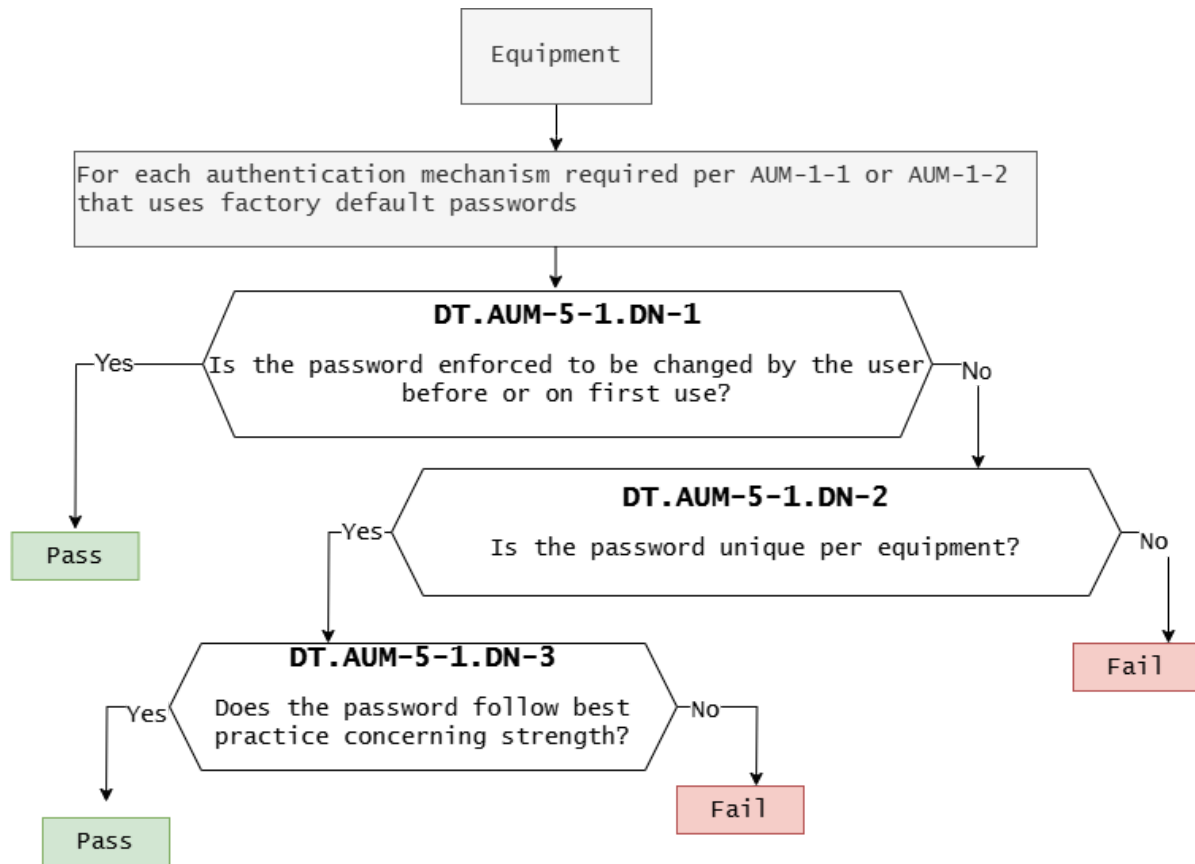


Figure 8 — Decision Tree for requirement AUM-5-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.AUM-5-1)
AUMA-A AUMA-B	DT.AUM-5-1.DN-1	No	Users are not required to change their passwords upon initial use.
	DT.AUM-5-1.DN-2	Yes	The password is unique, with each device assigned a different value.
	DT.AUM-5-1.DN-3	Yes	The password policy mandates a



			minimum length of 8 characters and must include a mix of uppercase, lowercase, numeric, and special characters.
--	--	--	--

Verdict: PASS

【AUM-5-1 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.

Verdict: NOT NECESSARY

【AUM-5-1 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	Y
AUMA-B	Y

Verdict: PASS

【Supporting Evidence】

- Each device is provisioned with a unique default password that is randomly generated through a secure method.
- The password meets established complexity requirements and is user-modifiable.
- The product implements best practices by ensuring every device is assigned a distinct default password.



- This measure effectively reduces the risk of credential reuse and unauthorized exposure.

AUM-5-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

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

【Requirement】

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 authorized 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 authorized entities.

NOTE: The user can choose to not use any password



【AUM-5-2 Conceptual assessment】

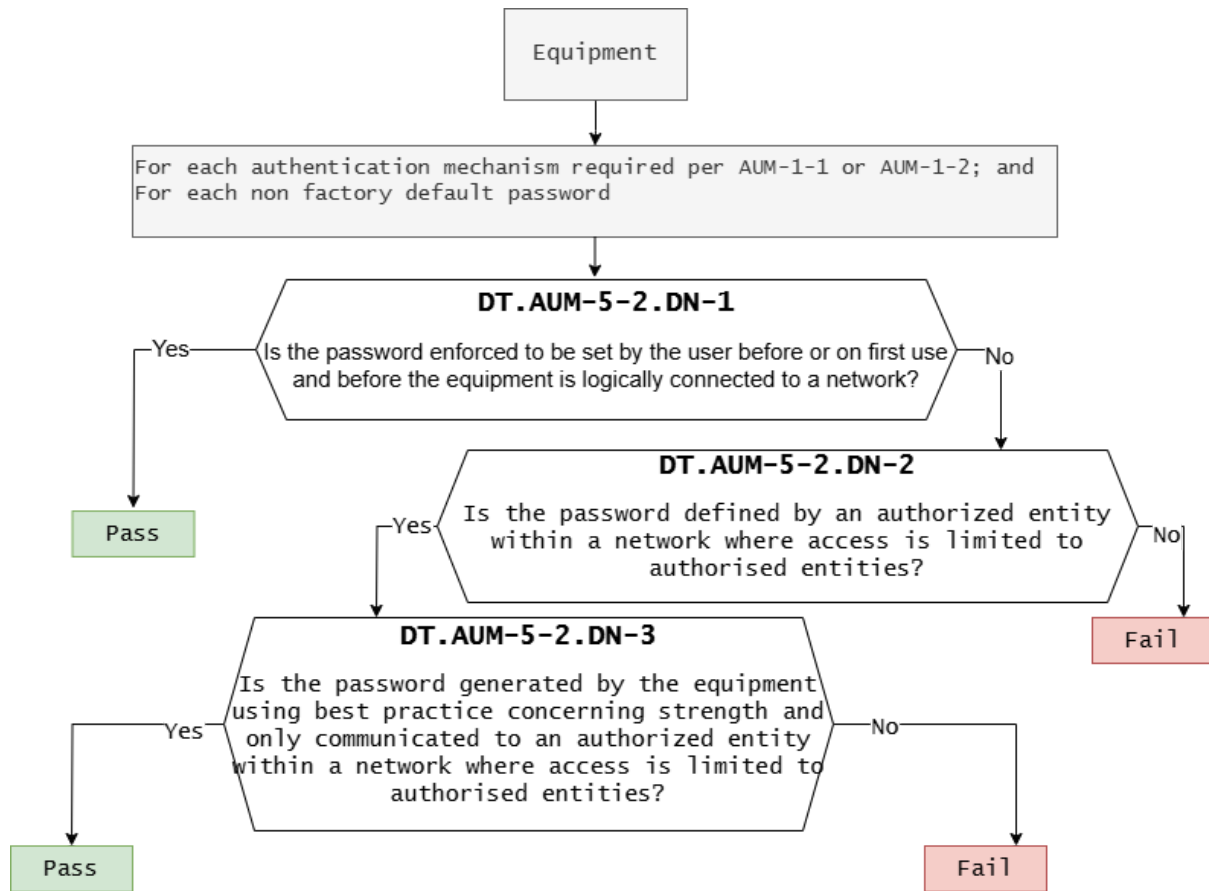


Figure 9 — Decision Tree for requirement AUM-5-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.AUM-5-2)
AUMA-A AUMA-B	DT.AUM-5-2.DN-1	-	The Device Under Test (DUT) includes an accessible factory default account.
	DT.AUM-5-2.DN-2	-	-
	DT.AUM-5-2.DN-3	-	-

Verdict: NOT APPLICABLE

【AUM-5-2 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.

Verdict : NOT NECESSARY

【AUM-5-2 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	N/A
AUMA-B	N/A

Verdict: NOT APPLICABLE

【Supporting Evidence】

The DUT factory default account available

AUM-5-2 Summary Assessment	Verdict
Conceptual assessment	NOT APPLICABLE
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	NOT APPLICABLE

【AUM-6】 Brute force protection

【Requirement】

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

【AUM-6 Conceptual assessment】

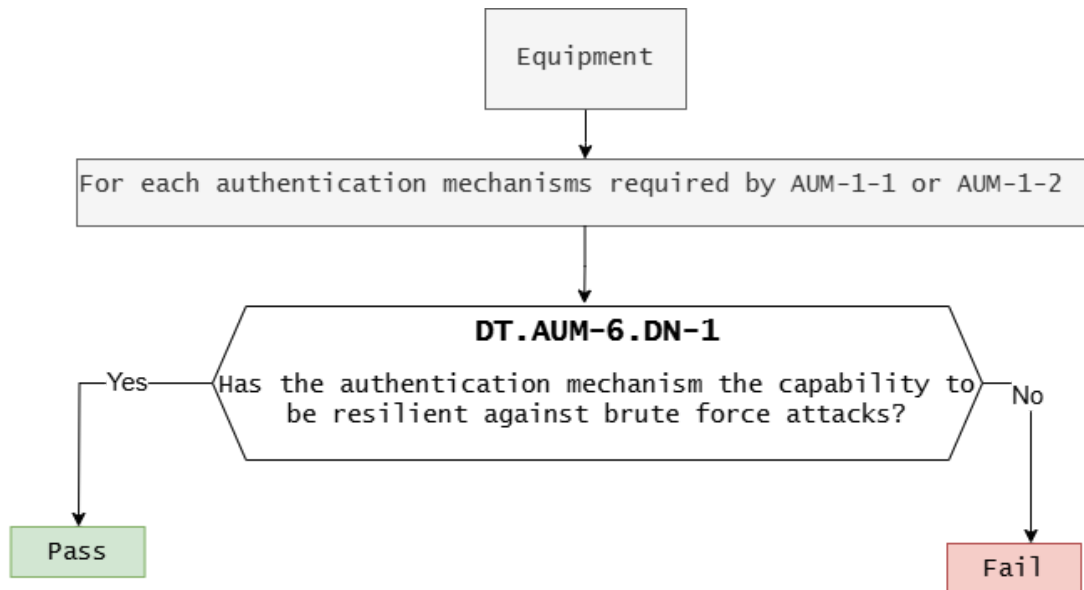


Figure 10 — Decision Tree for requirement AUM-6

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.AUM-6)
AUMA-A AUMA-B	DT.AUM-6.DN-1	Yes	A protective mechanism against brute force cracking attempts is in place.

Verdict: PASS

【AUM-6 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.

Verdict: NOT NECESSARY



【AUM-6 Functional sufficiency assessment】

Asset No.	Implemented
AUMA-A	Y
AUMA-B	Y

Verdict: PASS

【Supporting Evidence】

There are time delays and login limits

GUI

Authorization Required

Please enter your username and password.

Invalid username and/or password! Please try again.

Username

Password

Login limit reached, please wait for 5 minutes before you try again.

LOGIN

SSH

```
root@Joey-T480:~#  
root@Joey-T480:~# ssh root@192.168.11.172  
root@192.168.11.172's password:  
Permission denied, please try again.  
root@192.168.11.172's password:  
Permission denied, please try again.  
root@192.168.11.172's password:  
root@192.168.11.172: Permission denied (publickey,password).  
root@Joey-T480:~# █
```

AUM-6 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

4.3 [SUM]Secure update mechanism

[SUM-1] Applicability of update mechanisms

【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.



【SUM-1 Assets】

Asset No.	Asset	Update mechanisms
SUMA-A	update function	The update mechanism includes automatic update or manual update

【SUM-1 Conceptual assessment】

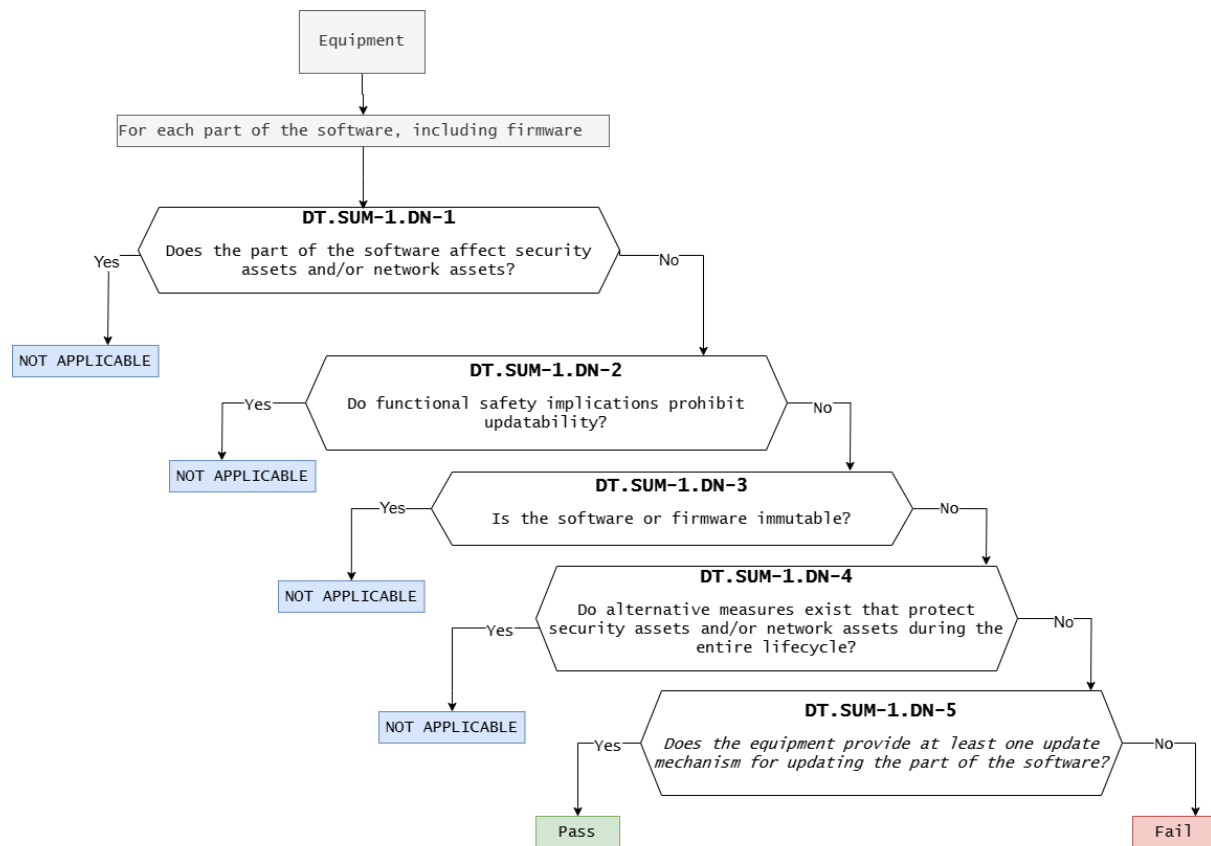


Figure 11 — Decision Tree for requirement SUM-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SUM-1)
SUMA-A	DT.SUM-1.DN-1	Yes	The update will affect assets
	DT.SUM-1.DN-2	No	Updates are permitted, as

			functional safety requirements do not impose any limitations
	DT.SUM-1.DN-3	No	The system allows changes to its software and firmware
	DT.SUM-1.DN-4	Yes	Continuous software updates are supported, removing the necessity for backup or contingency mechanisms.
	DT.SUM-1.DN-5	Yes	The device has an update mechanism

Verdict: PASS

【SUM-1 Functional completeness assessment】

NONE


Verdict: NONE

【SUM-1 Functional sufficiency assessment】

Asset No.	Implemented
SUMA-A	Y

Verdict: PASS

【Supporting Evidence】

 opdk-1.01.91

System
Administration
Restore
System Firmware
LoRa
Network
Firewall

[Logout](#)

Firmware Information

Current firmware version: opdk-1.01.91

Please select a file to upgrade: No file chosen

System - System Upgrade Now...

The system is upgrading now, please wait...



Waiting for changes to be applied.

SUM-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NONE
Functional sufficiency assessment	PASS

[SUM-2] Secure updates

【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.

