CYBERSECURITY EVALUATION
RED DIRECTIVE
SUPPLEMENTAL REGULATION
EU 2022/30
TEST REPORT

Shaping a World of Trust

AC Charger

Prepared by:	Chloe Lv
Reviewed by:	Lukas Su
Test laboratory:	BUREAU VERITAS LCIE CHINA COMPANY LIMITED
Issued on:	2026/09/16
Test Report n°	ASBJ-WDG-P26070365

Shaping a World of Trust

SUMMARY

1 REPORT HISTORY 4
1.1 PRODUCT/SYSTEM VERSION 4
1.2 REPORT TEMPLATE REVISION HISTORY 4
1.3 REPORT REVISION HISTORY 4
2 INTRODUCTION 5
2.1 Scope 5
2.2 Terms and Conditions 5
2.3 Definitions, acronyms and abbreviations 6
3 DEVICE OVERVIEW 7
3.1 GENERAL DUT INFORMATION 7
3.2 FEATURES DESCRIPTIONS 8
3.2.1 Hardware interfaces / Software 8
3.2.2 Supported Communication Protocols 8
3.2.3 Services exposed 8
3.3 TEST SETUP DETAILS 8
4 TEST OVERVIEW 10
5 PROVISIONS ASSESSEMENT 12
5.1 [ACM] Access control mechanism 12
5.1.1 [ACM-1] Applicability of access control mechanisms 12
5.1.2 [ACM-2] Appropriate access control mechanisms 14
5.2 [AUM] Authentication mechanism 15
5.2.1 [AUM-1-1] Requirement network interface 15
5.2.2 [AUM-1-2] Requirement user interface 17
5.2.3 [AUM-2] Appropriate authentication mechanisms 19
5.2.4 [AUM-3] Authenticator validation 21
5.2.5 [AUM-4] Changing authenticators 23
5.2.6 [AUM-5-1] Requirement for factory default passwords 25
5.2.7 [AUM-5-2] Requirement for non-factory default passwords 27
5.2.8 [AUM-6] Brute force protection 29
5.3 [SUM] Secure update mechanism 31
5.3.1 [SUM-1] Applicability of update mechanisms 31
5.3.2 [SUM-2] Secure updates 33
5.3.3 [SUM-3] Automated updates 35
5.4 [SSM] Secure storage mechanism 37
5.4.1 [SSM-1] Applicability of secure storage mechanisms 37
5.4.2 [SSM-2] Appropriate integrity protection for secure storage mechanisms 39
5.4.3 [SSM-3] Appropriate confidentiality protection for secure storage mechanisms 41
5.5 [SCM] Secure communication mechanism 43
5.5.1 [SCM-1] Applicability of secure communication mechanisms 43
5.5.2 [SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms 45
5.5.3 [SCM-3] Appropriate confidentiality protection for secure communication mechanisms 47

5.5.4 [SCM-4] Appropriate replay protection for secure communication mechanisms 49

5.6 [RLM] Resilience mechanism 50
5.6.1 [RLM-1] Applicability and appropriateness of resilience mechanisms 50

5.7 [NMM] Network monitoring mechanism 52
5.7.1 [NMM-1] Applicability and appropriateness of network monitoring mechanisms 52

5.8 [TCM] Traffic control mechanism 53
5.8.1 [TCM-1] Applicability of and appropriate traffic control mech 53

5.9 [CCK] Confidential cryptographic keys 55
5.9.1 [CCK-1] Appropriate CCKs 55
5.9.2 [CCK-2] CCK generation mechanisms 57
5.9.3 [CCK-3] Preventing static default values for preinstalled CCKs 59

5.10 [GEC] General equipment capabilities 61
5.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities 61
5.10.2 [GEC-2] Limit exposure of services via related network interfaces 63
5.10.3 [GEC-3] Configuration of optional services and the related exposed network interfaces 65
5.10.4 [GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces 67
5.10.5 [GEC-5] No unnecessary external interfaces 68
5.10.6 [GEC-6] Input validation 69

5.11 [CRY] Cryptography 71
5.11.1 [CRY-1] Best practice cryptography 71

1 REPORT HISTORY

1.1 PRODUCT/SYSTEM VERSION

Target of Evaluation	Serial number	Additional information
AC Charger	5022KCAC267L2210	/

1.2 REPORT TEMPLATE REVISION HISTORY

Report Type	Date	Revision ID	Comments
Template	2025/03/01	1.0	Creation

1.3 REPORT REVISION HISTORY

Report Type	Date	Revision ID	Comments
Draft	2026/09/14	1.0	/
Final	2026/09/16	1.0	/

REFERENCEs

Document	Date	Rev ID	Comments
EN 18031-1:2024	August 2024	V1.00	/

2 INTRODUCTION

2.1 Scope

This report falls under the scope of work defined by EN 18031 series, which addresses common security requirements for internet-connected radio equipment. This document specifies the necessary security measures and assessment criteria that should be implemented for internet-connected devices to ensure they meet the required standards of cybersecurity.

This test covers the compliance assessment of EN 18031-1 according to the application requirements. This means that under common requirements, testers need to consider the input requirements of the standard (assets and asset analysis, etc.) and take them into account in the verdict. Please refer to 4 TEST OVERVIEW for the generated test items.

The evaluation of compliance with the EN 18031 series standard is assumed to involve collaboration with product developers at various stages, particularly for providing access to technical documentation and product design.

This assessment has been carried out from "07/2026" to "09/2026"

The report outlines the security assessment for a product already in use, under the assumption that the evaluators have access to product developers and crucial product details, such as source code or design specifications.

The verdicts for the tests performed are: PASS, FAIL, or N/A. An N/A result may be updated to PASS or FAIL upon acquiring additional information.

2.2 Terms and Conditions

This report is governed by, and incorporates by reference, the Conditions of Testing as posted at the date of issuance of this report at http://www.bureauveritas.com/home/about-us/our-business/cps/about-us/terms-conditions/ and is intended for your exclusive use. Any copying or replication of this report to or for any other person or entity, or use of our name or trademark, is permitted only with our prior written permission. This report sets forth our findings solely with respect to the test samples identified herein. The results set forth in this report are not indicative or representative of the quality or characteristics of the lot from which a test sample was taken or any similar or identical product unless specifically and expressly noted. Our report includes all of the tests requested by you and the results thereof based upon the information that you provided to us. Measurement uncertainty is only provided upon request for accredited tests. Statements of conformity are based on simple acceptance criteria without taking measurement uncertainty into account, unless otherwise requested in writing. You have 60 days from date of issuance of this report to notify us of any material error or omission caused by our negligence or if you require measurement uncertainty; provided, however, that such notice shall be in writing and shall specifically address the issue you wish to raise. A failure to raise such issue within the prescribed time shall constitute your unqualified acceptance of the completeness of this report, the tests conducted and the correctness of the report contents.

2.3 Definitions, acronyms and 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
NMM	network monitoring mechanism
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

3 DEVICE OVERVIEW

3.1 GENERAL DUT INFORMATION

Apparatus under test	
Applicant	**GoodWe Technologies Co., Ltd.**
Product	**AC Charger**
Trade mark	GOODWE
Manufacturer	**GoodWe Technologies Co., Ltd.**
Model under test	**GW7K-HCA-G30**
Software Version	**V1.00**

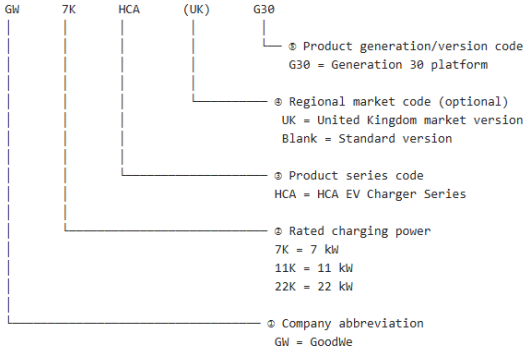


Equipment Under Test

Scope of application：

The product series includes the following models: GW7K-HCA-G30, GW11K-HCA-G30, GW22K-HCA-G30, GW7K-HCA-UK-G30, GW11K-HCA-UK-G30, GW22K-HCA-UK-G30

Naming Rules for Models:



Note: The testers checked the consistency between the models based on the above list, and they used the same software system version and system architecture. These models are family series models and not tested for in this report. Only the main model is tested as a representative.

3.2 FEATURES DESCRIPTIONS

3.2.1 Hardware interfaces / Software

HARDWARE INTERFACE		
Interfaces	**Visible**	**Use cases**
AC Line Input Port	Y	Connect single-phase or three-phase AC.
RS485 communication port	Y	Connect the RS485 cable for communication with the inverter or meter.
LAN communication port	Y	Cable connecting to the router for communication.
Charging connector	Y	Used to connect the electric vehicle charging port.

3.2.2 Supported Communication Protocols

The list of supported by the device communication protocols

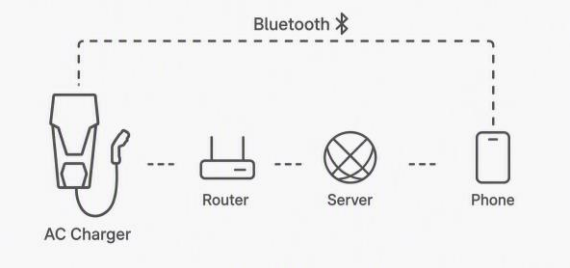
Protocol	Description
Bluetooth communication	BLE secure communication using LE Secure Connections
Wi-Fi secure communication	Wi-Fi protected by WPA and TLS
Ethernet communication	TCP/IP communication with optional TLS protection
MDNS communication	Used for local device discovery; no security-sensitive data transmitted

3.2.3 Services exposed

Services	Network Interface	Port	Enabled by Default
MDNS	UDP	5353	Yes

3.3 TEST SETUP DETAILS

The device evaluation is performed as per the EN 18031 series Cybersecurity Evaluation Methodology



Test setup

Tools	Version	Others information
NMAP	7.92	/
burpsuite	Free Edition v1.6	/
OpenVAS Scanner	23.16.1	/
Wireshark	3.4.5	/
Scapy	2.4.5	/
Nessus	10.5.x	/

4 TEST OVERVIEW

Improve network resilience (§3.3.d harmonized standard EN 18031-1:2024): Wireless devices and products will have to incorporate features to avoid harming communication networks and prevent the possibility that the devices are used to disrupt website or other services functionality.
Better protect consumers' privacy (§3.3.e harmonized standard EN 18031-2:2024): Wireless devices and products will need to have features to guarantee the protection of personal data. The protection of children's rights will become an essential element of this legislation. For instance, manufacturers will have to implement new measures to prevent unauthorised access or transmission of personal data.
Reduce the risk of monetary fraud (§3.3.f harmonized standard EN 18031-3:2024): Wireless devices and products will have to include features to minimise the risk of fraud when making electronic payments. For example, they will need to ensure better authentication control of the user in order to avoid fraudulent payments.

