

Prüfbericht-Nr.: <i>Test report no.:</i>	CN26OVPS 001	Auftrags-Nr.: <i>Order no.:</i>	326188271 P02434245	Seite 1 von 24 Page 1 of 24
Kunden-Referenz-Nr.: <i>Client reference no.:</i>	2089836	Auftragsdatum: <i>Order date:</i>	2026-05-21	
Auftraggeber: <i>Client:</i>	Pylon Technologies Co., Ltd. No.300, Miaoqiao Road, Kangqiao Town, Pudong New Area, 201315 Shanghai, P.R. China			
Prüfgegenstand: <i>Test item:</i>	LFP Lithium Ion Energy Storage Battery System			
Bezeichnung / Typ-Nr.: <i>Identification / Type no.:</i>	RM-15, RM-22, RM-30, RM-37, RM-45, RM-52, RM-60, RM-67, RM-75; RM-15-Pro, RM-22-Pro, RM-30-Pro, RM-37-Pro, RM-45-Pro, RM-52-Pro, RM-60-Pro, RM-67-Pro, RM-75-Pro			
Auftrags-Inhalt: <i>Order content:</i>	EN 18031-2 test report			
Prüfgrundlage: <i>Test specification:</i>	EN 18031-2:2024			
Wareneingangsdatum: <i>Date of sample receipt:</i>	2026-07-16			
Prüfmuster-Nr.: <i>Test sample no.:</i>	A004337478-001 to A004337478-005			
Prüfzeitraum: <i>Testing period:</i>	2026-07-15			
Ort der Prüfung: <i>Place of testing:</i>	No. 38 Jingfan Road, Bacheng, Kunshan, Jiangsu, China			
Prüflaboratorium: <i>Testing laboratory:</i>	TÜV Rheinland (Shanghai) Co., Ltd.			
Prüfergebnis*: <i>Test result*:</i>	PASS			
geprüft von: <i>tested by:</i>	Songcheng Bian / Camus Xu		genehmigt von: <i>authorized by:</i>	Ding Guan
Datum: <i>Date:</i>	2026-08-06		Ausstellungsdatum: <i>Issue date:</i>	2026-08-07
Stellung / Position:	Trainee / Project Engineer		Stellung / Position:	Authorizer
Sonstiges / <i>Other:</i>	See the following pages for general product information and comment for details.			
Zustand des Prüfgegenstandes bei Anlieferung: <i>Condition of the test item at delivery:</i>	Test item complete and undamaged			
* Legende:	P(ass) = entspricht o.g. Prüfgrundlage(n)	F(ail) = entspricht nicht o.g. Prüfgrundlage(n)	N/A = nicht anwendbar	N/T = nicht getestet
* Legend:	P(ass) = passed a.m. test specification(s)	F(ail) = failed a.m. test specification(s)	N/A = not applicable	N/T = not tested
Dieser Prüfbericht bezieht sich nur auf das o.g. Prüfmuster und darf ohne Genehmigung der Prüfstelle nicht auszugsweise vervielfältigt werden. Dieser Bericht berechtigt nicht zur Verwendung eines Prüfzeichens. <i>This test report only relates to the above mentioned test sample as. Without permission of the test center this test report is not permitted to be duplicated in extracts. This test report does not entitle to carry any test mark.</i>				

V05

Prüfbericht-Nr.: CN26OVPS 001
Test report no.:

Seite 2 von 24
Page 2 of 24

Absatz Clause	Anforderungen - Prüfungen / Requirements - Tests	Messergebnisse – Bemerkungen/ Measuring results - Remarks	Ergebnis Result
1	Alle eingesetzten Prüfmittel waren zum angegebenen Prüfzeitraum gemäß eines festgelegten Kalibrierungsprogramms unseres Prüfhauses kalibriert. Sie entsprechen den in den Prüfprogrammen hinterlegten Anforderungen. Die Rückverfolgbarkeit der eingesetzten Prüfmittel ist durch die Einhaltung der Regelungen unseres Managementsystems gegeben. Detaillierte Informationen bezüglich Prüfkonditionen, Prüfequipment und Messunsicherheiten sind im Prüflabor vorhanden und können auf Wunsch bereitgestellt werden. <i>The equipment used during the specified testing period was calibrated according to our test laboratory calibration program. The equipment fulfils the requirements included in the relevant standards. The traceability of the test equipment used is ensured by compliance with the regulations of our management system.</i> <i>Detailed information regarding test conditions, equipment and measurement uncertainty is available in the test laboratory and could be provided on request.</i>		
2	Wie vertraglich vereinbart, wurde dieses Dokument nur digital unterzeichnet. Der TÜV Rheinland hat nicht überprüft, welche rechtlichen oder sonstigen diesbezüglichen Anforderungen für dieses Dokument gelten. Diese Überprüfung liegt in der Verantwortung des Benutzers dieses Dokuments. Auf Verlangen des Kunden kann der TÜV Rheinland die Gültigkeit der digitalen Signatur durch ein gesondertes Dokument bestätigen. Diese Anfrage ist an unseren Vertrieb zu richten. Eine Umweltgebühr für einen solchen zusätzlichen Service wird erhoben. <i>As contractually agreed, this document has been signed digitally only. TÜV Rheinland has not verified and unable to verify which legal or other pertaining requirements are applicable for this document. Such verification is within the responsibility of the user of this document. Upon request by its client, TÜV Rheinland can confirm the validity of the digital signature by a separate document. Such request shall be addressed to our Sales department. An environmental fee for such additional service will be charged.</i>		
3	Prüfklausel mit der Note * wurden an qualifizierte Unterauftragnehmer vergeben und sind unter der jeweiligen Prüfklausel des Berichts beschrieben. Abweichungen von Prüfspezifikation(en) oder Kundenanforderungen sind in der jeweiligen Prüfklausel im Bericht aufgeführt. <i>Test clauses with remark of * are subcontracted to qualified subcontractors and described under the respective test clause in the report.</i> <i>Deviations of testing specification(s) or customer requirements are listed in specific test clause in the report.</i>		
4	Die Entscheidungsregel für Konformitätserklärungen basierend auf numerischen Messergebnissen in diesem Prüfbericht basiert auf der "Null-Grenzwert-Regel" und der "Einfachen Akzeptanz" gemäß ILAC G8:2019 und IEC Guide 115:2021, es sei denn, in der auf Seite 1 dieses Berichts genannten angewandten Norm ist etwas anderes festgelegt oder vom Kunden gewünscht. Dies bedeutet, dass die Messunsicherheit nicht berücksichtigt wird und daher auch nicht im Prüfbericht angegeben wird. Zu weiteren Informationen bezüglich des Risikos durch diese Entscheidungsregel siehe ILAC G8:2019. <i>The decision rule for statements of conformity, based on numerical measurement results, in this test report is based on the "Zero Guard Band Rule" and "Simple Acceptance" in accordance with ILAC G8:2019 and IEC Guide 115:2021, unless otherwise specified in the applied standard mentioned on Page 1 of this report or requested by the customer. This means that measurement uncertainty is not taken in account and hence also not declared in the test report. For additional information to the resulting risk based of this decision rule please refer to ILAC G8:2019.</i>		