【SUM-2 Conceptual assessment】

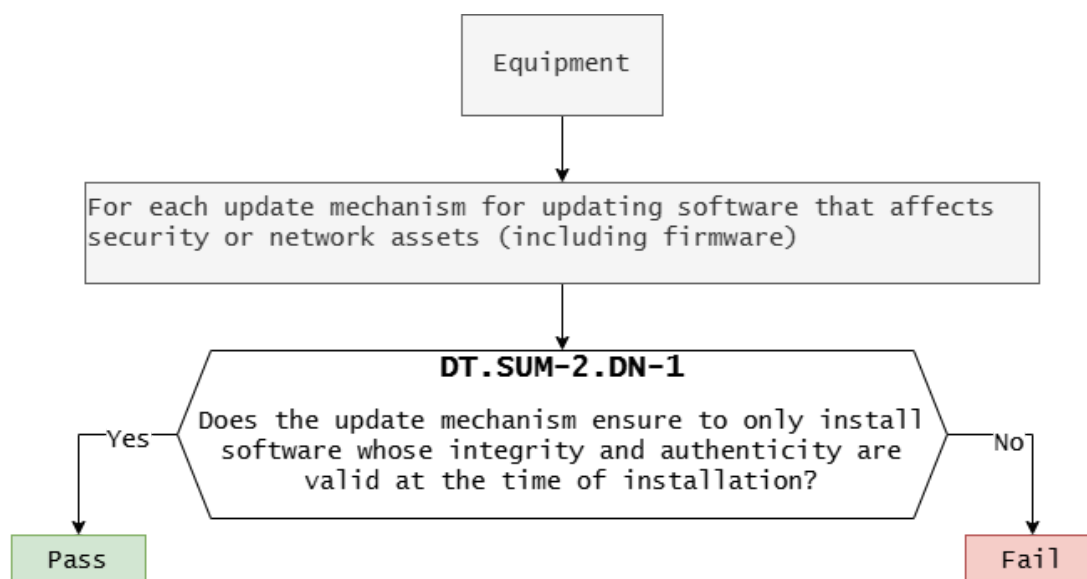


Figure 12 — Decision Tree for requirement SUM-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SUM-2)
SUMA-A	DT.SUM-2.DN-1	Yes	The software includes a verification mechanism to ensure its integrity.

Verdict: PASS

【SUM-2 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.

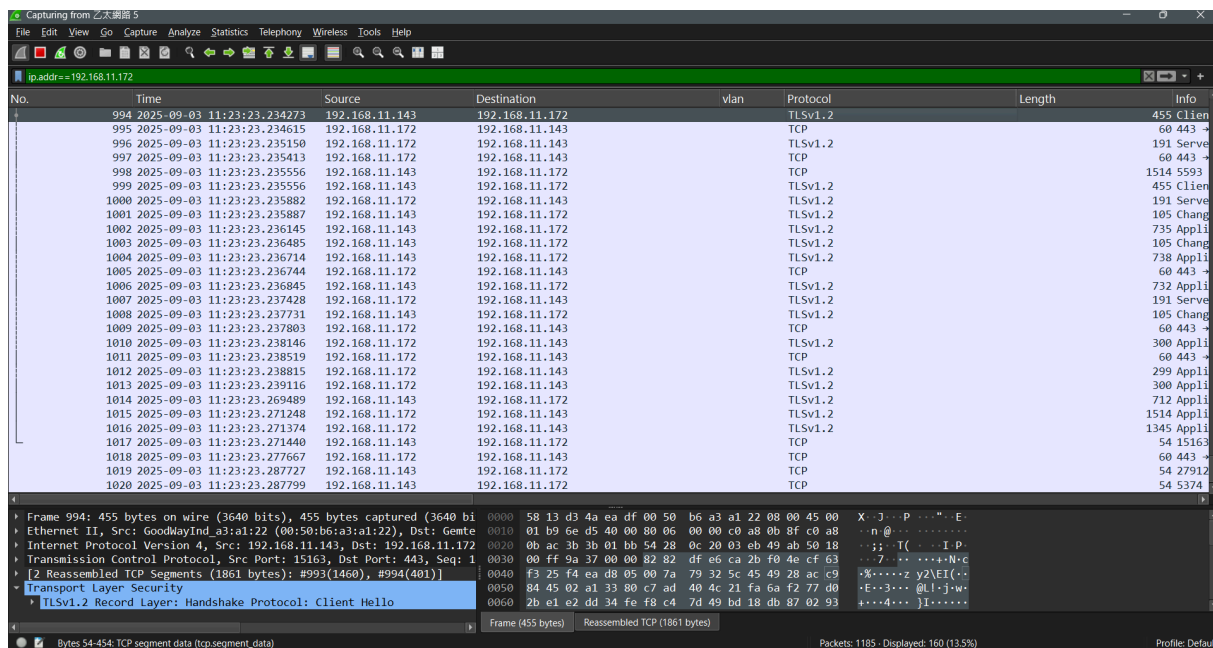
Verdict : NOT NECESSARY

【SUM-2 Functional sufficiency assessment】

Asset No.	Implemented
SUMA-A	Y

Verdict: PASS

【Supporting Evidence】



The screenshot displays a Wireshark capture of network traffic. The packet list on the left shows a series of packets, with packet 994 being a TLSv1.2 Client Hello. The packet details pane on the right shows the structure of the Client Hello message, including the 'Handshake Protocol' and 'Client Hello' fields. The packet bytes pane at the bottom shows the raw data of the message.



Firmware Information

Current firmware version: opdk-1.01.91

Please select a file to upgrade: 未選擇任何檔案

Invalid firmware file

SUM-2 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

[SUM-3] Automated updates

【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.



【SUM-3 Conceptual assessment】

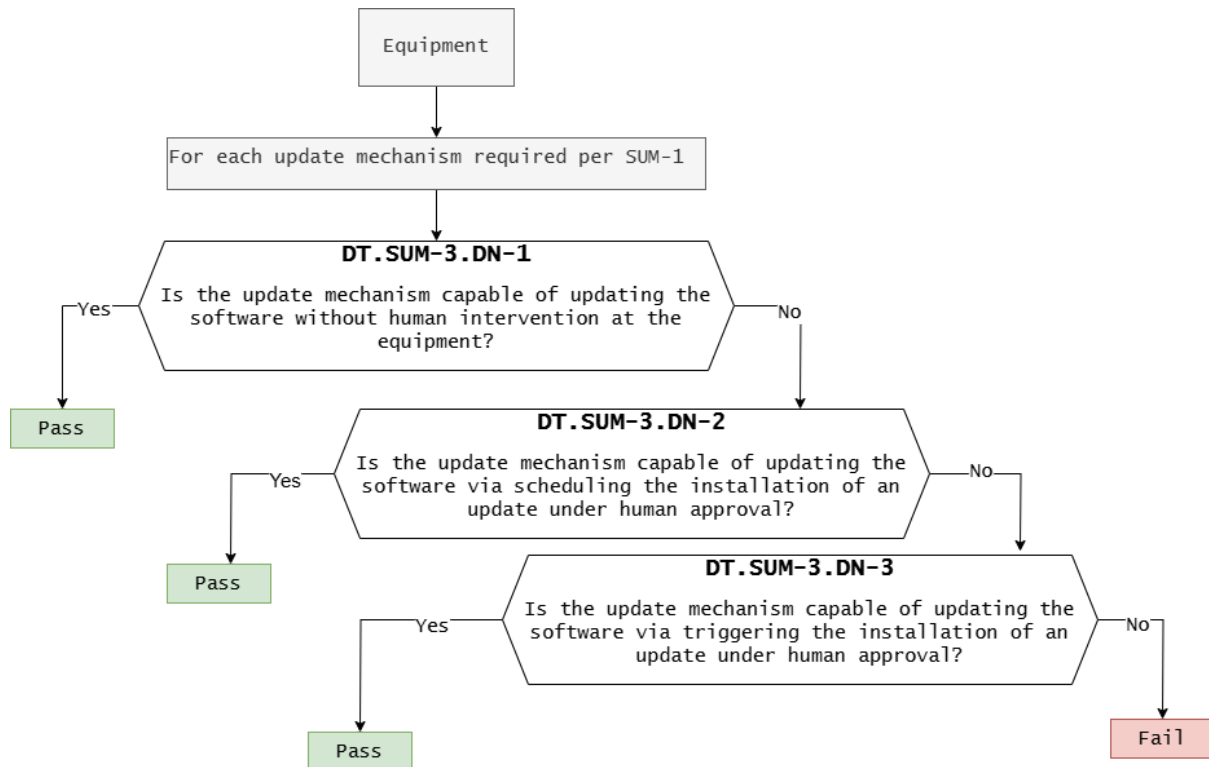


Figure 13 — Decision Tree for requirement SUM-3

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SUM-3)
SUMA-A	DT.SUM-3.DN-1	No	The device supports online automatic updates
	DT.SUM-3.DN-2	No	The device supports scheduled updates.
	DT.SUM-3.DN-3	Yes	The device supports manual update installation

Verdict: PASS



【SUM-3 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.

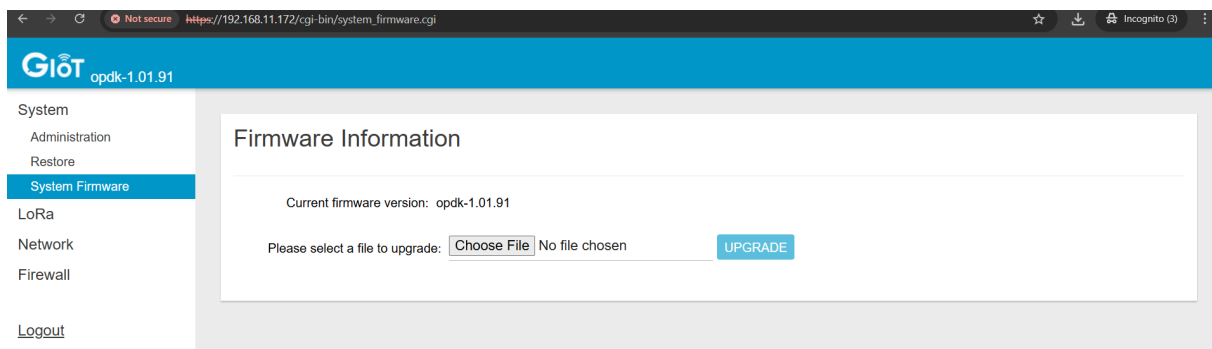
Verdict: NOT NECESSARY

【SUM-3 Functional sufficiency assessment】

Asset No.	Implemented
SUMA-A	Y

Verdict: PASS

【Supporting Evidence】



SUM-3 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

4.4 [SSM] Secure storage mechanism

[SSM-1] Applicability of secure storage mechanisms

【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.

【SSM-1 Assets】

Asset No.	Asset	Type	Store Mechanism
SSMA-A	TLS private key and certificate	Security	Web GUI
SSMA-B	SSH Key	Security	Web GUI
SSMA-C	Web login password	Security	Web GUI



【SSM-1 Conceptual assessment】

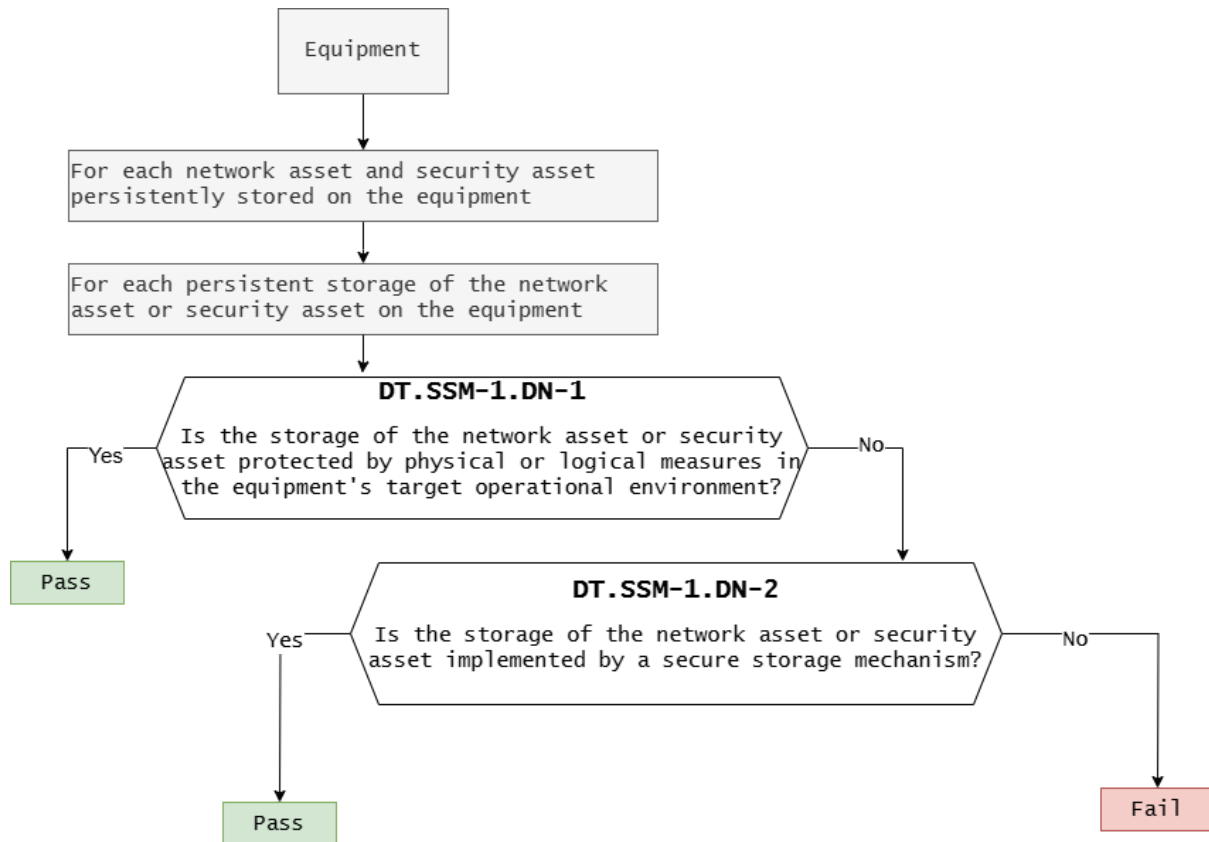


Figure 14 — Decision Tree for requirement SSM-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SSM-1)
SSMA-A	DT.SSM-1.DN-1	No	No logical or physical protection measures are present in the DUT.
SSMA-B	DT.SSM-1.DN-2	Yes	Assets are stored within SSH and are accessible only with administrator privileges.
SSMA-C			

Verdict: PASS



【SSM-1 Functional completeness assessment】

Asset No.	Document Verification
SSMA-A	Y
SSMA-B	Y
SSMA-C	Y

Verdict: PASS

【SSM-1 Functional sufficiency assessment】

Asset No.	Implemented
SSMA-A	Y
SSMA-B	Y
SSMA-C	Y

Verdict: PASS

【Supporting Evidence】

Using PBKDF2 encryption

```
root@OutdoorAP:~# cat /etc/shadow
root:$6$KdtyYHpr$bzHf.gIUxN89w4pEhkLuNsR3DvxDJgVCNG3nSEWtnEIuAKF4up5KpSqHsskJWI9ughQfA5ICESFBYx9fsB8Iv0:20334:0:99999:7:::
daemon*:16273:0:99999:7:::
bin*:16273:0:99999:7:::
sys*:16273:0:99999:7:::
sync*:16273:0:99999:7:::
games*:16273:0:99999:7:::
man*:16273:0:99999:7:::
lp*:16273:0:99999:7:::
mail*:16273:0:99999:7:::
news*:16273:0:99999:7:::
uucp*:16273:0:99999:7:::
proxy*:16273:0:99999:7:::
www-data*:16273:0:99999:7:::
backup*:16273:0:99999:7:::
list*:16273:0:99999:7:::
irc*:16273:0:99999:7:::
gnats*:16273:0:99999:7:::
nobody*:16273:0:99999:7:::
libuuid!:16273:0:99999:7:::
syslog*:16273:0:99999:7:::
sshd*:16412:0:99999:7:::
mysql!:16450:0:99999:7:::
dhcpcd*:16465:0:99999:7:::
ntp*:16758:0:99999:7:::
root@OutdoorAP:~#
```



```
root@OutdoorAP:~# cat /etc/ssh/ssh_host_ed25519_key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACAip/8brCoBle0L4RI4x/zAxEYLhTnNSzb5zbb+d0F1QwAAAjhsTxvfbE8b
3wAAAAtzc2gtZWQyNTUxOQAAACAip/8brCoBle0L4RI4x/zAxEYLhTnNSzb5zbb+d0F1Qw
AAAECPeCY9itFyQqqDfQTdEWMBpBpuQ0NIGEsfopwy43PjiSKn/xusKgHV7QvhEjjH/MDE
RguF0c1LNvnNtv53QXVDAADnJvb3RAT3V0ZG9vcKFAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
```

```
root@OutdoorAP:~# cat /etc/lighttpd/certs/lighttpd.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmQ0d/xY2YXW0U0+hIDqpEv4LHB0IY6swj dkkpMT2AuCTArW9
YGOaZS0WokU4May4wg5EGkVZfBB0K0bTbDhG1wAvmUjdPnDpVHZkFQX5j3bzI1pv
w3j7M4bq2DeyQDnI/5nIFIJEfE0S2EMgyQYSHvN0K7Q2UwzP/VB6+LLKpFpYUj+I
QKGWSRgvPvilsQib5X+ZnqG6PIXZXUQuEKpkX+iRVBtKHZk1e8yl6EJ/KR04uXj3
z6L5GHAD8f2Ea6dV+FVyBIbiy9Mv6HeMwEEaDrs7vcVetSRj27Ysh0ImgZLZ3hh4
YZGNfwx3wv0Iznwjt+xUjVNWoEamQ04HD30WRQIDAQABAoIBAHPJ3bC3cErJTTrKQ
p9iHKJRqx6LsQAWPZLtb1QIm1GuW1QG01wf0Mudqdh4rufiy0FBXlKQ/ZRScDVdm
TnsptBXXGSuhWWg86fl2Mzg2ffhQqF9NsxIy0/Fel9seP+ehD/R3tkv1xbQxNy4P
kwUiZ6Es0+2geBuf87aUJYRzVyWA3Iav8qLlsuokX0ZIRLeKz1/04Lx0uxu8I+MW
fdoSHrn+ubkprnWb0M3w3Ro8ZMshq0lxaDANCK3wkk0XpmK1pjZexQSFwzRkdcWz
epHtoWpirsbi4M0YZhyPQ7UUZ9i0/cS9tf79WE0bSLRnl1KVdI3Mw/x4lQIc2UBh
lv3PaaECgYEAy0HyL0pHW600C5tiNyiGUk08/hTE+Q7Jwr4X0nQSmqz3tQqFMwzm
qP+VEeJka7F27pysTsZ4rB9pGDlqABkKxV0k0d6yvLvHWh/R9n3MzzQoQwbdKim
I0F/P1iQDBnQ9mH+KVS7FN8fiZfLUD84qNoQGrkR2l8GAL1Lo89FGk0CgYEAwMQM
b/XQJ2iWSGCgp7EMVpUVXo8ApZAmhqNAE6IBEWaUNlcwft/+oJ2v5x1o0BrLzw5V
JQGb7xUDi1lWqIbPtU16tRITa288GKldD6gQWojrvD/hzit+QjYkPyCheQK9kxs
NGoVqxSWM4nxntCN5GsDFKG4T3MayExGSzFwd9kCgYAs6JUdp1ns1W6iYeKbWLA
LHCdctLSbgIGFRo0VbcGldDlHz3u2ZrdHBtDqFGnub4dWl0Ei5pci8I233HefLeL
DUAepAZtcN+ED+KpBYlAuN8fth0a2WhbwcZrohWxlsKkrWIKn732DpZZQECbqlxK
cm08g8d+CCC7aRedSd5qwQKBgQC7mpGYLR3GHM2V5ySzz2V4pmNDwd0ZRK+Z/SuR
b+umKbU5JaX1X+DKJG1beo3Vax7LhuFqwKP5+Km9moS3rmjhxibIqo2Tu/DT6s2n
0oNY5pmP2tB1o739TpSmlnlz6cqZZksWv8YS2Fh0FIRO0gQmN9eprrKX8Cgyo7kN
2THiEQKBgQC6UunmxljLIbeHb91hYgR1tsuZW2VHN0N2xSGYDoEQ6RIXghooe0cf
iP6ZSgf9XmToBG6qFzgr/03my6JEXt+S0+LRPn2Ji47DLCb+aLLqu2fvq0BEW0Uu
60j9z/Ia380Y/y0ZeKBffQklqKU3lBtGUYSKVDfhdabf5/cnh3SQEQ==
-----END RSA PRIVATE KEY-----
```