§3(3)d Network	§3(3)e Privacy	§3(3)f Money	Provision	Description	Verdict
/			ACM Access control mechanism		
√	/	/	ACM-1	Applicability of access control mechanisms	Pass
√	/	/	ACM-2	Appropriate access control mechanisms	Pass
√	/	/	AUM Authentication mechanism		
/			AUM-1 Applicability of authentication mechanisms		
√	/	/	AUM-1-1	Requirement network interface	Pass
√	/	/	AUM-1-2	Requirement user interface	Pass
√	/	/	AUM-2	Requirement one factor authentication	Pass
√	/	/	AUM-3	Authenticator validation	Pass
√	/	/	AUM-4	Changing authenticators	Pass
√	/	/	AUM-5 Password strength		
√	/	/	AUM-5-1	Requirement for factory default passwords	Pass
√	/	/	AUM-5-2	Requirement for non-factory default passwords	Pass
√	/	/	AUM-6	Brute force protection	Pass
/			SUM Secure update mechanism		Pass
√	/	/	SUM-1	Applicability of update mechanisms	Pass
√	/	/	SUM-2	Secure updates	Pass
√	/	/	SUM-3	Automated updates	Pass
/			SSM Secure storage mechanism		
√	/	/	SSM-1	Applicability of secure storage mechanisms	Pass
√	/	/	SSM-2	Appropriate integrity protection for secure storage mechanisms	Pass
√	/	/	SSM-3	Appropriate confidentiality protection for secure storage mechanisms	Pass
/			SCM Secure communication mechanism		
√	/	/	SCM-1	Applicability of secure communication mechanisms	Pass
√	/	/	SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	Pass
√	/	/	SCM-3	Appropriate confidentiality protection for secure communication mechanisms	Pass
√	/	/	SCM-4	Appropriate replay protection for secure communication mechanisms	Pass
/			RLM Resilience mechanism		

√	/	/	RLM-1	Applicability and appropriateness of resilience mechanisms	**Pass**
/			NMM Network monitoring mechanism		
√	/	/	NMM-1	Applicability and appropriateness of network monitoring mechanisms	**Pass**
/			TCM Traffic control mechanism		
√	/	/	TCM-1	Applicability of and appropriate traffic control mechanisms	**Pass**
/			CCK Confidential cryptographic keys		
√	/	/	CCK-1	Appropriate CCKs	**Pass**
√	/	/	CCK-2	CCK generation mechanisms	**Pass**
√	/	/	CCK-3	Preventing static default values for preinstalled CCKs	**N/A**
/			GEC General equipment capabilities		
√	/	/	GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	**Pass**
√	/	/	GEC-2	Limit exposure of services via related network interfaces	**Pass**
√	/	/	GEC-3	Configuration of optional services and the related exposed network interfaces	**Pass**
√	/	/	GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	**Pass**
√	/	/	GEC-5	No unnecessary external interfaces	**Pass**
√	/	/	GEC-6	Input validation	**Pass**
/			CRY Cryptography		
√	/	/	CRY-1	Best practice cryptography	**Pass**

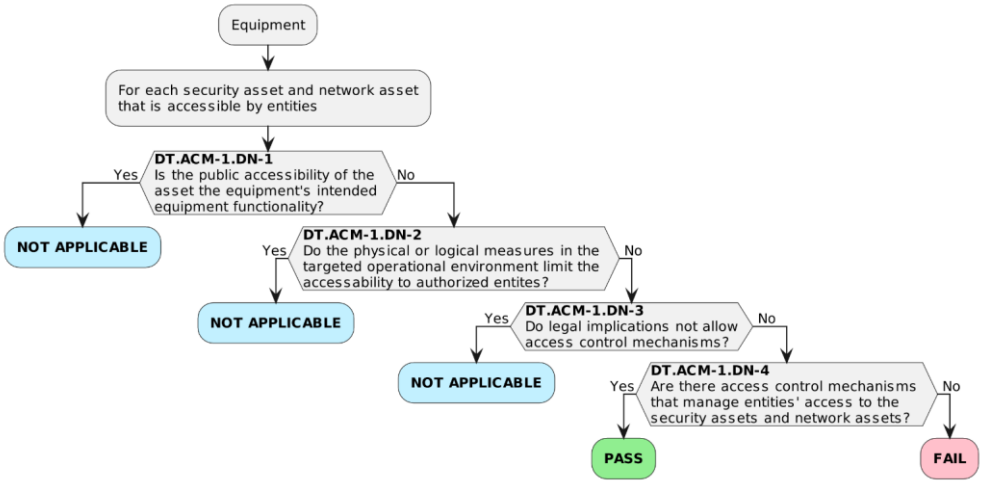
5 PROVISIONS ASSESSEMENT

5.1 [ACM] Access control mechanism

5.1.1 [ACM-1] Applicability of access control mechanisms

5.1.1.1 Conceptual assessment

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



Comments	**Verdict**
The testing engineer reviewed the ACM-1 section of the ID01 TechnicalDoc_AC Charger. Before accessing configuration of the device, end users must pass authentication, otherwise they cannot access the device passpath, so it is not involved. Types of assets that can be accessed and the relevant access control have been listed.	Pass

5.1.1.2 Functional completeness assessment

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

Comments	**Verdict**
After verification by testers, all discovered security assets are recorded in [Overview-SecAssets] and all discovered network assets are recorded in [Overview-NetAssets]. Specific asset information can be found in chapters such as AUM, SUM, SSM, SCM, RLM, and no additional assets not listed in the vendor's documentation were found.	Pass

5.1.1.3 Functional sufficiency assessment

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

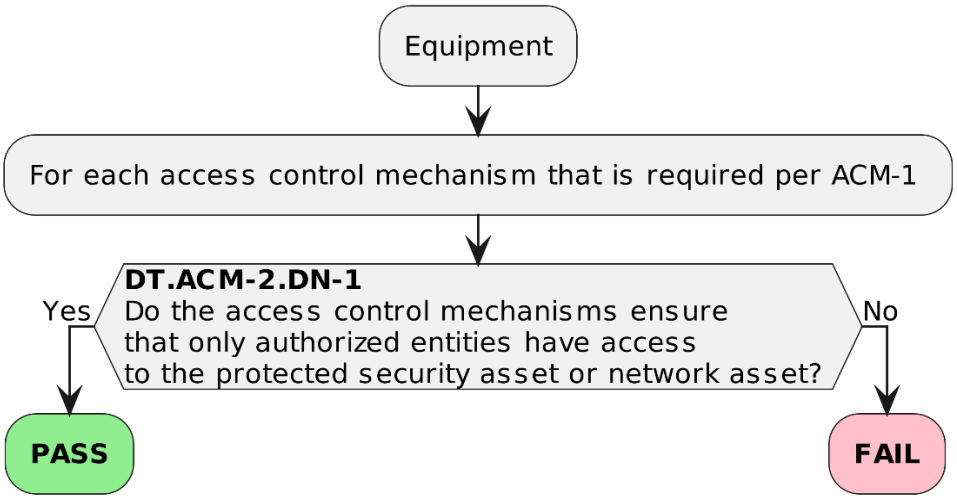
Comments	Verdict
Testers reviewed the access control mechanisms described in [ACM-1.SecAsset] and [ACM-1.NetAsset]. It is found that the relevant access mechanisms were recorded in the documents. The existence of the access control mechanisms will be confirmed functionally below. Testers logged in by user account to confirm that it had suitable access control mechanisms.	Pass

5.1.2 [ACM-2] Appropriate access control mechanisms

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

5.1.2.1 Conceptual assessment

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.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc AC Charger [ACM-2.SecAsset] and [ACM-2.NetAsset]. The tester continued to review the ACM-2 section of the ID01 TechnicalDoc AC Charger. These ensure that only authorized entities have access to the protected assets.	Pass

5.1.2.2 Functional completeness assessment

The functional completeness assessment is covered by the functional sufficiency assessment of the access control mechanism's applicability.
Therefore, this functional completeness assessment is not necessary.

5.1.2.3 Functional sufficiency assessment

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

Comments	Verdict
Testers found through testing that, the access control mechanisms documented in [ACM-2.SecAsset] and [ACM-2.NetAsset] belong to [IC.ACM-2.RBAC] and [IC.ACM-2.DAC]. The implementation of RBAC access control is account password based authentication. The implementation of DAC access control is certificates based authentication. As shown in ID02 Access Control Mechanisms.	Pass

5.2 [AUM] Authentication mechanism

5.2.1 [AUM-1-1] Requirement network interface

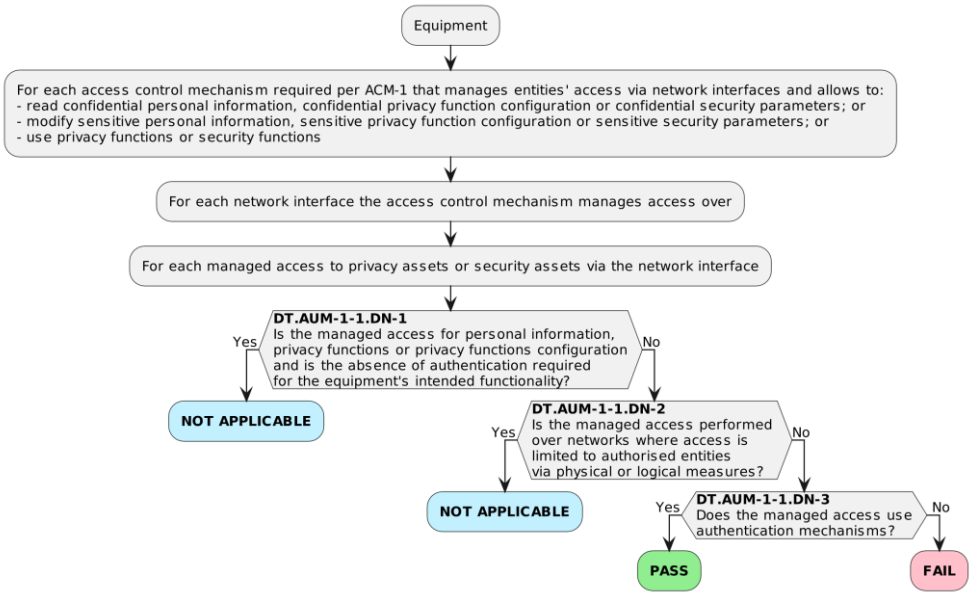
5.2.1.1 Conceptual assessment

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,

— read confidential personal information, confidential privacy function configuration or confidential security parameters; or
— modify sensitive personal information, sensitive privacy function configuration or sensitive security parameters; or
— use privacy functions or security functions,

except for access:

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



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [AUM-1-1.ACM]. Access control mechanisms required per ACM-1 use authentication mechanisms for managing entities' access. Therefore, managed access use AUM mechanism.	Pass

5.2.1.2 Functional completeness assessment

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.ACM].