**TEST REPORT
EN 18031-2**
Common security requirements for radio equipment - Part 2: Radio equipment processing data

Report Number	CN26OVPS 001
Date of issue	To be assigned at issue
Total number of pages	24
Name of Testing Laboratory preparing the Report.....	TÜV Rheinland (Shanghai) Co., Ltd. Kunshan Branch No. 38 Jingfan Road, Bacheng, Kunshan, Jiangsu, China
Applicant's name	Pylon Technologies Co., Ltd.
Address	No.300, Miaoqiao Road, Kangqiao Town, Pudong New Area, 201315 Shanghai, P.R. China
Test specification:	
Standard.....	EN 18031-2:2024
Test procedure	TÜV Rheinland EN 18031-2 assessment procedure using functional completeness and functional sufficiency testing
Non-standard test method	N/A
Test Report Form No.	EN18031-2_TUV
Test Report Form(s) Originator	TÜV Rheinland (Shanghai) Co., Ltd.
Master TRF.....	2026-07
Copyright © 2018 IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE System). All rights reserved. This publication may be reproduced in whole or in part for non-commercial purposes as long as the IECEE is acknowledged as copyright owner and source of the material. IECEE takes no responsibility for and will not assume liability for damages resulting from the reader's interpretation of the reproduced material due to its placement and context.	
General disclaimer: The test results presented in this report relate only to the object tested. The authenticity of this Test Report and its contents can be verified by contacting the NCB, responsible for this Test Report.	

Test Item description	LFP Lithium Ion Energy Storage Battery System	
Trademark		
Manufacturer.....	Pylon Technologies Co., Ltd. No.300, Miaoqiao Road, Kangqiao Town, Pudong New Area, 201315 Shanghai, P.R. China	
Model/Type reference	RM-15, RM-22, RM-30, RM-37, RM-45, RM-52, RM-60, RM-67, RM-75; RM-15-Pro, RM-22-Pro, RM-30-Pro, RM-37-Pro, RM-45-Pro, RM-52-Pro, RM-60-Pro, RM-67-Pro, RM-75-Pro	
Type of MCU	STM32H725	
Type of encryption chip	N/A - no discrete encryption chip identified; mbedTLS/X.509 cryptography is implemented in firmware	
Type of communication module	FCM360W, PCB MWCU_WIFI_V20 (2.4 GHz Wi-Fi, BLE 5.1 and wired LAN functions)	
Runtime environment/Operating system	Embedded firmware on FCM360W	
Firmware version in factory setting: FCM360W_P002C005V002		
Responsible Testing Laboratory (as applicable), testing procedure and testing location(s):		
☐ CS Testing Laboratory:	TÜV Rheinland (Shanghai) Co., Ltd.	
Testing location/ address	TÜV Rheinland (Shanghai) Co., Ltd.	
Tested by (name, function, signature)		
Approved by (name, function, signature) ...:		
☐ Testing procedure: CTF Stage 1:	N/A	
Testing location/ address	N/A	
Tested by (name, function, signature)		
Approved by (name, function, signature) ...:		
☐ Testing procedure: CTF Stage 2:	N/A	
Testing location/ address	N/A	
Tested by (name + signature)		
Witnessed by (name, function, signature) ..:		
Approved by (name, function, signature) ...:		
☐ Testing procedure: CTF Stage 3:	N/A	
☐ Testing procedure: CTF Stage 4:	N/A	
Testing location/ address	N/A	
Tested by (name, function, signature)		
Witnessed by (name, function, signature) ..:		

Approved by (name, function, signature) ...:		
Supervised by (name, function, signature) :		

List of Attachments / supporting information: N/A

Summary of compliance with National Differences (List of countries addressed): N/A

Copy of marking plate (source: safety/product report CN26V06H 001):