SSM-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

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

【Requirement】

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

【SSM-2 Conceptual assessment】

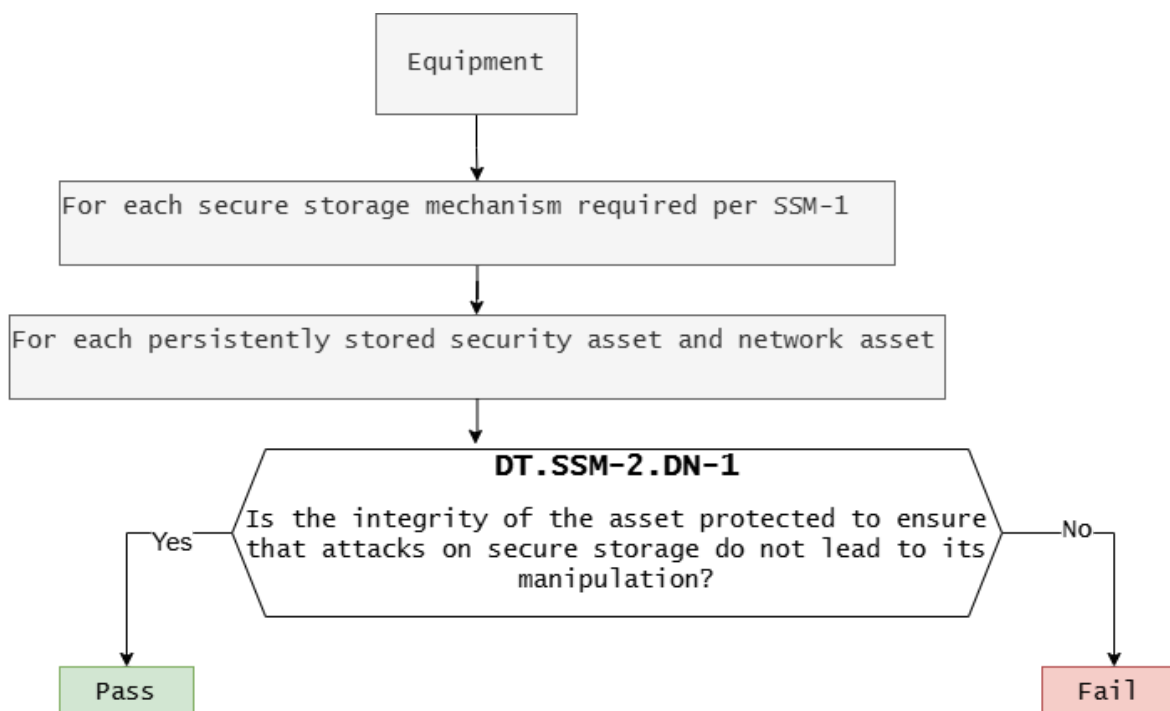


Figure 15 — Decision Tree for requirement SSM-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SSM-2)
SSMA-A SSMA-B SSMA-C	DT.SSM-2.DN-1	Yes	Assets are stored in SSH and access is restricted to administrator privileges.



Verdict: PASS

【SSM-2 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.

Verdict : NOT NECESSARY

【SSM-2 Functional sufficiency assessment】

Asset No.	Implemented
SSMA-A	Y
SSMA-B	Y
SSMA-C	Y

Verdict: PASS

【Supporting Evidence】

Follow SSM-1

SSM-2 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

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

【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.

【SSM-3 Conceptual assessment】

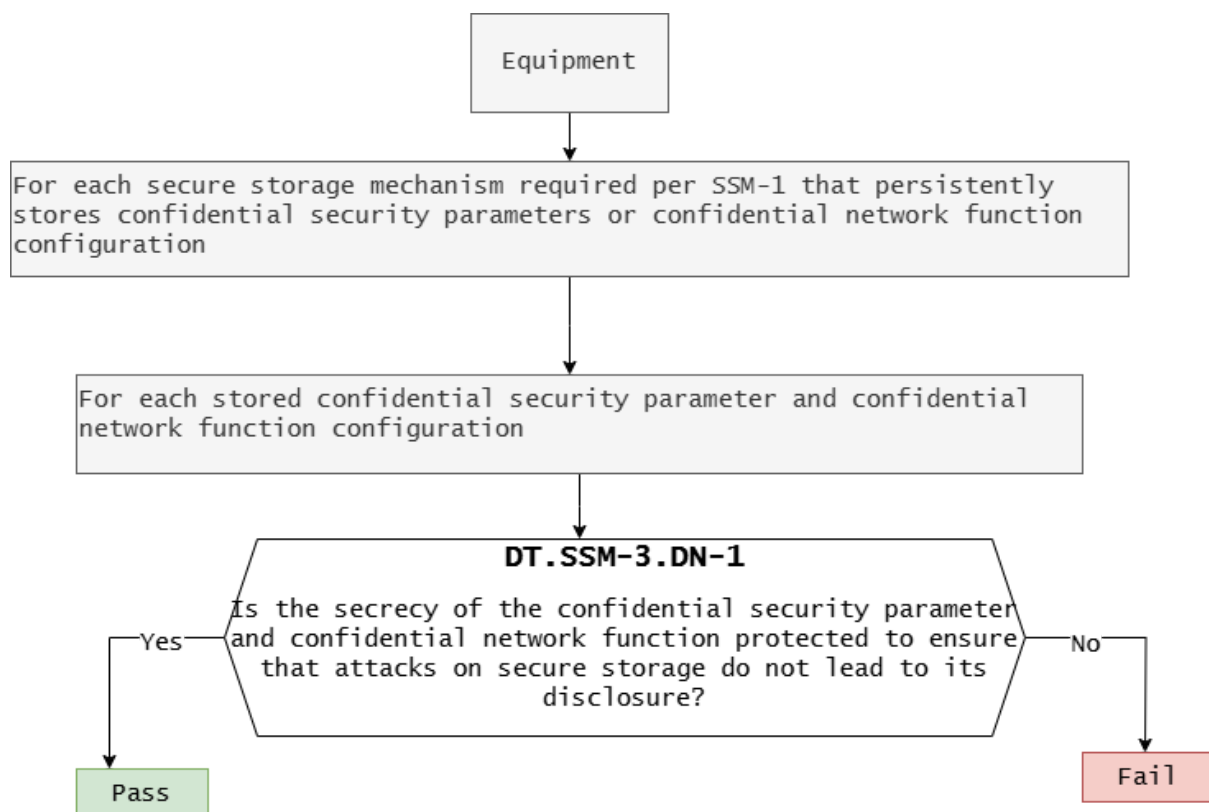


Figure 16 — Decision Tree for requirement SSM-3

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SSM-3)
SSMA-A SSMA-B SSMA-C	DT.SSM-3.DN-1	Yes	Assets are stored within SSH and are accessible only with administrator privileges.

Verdict: PASS

【SSM-3 Functional completeness assessment】

Asset No.	Document Verification
SSMA-A	Y
SSMA-B	Y
SSMA-C	Y

Verdict: PASS

【SSM-3 Functional sufficiency assessment】

Asset No.	Implemented
SSMA-A	Y
SSMA-B	Y
SSMA-C	Y

Verdict: PASS

【Supporting Evidence】

Follow SSM-1



SSM-3 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

4.5 [SCM] Secure communication mechanism

【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 unauthorized 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.

【SCM-1 Assets】

Asset No.	Asset	Type	Connect Mechanism
SCMA-A	Ethernet	Network	Network interface

【SCM-1 Conceptual assessment】

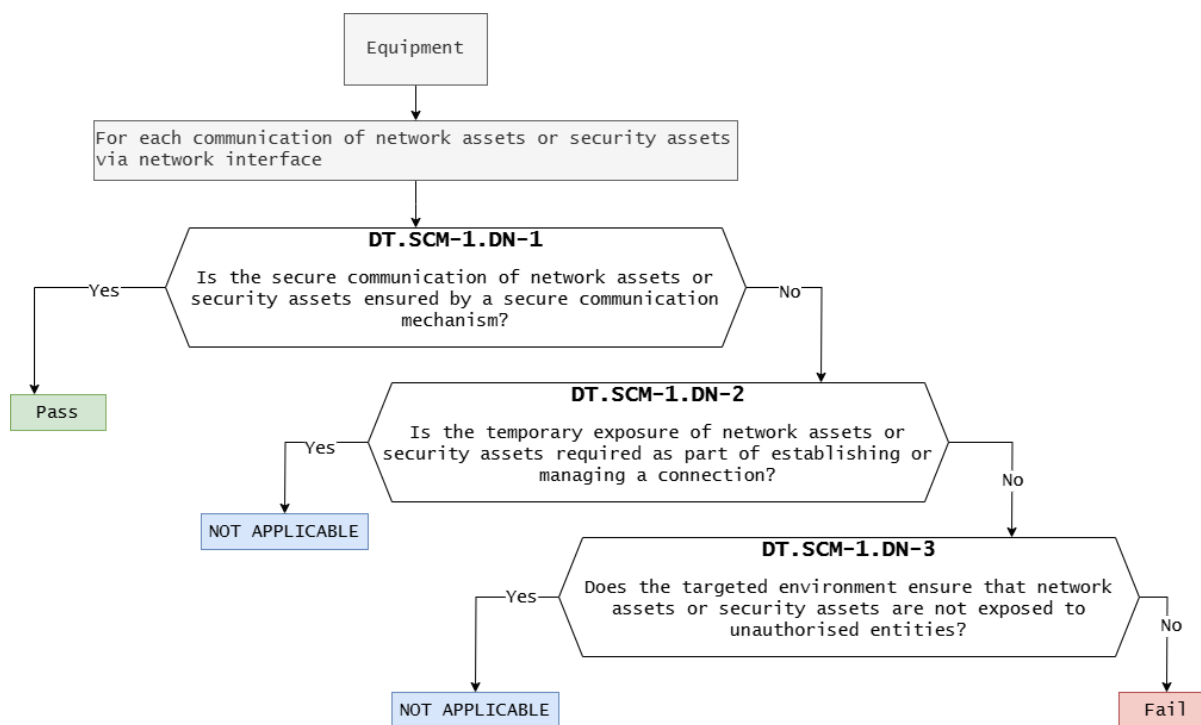


Figure 17 — Decision Tree for requirement SCM-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SCM-1)
SCMA-A	DT.SCM-1.DN-1	Yes	Measurement data transmission is protected through TLS 1.2 encryption.
	DT.SCM-1.DN-2	-	-
	DT.SCM-1.DN-3	-	-

Verdict: PASS



【SCM-1 Functional completeness assessment】

Asset No.	Document Verification
SCMA-A	Y

Verdict : PASS

【SCM-1 Functional sufficiency assessment】

Asset No.	Implemented
SCMA-A	Y

Verdict : PASS

【Supporting Evidence】

The screenshot displays a Wireshark packet capture from interface 乙次網路 5. The filter is set to ip.addr==192.168.11.172. The packet list shows a series of connections between 192.168.11.143 and 192.168.11.172, primarily using SSHv2 and TCP. The selected packet (Frame 994) is a Transport Layer Security (TLS) record layer handshake protocol client hello, 455 bytes captured. The packet details pane shows the following structure:

- Frame 994: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bits) on interface 乙次網路 5
- Ethernet II, Src: GoodWayInd_a3:a1:22 (00:50:b6:a3:a1:22), Dst: Gemte (08:00:27:00:00:00)
- Internet Protocol Version 4, Src: 192.168.11.143, Dst: 192.168.11.172
- Transmission Control Protocol, Src Port: 15163, Dst Port: 443, Seq: 1
- [2 Reassembled TCP Segments (1861 bytes): #993(1460), #994(401)]
- Transport Layer Security
- TLSv1.2 Record Layer: Handshake Protocol: Client Hello

The packet bytes pane shows the raw data of the client hello message, including the magic number 0x03030303 and the handshake protocol structure.



SCM-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

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

【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.



【SCM-2 Conceptual assessment】

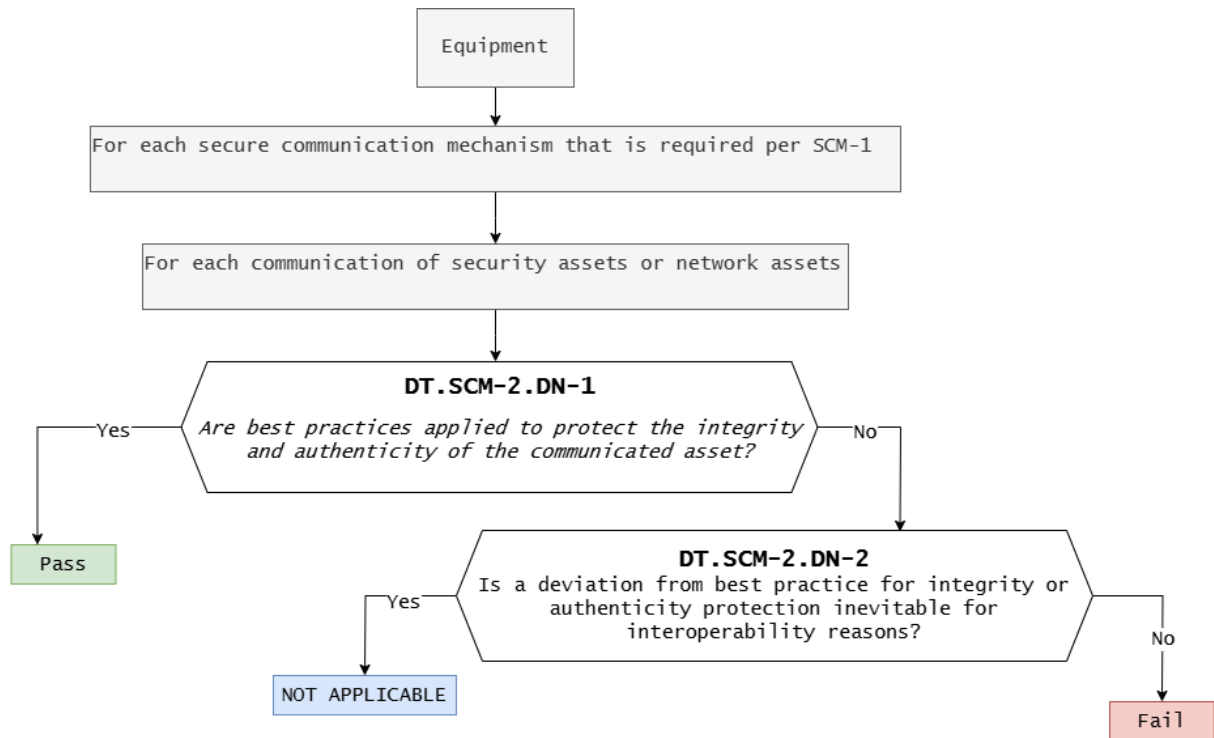


Figure 18 — Decision Tree for requirement SCM-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SCM-2)
SCMA-A	DT.SCM-2.DN-1	Yes	Measurement data transmission is protected through TLS 1.2 encryption.
	DT.SCM-2.DN-2	-	-

Verdict: PASS

【SCM-2 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.