Comments	Verdict
The laboratory testing engineer verified that DUT has no other ACM mechanism to access network and security assets without going through AUMs.	Pass

5.2.1.3 Functional sufficiency assessment

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

Comments	Verdict
The laboratory testing engineer verified that the AUMs meet the requirements. As shown in ID02 Access Control Mechanisms and ID03 Authentication Mechanisms.	Pass

5.2.2 [AUM-1-2] Requirement user interface

5.2.2.1 Conceptual assessment

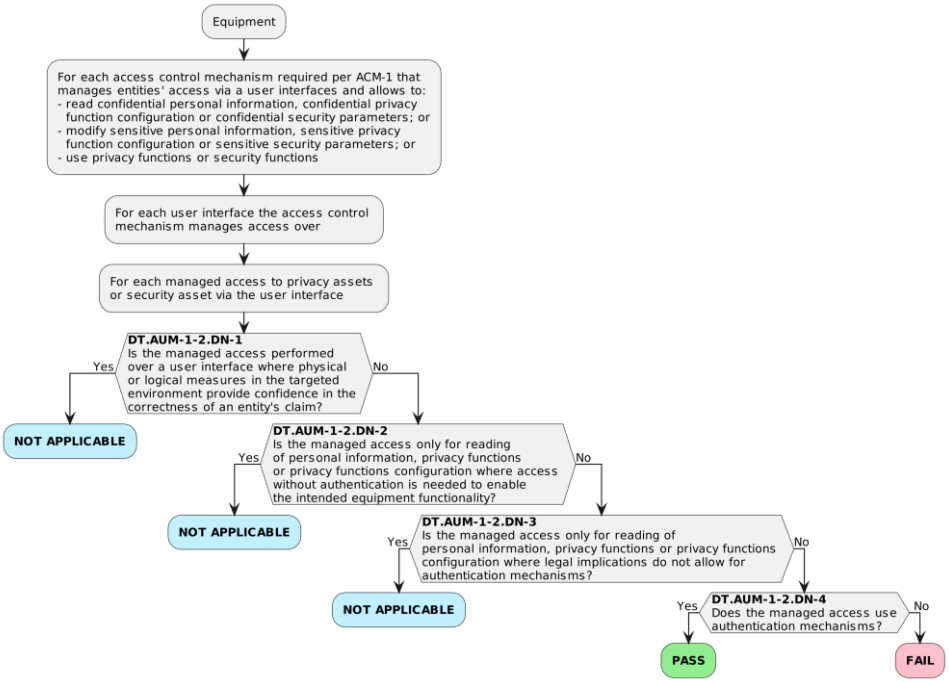
Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to:

— 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,

— read confidential personal information, confidential privacy function configuration or confidential security parameters; or
— modify sensitive personal information, sensitive privacy function configuration or sensitive security parameters; or
— use privacy 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 personal information,network functions, privacy functions or privacy function configuration where access without authentication is needed:
— to enable the intended equipment functionality or
— because legal implications do not allow for authentication mechanisms.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [AUM-1-2.ACM]. Access control mechanisms required per ACM-1 use authentication mechanisms for managing entities' access.	Pass

5.2.2.2 Functional completeness assessment

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.ACM].

Comments	Verdict
The laboratory testing engineer verified that DUT has no other ACM mechanism to access network and security assets without going through AUMs.	Pass

5.2.2.3 Functional sufficiency assessment

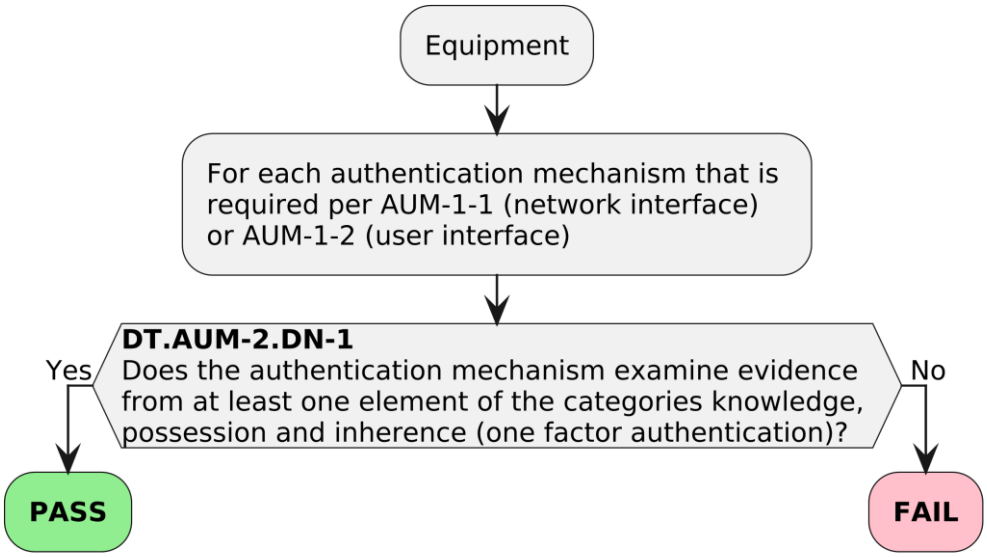
The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1 are implemented.

Comments	Verdict
The laboratory testing engineer verified that the authentication mechanism meets the requirements. As shown in ID02 Access Control Mechanisms and ID03 Authentication Mechanisms.	Pass

5.2.3 [AUM-2] Appropriate authentication mechanisms

5.2.3.1 Conceptual assessment

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).



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [AUM-2.AUM]. At least one factor authentication is used by AUMs.	Pass

5.2.3.2 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.

5.2.3.3 Functional sufficiency assessment

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

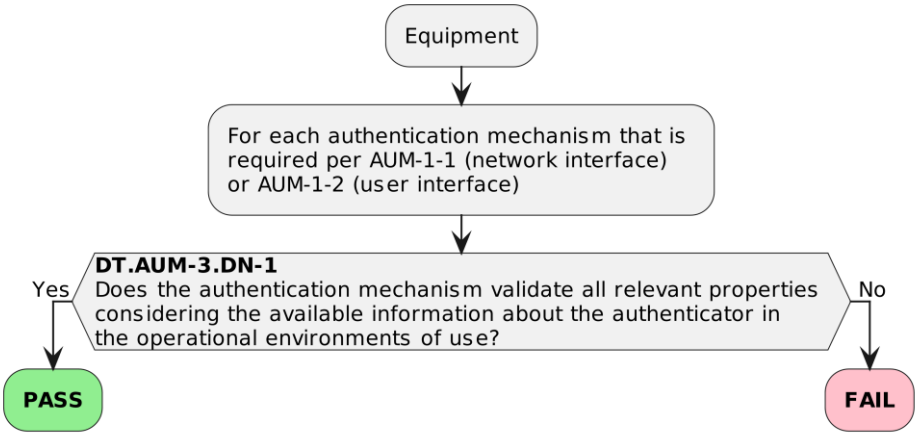
Comments	Verdict
Testers evaluate the AUM performs at least one authentication and check if the authentication mechanism is implemented as recorded. The detailed testing process can be found in ID03 Authentication Mechanisms.	Pass

5.2.4 [AUM-3] Authenticator validation

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.

5.2.4.1 Conceptual assessment

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 network assets,security assets and/or privacy assets required by AUM-1- 1 or AUM-1-2.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [AUM-3.AUM]. The authentication mechanisms validate all relevant properties considering the available information about the authenticator in the operational environments of use.	Pass

5.2.4.2 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.

5.2.4.3 Functional sufficiency assessment

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.

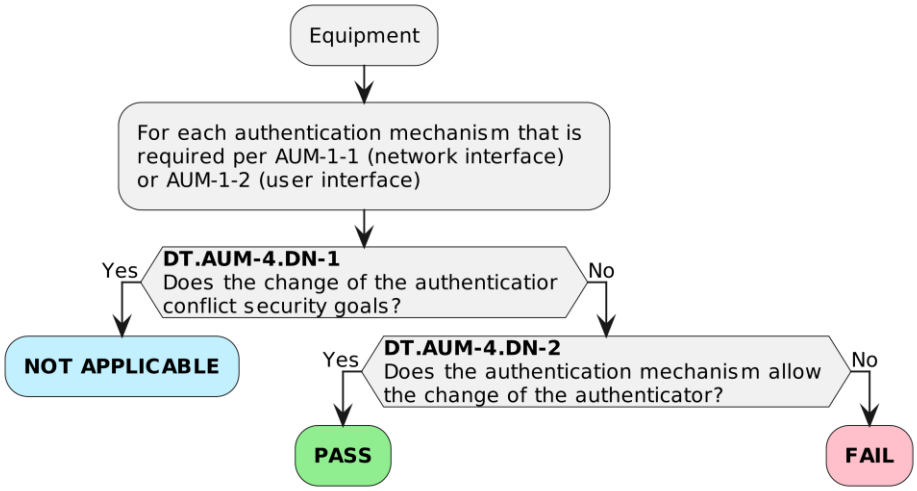
Comments	Verdict
The testers tried logging in with an incorrect password and login failed. After multiple failed logins, it is verified that the account verification mechanisms are effective, as shown in ID03 Authentication Mechanisms.	Pass

5.2.5 [AUM-4] Changing authenticators

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.

5.2.5.1 Conceptual assessment

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.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [AUM-4.AUM]. Meanwhile, according to the analysis of the technical document, the device user can modify and update credentials.	Pass

5.2.5.2 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.

5.2.5.3 Functional sufficiency assessment

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].

Comments	Verdict
For authentication mechanisms, the testers conducted modification test and verified that the product has the appropriate function to change the authenticators. As shown in ID04 Change Authenticators.	Pass

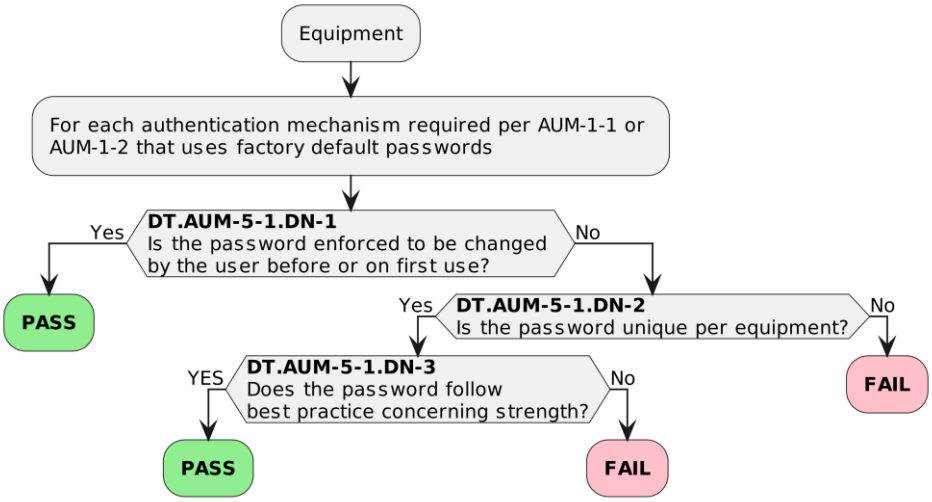
5.2.6 [AUM-5-1] Requirement for factory default passwords

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.

5.2.6.1 Conceptual assessment

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.



Comments	Verdict
When registering for application and platform the first time, users must set their own passwords. When connecting the device via Bluetooth for the first time, after entering the default password "1234" in the app interface, the user will be forced to set a password by themselves immediately. Therefore, the default factory password does not apply to the device.	Pass

5.2.6.2 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.

5.2.6.3 Functional sufficiency assessment

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.