Registration



Manual



PYLONTECH

Battery Category: Industrial Battery

Chemistry: LiFePO₄/LiPF₆/Graphite

Usable Fire-extinguishing Agent: A/B/C/F

Hazardous Substances: /

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

Model

Model	Max.Charging/Discharging Current	Energy	Weight	Nominal Voltage/Charge Voltage
RM-15	50A	15.0kWh	136kg	147.2V/163.3Vd.c
RM-22	50A	22.5kWh	194kg	220.8V/244.95Vd.c
RM-30	50A	30.0kWh	252kg	294.4V/326.6Vd.c
RM-37	50A	37.5kWh	310kg	368.0V/408.25Vd.c
RM-45	50A	45.0kWh	368kg	441.6V/489.9Vd.c
RM-52	50A	52.5kWh	426kg	515.2V/571.55Vd.c
RM-60	50A	60.0kWh	484kg	588.8V/653.2Vd.c
RM-67	50A	67.5kWh	542kg	662.4V/734.85Vd.c
RM-75	50A	75.0kWh	600kg	736.0V/816.5Vd.c

Energy

Weight

Nominal Voltage/Charge Voltage

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

DANGER

DANGER HIGH DC VOLTAGE INSIDE
DANGER HAUTE TENSION A L'INTERIEUR
DANGER ARC FLASH & SHOCK HAZARD
DANGER D'ARC ELECTRIQUE ET DE RISQUE D'ELECTROCUTION

- Do not disconnect, disassemble or repair by yourself.
- * Ne pas débrancher, désassembler ou réparer soi-même.
- Do not drop, deform, impact, cut or spear with a sharp object.
- * Ne pas échanger, déformer, frapper, couper ou transpercer avec un objet pointu.
- Do not place near open flame or incinerate.
- * Ne pas placer près des flammes nues ou incinérer.
- Do not sit or put heavy things on battery.
- * Ne pas s'asseoir ou mettre des objets lourds sur la batterie.
- Keep away from moisture or liquid.
- * Tenir loin de l'humidité ou de tout liquide.
- Keep out of reach of children, animals or insects.
- * Garder hors de la portée des enfants, des animaux ou des insectes.
- Contact your supplier within 24 hours if anything failure happens.
- * Contactez votre fournisseur dans les 24 heures en cas de panne.

System label: RM-15, RM-22, RM-30, RM-37, RM-45, RM-52, RM-60, RM-67 and RM-75

Registration



Manual



PYLONTECH

Battery Category: Industrial Battery

Chemistry: LiFePO₄/LiPF₆/Graphite

Usable Fire-extinguishing Agent: A/B/C/F

Hazardous Substances: /

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000-Pro

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

Model

Model	Max.Charging/Discharging Current	Energy	Weight	Nominal Voltage/Charge Voltage
RM-15-Pro	50A	15.0kWh	136kg	147.2V/163.3Vd.c
RM-22-Pro	50A	22.5kWh	194kg	220.8V/244.95Vd.c
RM-30-Pro	50A	30.0kWh	252kg	294.4V/326.6Vd.c
RM-37-Pro	50A	37.5kWh	310kg	368.0V/408.25Vd.c
RM-45-Pro	50A	45.0kWh	368kg	441.6V/489.9Vd.c
RM-52-Pro	50A	52.5kWh	426kg	515.2V/571.55Vd.c
RM-60-Pro	50A	60.0kWh	484kg	588.8V/653.2Vd.c
RM-67-Pro	50A	67.5kWh	542kg	662.4V/734.85Vd.c
RM-75-Pro	50A	75.0kWh	600kg	736.0V/816.5Vd.c

Energy

Weight

Nominal Voltage/Charge Voltage

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000-Pro

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

DANGER

DANGER HIGH DC VOLTAGE INSIDE
DANGER HAUTE TENSION A L'INTERIEUR
DANGER ARC FLASH & SHOCK HAZARD
DANGER D'ARC ELECTRIQUE ET DE RISQUE D'ELECTROCUTION

- Do not disconnect, disassemble or repair by yourself.
- * Ne pas débrancher, désassembler ou réparer soi-même.
- Do not drop, deform, impact, cut or spear with a sharp object.
- * Ne pas échanger, déformer, frapper, couper ou transpercer avec un objet pointu.
- Do not place near open flame or incinerate.
- * Ne pas placer près des flammes nues ou incinérer.
- Do not sit or put heavy things on battery.
- * Ne pas s'asseoir ou mettre des objets lourds sur la batterie.
- Keep away from moisture or liquid.
- * Tenir loin de l'humidité ou de tout liquide.
- Keep out of reach of children, animals or insects.
- * Garder hors de la portée des enfants, des animaux ou des insectes.
- Contact your supplier within 24 hours if anything failure happens.
- * Contactez votre fournisseur dans les 24 heures en cas de panne.

System label: RM-15-Pro, RM-22-Pro, RM-30-Pro, RM-37-Pro, RM-45-Pro, RM-52-Pro, RM-60-Pro, RM-67-Pro and RM-75-Pro

Registration



Manual



PYLONTECH

Battery Category: Industrial Battery

Chemistry: LiFePO₄/LiPF₆/Graphite

Usable Fire-extinguishing Agent: A/B/C/F

Hazardous Substances: /

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000-Pro

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

Model

Model	Max.Charging/Discharging Current	Energy	Weight	Nominal Voltage/Charge Voltage
RMB70100	50A	75.0kWh	58kg	73.6Vd.c

Energy

Weight

Nominal Voltage/Charge Voltage

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000-Pro

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

DANGER

DANGER HIGH DC VOLTAGE INSIDE
DANGER HAUTE TENSION A L'INTERIEUR
DANGER ARC FLASH & SHOCK HAZARD
DANGER D'ARC ELECTRIQUE ET DE RISQUE D'ELECTROCUTION