Verdict : NOT NECESSARY

【SCM-2 Functional sufficiency assessment】

Asset No.	Implemented
SCMA-A	Y

Verdict : PASS

【Supporting Evidence】

Follow SCM-1

SCM-2 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

【SCM-3】Appropriate confidentiality protection for secure communication mechanisms

【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.

【SCM-3 Conceptual assessment】

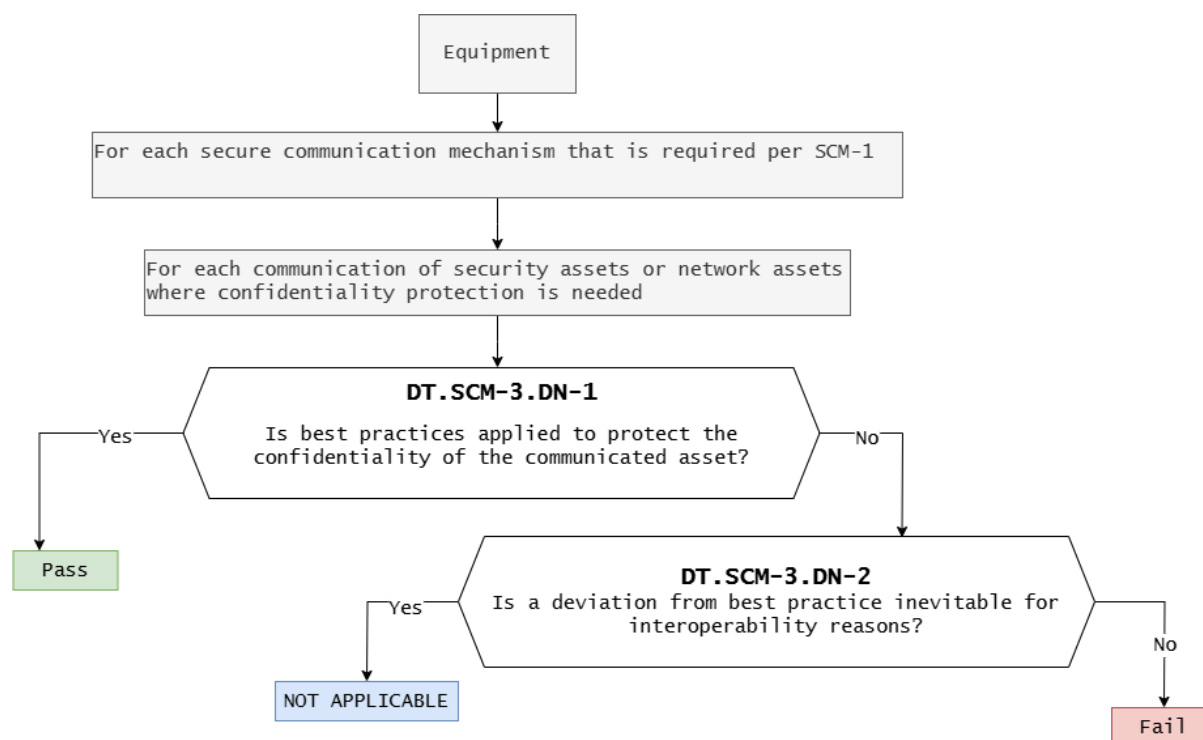


Figure 19 — Decision Tree for requirement SCM-3

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SCM-3)
SCMA-A	DT.SCM-3.DN-1	Yes	Measurement data transmission is protected through TLS 1.2 encryption.
	DT.SCM-3.DN-2	-	-

Verdict: PASS

【SCM-3 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.

Verdict: NOT NECESSARY

【SCM-3 Functional sufficiency assessment】

Asset No.	Implemented
SCMA-A	Y

Verdict : PASS

【Supporting Evidence】

Follow SCM-1

SCM-3 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

【SCM-4】 Appropriate replay protection for secure communication mechanisms

【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.

【SCM-4 Assets】

Asset No.	Asset	Type	Connect Mechanism
SCMA-B	Web GUI login	Network	Web GUI

【SCM-4 Conceptual assessment】

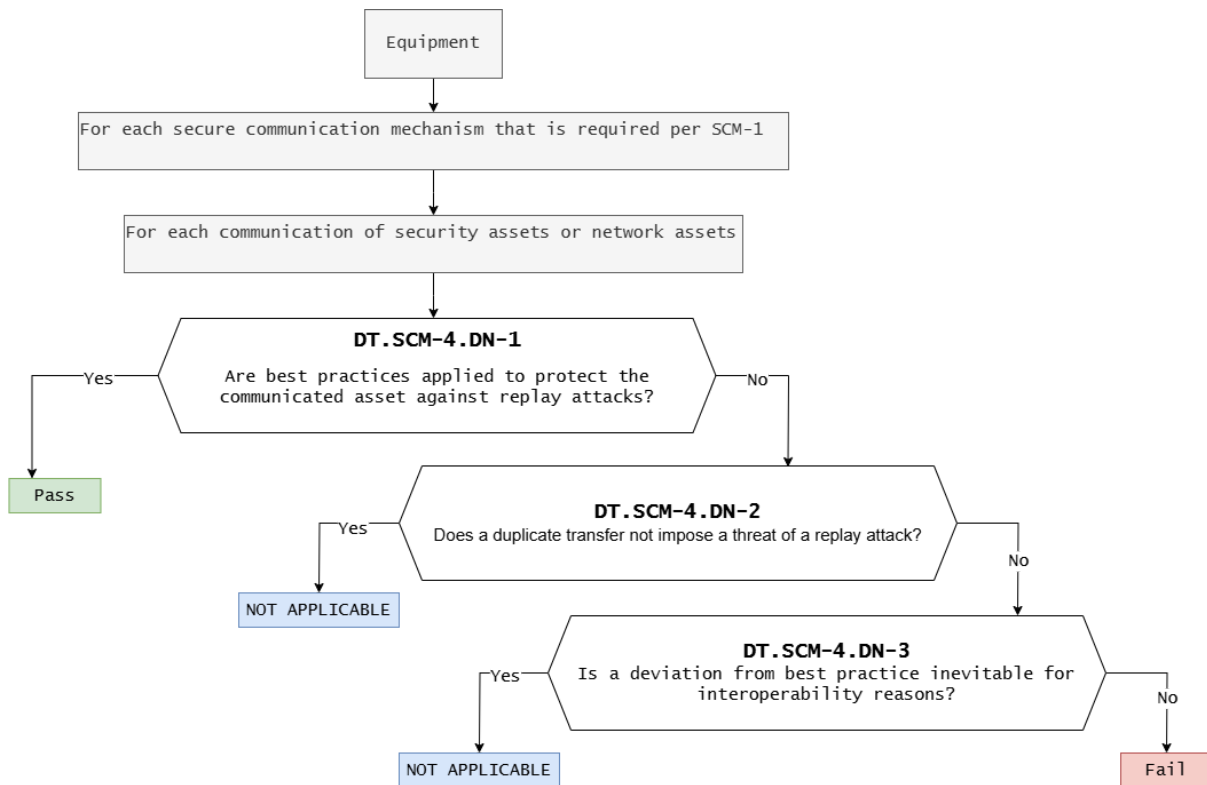


Figure 20 — Decision Tree for requirement SCM-4

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.SCM-4)
SCMA-B	DT.SCM-4.DN-1	Yes	Randomized access attempts result in 400/401/403 unauthorized access responses, with variable response lengths..
	DT.SCM-4.DN-2	-	-
	DT.SCM-4.DN-3	-	-

Verdict: PASS
【SCM-4 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.

Verdict: NOT NECESSARY
【SCM-4 Functional sufficiency assessment】

Asset No.	Implemented
SCMA-B	Y

Verdict : PASS

【Supporting Evidence】

replay attack test

```
C:\Windows\System32\cmd.exe x + v
C:\Users\Joey\AppData\Local\Programs\Python\Python39\lib\site-packages\urllib3\connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.11.172'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
warnings.warn(
[6] 狀態碼: 403 | 回應: Unauthorized access attempt.
..... | 回應長度: 64 | 導向: None
C:\Users\Joey\AppData\Local\Programs\Python\Python39\lib\site-packages\urllib3\connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.11.172'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
warnings.warn(
[7] 狀態碼: 401 | 回應: Unauthorized access attempt.
..... | 回應長度: 53 | 導向: None
C:\Users\Joey\AppData\Local\Programs\Python\Python39\lib\site-packages\urllib3\connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.11.172'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
warnings.warn(
[8] 狀態碼: 401 | 回應: Unauthorized access attempt.
..... | 回應長度: 39 | 導向: None
C:\Users\Joey\AppData\Local\Programs\Python\Python39\lib\site-packages\urllib3\connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.11.172'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
warnings.warn(
[9] 狀態碼: 403 | 回應: Unauthorized access attempt.
..... | 回應長度: 66 | 導向: None
C:\Users\Joey\AppData\Local\Programs\Python\Python39\lib\site-packages\urllib3\connectionpool.py:1064: InsecureRequestWarning: Unverified HTTPS request is being made to host '192.168.11.172'. Adding certificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/1.26.x/advanced-usage.html#ssl-warnings
warnings.warn(
[10] 狀態碼: 400 | 回應: Unauthorized access attempt.
..... | 回應長度: 88 | 導向: None
```

SCM-4 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

4.6 [RLM] Resilience mechanism

[RLM-1] Applicability and appropriateness of resilience mechanisms

【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.

【RLM-1 Assets】

Asset No.	Asset	Type	Connect Mechanism
RLMA-A	Ethernet	Network	Network interface

【RLM-1 Conceptual assessment】

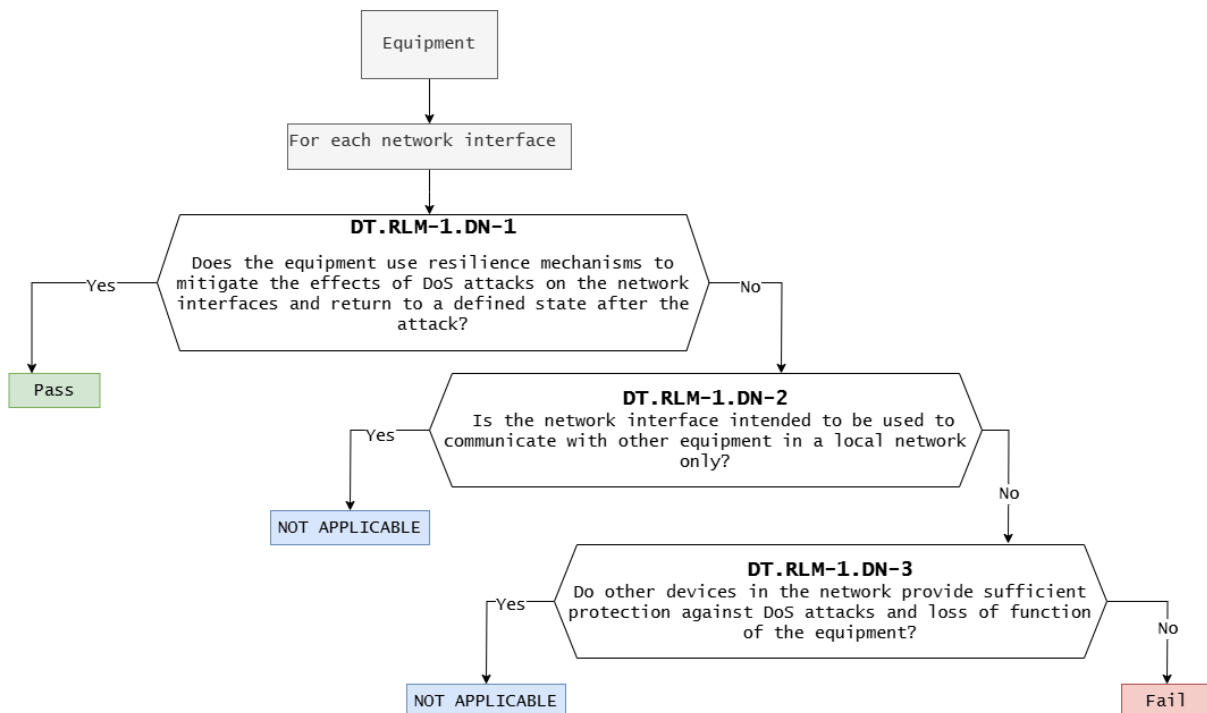


Figure 21 — Decision Tree for requirement RLM-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.RLM-1)
RLMA-A	DT.RLM-1.DN-1	Yes	There is a recovery mechanism, and the log will record logs (DROP SYN FLOOD or DROP TCP PORT 0 tag).
	DT.RLM-1.DN-2	-	-
	DT.RLM-1.DN-3	-	-

Verdict: PASS
【RLM-1 Functional completeness assessment】

Asset No.	Document Verification
RLMA-A	Y
RLMA-B	Y

Verdict : PASS
【RLM-1 Functional sufficiency assessment】

Asset No.	Implemented
RLMA-A	Y

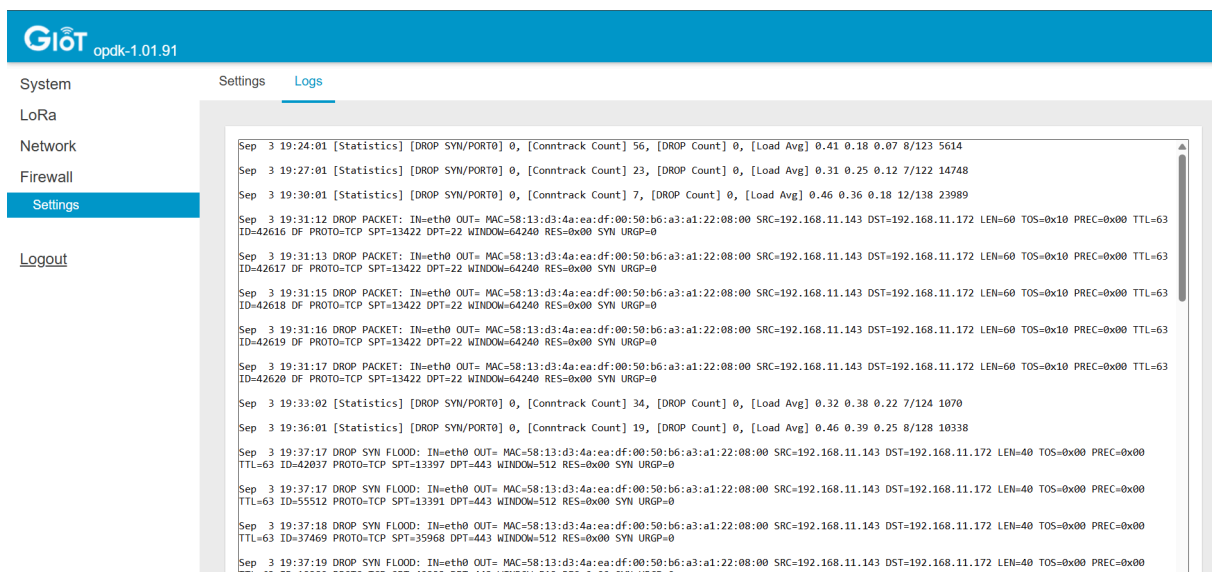
Verdict : PASS



【Supporting Evidence】

```
root@Joey-T480:~# hping3 -S -p 443 --flood 192.168.11.172
HPING 192.168.11.172 (eth0 192.168.11.172): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