Comments	Verdict
When registering for application and platform the first time, users must set their own passwords. When connecting the device via Bluetooth for the first time, after entering the default password "1234" in the app interface, the user will be forced to set a password by themselves immediately. Therefore, the default factory password does not apply to the device.	Pass

5.2.7 [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

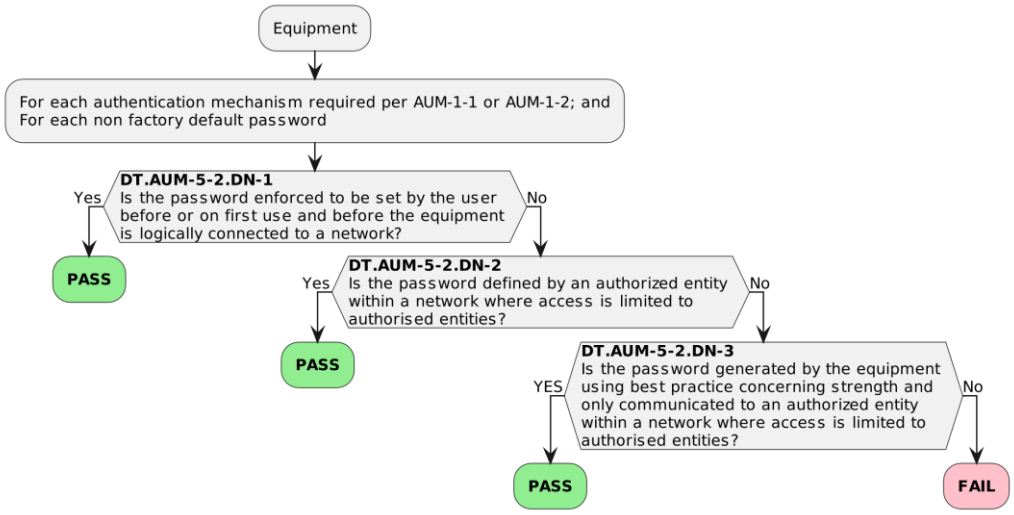
— be defined by an authorized entity within a network where access is limited to authorised entities; or

— 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 can choose to not use any password.

5.2.7.1 Conceptual assessment

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.



Comments	Verdict
When registering for application and platform the first time, users must set their own passwords. When connecting the device via Bluetooth for the first time, after entering the default password "1234" in the app interface, the user will be forced to set a password by themselves immediately. The complexity requirements for passwords are : Supports 8-16 characters, a combination of numbers and letters. Therefore, the device meets the requirements.	Pass

5.2.7.2 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.

5.2.7.3 Functional sufficiency assessment

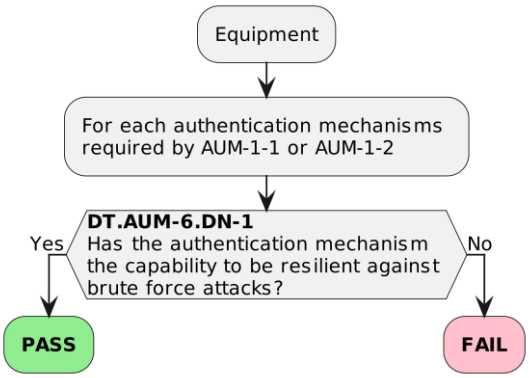
The purpose of this assessment case is the functional assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 are implemented as required per AUM-5-2.

Comments	Verdict
When registering for application and platform the first time, users must set their own passwords. When connecting the device via Bluetooth for the first time, after entering the default password "1234" in the app interface, the user will be forced to set a password by themselves immediately. The complexity requirements for passwords are : Supports 8-16 characters, a combination of numbers and letters. As shown in ID02 Access Control Mechanisms, ID03 Authentication Mechanisms and ID05 Complexity of Password.	Pass

5.2.8 [AUM-6] Brute force protection

5.2.8.1 Conceptual assessment

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 per AUM-6.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [AUM-6.AUM]. For user authentication, after multiple failed logins, it is verified that the account verification mechanism will be activated.	Pass

5.2.8.2 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.

5.2.8.3 Functional sufficiency assessment

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.

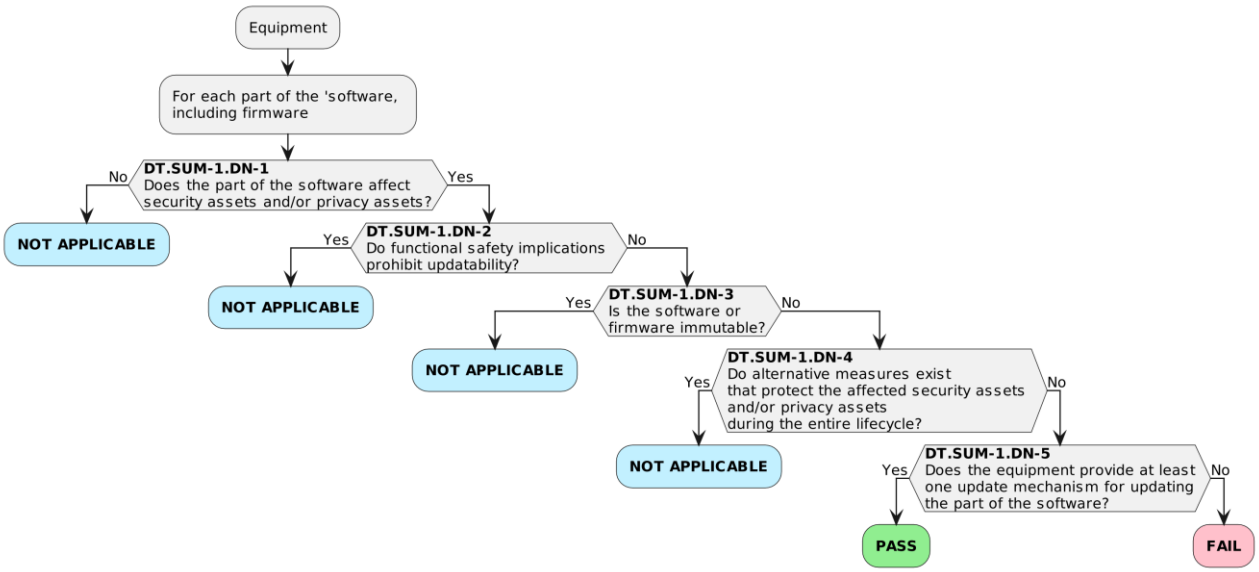
Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [AUM-6.AUM]. After multiple failed logins, it is verified that the account verification mechanism will be activated, as shown in ID06 Bruce Force Protection.	Pass

5.3 [SUM] Secure update mechanism

5.3.1 [SUM-1] Applicability of update mechanisms

5.3.1.1 Conceptual assessment

The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets,network assets and/or privacy 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 privacy assets during the entire lifecycle of the equipment.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [SUM-1.PartOfSW]. It is confirmed that the firmware is updatable. Based on the conceptual analysis of the technical document above, the corresponding SUMs have been determined as Pass.	Pass

5.3.1.2 Functional completeness assessment

None.

5.3.1.3 Functional sufficiency assessment

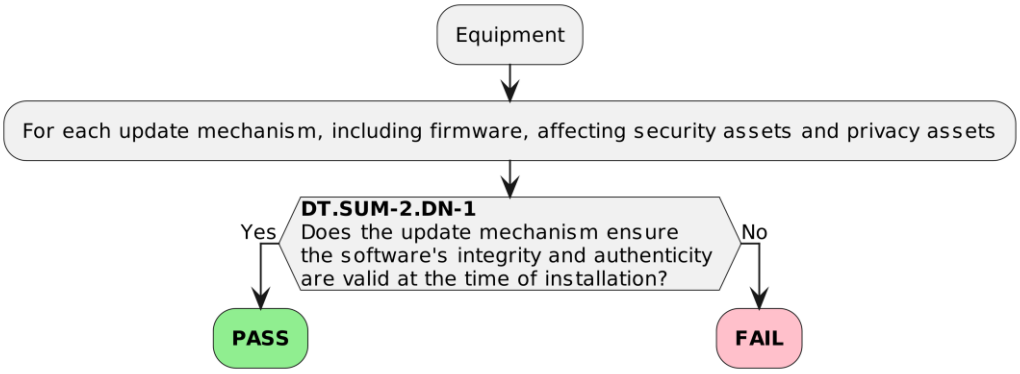
The purpose of this assessment case is the functional assessment whether the equipment supports update mechanisms for parts of the software affecting security assets,network assets and/or privacy assets as documented in [E.Info.SUM-1.PartOfSoftw.SUM].

Comments	Verdict
The testers conducted mechanism testing on the update mechanism and found that the firmware is updatable. As shown in ID07 Secure Update Mechanism.	Pass

5.3.2 [SUM-2] Secure updates

5.3.2.1 Conceptual assessment

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



Comments	Verdict
According to ID01 TechnicalDoc_AC Charger, the upgrade package has been firmware signed to verify the authenticity and integrity.	Pass

5.3.2.2 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.

5.3.2.3 Functional sufficiency assessment

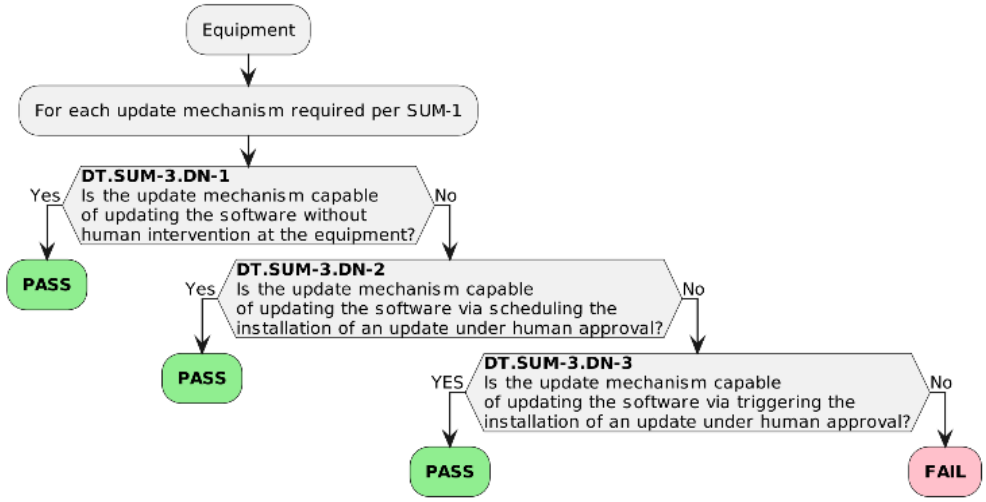
The purpose of this assessment case is the functional assessment whether the update mechanisms for parts of the software affecting security assets,network assets and/or privacy assets only install software whose integrity and authenticity are valid at the time of the installation as documented in [E.Info.SUM-2.SUM].

Comments	Verdict
The testers found that after deleting the digital signature file from the software package and attempted to use the unsigned incomplete software package but failed. Testers found that the tampered with the digital signature file of the target update software package and attempted to use the software package with the tampered signature but failed. As shown in ID08 The Integrity Verification and ID09 The Authenticity Verification. Therefore, both the integrity and the authenticity firmware protection are effective.	Pass

5.3.3 [SUM-3] Automated updates

5.3.3.1 Conceptual assessment

When the equipment is internet-connected, 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.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [SUM-3.SUM]. It is declared that the upgrade mechanisms require limited manual activation to begin.	Pass

5.3.3.2 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.