- Do not disconnect, disassemble or repair by yourself.
- * Ne pas débrancher, désassembler ou réparer soi-même.
- Do not drop, deform, impact, cut or spear with a sharp object.
- * Ne pas échanger, déformer, frapper, couper ou transpercer avec un objet pointu.
- Do not place near open flame or incinerate.
- * Ne pas placer près des flammes nues ou incinérer.
- Do not sit or put heavy things on battery.
- * Ne pas s'asseoir ou mettre des objets lourds sur la batterie.
- Keep away from moisture or liquid.
- * Tenir loin de l'humidité ou de tout liquide.
- Keep out of reach of children, animals or insects.
- * Garder hors de la portée des enfants, des animaux ou des insectes.
- Contact your supplier within 24 hours if anything failure happens.
- * Contactez votre fournisseur dans les 24 heures en cas de panne.

Battery pack label: RMB70100 (without heating function)

Registration



Manual



PYLONTECH

Battery Category: Industrial Battery

Chemistry: LiFePO₄/LiPF₆/Graphite

Usable Fire-extinguishing Agent: A/B/C/F

Hazardous Substances: /

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000-Pro

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

Model

Model	Max.Charging/Discharging Current	Energy	Weight	Nominal Voltage/Charge Voltage
RMB70100-Pro	50A	75.0kWh	58kg	73.6Vd.c

Energy

Weight

Nominal Voltage/Charge Voltage

IP Rating: IP65

Protection Class: I

Critical Raw Materials: Li>0.1%

Controller Model: RMC1000-Pro

Short Current/Duration time: <6000A/3ms

Rated Capacity: 102Ah

Part Number:

DANGER

DANGER HIGH DC VOLTAGE INSIDE
DANGER HAUTE TENSION A L'INTERIEUR
DANGER ARC FLASH & SHOCK HAZARD
DANGER D'ARC ELECTRIQUE ET DE RISQUE D'ELECTROCUTION

- Do not disconnect, disassemble or repair by yourself.
- * Ne pas débrancher, désassembler ou réparer soi-même.
- Do not drop, deform, impact, cut or spear with a sharp object.
- * Ne pas échanger, déformer, frapper, couper ou transpercer avec un objet pointu.
- Do not place near open flame or incinerate.
- * Ne pas placer près des flammes nues ou incinérer.
- Do not sit or put heavy things on battery.
- * Ne pas s'asseoir ou mettre des objets lourds sur la batterie.
- Keep away from moisture or liquid.
- * Tenir loin de l'humidité ou de tout liquide.
- Keep out of reach of children, animals or insects.
- * Garder hors de la portée des enfants, des animaux ou des insectes.
- Contact your supplier within 24 hours if anything failure happens.
- * Contactez votre fournisseur dans les 24 heures en cas de panne.

Battery pack label: RMB70100-Pro (with heating function)

POSSIBLE TEST CASE VERDICTS:	
- test case does not apply to the test object.....:	N/A
- test object does meet the requirement	P (Pass)
- test object does not meet the requirement	F (Fail)
TESTING:	
Date of receipt of test item	2026-07-16
Date (s) of performance of tests	
GENERAL REMARKS:	
"(See Enclosure #)" refers to additional information appended to the report. "(See appended table)" refers to a table appended to the report. This Test Report is only applicable to controls using software. This TRF is to be used in conjunction with the IEC 60730-1, Edition 5.1 Test Report. Throughout this report a ☐ comma / ☒ point is used as the decimal separator. When differences exist; they shall be identified in the General product information section.	
Name and address of factory (ies)	Factory 1: Anhui Pylon Technologies Co., Ltd., Intersection of Daqianshan Road and Gaocheng Road, Economic Development Zone, Feixi County, Hefei, Anhui, P.R. China. Factory 2: Jiangsu Pylon Battery Co., Ltd., No. 7, Keyan 3rd Road, Yizheng Economic Development Zone, Yangzhou, Jiangsu, P.R. China.
GENERAL PRODUCT INFORMATION:	
Product description and construction: The LFP Lithium Ion Energy Storage Battery System is intended for stationary energy-storage applications and consists of one control box and a series-connected quantity of battery packs. Each RMB70100 or RMB70100-Pro battery pack contains 23 series-connected cells (23S), a fuse, a BMU board and associated interconnections. The BMU measures and collects the cell parameters of each pack. The system includes protection against overcharge, over-discharge, overcurrent and short circuit. The Pro models add the heating function; otherwise the corresponding base and Pro models have the same principal electrical ratings. Models and ratings: RM-15 / RM-15-Pro: 147.2 V d.c., 15.0 kWh; RM-22 / RM-22-Pro: 220.8 V d.c., 22.5 kWh; RM-30 / RM-30-Pro: 294.4 V d.c., 30.0 kWh; RM-37 / RM-37-Pro: 368.0 V d.c., 37.5 kWh; RM-45 / RM-45-Pro: 441.6 V d.c., 45.0 kWh; RM-52 / RM-52-Pro: 515.2 V d.c., 52.5 kWh; RM-60 / RM-60-Pro: 588.8 V d.c., 60.0 kWh; RM-67 / RM-67-Pro: 662.4 V d.c., 67.5 kWh; RM-75 / RM-75-Pro: 736.0 V d.c., 75.0 kWh. All system models are rated 102 Ah, with maximum continuous charging and discharging current of 50 A (55 A for 15 min), IP65, Class I, and an operating altitude up to 4000 m. Standard discharging temperature is -10 °C to 55 °C. Standard charging temperature is 1 °C to 55 °C for the base series and -20 °C to 55 °C for the Pro series; With heating function. Heating is only started when the battery temperature is ≤ the set-opening temperature (Minimum opening temperature is 0). Dimensions (W x D x H) are 770 x 380 x 550/720/890/1060/1230/1400/1570/1740/1910 mm for RM-15 through RM-75, respectively; corresponding weights are 136/194/252/310/368/426/484/542/600 kg. Battery pack information: RMB70100 and RMB70100-Pro are rechargeable Li-ion battery packs rated 73.6 V d.c., 102 Ah, 7.5 kWh, 81.65 V d.c. declared charging voltage, 83.95 V d.c. upper-limit charging voltage, 50 A maximum continuous charging/discharging current (55 A for 15 min), 770 x 380 x 170 mm, 58 +/- 2 kg, IP65 and Class I. RMB70100-Pro includes the heating function.	