```
Reply from 192.168.11.172: bytes=32 time=2ms TTL=64
Reply from 192.168.11.172: bytes=32 time<1ms TTL=64
Reply from 192.168.11.172: bytes=32 time=1ms TTL=64
Reply from 192.168.11.172: bytes=32 time=1ms TTL=64
Reply from 192.168.11.172: bytes=32 time=7ms TTL=64
Reply from 192.168.11.172: bytes=32 time=1ms TTL=64
Reply from 192.168.11.172: bytes=32 time=1ms TTL=64
Reply from 192.168.11.172: bytes=32 time=35ms TTL=64
Reply from 192.168.11.172: bytes=32 time=28ms TTL=64
Reply from 192.168.11.172: bytes=32 time=14ms TTL=64
Reply from 192.168.11.172: bytes=32 time=21ms TTL=64
Reply from 192.168.11.172: bytes=32 time=36ms TTL=64
Reply from 192.168.11.172: bytes=32 time=8ms TTL=64
Reply from 192.168.11.172: bytes=32 time=350ms TTL=64
Reply from 192.168.11.172: bytes=32 time=226ms TTL=64
Reply from 192.168.11.172: bytes=32 time=1ms TTL=64
Reply from 192.168.11.172: bytes=32 time=13ms TTL=64
Reply from 192.168.11.172: bytes=32 time=55ms TTL=64
Reply from 192.168.11.172: bytes=32 time=51ms TTL=64
```



RLM-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

4.7 [NMM] Network monitoring mechanism

[NMM-1] Applicability and appropriateness of network monitoring mechanisms

【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.

【NMM-1 Assets】

Asset No.	Asset	Type	Connect Mechanism
NMMA-A	Web GUI	Network	Network interface

【NMM-1 Conceptual assessment】

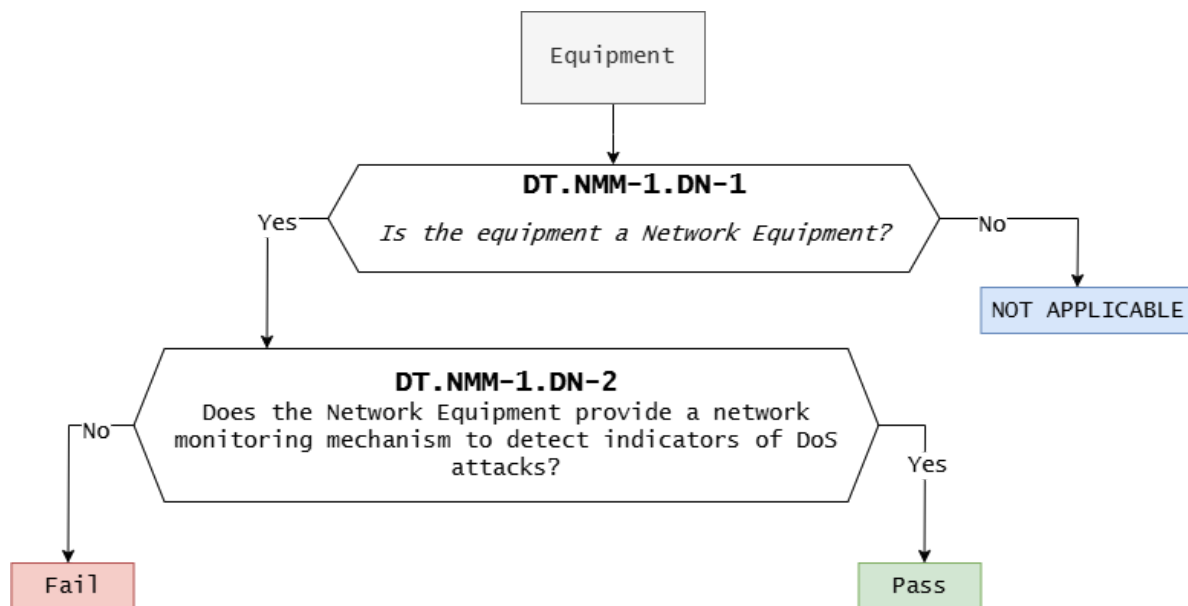


Figure 22 — Decision Tree for requirement NMM-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.NMM-1)
----------	---------------	----------	------------------------------------

NMMA-A	DT.NMM-1.DN-1	Yes	DUT is network equipment
	DT.NMM-1.DN-2	Yes	A network monitoring mechanism is implemented in the system.

Verdict: PASS

【NMM-1 Functional completeness assessment】

Functional completeness assessment is Not Necessary in this clause since the network monitoring mechanism is always mandatory for network equipment.

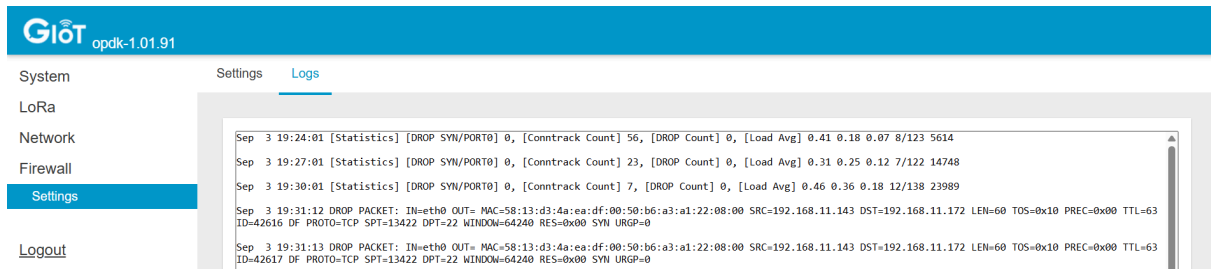
Verdict : NOT NECESSARY

【NMM-1 Functional sufficiency assessment】

Asset No.	Document Verification
NMMA-A	Y

Verdict : PASS

【Supporting Evidence】



NMM-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	NOT NECESSARY
Functional sufficiency assessment	PASS

4.8 [TCM] Traffic control mechanism

[TCM-1] Applicability of and appropriate traffic control mechanisms

【Requirement】

If the equipment is a network equipment, the equipment shall provide network traffic control mechanism(s).

【TCM-1 Assets】

Asset No.	Asset	Type	Connect Mechanism
TCMA-A	Web GUI	Network	Network interface



【TCM-1 Conceptual assessment】

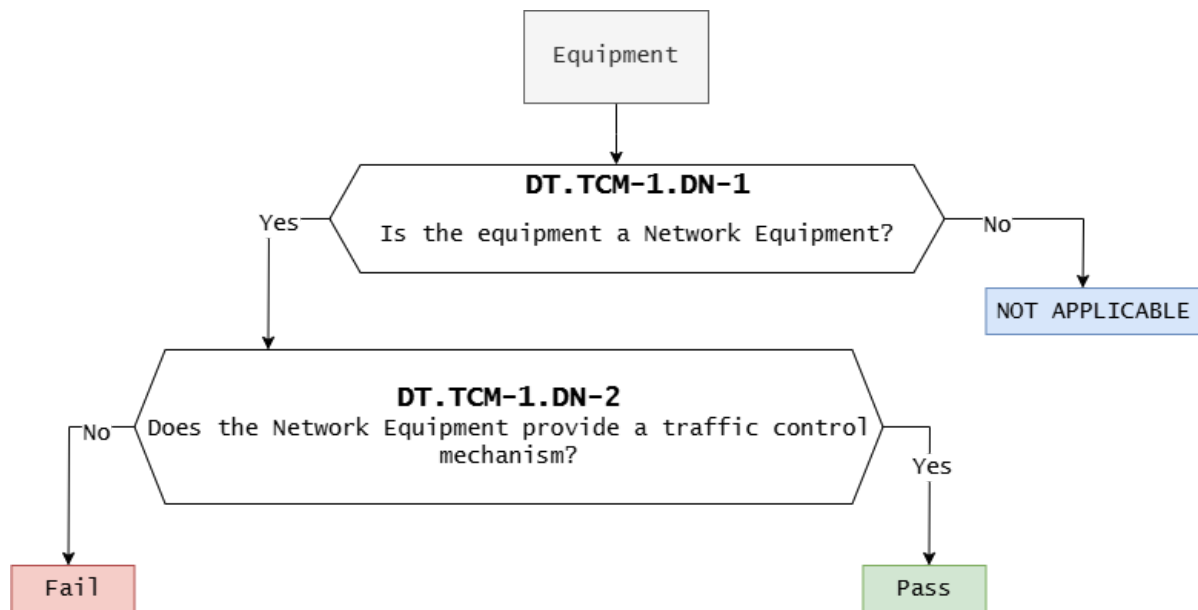


Figure 23 — Decision Tree for requirement TCM-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.TCM-1)
TCMA-A	DT.TCM-1.DN-1	Yes	DUT is network equipment
	DT.TCM-1.DN-2	Yes	A traffic control mechanism is implemented in the DUT.

Verdict : PASS

【TCM-1 Functional completeness assessment】

Functional completeness assessment is Not Necessary in this clause since the traffic control mechanism is always mandatory for network equipment.

Verdict : NOT NECESSARY



【TCM-1 Functional sufficiency assessment】

Asset No.	Document Verification
TCMA-A	Y

Verdict : PASS

【Supporting Evidence】

Statistics on the number of connections to the current system every 3 minutes.

```
Sep 3 19:24:01 [Statistics] [DROP SYN/PORT0] 0, [Conntrack Count] 56, [DROP Count] 0, [Load Avg] 0.41 0.18 0.07 8/123 5614
Sep 3 19:27:01 [Statistics] [DROP SYN/PORT0] 0, [Conntrack Count] 23, [DROP Count] 0, [Load Avg] 0.31 0.25 0.12 7/122 14748
Sep 3 19:30:01 [Statistics] [DROP SYN/PORT0] 0, [Conntrack Count] 7, [DROP Count] 0, [Load Avg] 0.46 0.36 0.18 12/138 23989
```

TCM-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

4.9 [CCK] Confidential cryptographic keys

[CCK-1] Appropriate CCKs

【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 can impose one single option for cryptographic algorithms and their respective keys.

【CCK-1 Assets】

Asset No.	Asset	Type
CCKA-A	SSH key	Security
CCKA-B	TLS key	Security



【CCK-1 Conceptual assessment】

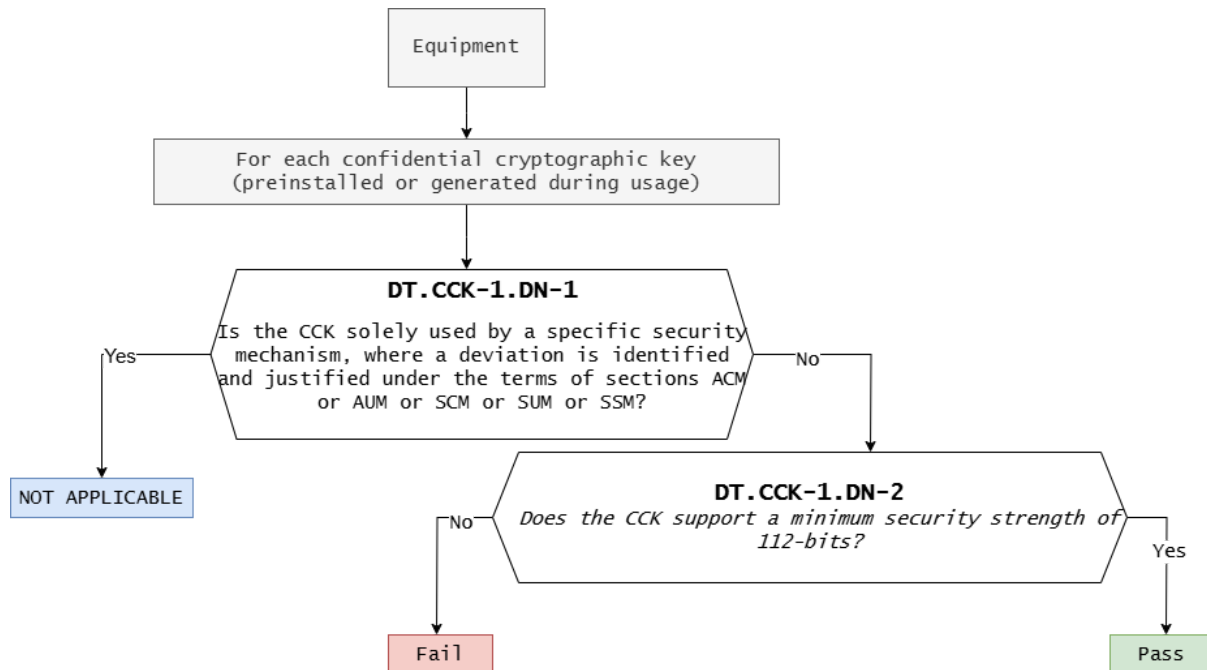


Figure 24 — Decision Tree for requirement CCK-1

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.TCM-1)
CCKA-A	DT.CCK-1.DN-1	No	Not used in specific security mechanisms
CCKA-B	DT.CCK-1.DN-2	Yes	TLS key: RSA 2048,112bits SSH key: Ed25519,128bits

Verdict : PASS

【CCK-1 Functional completeness assessment】

Asset No.	Document Verification
CCKA-A	Y
CCKA-B	Y

Verdict : PASS

【CCK-1 Functional sufficiency assessment】

Asset No.	Implemented
CCKA-A	Y
CCKA-B	Y

Verdict : PASS

【Supporting Evidence】

TLS Key:

/etc/lighttpd/certs/lighttpd.pem



```
root@OutdoorAP:~# cat /etc/lighttpd/certs/lighttpd.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA mQ0d/xY2YXW0U0+hIDqpEv4LHB0IY6swj dkkpMT2AuCTArW9
YG0aZS0WokU4May4wg5EGkVZfBB0K0bTbDhG1wAvmUj dPnDpVHzKFQX5j3bzI1pv
w3j7M4bq2DeyQDnI/5nIFIJEfE0S2EMgyQYSHvN0K7Q2UWzP/VB6+LLKpFpYUj+I
QKGWSRgvPvilsQib5X+ZnqG6PIXZXUQuEKpkX+iRVBtKHZk1e8yl6EJ/KR04uXj3
z6L5GHad8f2Ea6dV+FVyBIbiy9Mv6HeMwEEaDrs7vcVetSRj27Ysh0ImgZLZ3hh4
YZGNfwx3wv0Iznwjt+xUjVNWoEamQ04HD30WRQIDAQABAoIBAHPJ3bC3cErJTrKQ
p9iHKJRqx6LsQAWPZLtb1QIm1GuW1QG01wf0Mudqdh4rufiy0FBXlKQ/ZRScDVdm
TNsptBXXGSuhWWg86fl2Mzg2ffhQqF9NsxIy0/Fel9seP+ehD/R3tkv1xbQxNy4P
kwUiZ6Es0+2geBuf87aUJYRzVyWA3Iav8qLlsuokX0ZIRLeKz1/04Lx0uxu8I+MW
fdoSHrn+ubkprnWb0M3w3Ro8ZMshq0lxaDANCK3wkk0XpmK1pjZexQSFwzRkdcWz
epHtoWpirsbi4M0YZhyPQ7UUZ9i0/cS9tf79WE0bSLRnl1KVdI3Mw/x4lQIc2UBh
lv3PaaECgYEAY0HyL0pHW600C5tiNyiGUk08/hTE+Q7Jwr4X0nQSmqz3tQqFMwzm
qP+VEeJka7F27pycsTsZ4rB9pGDlqABkKxV0k0d6yvLvHWh/R9n3MzzQoQwbdKim
I0F/P1iQDBnQ9mH+KVS7FN8fiZfLUD84qNoQGrkR2l8GAL1Lo89FGk0CgYEAwMQM
b/XQJ2iWSGCgp7EMVpUVXo8ApZAmhqNAE6IBEWaUNlcwFT/+oJ2v5x1o0BrLzw5V
JQGbV7xUDi1lWqIbPtU16tRITa288GKldD6gQWojrvD/hzit+QjYkPyCheQK9kxs
NGoVqxSWM4nxntCN5GsDFKG4T3MayExGSzFwd9kCgYAs6JUplns1W6iYeKBbWLA
LHCdctlSbgIGFRo0VbcGldDlHz3u2ZrdHBtDqFGnub4dWl0Ei5pci8I233HefLe1
DUAepAZtcN+ED+KPbYlAuN8fth0a2WhbwcZrohWxlsKkrWIKn732DpZZQECbqlxK
cm08g8d+CCC7aRedSd5qwQKBgQC7mpGYLR3GHM2V5ySzz2V4pmNDwd0ZRK+Z/SuR
b+umKbU5JaX1X+DKJG1beo3Vax7LhuFqwKP5+Km9moS3rmjhxibIQo2Tu/DT6s2n
0oNY5pmP2tB1o739TpSmlnlz6cqZZksWv8YS2Fh0FIRo0gQmN9eprKX8Cgyo7kN
2THiEQKBgQC6UunmxljLIbeHb91hYgR1tsuZW2VHN0N2xSGYDoEQ6RIXghooe0cf
iP6ZSgf9XmToBG6qFzgr/03my6JEXt+S0+LRPn2Ji47DLCb+alLqu2fvq0BEW0Uu
60j9z/Ia380Y/y0ZeKBffQklqKU3lBtGUYSKVDfhdabf5/cnh3SQEQ==
-----END RSA PRIVATE KEY-----
```

SSH Key:

/etc/ssh/ssh_host_ed25519_key