5.3.3.3 Functional sufficiency assessment

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

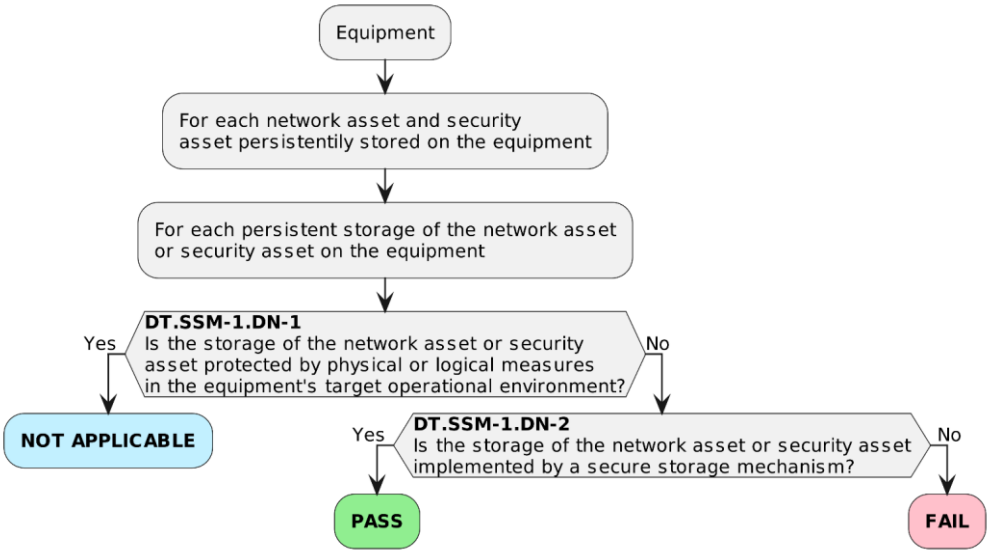
Comments	**Verdict**
The upgrade mechanisms require limited manual approval to upgrade the device. As shown in the ID07 Secure Update Mechanism.	**Pass**

5.4 [SSM] Secure storage mechanism

5.4.1 [SSM-1] Applicability of secure storage mechanisms

5.4.1.1 Conceptual assessment

The equipment shall always use secure storage mechanisms for protecting the security assets,network assets and privacy assets persistently stored on the equipment, except for persistently stored security assets,network assets and privacy assets where:
— the physical or logical measures in the target environment ensures the security asset,network assets or privacy asset stored on the equipment accessibility is limited to authorized entities.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [SSM-1.SecAsset] and [SSM-1.NetAsset]. The relevant assets are securely stored by the access control, hardware protection and encryption.	Pass

5.4.1.2 Functional completeness assessment

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

Comments	Verdict
The laboratory testers investigated the relevant assets. Suitable secure storage mechanism are selected to these assets.	Pass

5.4.1.3 Functional sufficiency assessment

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

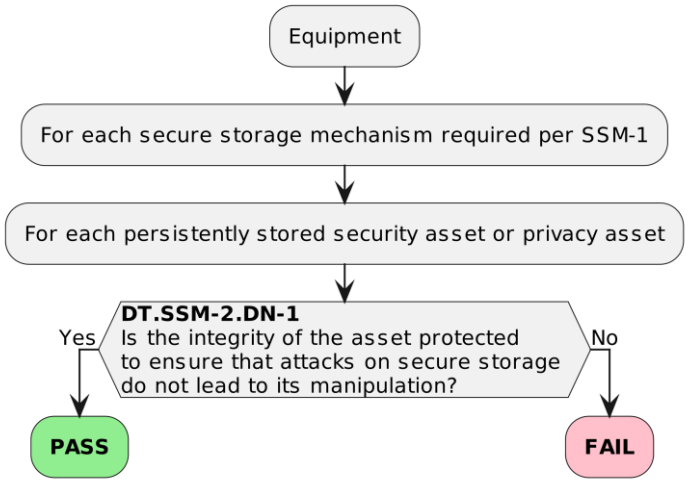
Comments	Verdict
The testers attempted to verify that the relevant assets listed in the technical document are stored appropriately. No one can obtain the internal development tool after it leaves the factory. The main secure storage methods are encryption and hardware protection, which makes it difficult for testers to recognize the stored content. As shown in ID10 Secure Storage Mechanism.	Pass

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

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

5.4.2.1 Conceptual assessment

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.



Comments	Verdict
The testers reviewed the ID01 TechnicalDoc_AC Charger. As per the analysis results, the secure storage mechanisms selected meet the requirements of this clause.	Pass

5.4.2.2 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.

5.4.2.3 Functional sufficiency assessment

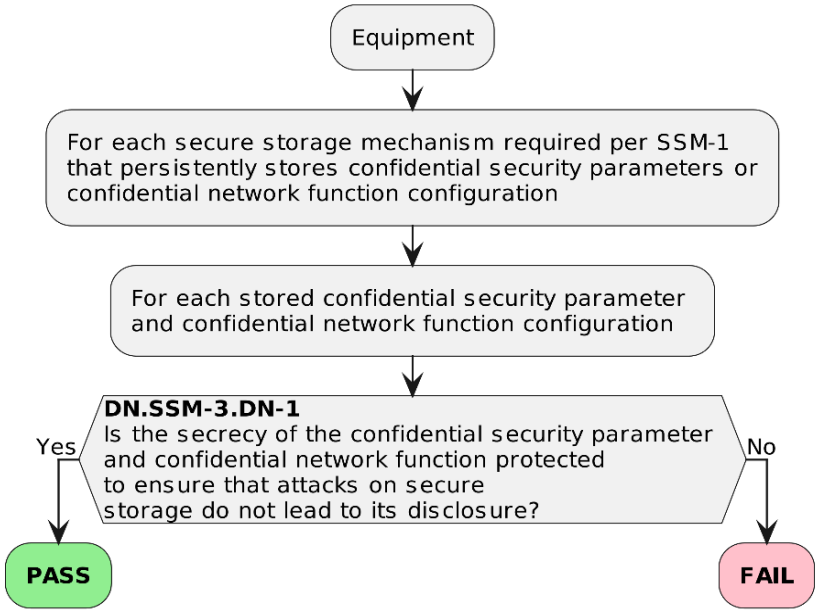
The purpose of this assessment case is the functional assessment whether the secure storage mechanisms required per SSM-1 provide the required integrity protection.

Comments	Verdict
The testers confirmed that the relevant assets could be stored securely. Secure storage mechanisms can guarantee the security of assets. As shown in ID10 Secure Storage Mechanism.	Pass

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

Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential personal information, confidential privacy function configuration, and confidential security parameter persistently stored on the equipment

5.4.3.1 Conceptual assessment



Comments	**Verdict**
The testers reviewed the ID01 TechnicalDoc_AC Charger. As per the analysis results, the secure storage mechanisms selected meet the requirements of this clause.	**Pass**

5.4.3.2 Functional completeness assessment

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

Comments	**Verdict**
Testers reviewed and referred to the manual to confirm the functions and parameters need to be securely stored. These can correspond to the list of assets that require persistent storage listed in [SSM-3.SSM].	**Pass**

5.4.3.3 Functional sufficiency assessment

Comments	Verdict
Through SSM-1 testing, it was found that the relevant assets are stored in the DUT securly. It is verified that the secure storage mechanisms can ensure the integrity of the relevant assets. As shown in ID10 Secure Storage Mechanism.	Pass

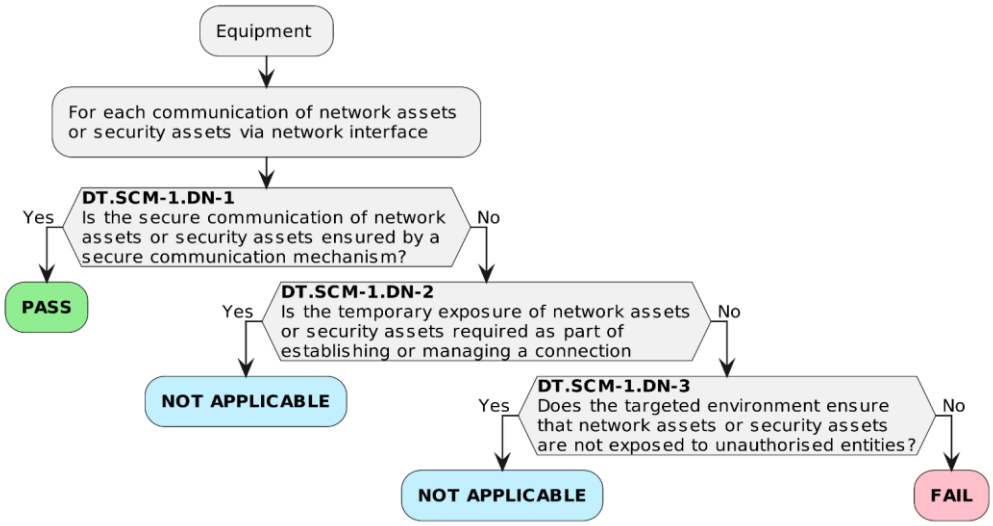
5.5 [SCM] Secure communication mechanism

5.5.1 [SCM-1] Applicability of secure communication mechanisms

The equipment shall always use secure communication mechanisms for communicating security assets,network assets and privacy assets with other entities via network interfaces, except for:
— communicating security assets,network assets or privacy assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that security assets or privacy 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.

5.5.1.1 Conceptual assessment



Comments	Verdict
The testers reviewed the ID01 TechnicalDoc_AC Charger [SCM-1.SCM]. The tester confirmed that the security assets and network assets use the suitable communication protocol to transfer. According to the technical document results, relevant communication mechanisms rely on encryption protection and meet the requirements.	Pass

5.5.1.2 Functional completeness assessment

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

Comments	Verdict
The testing engineer checked the various communication functions of the ID13 User Manual. Based on the network connection scan results ID12 Ports Scan, the testers confirmed that corresponding assets have been included in the communication scenarios listed in ID01 TechnicalDoc_AC Charger.	Pass

5.5.1.3 Functional sufficiency assessment

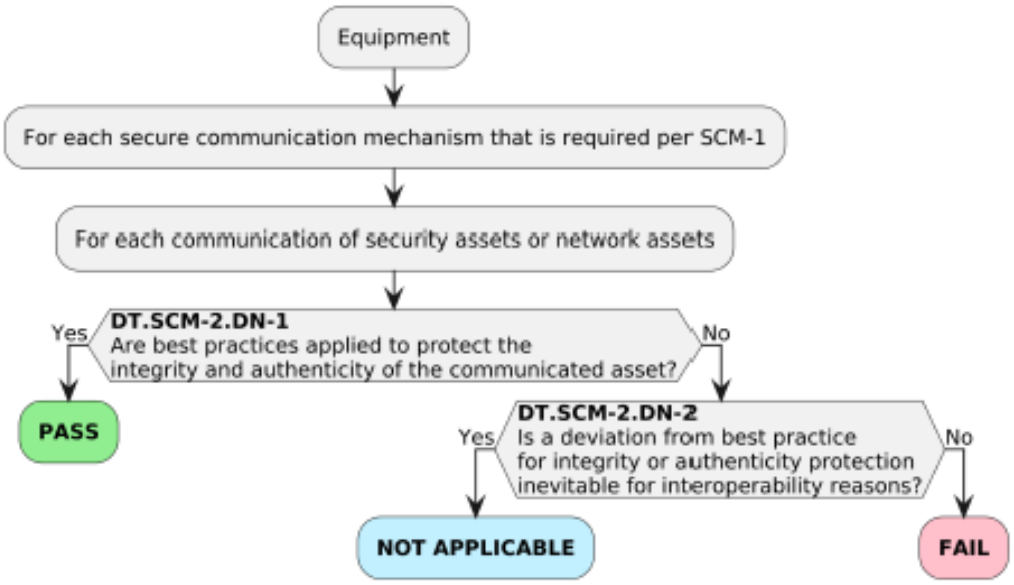
The purpose of this assessment case is the functional assessment whether the secure communication mechanisms are implemented when they are required.