Cybersecurity-relevant configuration:

Main control MCU: STM32H725. Communication module: FCM360W on PCB MWCU_WIFI_V20, supporting 2.4 GHz Wi-Fi, BLE 5.1 and wired LAN functions. Factory firmware version: FCM360W_P002C005V002. The runtime is embedded firmware on FCM360W. TLS 1.2/X.509 cryptographic functions are implemented using mbedTLS and device credentials. Network interfaces comprise Wi-Fi, BLE and RJ45 LAN; machine interfaces comprise RJ45, RS485 and CAN. Firmware can be updated through authenticated cloud or BLE OTA with authenticity and integrity verification.

Report scope:

This report covers EN 18031-2:2024 for radio equipment processing data. The assessment addresses security and privacy assets, exposed interfaces, and the privacy and personal-data protection mechanisms applicable to the DUT.

Additional application considerations - (Considerations used to test a component) - N/A

EN 18031 - 2

Clause	Requirement + Test	Result - Remark	Verdict
6.1	[ACM] Access control mechanism		P
6.1.1	[ACM-1] Applicability of access control mechanisms		P
	The equipment shall use access control mechanisms to manage entities' access to security 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.	[E.Info.ACM-1.SecurityAsset] and [E.Info.ACM-1.PrivacyAsset] are provided. The functional integrity assessment has verified that all security and network assets of the product have been properly documented. The functional sufficiency assessment has ensured that the access control mechanisms implemented on the device are consistent with their documentation.	P
6.1.2	[ACM-2] Appropriate access control mechanisms	Implementation category(ies): [IC.ACM-2.Generic]	P
	Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and privacy assets.	[E.Info.ACM-2.SecurityAsset] and [E.Info.ACM-2.PrivacyAsset] are provided. The functional sufficiency assessment has confirmed the proper implementation of access controls. Specifically, it has verified that: • A unique identity is assigned to each user, along with specific authorization privileges. • These privileges adhere to the principle of least privilege. • Access to security and network assets is restricted to authorized users based on their identity. • Only authorized users have permission to modify identity records.	P
6.1.3	[ACM-3] Default access control for children in toys		N/A

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	If the equipment is a toy, for each privacy function where children can access external content and children's access is managed by access control mechanisms required per ACM-1, the access control mechanisms shall by default ensure that children's access to external content via the privacy function is restricted to content from authorized entities.	The DUT is not a toy or childcare radio equipment.	N/A
6.1.4	[ACM-4] Default access control to children's privacy assets for toys and childcare equipment		N/A
	If the equipment is a toy or childcare equipment, any children's privacy function and personal information access control mechanisms required per ACM-1 shall by default restrict, apart from the child's or their parental/guardians, any third-party access to the children's privacy function and personal information processed by the equipment, except for authorised accesses which are required for the equipment's intended functionality.	The DUT is not a toy or childcare radio equipment.	N/A
6.1.5	[ACM-5] Parental/Guardian access controls for children in toys		N/A
	If the equipment is a toy, for each security and privacy asset that is accessible by children, any access control mechanism required per ACM-1 managing the children's access, shall be configurable by an authorized entity to restrict children's access to the protected security and privacy assets.	The DUT is not a toy or childcare radio equipment.	N/A
6.1.6	[ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys		N/A
	If the equipment is a toy, for each children's privacy asset that is accessible by entities, other than the children or their parents or guardians, and where those other entities' access is managed by access control mechanisms required per ACM-1, the access control mechanisms shall be configurable by an authorized entity to restrict the other entities' access to the managed children's privacy assets.	The DUT is not a toy or childcare radio equipment.	N/A
6.2	[AUM] Authentication mechanism		P
6.2.1	[AUM-1-1] Requirement network interface		P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
6.2.1.1	Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to: — 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 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.	[E.Info.AUM-1-1.ACM] is provided. The functional completeness assessment covered authenticated access through Wi-Fi, LAN, BLE and cloud interfaces. Functional sufficiency testing confirmed that device/cloud access uses authenticated TLS and authorized accounts or device binding.	P
6.2.1.2	[AUM-1-2] Requirement user interface		P
	Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to: — 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; — because legal implications do not allow for authentication mechanisms.	[E.Info.AUM-1-2.ACM] is provided. The functional completeness assessment covered the App and cloud user interfaces. Functional sufficiency testing confirmed that security- and privacy-relevant functions require authorized binding or account access.	P
6.2.2	[AUM-2] Appropriate authentication mechanisms		P
6.2.2.1	[AUM-2-1] Requirement one factor authentication		P