```
root@OutdoorAP:~# cat /etc/ssh/ssh_host_ed25519_key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABG5vbmUAAAABbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACAip/8brCoB1e0L4RI4x/zAxEYLhTnNSzb5zbb+d0F1QwAAAJhsTxvfbE8b
3wAAAAtzc2gtZWQyNTUxOQAAACAip/8brCoB1e0L4RI4x/zAxEYLhTnNSzb5zbb+d0F1Qw
AAAECPeCY9itFyQqqDfQTdEWMBpBpuQONIGesfopwy43PjiSKn/xusKgHV7QvhEjjH/MDE
RguF0c1LNvnNt53QXVDAADnJvb3RAT3V0ZG9vckFQAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
root@OutdoorAP:~#
```

CCK-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

[CCK-2] CCK generation mechanisms**【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.

【CCK-2 Conceptual assessment】

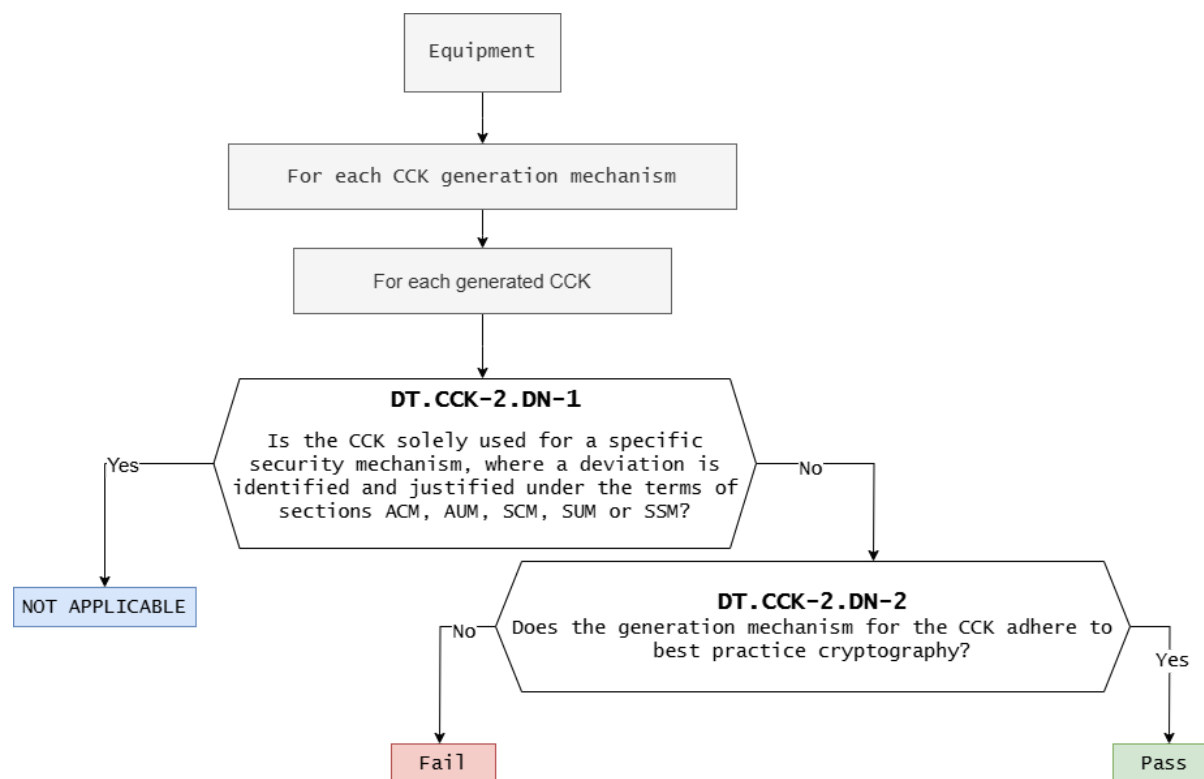


Figure 25 — Decision Tree for requirement CCK-2

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.CCK-2)
CCKA-A	DT.CCK-2.DN-1	No	Not utilized in specific security mechanisms.
CCKA-B	DT.CCK-2.DN-2	Yes	The generation mechanism adheres to established cryptographic best practices.

Verdict: PASS

【CCK-2 Functional completeness assessment】

Asset No.	Document Verification
CCKA-A	Y
CCKA-B	Y

Verdict : PASS**【CCK-2 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.

Verdict : NOT NECESSARY**【Supporting Evidence】**

Starting from firmware version v1.01.91, the device regenerates the SSH host key upon the first power-up, replacing the default key to ensure a unique SSH host key for each unit. The generation mechanism follows cryptographic best practices:

a) Entropy Source

- Keys are generated using the `/dev/urandom` entropy source provided by OpenSSL (or the system's cryptographic library).

b) Key Generation with `ssh-keygen`

- System uses the `ssh-keygen` utility to generate host keys with commonly recommended algorithms:



i) RSA key (2048 bits)

```
ssh-keygen -t rsa -b 2048 -f /etc/ssh/ssh_host_rsa_key -N ""
```

ii) ECDSA key (256 bits)

```
ssh-keygen -t ecdsa -b 256 -f /etc/ssh/ssh_host_ecdsa_key -N ""
```

iii) Ed25519 key