Comments	Verdict
The testing engineer verified the communication methods used by the equipment for asset transmissions. As shown in the result ID11 Secure Communication Mechanisms and ID14 Packet Capture. The corresponding communication mechanisms used secure transmission protection measures.	Pass

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

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 privacy assets communicated, network assets communicated,except for communicating security assets or privacy assets where:
— a deviation from best practice for integrity or authenticity protection is required for interoperability reasons.

5.5.2.1 Conceptual assessment



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [SCM-2.SCM]. Based on the analysis results of the technical document, relevant communication mechanisms are able to protect the authenticity and integrity of the asset without deviating from best practices.	Pass

5.5.2.2 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.

5.5.2.3 Functional sufficiency assessment

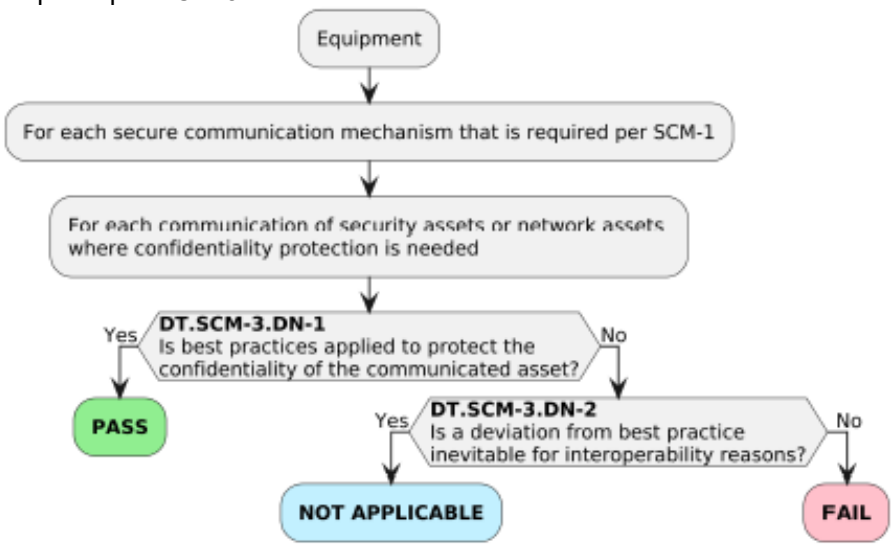
The purpose of this assessment case is the functional assessment whether the security assets and privacy assets communicated, network assets communicated are protected against unnoticed tampering.

Comments	Verdict
The testers verified the integrity protection mechanism of various communication methods and found that the device has appropriate communication mechanism. As shown in ID11 Secure Communication Mechanisms and ID14 Packet Capture.	Pass

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

5.5.3.1 Conceptual assessment

The purpose of this assessment case is the conceptual assessment whether each secure communication mechanism of the equipment is protecting the confidentiality of privacy assets (documented in [E.Info.SCM-3.PrivacyAsset]),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.



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [SCM-3.SCM]. Relevant communication mechanisms are the best practices.	Pass

5.5.3.2 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.

5.5.3.3 Functional sufficiency assessment

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

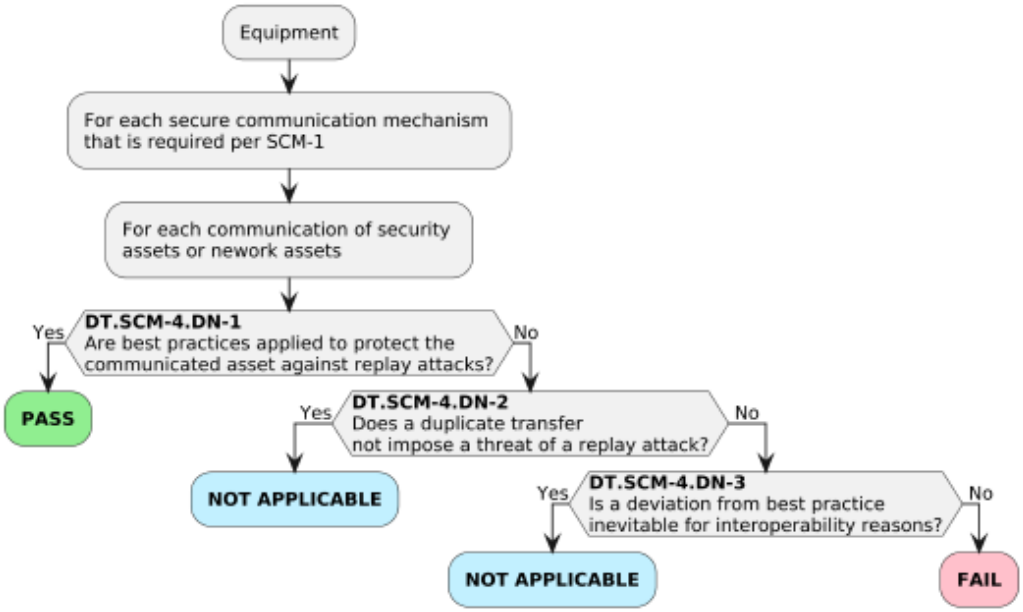
Comments	Verdict
Relevant communication mechanisms rely on encryption frameworks to complete and meet the best practices. Therefore, the communication mechanism can ensure the confidentiality of transmission.	Pass

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

5.5.4.1 Conceptual assessment

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



Comments	**Verdict**
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [SCM-4.SCM]. The relevant communication mechanisms of the device are using the current best practices in the industry.	**Pass**

5.5.4.2 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.

5.5.4.3 Functional sufficiency assessment

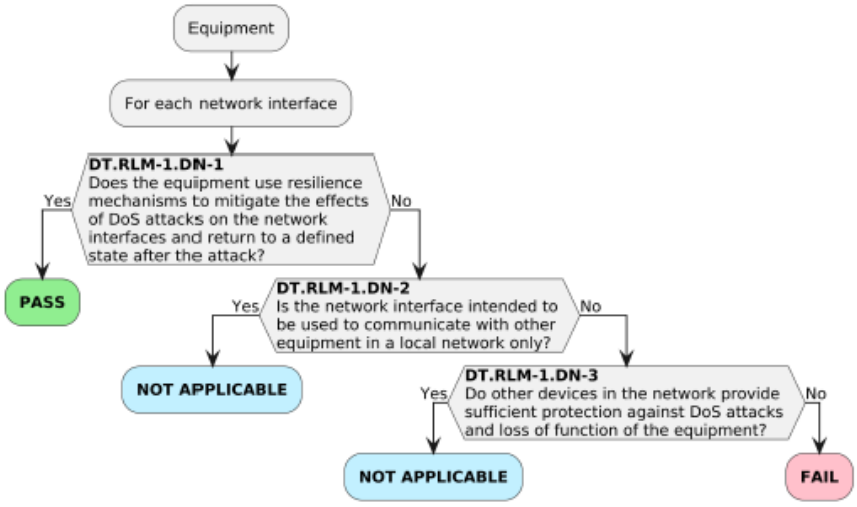
Comments	Verdict
It is confirmed that the corresponding secure communication mechanisms are using the current best practices in the industry. As shown in ID11 Secure Communication Mechanisms and ID14 Packet Capture.	Pass

5.6 [RLM] Resilience mechanism

5.6.1 [RLM-1] Applicability and appropriateness of resilience mechanisms

5.6.1.1 Conceptual assessment

The purpose of this assessment case is the conceptual assessment whether a resilience mechanism is implemented when it is required per RLM-1.



Comments	Verdict
The device depends on the access control lists (ACLs) of home routers, firewalls, and cloud brokers for protection against denial-of-service (DoS) attacks.	N/A

5.6.1.2 Functional completeness assessment

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.

Comments	Verdict
The device depends on the access control lists (ACLs) of home routers, firewalls, and cloud brokers for protection against denial-of-service (DoS) attacks.	**N/A**

5.6.1.3 Functional sufficiency assessment

The purpose of this assessment case is the functional assessment whether the resilience mechanisms are implemented when required per RLM-1.

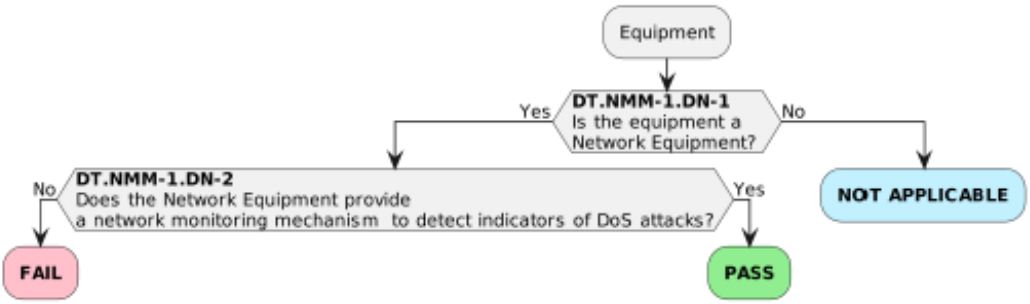
Comments	Verdict
The device depends on the access control lists (ACLs) of home routers, firewalls, and cloud brokers for protection against denial-of-service (DoS) attacks.	**N/A**

5.7 [NMM] Network monitoring mechanism

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

5.7.1.1 Conceptual assessment

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.



Comments	**Verdict**
The equipment is not network equipment.	**N/A**

5.7.1.2 Functional completeness assessment

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

5.7.1.3 Functional sufficiency assessment

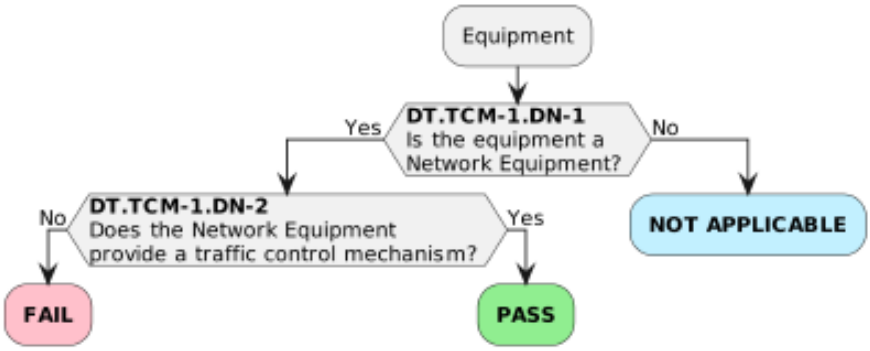
Comments	**Verdict**
The equipment is not network equipment.	**N/A**

5.8 [TCM] Traffic control mechanism

5.8.1 [TCM-1] Applicability of and appropriate traffic control mech

5.8.1.1 Conceptual assessment

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.