EN 18031 - 2

Clause	Requirement + Test	Result - Remark	Verdict
	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).	[E.Info.AUM-2-1.AuthenticationMechanism.AuthFactor] is provided. The functional sufficiency assessment verifies that the authentication mechanisms specified in the requirements (AUM-1-1 for network interfaces and AUM-2-2 for user interfaces) have been implemented correctly.	P
6.2.2.2	[AUM-2-2] Requirement two factor authentication		N/A
	If the primary equipment's intended functionality is specifically processing personal information of special categories, for each access to personal information of special categories via user interfaces over network interface the authentication mechanisms shall support the verification of an entity's claim based on evidence derived from at least two different elements of the categories knowledge, possession and inherence (two factor authentication).	The DUT's primary intended functionality does not specifically process special-category personal information.	N/A
6.2.3	[AUM-3] Authenticator validation	Implementation category(ies): [IC.AUM-3.CertificatePrivateKey]	P
	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.	[E.Info.AUM-3.AUM] is provided. The functional sufficiency assessment confirms that the authentication mechanisms mandated by AUM-1-1 and AUM-1-2 correctly validate all specified security properties.	P
6.2.4	[AUM-4] Changing authenticators		P
	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.	[E.Info.AUM-4.AUM] is provided. The functional sufficiency assessment verifies that the authentication mechanisms required by AUM-1-1 (network interface) and AUM-1-2 (user interface) support the ability to change authenticators.	P
6.2.5	[AUM-5] Pword strength		P
6.2.5.1	[AUM-5-1] Requirement for factory default Pwords	Implementation category(ies): N/A	N/A

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	If factory default Pwords 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.	No factory default Pword is used by the DUT; device-cloud authentication uses per-device X.509 credentials.	N/A
6.2.5.2	[AUM-5-2] Requirement for non-factory default Pwords	Implementation category(ies): [IC.AUM-5-2.SettingFirstUse]	P
	If Pwords other than factory default Pwords 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.	[E.Info.AUM-5-2.AUM] is provided. Wi-Fi credentials are defined by the user/router owner and provisioned through the authorized BLE binding session. Functional sufficiency testing confirmed that credentials are not exposed before authorized configuration.	P
6.2.6	[AUM-6] Brute force protection	Implementation category(ies): [IC.AUM-6.TimeDelay] [IC.AUM-6.LimitedAttempts]	P
	Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks.	[E.Info.AUM-6.AUM] is provided. Functional sufficiency testing confirmed that failed binding or TLS authentication closes the session and that repeated connection attempts are rate-limited.	P
6.3	[SUM] Secure update mechanism		P
6.3.1	[SUM-1] Applicability of update mechanisms		P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security 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.	[E.Info.SUM-1.PartOfSoftw] is provided. The functional sufficiency assessment verifies that the equipment supports update mechanisms for any software components that impact security or network assets, as specified in [E.Info.SUM-1.PartOfSoftw.SUM].	P
6.3.2	[SUM-2] Secure updates	Implementation category(ies): [IC.SUM-2.AuthIntVal.Sign] [IC.SUM-2.AuthIntVal.AccContMech]	P
	Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.	[E.Info.SUM-2.SUM] is provided. Functional sufficiency testing confirmed that modified or unauthenticated update packages are rejected and only signed firmware is installed.	P
6.3.3	[SUM-3] Automated updates		P
	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.	[E.Info.SUM-3.SUM] is provided. The functional sufficiency assessment verifies that the equipment can perform software updates without human intervention. This product adopts an automatic update mechanism under the supervision of administrators.	P
6.4	[SSM] Secure storage mechanism		P
6.4.1	[SSM-1] Applicability of secure storage mechanisms		P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	The equipment shall always use secure storage mechanisms for protecting the security assets and privacy assets persistently stored on the equipment, except for persistently stored security assets and privacy assets where: — the physical or logical measures in the target environment ensures the security asset or privacy asset stored on the equipment accessibility is limited to authorized entities.	[E.Info.SSM-1.SecurityAsset] and [E.Info.SSM-1.PrivacyAsset] are provided. The functional completeness assessment verifies the completeness of all security and network assets listed in [E.Info.SSM-1.SecurityAsset] and [E.Info.SSM-1.NetworkAsset], respectively. The functional sufficiency assessment validates that secure storage mechanisms are implemented as required by SSM-1.	P
6.4.2	[SSM-2] Appropriate integrity protection for secure storage mechanisms	Implementation category(ies): [IC.SSM-2.AccessControl] [IC.SSM-2.HardwareProtection]	P
	Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and privacy assets it stores persistently.	[E.Info.SSM-2.SSM] is provided. The functional sufficiency assessment verifies that the access control mechanism, as implemented per [E.Info.SSM-2.SSM.AccessControl], denies any unauthorized modification of stored security and network assets.	P
6.4.3	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	Implementation category(ies): [IC.SSM-3.Encryption] [IC.SSM-3.HardwareProtection]	P
	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.	[E.Info.SSM-3.SSM] is provided. The functional completeness assessment verifies that all confidential security parameters and network function configurations stored persistently on the equipment are listed in [E.Info.SSM-3.SSM.Asset]. The functional sufficiency assessment verifies that the secure storage mechanisms mandated by SSM-1 deliver the required level of confidentiality protection for stored confidential security parameters and network configurations.	P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
6.5	[SCM] Secure communication mechanism		P
6.5.1	[SCM-1] Applicability of secure communication mechanisms		P
	The equipment shall always use secure communication mechanisms for communicating security assets and privacy assets with other entities via network interfaces, except for: — communicating security 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 whose exposure is part of establishing or managing a connection combined with additional measures to authenticate the connection or trust relation.	[E.Info.SCM-1.NetworkInterface] [E.Info.SCM-1.SecurityAsset] [E.Info.SCM-1.PrivacyAsset] [E.Info.SCM-1.SCM] are provided. The functional completeness assessment confirms that the documentation is complete. The functional sufficiency assessment verifies that secure communication mechanisms are implemented as mandated by SCM-1.	P
6.5.2	[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	Implementation category(ies): [IC.SCM-2.Generic]	P
	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, except for communicating security assets or privacy assets where: — a deviation from best practice for integrity or authenticity protection is required for interoperability reasons.	[E.Info.SCM-2.SecurityAsset] [E.Info.SCM-2.PrivacyAsset] [E.Info.SCM-2.NetworkInterface] [E.Info.SCM-2.SCM] are provided. The functional sufficiency assessment verifies that all communicated security and network assets are protected against undetected tampering. This is achieved by ensuring that: •Forged certificates are rejected. •Messages with compromised integrity are rejected. •Messages without valid authentication are rejected. •Man-in-the-Middle (MitM) attacks are prevented on channel-based communications.	P
6.5.3	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	Implementation category(ies): [IC.SCM-3.MessageEnc] [IC.SCM-3.ChannelEnc]	P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated privacy assets and security assets where confidentiality protection of those is needed, except for communicating security assets or privacy assets where: — a deviation from best practice for protecting confidentiality is required for interoperability reasons.	[E.Info.SCM-3.SecurityAsset], [E.Info.SCM-3.PrivacyAsset], [E.Info.SCM-3.NetworkInterface], [E.Info.SCM-3.SCM] are provided. The functional sufficiency assessment verifies that communicated security and network assets are protected against eavesdropping by ensuring: •The encryption keys used within the communication channel cannot be intercepted; •The assets themselves cannot be eavesdropped during transmission.	P
6.5.4	[SCM-4] Appropriate replay protection for secure communication mechanisms	Implementation category(ies): [IC.SCM-4.SeqNumb] [IC.SCM-4.OneTimeEncKey]	P
	Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the privacy 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.	[E.Info.SCM-4.SecurityAsset], [E.Info.SCM-4.PrivacyAsset], [E.Info.SCM-4.NetworkInterface], [E.Info.SCM-4.SCM] are provided. The functional sufficiency assessment confirms protection against replay attacks by validating that messages with duplicate sequence numbers are rejected, thereby safeguarding transmitted security and network assets.	P
6.6	[LGM] Logging mechanism (EN 18031-2)		P
6.6.1	[LGM-1] Applicability of logging mechanisms		P
	The equipment shall use logging mechanisms for internal activities that are relevant to privacy assets and their protection (referred to as events), except for: — internal activities where a legal obligation prohibits logging.	[E.Info.LGM-1.PrivacyAssetEvent] is provided. Functional completeness testing covered privacy-relevant device, App and cloud events; functional sufficiency testing confirmed that the implemented logging matches the documented event scope.	P
6.6.2	[LGM-2] Persistent storage of log data		P