```
ssh-keygen -t ed25519 -f /etc/ssh/ssh_host_ed25519_key -N ""
```

c) Default Behavior

- By default, the system generates **RSA**, **ECDSA**, and **Ed25519** host keys during the initialization process, storing them in `/etc/ssh/`.
- These keys are unique to each device and are not pre-shared, reducing the risk of credential reuse or exposure.

CCK-2 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	NOT NECESSARY

[CCK-3] Preventing static default values for preinstalled CCKs

【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.

【CCK-3 Conceptual assessment】

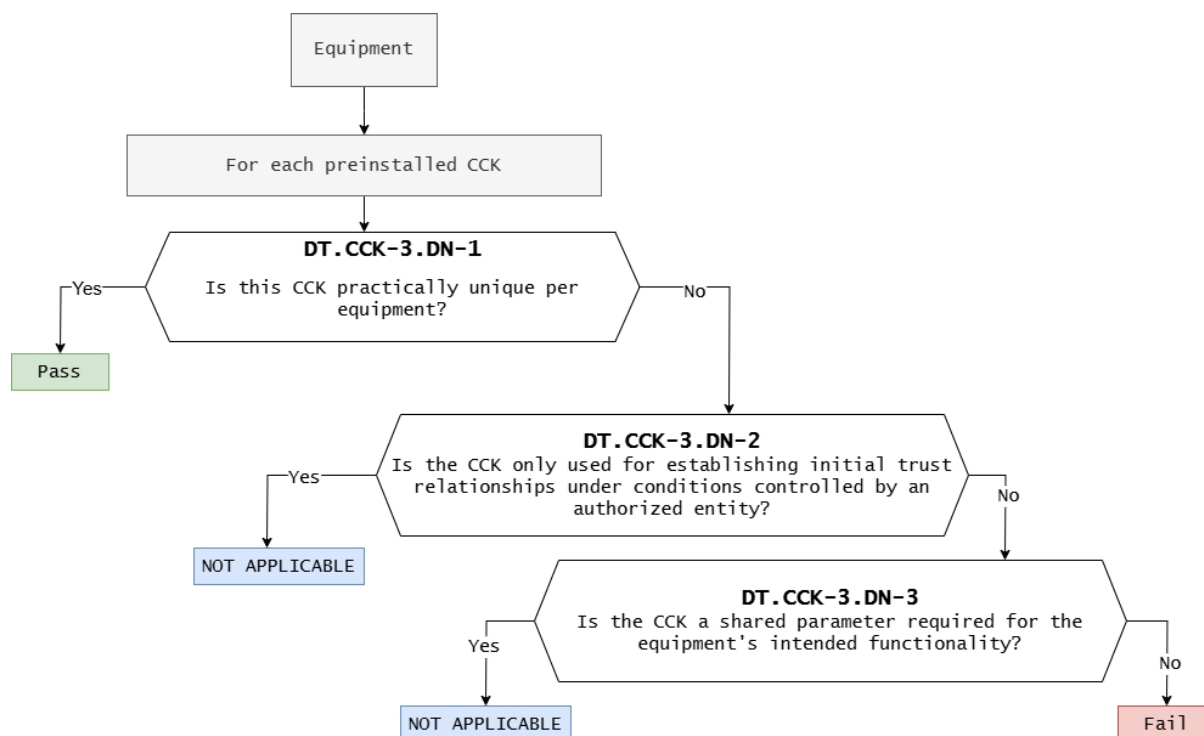


Figure 26 — Decision Tree for requirement CCK-3

【Assessment】

Asset ID	Decision Node	Decision	Justification (E.just.DT.CCK-3)
CCKA-A CCKA-B	DT.CCK-3.DN-1	Yes	The key is generated automatically upon the device's first startup, rather than being provisioned on the production line with identical keys.
	DT.CCK-3.DN-2	-	-
	DT.CCK-3.DN-3	-	-

Verdict: PASS

【CCK-3 Functional completeness assessment】

Asset No.	Document Verification
CCKA-A	Y
CCKA-B	Y

Verdict : PASS

【CCK-3 Functional sufficiency assessment】

Asset No.	Implemented
CCKA-A	Y
CCKA-B	Y

Verdict : PASS

【Supporting Evidence】

Follow CCK-1

CCK-3 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS



4.10 [GEC] General equipment capabilities

[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities

【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.

【GEC-1 Assets】

Asset No.	Asset	Software/Hardware
GECA-A	WAPS-233N_LW	Software



【GEC-1 Conceptual assessment】

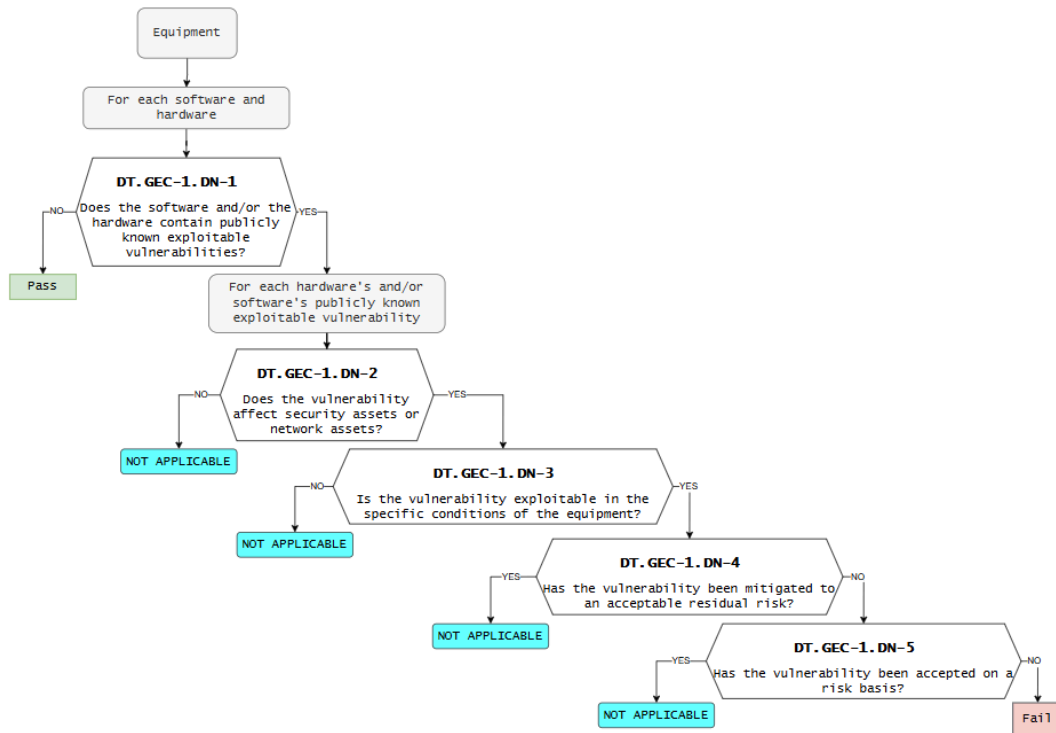


Figure 27 – Decision Tree for requirement GEC-1

【Assessment】

Asset ID	Decision Node	Decision	Justification E.just.DT.GEC-1
GECA-A	DT.GEC-1.DN-1	Yes	Vulnerabilities are identified through the use of vulnerability scanning software.
	DT.GEC-1.DN-2	Yes	Certain vulnerabilities may compromise the security or integrity of network assets.
	DT.GEC-1.DN-3	Yes	The vulnerabilities can be exploited only under specific conditions.
	DT.GEC-1.DN-4	Yes	The vulnerabilities are considered acceptable.

	DT.GEC-1.DN-5	-	
--	---------------	---	--

Verdict : NOT APPLICABLE

【GEC-1 Functional completeness assessment】

Asset No.	Document Verification
GECA-A	Y

Verdict : PASS

【GEC-1 Functional sufficiency assessment】

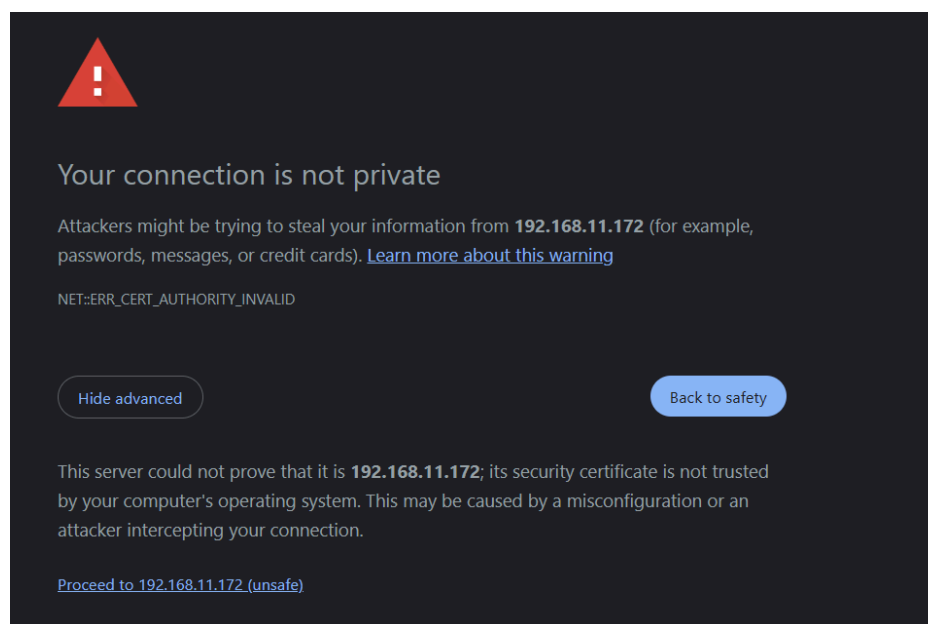
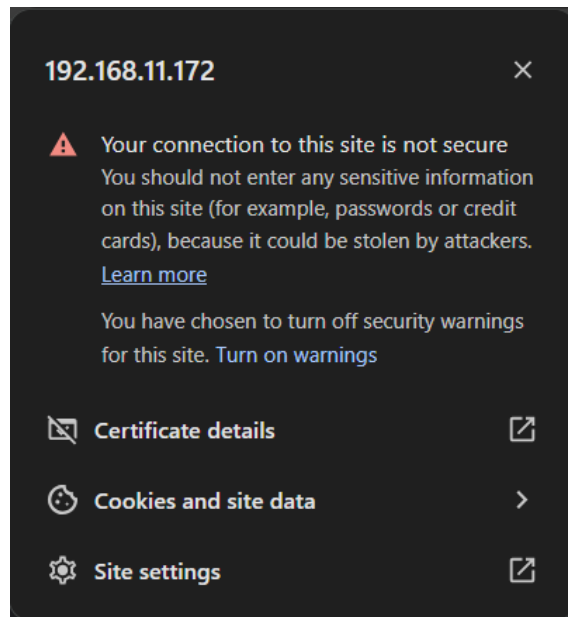
Asset No.	Implemented
GECA-A	Y

Verdict : PASS

【Supporting Evidence】

- 1. The services are not publicly accessible and do not rely on third-party trust.*
- 2. The use of a self-signed certificate is intentional and expected behavior.*

Accordingly, this alert is classified as non-actionable findings and does not impact the current risk level assessment.



GEC-1 Summary Assessment	Verdict
Conceptual assessment	NOT APPLICABLE
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

[GEC-2] Limit exposure of services via related network interfaces

【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.

【GEC-2 Assets】

Asset No.	Asset	Software/Hardware
GECA-B	SSH	Software

【GEC-2 Conceptual assessment】

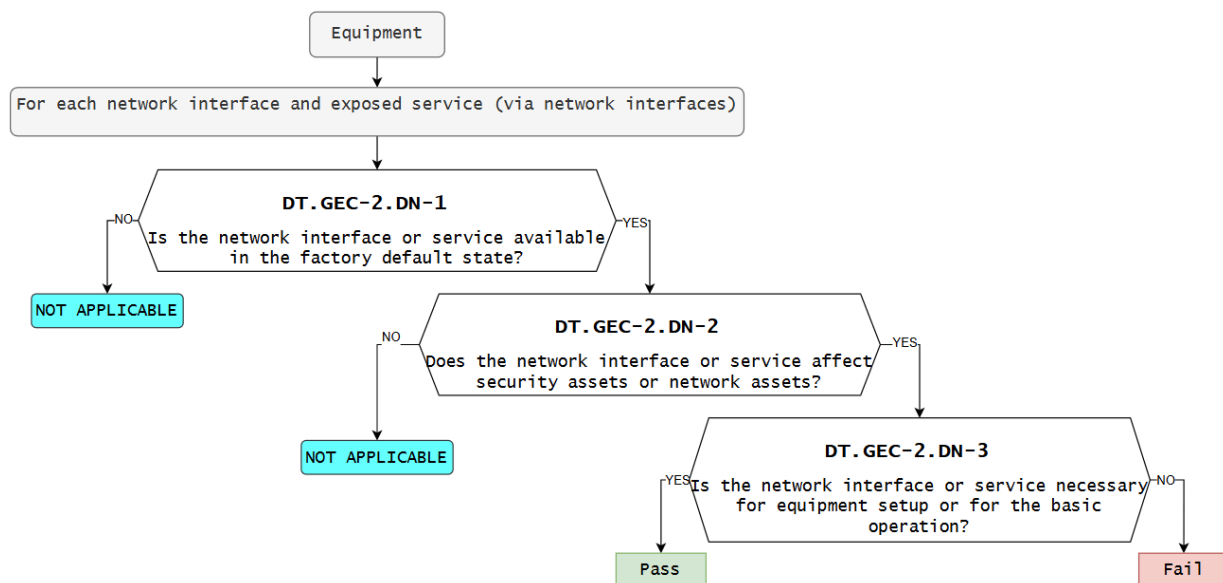


Figure 28 – Decision Tree for requirement GEC-2

【Assessment】

Asset ID	Decision Node	Decision	Justification E.just.DT.GEC-2
GECA-B	DT.GEC-2.DN-1	NO	SSH is not enabled by default.
	DT.GEC-2.DN-2	-	-
	DT.GEC-2.DN-3	-	-

Verdict : NOT APPLICABLE

【GEC-2 Functional completeness assessment】

Asset No.	Document Verification
GECA-B	N/A

Verdict: NOT APPLICABLE

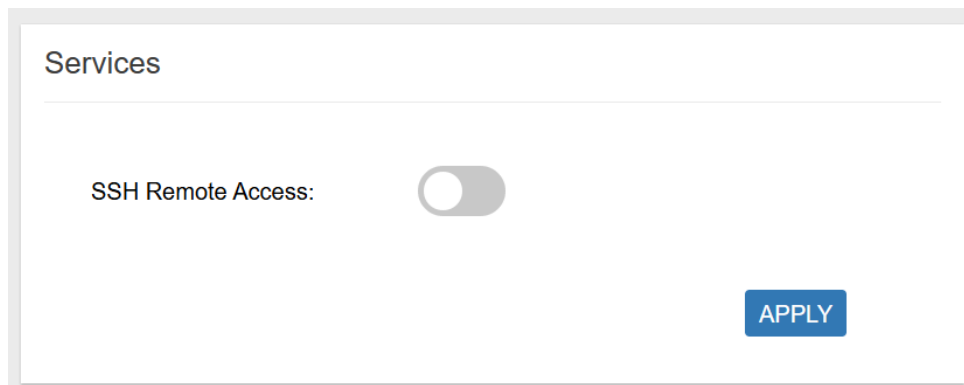
【GEC-2 Functional sufficiency assessment】

NOT APPLICABLE.

Verdict: NOT APPLICABLE

【Supporting Evidence】

The default setting is disabled





GEC-2 Summary Assessment	Verdict
Conceptual assessment	NOT APPLICABLE
Functional completeness assessment	NOT APPLICABLE
Functional sufficiency assessment	NOT APPLICABLE

[GEC-3] Configuration of optional services and the related exposed network interfaces

【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.

【GEC-3 Conceptual assessment】

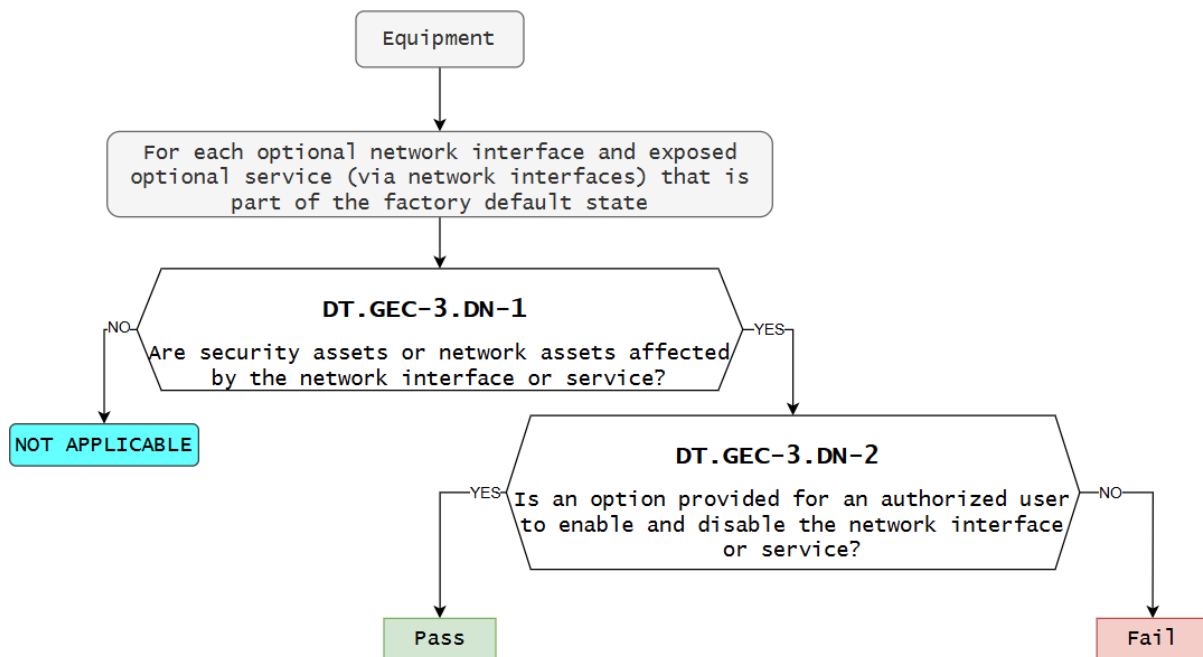


Figure 29 – Decision Tree for requirement GEC-3

【Assessment】

Asset ID	Decision Node	Decision	Justification E.just.DT.GEC-3
GECA-B	DT.GEC-3.DN-1	Yes	Network-facing interfaces or services may introduce risks to security-critical and network-connected assets.
	DT.GEC-3.DN-2	Yes	Can enable or disable through system settings

Verdict : PASS

【GEC-3 Functional completeness assessment】

Asset No.	Document Verification
GECA-B	Y

Verdict: PASS

【GEC-3 Functional sufficiency assessment】

Asset No.	Implemented
GECA-B	Y

Verdict: PASS



【Supporting Evidence】

Services

SSH Remote Access: ☒

APPLY



SSH Remote Access

Enabling remote SSH access may expose your device to unauthorized access and potential security risks.
Are you sure you want to enable SSH remote access?

Confirm

Cancel

GEC-3 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces

【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.

【GEC-4 Conceptual assessment】

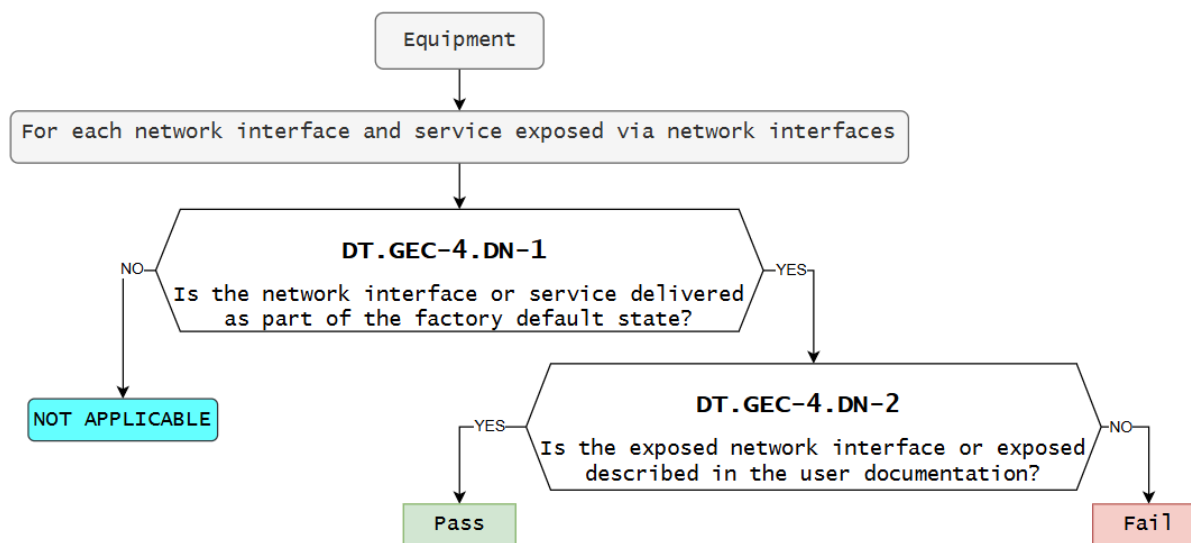


Figure 30 – Decision Tree for requirement GEC-4

【Assessment】

Asset ID	Decision Node	Decision	Justification E.just.DT.GEC-4
GECA-B	DT.GEC-4.DN-1	Yes	SSH service is available
	DT.GEC-4.DN-2	Yes	Details of the exposed network interfaces are provided in the user-facing documentation

Verdict : PASS

【GEC-4 Functional completeness assessment】

Asset No.	Document Verification
GECA-B	Y

Verdict : PASS

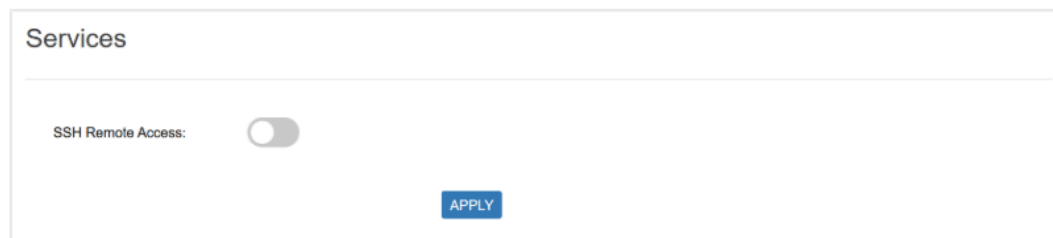
【GEC-4 Functional sufficiency assessment】

NONE

【Supporting Evidence】
3.1.2 Service

For security reasons, starting from version v1.01.91, the SSH service is disabled by default. To enable the SSH functionality, users must activate the service through the GUI.

Figure 3.1.2 Service



GEC-4 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	NONE



[GEC-5] No unnecessary external interfaces

【Requirement】

The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.

【GEC-5 Assets】

Asset No.	Asset	Software/Hardware
GECA-C	RJ45	Hardware
GECA-D	SIM Card	Hardware

【GEC-5 Conceptual assessment】

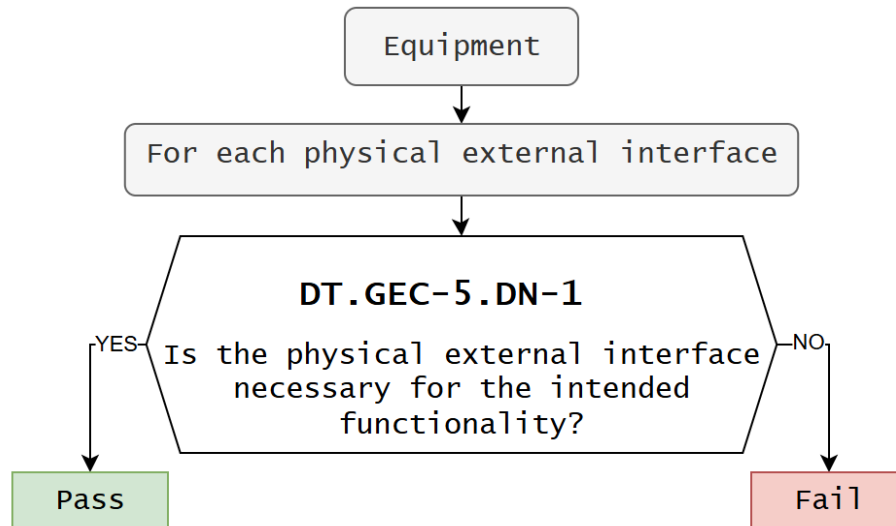


Figure 31 – Decision Tree for requirement GEC-5

【Assessment】

Asset ID	Decision Node	Decision	Justification E.just.DT.GEC-5
GECA-C GECA-D	DT.GEC-5.DN-1	Yes	The user manual includes descriptions of all external interfaces.

Verdict : PASS

【GEC-5 Functional completeness assessment】

Asset No.	Document Verification
GECA-C	Y
GECA-D	Y

Verdict : PASS

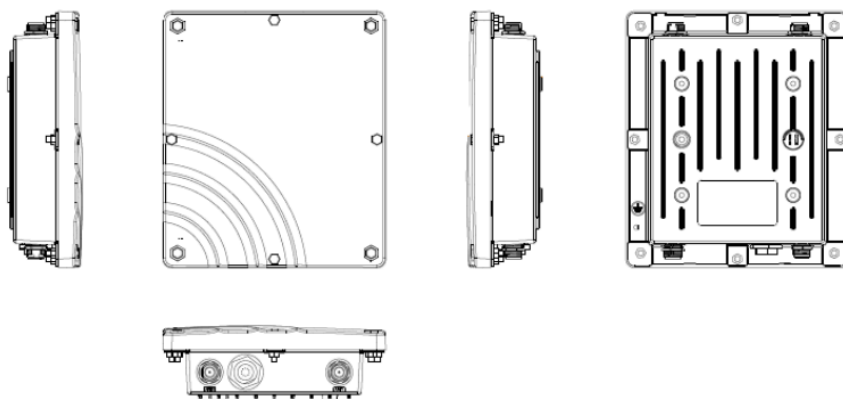
【GEC-5 Functional sufficiency assessment】

NOT APPLICABLE.

Verdict: NOT APPLICABLE

【Supporting Evidence】

The physical external interfaces are essential for the intended functionality, and these interfaces are mentioned in the user manual.



Port	Count	Description
ANT1	1	External N-Type GPS antenna
ANT2	1	External N-Type 3/4G antenna (Optional)
ANT3	1	External N-Type LoRa antenna for CH 1-8
ANT4	1	External N-Type LoRa antenna for CH 9-16
RJ45	1	10/100Mbps Ethernet port with power over Ethernet (PoE) function
SIM Slot	1	Mini SIM card slot for 3/4G module

GEC-5 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	NOT APPLICABLE

[GEC-6] Input validation

【Requirement】

The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets.

【GEC-6 Conceptual assessment】

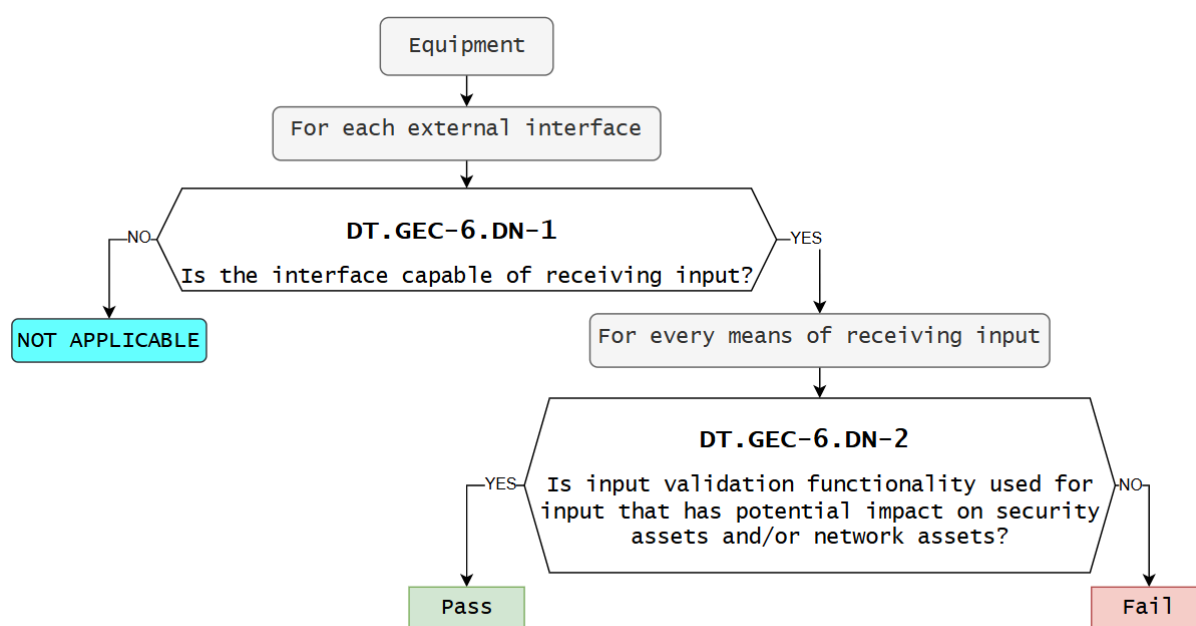


Figure 32 – Decision Tree for requirement GEC-6

【Assessment】

Asset ID	Decision Node	Decision	Justification E.just.DT.GEC-6
GECA-C	DT.GEC-6.DN-1	Yes	The WEB GUI and SSH interfaces are available for input operations.
	DT.GEC-6.DN-2	Yes	Entering special characters or strings is interpreted as



			an incorrect password.
--	--	--	------------------------

Verdict : PASS

【GEC-6 Functional completeness assessment】

Asset No.	Document Verification
GECA-C	Y

Verdict : PASS

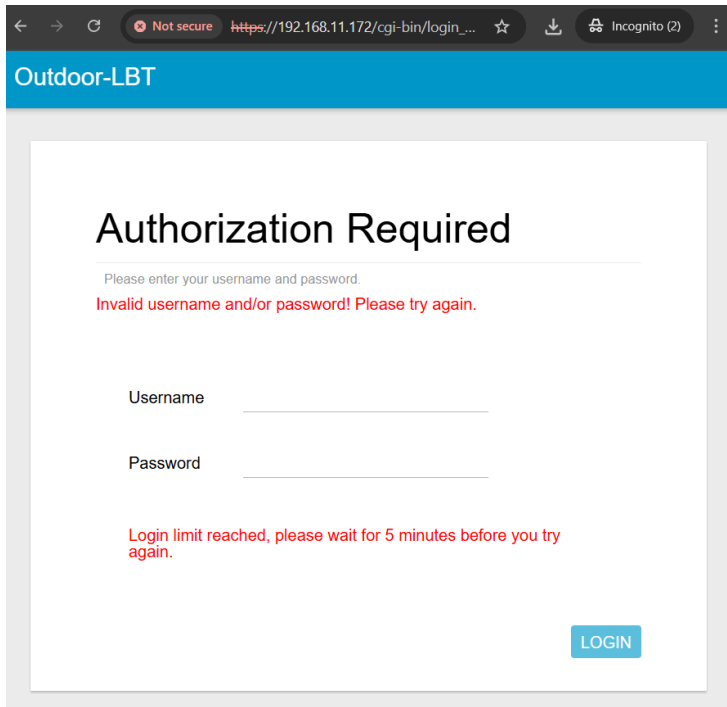
【GEC-6 Functional sufficiency assessment】

Asset No.	Implemented
GECA-C	Y

Verdict : PASS

【Supporting Evidence】

The interface is capable of accepting input, which may have implications for both security-critical assets and network-connected assets.



GEC-6 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

4.11 [CRY] Cryptography

[CRY-1] Best practice cryptography

【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.

【CRY-1 Assets】

Asset No.	Asset	Type
CRYA-A	WAPS-232N_LW	Security

【CRY-1 Conceptual assessment】

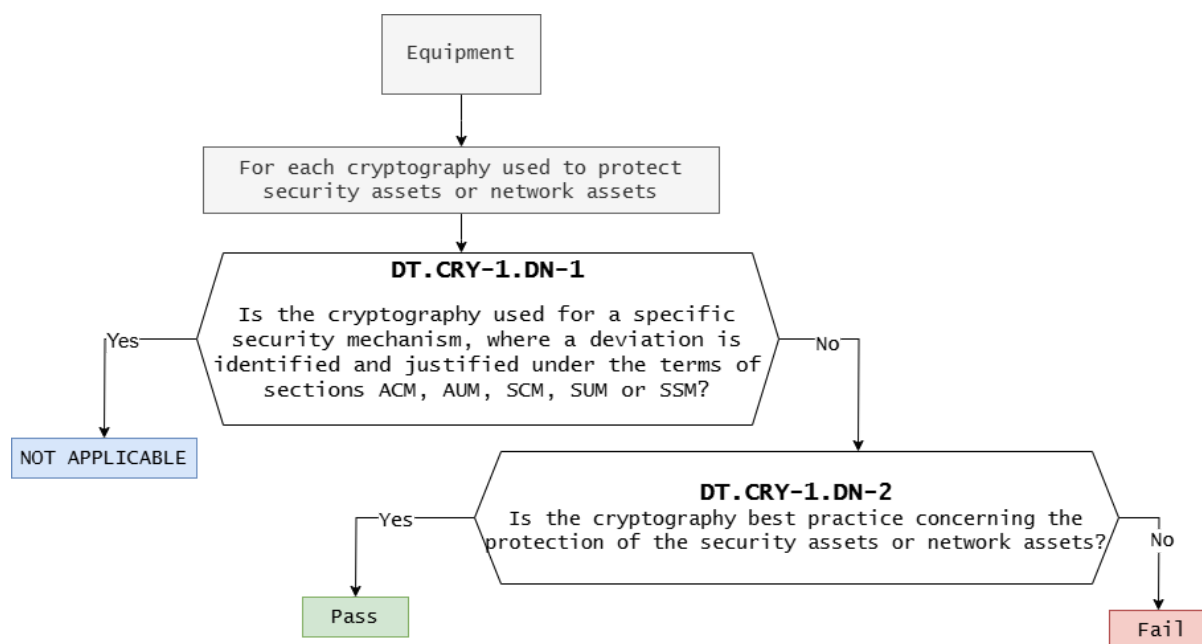


Figure 33 — Decision Tree for requirement CRY-1

【Assessment】

Asset ID	Decision Node	Decision	Justification E.just.DT.CRY-1
CRYA-A	DT.CRY-1.DN-1	No	There are no dedicated security protections implemented for ACM, AUM, SCM, SUM, or SSM
	DT.CRY-1.DN-2	Yes	Cryptographic methods following industry best

			practices are implemented to protect the confidentiality and integrity of security and network assets.
--	--	--	--

Verdict : PASS

【CRY-1 Functional completeness assessment】

Asset No.	Document Verification
CRYA-A	Y

Verdict : PASS

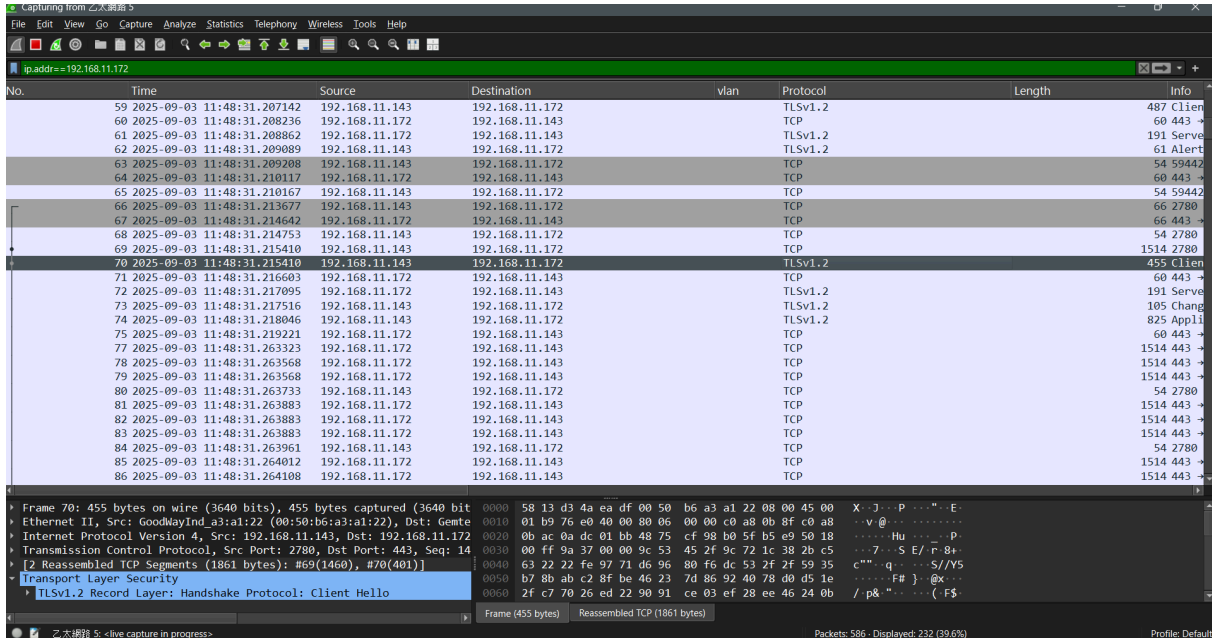
【CRY-1 Functional sufficiency assessment】

Asset No.	Implemented
CRYA-A	Y

Verdict : PASS

【Supporting Evidence】

Best-practice cryptographic methods are applied in the DUT to protect assets.



No.	Time	Source	Destination	vlan	Protocol	Length	Info
59	2025-09-03 11:48:31.207142	192.168.11.143	192.168.11.172		TLSv1.2	487	Client Hello
60	2025-09-03 11:48:31.208236	192.168.11.172	192.168.11.143		TCP	60	443 →
61	2025-09-03 11:48:31.208862	192.168.11.172	192.168.11.143		TLSv1.2	191	Server Hello
62	2025-09-03 11:48:31.209089	192.168.11.143	192.168.11.172		TLSv1.2	61	Alert
63	2025-09-03 11:48:31.209208	192.168.11.143	192.168.11.172		TCP	54	59442 →
64	2025-09-03 11:48:31.210117	192.168.11.172	192.168.11.143		TCP	60	443 →
65	2025-09-03 11:48:31.210167	192.168.11.143	192.168.11.172		TCP	54	59442 →
66	2025-09-03 11:48:31.213677	192.168.11.143	192.168.11.172		TCP	66	2780 →
67	2025-09-03 11:48:31.214642	192.168.11.172	192.168.11.143		TCP	66	443 →
68	2025-09-03 11:48:31.214753	192.168.11.143	192.168.11.172		TCP	54	2780 →
69	2025-09-03 11:48:31.215410	192.168.11.143	192.168.11.172		TCP	1514	2780 →
70	2025-09-03 11:48:31.215410	192.168.11.143	192.168.11.172		TLSv1.2	455	Client Hello
71	2025-09-03 11:48:31.216603	192.168.11.172	192.168.11.143		TCP	60	443 →
72	2025-09-03 11:48:31.217095	192.168.11.172	192.168.11.143		TLSv1.2	191	Server Hello
73	2025-09-03 11:48:31.217516	192.168.11.143	192.168.11.172		TLSv1.2	105	Change
74	2025-09-03 11:48:31.218046	192.168.11.143	192.168.11.172		TLSv1.2	825	Application Data
75	2025-09-03 11:48:31.219221	192.168.11.172	192.168.11.143		TCP	60	443 →
77	2025-09-03 11:48:31.263323	192.168.11.172	192.168.11.143		TCP	1514	443 →
78	2025-09-03 11:48:31.263568	192.168.11.172	192.168.11.143		TCP	1514	443 →
79	2025-09-03 11:48:31.263568	192.168.11.172	192.168.11.143		TCP	1514	443 →
80	2025-09-03 11:48:31.263733	192.168.11.143	192.168.11.172		TCP	54	2780 →
81	2025-09-03 11:48:31.263883	192.168.11.172	192.168.11.143		TCP	1514	443 →
82	2025-09-03 11:48:31.263883	192.168.11.172	192.168.11.143		TCP	1514	443 →
83	2025-09-03 11:48:31.263883	192.168.11.172	192.168.11.143		TCP	1514	443 →
84	2025-09-03 11:48:31.263961	192.168.11.143	192.168.11.172		TCP	54	2780 →
85	2025-09-03 11:48:31.264012	192.168.11.172	192.168.11.143		TCP	1514	443 →
86	2025-09-03 11:48:31.264108	192.168.11.172	192.168.11.143		TCP	1514	443 →

Frame 70: 455 bytes on wire (3640 bits), 455 bytes captured (3640 bit) on interface 0
Ethernet II, Src: GoodWayInd_a3:a1:22 (00:50:b6:a3:a1:22), Dst: Gemtek_12:34:56 (08:00:27:12:34:56)
Internet Protocol Version 4, Src: 192.168.11.143, Dst: 192.168.11.172
Transmission Control Protocol, Src Port: 2780, Dst Port: 443, Seq: 1441111111, Len: 455
[2 Reassembled TCP Segments (1861 bytes): #69(1460), #70(401)]
Transport Layer Security
* TLSv1.2 Record Layer: Handshake Protocol: Client Hello