Comments	Verdict
The equipment is not network equipment.	**N/A**

5.8.1.2 Functional completeness assessment

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

5.8.1.3 Functional sufficiency assessment

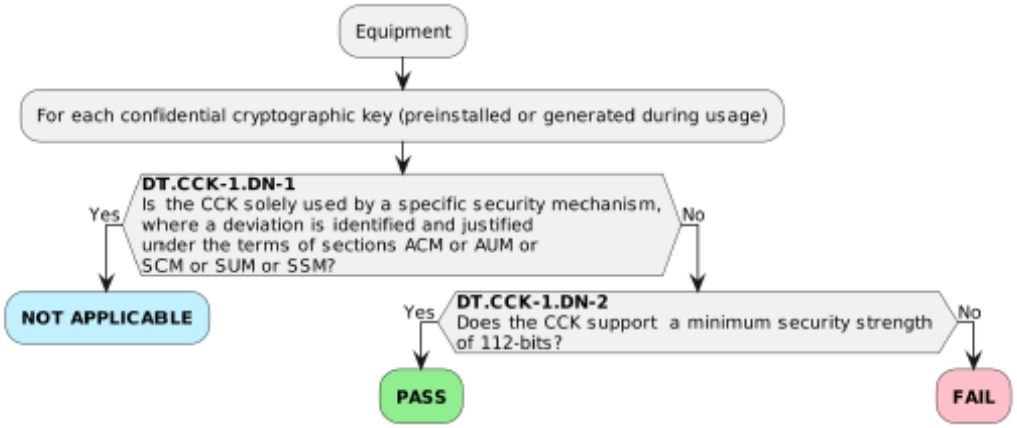
Comments	Verdict
The equipment is not network equipment.	**N/A**

5.9 [CCK] Confidential cryptographic keys

5.9.1 [CCK-1] Appropriate CCKs

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.

5.9.1.1 Conceptual assessment



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc AC Charger [CCK-1.CCK]. The scenarios where the device use keys to protect network/security assets are listed. According to asset analysis and decision tree results, the minimum supported key strength is not less than 112 bits.	Pass

5.9.1.2 Functional completeness assessment

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

Comments	Verdict
According to the definition of CCK and the anaysis of the asset information. The usage requirements that require keys have corresponding keys, and the list of CCKs is complete.	Pass

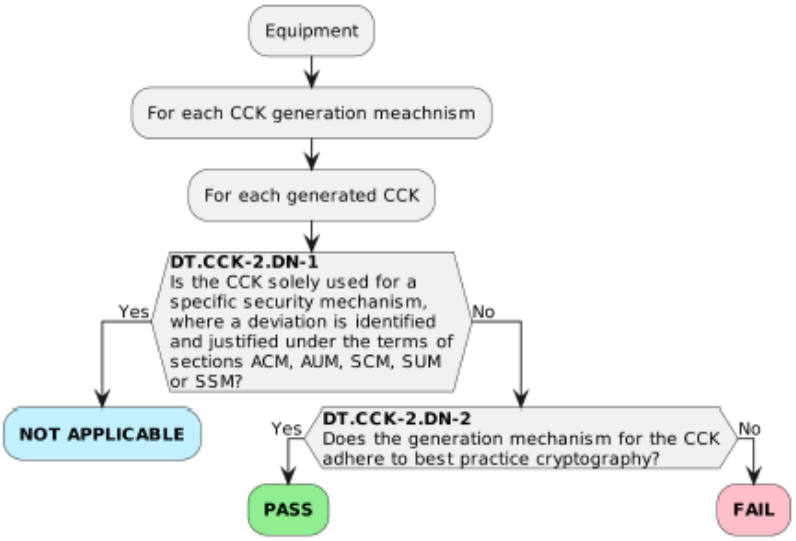
5.9.1.3 Functional sufficiency assessment

Comments	Verdict
The testers verified the existence and strength of types of keys, examined the data packets for the parts that could be sniffed. As shown in ID11 Secure Communication Mechanisms and ID14 Packet Capture.	Pass

5.9.2 [CCK-2] CCK generation mechanisms

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.

5.9.2.1 Conceptual assessment



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc AC Charger [CCK-2.Generation] and [CCK-2.CCK]. The generation of secure keys follows the SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, which ensures that the generation follows best practices and has sufficient randomness and security. As shown in ID15 SOGIS-Agreed-Cryptographic-Mechanisms-1.3.1.	Pass

5.9.2.2 Functional completeness assessment

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].

Comments	Verdict
It is confirmed that generation mechanisms for confidential cryptographic keys on the equipment are documented in [CCK-2.Generation].	Pass

5.9.2.3 Functional sufficiency assessment

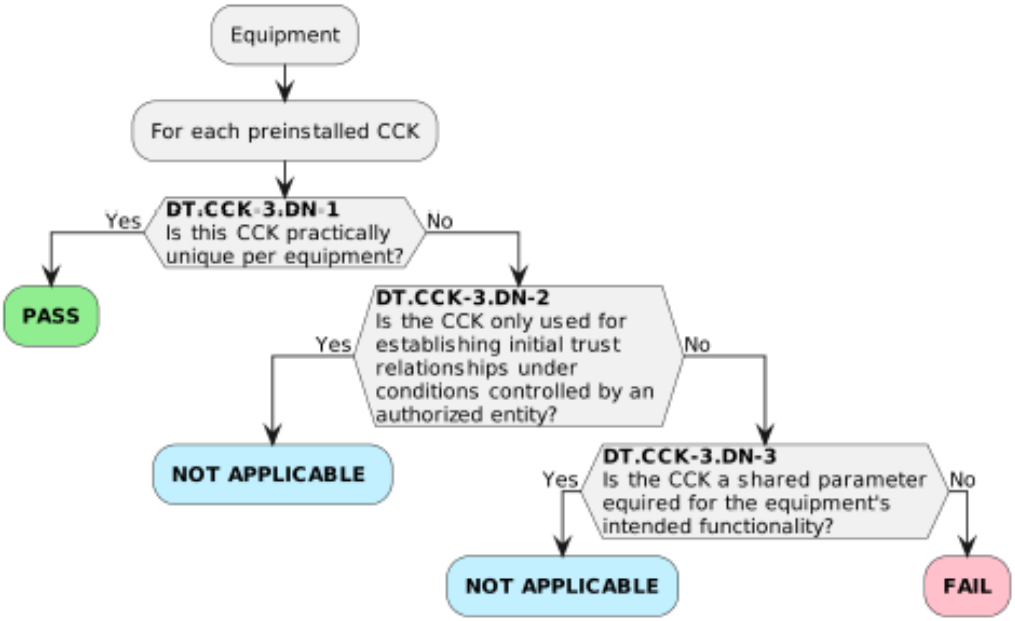
Comments	Verdict
Based on the ID15 SOGIS-Agreed-Cryptographic-Mechanisms-1.3.1, the used entropy source can meet the security requirements of upper level cryptographic algorithm applications.	Pass

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

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 that are shared parameters required for the equipment's intended functionality.

5.9.3.1 Conceptual assessment



Comments	**Verdict**
The testing engineer reviewed the ID01 TechnicalDoc AC Charger [CCK-3.CCK]. The manufacturer declares that there is no preinstalled CCK in the device. Therefore, it is not applicable.	**N/A**

5.9.3.2 Functional completeness assessment

The purpose of this assessment case is the functional assessment whether all preinstalled CCKs are documented.

Comments	**Verdict**
The testing engineer reviewed the ID01 TechnicalDoc AC Charger [CCK-3.CCK]. The manufacturer declares that there is no preinstalled CCK in the device. Therefore, it is not applicable.	**N/A**

5.9.3.3 Functional sufficiency assessment

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.

Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [CCK-3.CCK]. The manufacturer declares that there is no preinstalled CCK in the device. Therefore, it is not applicable.	**N/A**

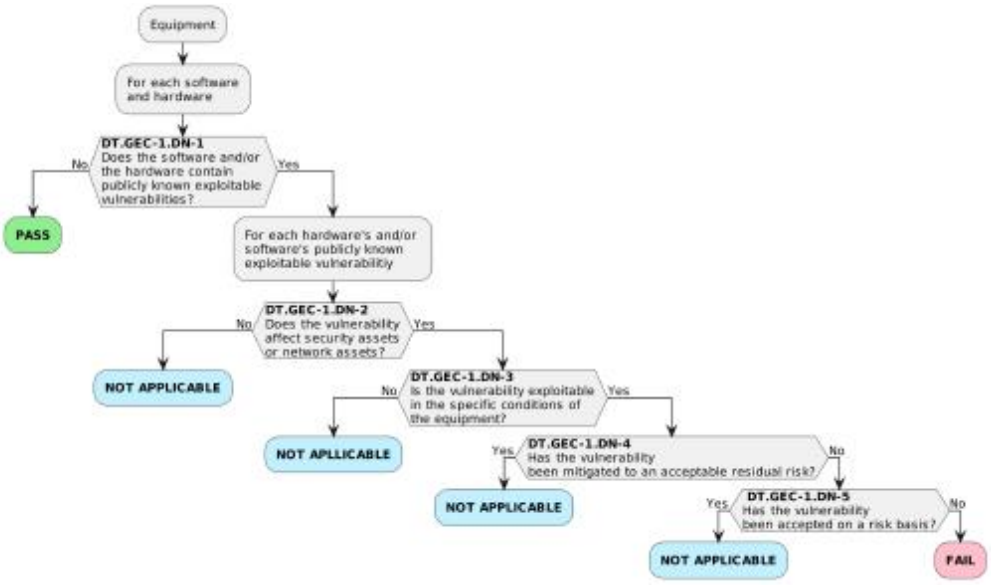
5.10 [GEC] General equipment capabilities

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

The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets,network assets and privacy 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.

5.10.1.1 Conceptual assessment

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 privacy assets or security assets, if exploited as required per GEC-1.



Comments	Verdict
According to ID01 TechnicalDoc_AC Charger [GEC-1.ListVuln], the tester continued to review the GEC-1 sheet of the ID01. The manufacturer claimed that the GEC-1 meets the requirements.	Pass

5.10.1.2 Functional completeness assessment

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 privacy assets,network assets or security assets are only those listed in [E.Info.GEC-1.ListOfVulnerabilities].

Comments	Verdict
Testers used the vulnerability scanning tool Nessus to scan the DUT and found the result is consistent with what the manufacturer claimed.	Pass

5.10.1.3 Functional sufficiency assessment

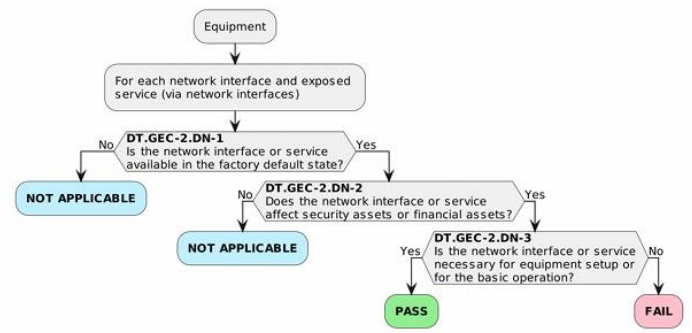
The purpose of this assessment case is the functional assessment if the vulnerabilities present in the equipment which are listed in [E.Info.GEC-1.ListOfVulnerabilities] are not able to affect security assets,network assets or privacy assets, if exploited.