EN 18031 - 2

Clause	Requirement + Test	Result - Remark	Verdict
	Logging mechanisms that are required per LGM-1 shall store log data for related events in the equipment's persistent storage, except for events where: — related log data is stored outside the equipment.	[E.Info.LGM-2.LGM] is provided. Relevant log data is stored persistently by the associated App/cloud service where it is protected outside the equipment.	P
6.6.3	[LGM-3] Minimum number of persistently stored events		P
	All log data stored in equipment's persistent storage by logging mechanisms that are required per LGM-1 shall always include: — a minimum number of the latest events; and — the latest event.	[E.Info.LGM-3.Events] and [E.Info.LGM-3.Quantity] are provided. Functional sufficiency testing confirmed retention of the defined minimum number of recent events, including the latest event.	P
6.6.4	[LGM-4] Time-related information of persistently stored log data		P
	All log data stored in equipment's persistent storage by logging mechanisms that are required per LGM-1 shall include: — a timestamp if real time is available on the equipment; and — time-related information if real time is not available on the equipment.	[E.Info.LGM-4.Events] and [E.Info.LGM-4.LGM] are provided. Functional sufficiency testing confirmed that stored events include time-related information and timestamps where real time is available.	P
p			
6.7	[DLM] Deletion mechanism (EN 18031-2)		P
6.7.1	[DLM-1] Applicability of deletion mechanisms		P
	The equipment shall provide a deletion mechanism that allows a user to delete their personal data and sensitive security parameters stored on the equipment.	[E.Info.DLM-1.PersonalData] and [E.Info.DLM-1.SenSecParam] are provided. Functional sufficiency testing confirmed that local reset and authorized App/account functions delete user configuration, binding data and applicable personal data.	P
6.8	User notification mechanism (EN 18031-2)		P
6.8.1	[UNM-1] Applicability of user notification mechanisms		P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	The equipment shall provide user notification mechanism(s) for informing the user of the equipment about changes affecting the protection or privacy of personal information, except for changes where: — other methods of informing the user exist, which do not involve the equipment.	[E.Info.UNM-1.PersonalInformation] is provided. Functional completeness and sufficiency testing confirmed that the App/cloud notification mechanism informs the user about relevant security and privacy changes.	P
6.8.2	[UNM-2] Appropriate user notification content		P
	The content of a notification provided by a user notification mechanism that is required per UNM-1 shall include at least: — a description of a change; and — a description of how a change will affect the protection and privacy of personal information.	[E.Info.UNM-2.Notifications] is provided. Tested notifications describe the relevant change and how it affects the protection or privacy of personal information.	P
6.9	[CCK] Confidential cryptographic keys		P
6.9.1	[CCK-1] Appropriate CCKs		P
	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.	[E.Info.CCK-1.CCK] is provided. CCK support a minimum security strength of 112-bits.	P
6.9.2	[CCK-2] CCK generation mechanisms		P
	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.	[E.Info.CCK-2.Generation] is provided. The generation mechanism for the CCK adhere to best practice Cryptography.	P
6.9.3	[CCK-3] Preventing static default values for preinstalled CCKs		P
	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.	[E.Info.CCK-3.CCK] is provided. Functional sufficiency testing confirmed that per-device X.509 credentials and device-specific confidential keys are used rather than static default values.	P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict

6.10	[GEC] General equipment capabilities		P
6.10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities		P
	The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security 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.	[E.Info.GEC-1.SecurityAsset], [E.Info.GEC-1.PrivacyAsset], software/hardware documentation and the vulnerability assessment are provided. Vulnerability scanning and functional assessment found no publicly known exploitable vulnerability affecting the assessed security or privacy assets.	P
6.10.2	[GEC-2] Limit exposure of services via related network interfaces		P
	In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces affecting security assets and privacy assets which are necessary for equipment setup or for basic operation of the equipment.	[E.Info.GEC-2.NetworkInterface.Exposure], [E.Info.GEC-2.SecurityAsset], [E.Info.GEC-2.PrivacyAsset] are provided. The functional completeness assessment confirms that the factory default configuration exposes only network interfaces and services strictly required for setup and core operational functionality.	P
6.10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces		P
	Optional network interfaces or optional services exposed via network interfaces affecting security 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.	[E.Info.GEC-3.NetworkInterface.Exposure], [E.Info.GEC-3.SecurityAsset], [E.Info.GEC-3.PrivacyAsset] are provided. The assessment verifies that all optional network interfaces and services in the factory default configuration are user-configurable, with at least the capability to enable or disable each service.	P
6.10.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces		P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	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.	[E.Info.GEC-4.UserDoc.NetworkInterface.Exposure] , [E.Info.GEC-4.NetworkInterface.Exposure] are provided. The functional completeness assessment confirms that the user manual comprehensively describes all network interfaces and exposed services delivered in the factory default state.	P
6.10.5	[GEC-5] No unnecessary external interfaces		P
	The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.	[E.Info.GEC-5.PhysicalExternalInterface], [E.Info.GEC-5.IntFunc] are provided. The assessment verifies that exposed physical external interfaces are limited to those essential for intended functionality, per specifications in [E.Info.GEC-5.PhysicalExternalInterface].	P
6.10.6	[GEC-6] Input validation		P

EN 18031 - 2			
Clause	Requirement + Test	Result - Remark	Verdict
	The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or privacy assets.	[E.Info.GEC-6.ExternalInterface], [E.Info.GEC-6.SecurityAsset], [E.Info.GEC-6.PrivacyAsset] are provided. The functional completeness assessment confirms that all external interfaces and their associated input mechanisms are fully documented. This verification involves: •Functionally assessing traffic on network interfaces (e.g., using network analysis tools) to identify input methods, guided by the specifications in [E.Info.GEC-6.ExternalInterface]; •Functionally evaluating non-network external interfaces through visual inspection, user manuals, and design documentation to reveal input methods; •Triggering all documented input methods as described in [E.Info.GEC-6.ExternalInterface.Capabilities] to validate their implementation and behavior. The functional sufficiency assessment confirms interface resilience by: Adversarial testing using invalid inputs and attack methods attempting to misuse assets defined in [E.Info.GEC-6.SecurityAsset] and [E.Info.GEC-6.NetworkAsset]; Ensuring actual system behavior under attack matches documented expectations in [E.Info.GEC-6.ExternalInterface].	P
6.10.7	[GEC-7] Documentation of external sensing capabilities		N/A
	All external sensing capabilities of the equipment that are related to the user's or subscriber's privacy shall be documented for the user.	The DUT has no external sensing capability related to user or subscriber privacy.	N/A
6.11	[CRY] Cryptography		P
6.11.1	[CRY-1] Best practice cryptography		P

EN 18031 - 2

Clause	Requirement + Test	Result - Remark	Verdict
	The equipment shall use best practice for cryptography that is used for the protection of the security 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.	[E.Info.CRY-1.Assets] is provided. Functional sufficiency testing confirmed the documented use of TLS 1.2/X.509 and WPA2 AES-CCMP mechanisms; cryptographic practice was evaluated using SOGIS Agreed Cryptographic Mechanisms V1.2.	P

EN 18031 - 2

Clause	Requirement + Test	Result - Remark	Verdict
--------	--------------------	-----------------	---------

No.	Document List	Version
1	EN 18031 General Information / Assets	V0.4
2	EN 18031 Conceptual Assessment	V0.4
3	Vulnerability Scanning Report	Completed
4	User Manual	Provided / version not stated
5	Test Evidence / Records	Completed - EN 18031-2 results recorded
6	Safety report / product data	CN26V06H 001 (IEC 62619 / IEC 63056)

No.	Testing Tools List	Version
1	VMware Workstation 17 pro	17.6.1 build-24319023
2	Kali	Linux 6.12.13-am64
3	Nmap	7.95
4	Wireshark	4.4.5
5	Python	3.13.2
6	CVE Binary Tool	5.4.2
7	Binwalk	V3
8	Nessus	10.8.4

- End of Test Report -