```
root@OutdoorAP:~# cat /etc/shadow
root:$6$KdtyYHpr$bZhf.gIUxN89w4pEhkLuNsR3DvxDJgVCNG3nSEWtnEiUAKF4up5KpSqHsskJWI9ughQfA5ICESFBYx9fsB8Iv0:20334:0:99999:7:::
daemon*:16273:0:99999:7:::
bin*:16273:0:99999:7:::
sys*:16273:0:99999:7:::
sync*:16273:0:99999:7:::
games*:16273:0:99999:7:::
man*:16273:0:99999:7:::
lp*:16273:0:99999:7:::
mail*:16273:0:99999:7:::
news*:16273:0:99999:7:::
uucp*:16273:0:99999:7:::
proxy*:16273:0:99999:7:::
www-data*:16273:0:99999:7:::
backup*:16273:0:99999:7:::
list*:16273:0:99999:7:::
irc*:16273:0:99999:7:::
gnats*:16273:0:99999:7:::
nobody*:16273:0:99999:7:::
libuuid!:16273:0:99999:7:::
syslog*:16273:0:99999:7:::
sshd*:16412:0:99999:7:::
mysql!:16450:0:99999:7:::
dhcpcd*:16465:0:99999:7:::
ntp*:16758:0:99999:7:::
root@OutdoorAP:~#
```

```
root@OutdoorAP:~# cat /etc/ssh/ssh_host_ed25519_key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktZjEAAAAABG5vbmUAAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAAtzc2gtZW
QyNTUxOQAAACAip/8brCoB1e0L4RI4x/zAxEYLhTnNSzb5zbb+d0F1QwAAAJhsTxvfbE8b
3wAAAAAtzc2gtZWQyNTUxOQAAACAip/8brCoB1e0L4RI4x/zAxEYLhTnNSzb5zbb+d0F1Qw
AAAECPeCY9itFyQqqDfQTDewMBpBpuQ0NIGEsfopwy43PjiSKn/xusKgHV7QvhEjjH/MDE
RguF0c1LNvnNtv53QXVDAAADnJvb3RAT3V0ZG9vcKFAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
root@OutdoorAP:~#
```



```
root@OutdoorAP:~# cat /etc/lighttpd/certs/lighttpd.pem
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAmQ0d/xY2YXW0U0+hIDqpEv4LHB0IY6swj dkkpMT2AuCTArW9
YG0aZS0WokU4May4wg5EGkVZfBB0K0bTbDhG1wAvmUjdPnDpVHzKFQX5j3bzI1pv
w3j7M4bq2DeyQDnI/5nIFIJEfE0S2EMgyQYSHvN0K7Q2UWzP/VB6+LLKpFpYUj+I
QKGWSRgvPvilsQib5X+ZnqG6PIXZXUQuEKpkX+iRVBtKHZk1e8yl6EJ/KR04uXj3
z6L5GHaD8f2Ea6dV+FVyBIbiy9Mv6HeMwEEaDrs7vcVetSRj27Ysh0ImgZLZ3hh4
YZGNfwx3wv0Iznwjt+xUjVNWoEamQ04HD30WRQIDAQABAoIBAHPJ3bC3cErJTrKQ
p9iHKJRqx6LsQAWPZLtb1QIm1GuW1QG01wf0Mudqdh4rufiy0FBXlKQ/ZRScdVdm
TNsptBXXGSuhWWg86f12Mzg2ffhQqF9NsxIy0/Fel9seP+ehD/R3tkv1xbQxNy4P
kwUiZ6Es0+2geBuf87aUJYRzVyWA3Iav8qLlsuokX0ZIRLeKz1/04Lx0uxu8I+MW
fdoSHrn+ubkprnWb0M3w3Ro8ZMshq0lxaDANCK3wkk0XpmK1pjZexQSFwzRkdcWz
epHtoWpirsbi4M0YZhyPQ7UUZ9i0/cS9tf79WE0bSLRn11KVdI3Mw/x4lQic2UBh
lv3PaaECgYEAy0HyL0pHW600C5tiNyiGUK08/hTE+Q7Jwr4X0nQSmqz3tQqFMwzm
qP+VEeJka7F27pycsTsZ4rB9pGDlqABkKxV0k0d6yvLvHWh/R9n3MzzQoQwbdKim
I0F/P1iQDBnQ9mH+KVS7FN8fiZfLUD84qNoQGrkR2l8GAL1Lo89FGk0CgYEAwMQM
b/XQJ2iWSGCgp7EMVpUVXo8ApZAmhqNAE6IBEWaUNlcwft/+oJ2v5x1o0BrLzw5V
JQGbV7xUDi1lWqIbPtU16tRITa288GKldD6gQWojrvD/hzit+QjYkPyCheQK9kxs
NGoVqxSWM4nxntCN5GsDFKG4T3MayExGSzFwd9kCgYAs6JUpd1ns1W6iYeKBbWLA
LHCdctLSbgIGFRo0VbcGldLHz3u2ZrdHBtDqFGnub4dWl0Ei5pci8I233HefLe1
DUAepAZtcN+ED+KPbYLAuN8fth0a2WhbwcZrohWx1sKkrWIKn732DpZZQECbqlxK
cm08g8d+CCC7aRedSd5qwQKBgQC7mpGYLR3GHM2V5ySzz2V4pmNDwd0ZRK+Z/SuR
b+umKbU5JaX1X+DKJG1beo3Vax7LhuFqwKP5+Km9moS3rmjhxibIQo2Tu/DT6s2n
0oNY5pmp2tB1o739TpSm1nlz6cqZZksWv8YS2Fh0FIRo0gQmN9eprKX8Cgyo7kN
2THiEQKBgQC6UunmxljLIbeHb91hYgR1tsuZW2VHN0N2xSGYDoEQ6RIXghooe0cf
iP6ZSgf9XmToBG6qFzgr/03my6JEXt+S0+LRPn2Ji47DLCb+aLLqu2fvq0BEW0Uu
60j9z/Ia380Y/y0ZeKBffQklqKU3lBtGUYSKVDfhdabf5/cnh3SQEQ==
-----END RSA PRIVATE KEY-----
```

CRY-1 Summary Assessment	Verdict
Conceptual assessment	PASS
Functional completeness assessment	PASS
Functional sufficiency assessment	PASS

-----THE END OF REPORT-----