Comments	Verdict
The tester reviewed manufacturer's analysis and the scan report, which can prove that there is no publicly known exploitable vulnerabilities and meet the GEC-1 requirements. As shown in ID17 Scan Report and ID18 Analysis Report.	Pass

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

In factory default state the equipment shall only expose
— network interfaces; and
— services via network interfaces
affecting security assets,network assets and privacy assets which are necessary for equipment setup or for basic operation of the equipment.

5.10.2.1 Conceptual assessment



Comments	**Verdict**
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [GEC-2.NetIntfAndServ]. The interfaces that are turned on are necessary for network services and device configuration. Therefore, the analysis of technical document meets the requirements. Only necessary interfaces that are used are open and available.	Pass

5.10.2.2 Functional completeness assessment

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.

Comments	Verdict
According to ID01 TechnicalDoc_AC Charger, two network interfaces are enabled by default, and the relevant services are exposed by default. It is confirmed that the device only exposes the necessary interfaces and services. As shown in ID12 Ports Scan and ID13 User Manual.	Pass

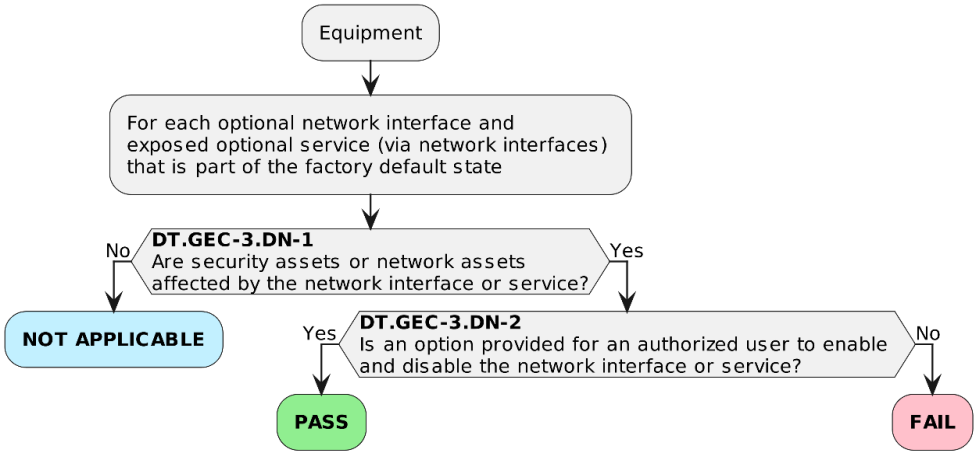
5.10.2.3 Functional sufficiency assessment

Not applicable.

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

Optional network interfaces or optional services exposed via network interfaces affecting security assets,network assets or privacy 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.

5.10.3.1 Conceptual assessment



Comments	Verdict
The testing engineer reviewed the ID01 TechnicalDoc_AC Charger [GEC-3.NetIntfAndServ]. It is examined both network interfaces and found that the default closed and other optional interfaces were not in the default state. The interfaces that must be enabled by default have been analyzed by the technical document and their optional configuration functions are explained in the application manual.	Pass

5.10.3.2 Functional completeness assessment

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.

Comments	Verdict
It is verified that the user documentations include the exposed interfaces and services. As shown in ID12 Ports Scan, ID13 User Manual and ID16 App_User Manual.	Pass

5.10.3.3 Functional sufficiency assessment

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.

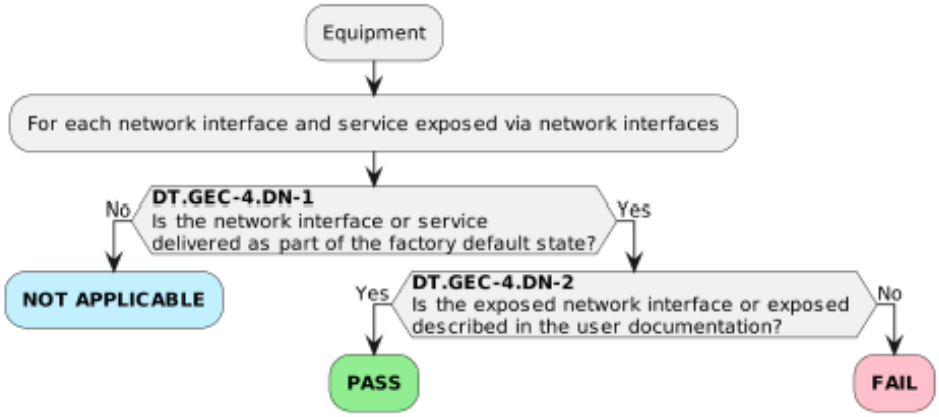
Comments	Verdict
It is verified that the exposed interfaces and services on the factory default state are documented in the user documentation. Other optional interfaces and services which are disabled by default can be configurated via the application. As shown in ID12 Ports Scan, ID13 User Manual and ID16 App_User Manual.	Pass

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

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.

5.10.4.1 Conceptual assessment



Comments	Verdict
The tester reviewed the GEC-4 sheet of the ID01 TechnicalDoc_AC Charger. Testers check the content of the user manual. The exposed interfaces and services are described, except for the service that are disabled by default.	Pass

5.10.4.2 Functional completeness assessment

Comments	Verdict
The exposed interfaces and services are described in the user manual. As shown in ID13 User Manual and ID16 App_User Manual.	Pass

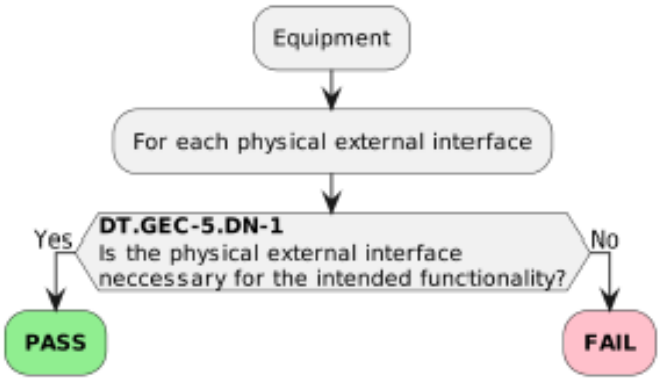
5.10.4.3 Functional sufficiency assessment

None.

5.10.5 [GEC-5] No unnecessary external interfaces

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

5.10.5.1 Conceptual assessment



Comments	Verdict
According to GEC-5 sheet of the ID01 TechnicalDoc_AC Charger and the user manual, there is no unnecessary external interface.	Pass

5.10.5.2 Functional completeness assessment

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].

Comments	Verdict
According to GEC-5 sheet of the ID01 TechnicalDoc_AC Charger and the user manual, there is no unnecessary external interface.	Pass

5.10.5.3 Functional sufficiency assessment

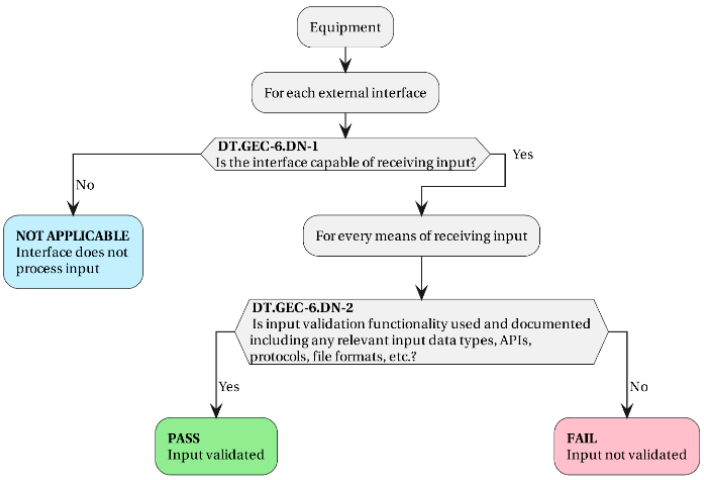
Not applicable.

5.10.6 [GEC-6] Input validation

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

5.10.6.1 Conceptual assessment

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,network assets and/or privacy assets against common attacks considering the intended functionality of the equipment as required per GEC-6.



Comments	Verdict
According to the GEC-6 sheet of the ID01 TechnicalDoc_AC Charger, the uploaded upgrade package and the password set will be verified for compliance with the rules.	Pass

5.10.6.2 Functional completeness assessment

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.

Comments	Verdict
The interface for verifying data input by testers only involves the upgrade interface and account modification interface.	Pass

5.10.6.3 Functional sufficiency assessment

The purpose of this assessment case is the functional assessment of the techniques to verify the implementation of the documented techniques.

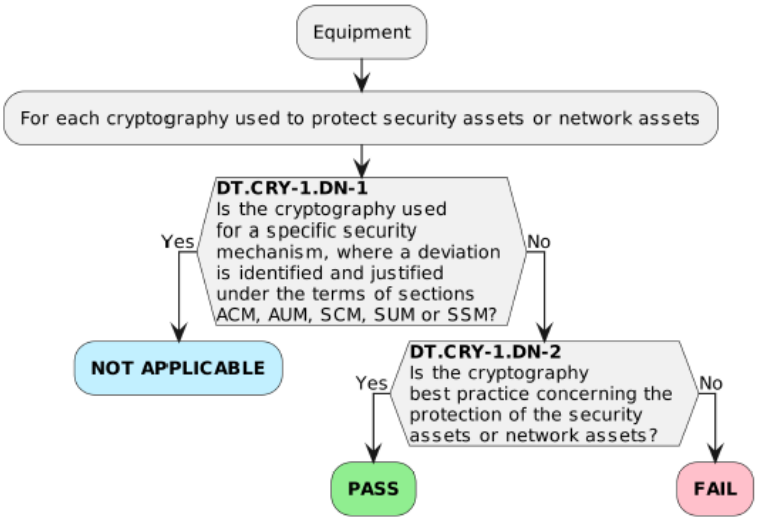
Comments	Verdict
The tester upgraded and set the password, and confirmed the input verification mechanism, as shown in evidence ID02 Access Control Mechanisms, ID08 The Integrity Verification and ID09 The Authenticity Verification.	Pass

5.11 [CRY] Cryptography

5.11.1 [CRY-1] Best practice cryptography

The equipment shall use best practice for cryptography that is used for the protection of the security assets,network assets or privacy 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.

5.11.1.1 Conceptual assessment



Comments	Verdict
According to ID01 TechnicalDoc_AC Charger [CRY-1.Assets], all encryption algorithms are used in accordance with best practices.	Pass

5.11.1.2 Functional completeness assessment

The purpose of this assessment case is the functional assessment whether the documentation in [E.Info.CRY-1.Assets.Cryptography] is complete.

Comments	Verdict
No unknown encryption algorithm or encryption strength exists.	Pass

5.11.1.3 Functional sufficiency assessment

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.

Comments	Verdict
The tester conducted algorithm retrieval during the trial process, and the results are shown in CCK, which conforms to the listing of assets and best practices. As shown in ID11 Secure Communication Mechanisms and ID14 Packet Capture.	Pass

END