| | | | | |
|---|---|---|---|---|
| **Prüfbericht-Nr.:** *Test report no.:* | CN252MSV 001 | **Auftrags-Nr.:** *Order no.*: | 326095254 | **Seite 1 von 21** *Page 1 of 21* |
| **Kunden-Referenz-Nr.:** *Client reference no.:* | 2089836 | **Auftragsdatum:** *Order date:* | 2025-02-14 | |
| **Auftraggeber:** *Client:* | **Pylon Technologies Co., Ltd.** No.300, Miaoqiao Road, Kangqiao Town, Pudong New Area, 201315 SHANGHAI, P.R. CHINA | | | |
| **Prüfgegenstand:** *Test item:* | WiFi Stick | | | |
| **Bezeichnung / Typ-Nr.:** *Identification / Type no.:* | Pyiot-wifi | | | |
| **Auftrags-Inhalt:** *Order content*: | Test report | | | |
| **Prüfgrundlage:** *Test specification:* | EN 18031-1: 2024 | | | |

| | |
|---|---|
| **Wareneingangsdatum:** *Date of sample receipt:* | 2025-03-15 |
| **Prüfmuster-Nr.:** *Test sample no:* | Engineering sample |
| **Prüfzeitraum:** *Testing period:* | 2025-03-19 - 2025-04-21 |
| **Ort der Prüfung:** *Place of testing:* | Pylon Technologies Co., Ltd. |
| **Prüflaboratorium:** *Testing laboratory:* | TÜV Rheinland (Shanghai) Co., Ltd. |
| **Prüfergebnis*:** *Test result*:* | Pass |

| | | | |
|---|---|---|---|
| **geprüft von:** *tested by:* | Ding Guan | **genehmigt von:** *authorized by:* | |
| **Datum:** *Date:* 2025-04-23 | Ding Guan | **Ausstellungsdatum:** *Issue date:* 2025-04-23 | Bowen Dong |
| **Stellung** / *Position:* | Engineer | **Stellung** / *Position:* | Authorizer |

**Sonstiges** / *Other:* See the following pages for general product information and comment for details.

**Zustand des Prüfgegenstandes bei Anlieferung:** Prüfmuster vollständig und unbeschädigt
*Condition of the test item at delivery:* *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* |

| **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.<br>Detaillierte Informationen bezüglich Prüfkonditionen, Prüfequipment und Messunsicherheiten sind im Prüflabor vorhanden und können auf Wunsch bereitgestellt werden.<br><br>*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.*<br>*Detailed information regarding test conditions, equipment and measurement uncertainty is available in the test laboratory and could be provided on request.* |
| 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.<br><br>*As contractually agreed, this document has been signed digitally only. TUV 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, TUV 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.* |
| 3 | Prüfklausel mit der Note * wurden an qualifizierte Unterauftragnehmer vergeben und sind unter der jeweiligen Prüfklausel des Berichts beschrieben.<br>Abweichungen von Prüfspezifikation(en) oder Kundenanforderungen sind in der jeweiligen Prüfklausel im Bericht aufgeführt.<br><br>*Test clauses with remark of * are subcontracted to qualified subcontractors and descripted under the respective test clause in the report.*<br>*Deviations of testing specification(s) or customer requirements are listed in specific test clause in the report.* |
| 4 | Die Entscheidungsregel für Konformitätserklärungen basierend auf numerischen Messergebnisen 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 bezueglich des Risikos durch diese Entscheidungsregel siehe ILAC G8:2019.<br><br>*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.* |

**Test Report issued under the responsibility of:**

TÜVRheinland®

# TEST REPORT

**EN 18031-1**

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

| | |
|---|---|
| **Report Number. .....:** | **CN252MSV 001** |
| **Date of issue .....:** | **See cover page** |
| **Total number of pages.....:** | **See cover page** |
| **Name of Testing Laboratory preparing the Report.....:** | **See cover page** |
| **Applicant's name.....:** | **See cover page** |
| **Address .....:** | **See cover page** |
| **Test specification:** | |
| **Standard .....:** | **See cover page** |
| **Test procedure.....:** | **See cover page** |
| **Non-standard test method.....:** | N/A |
| **Test Report Form No.....:** | EN18031-1_TUV |
| **Test Report Form(s) Originator.....:** | TÜV Rheinland (Shanghai) Co., Ltd. |
| **Master TRF .....:** | 2024-12 |



**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 ..... | WiFi Stick |
| Trademark ..... | PYLONTECH |
| Manufacturer ..... | See cover page |
| Model/Type reference ..... | See cover page |
| Type of MCU | Quectel FCM360W (Eswin ECR6600) |
| Type of encryption chip | Quectel FCM360W (Eswin ECR6600) |
| Type of communication module | Quectel FCM360W (Eswin ECR6600) |
| Runtime environment/Operating system | FreeRTOS Kernel V10.4.1 |
| Firmware version in factory setting | V1.3.4 |

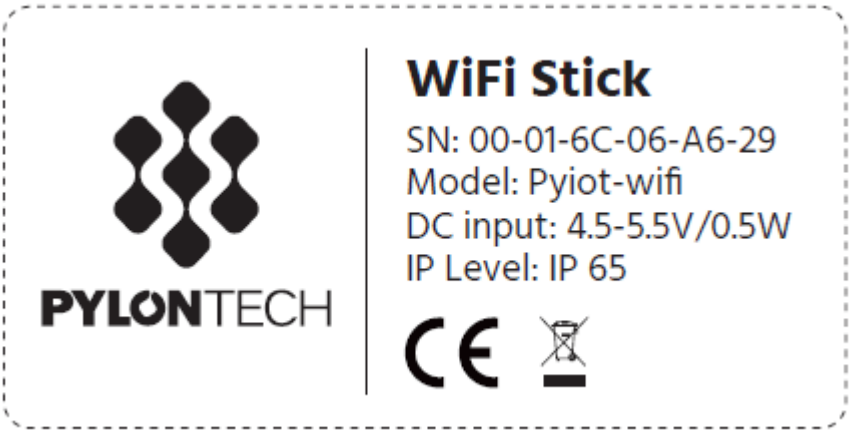
| | | | |
|---|---|---|---|
| **Responsible Testing Laboratory (as applicable), testing procedure and testing location(s):** | | | |
| ☐ | **CB Testing Laboratory:** | | |
| **Testing location/ address.....:** | | | |
| **Tested by (name, function, signature).....:** | | | |
| **Approved by (name, function, signature)...:** | | | |
| ☐ | **Testing procedure: CTF Stage 1:** | | |
| **Testing location/ address.....:** | | | |
| **Tested by (name, function, signature).....:** | | | |
| **Approved by (name, function, signature)...:** | | | |
| ☐ | **Testing procedure: CTF Stage 2:** | | |
| **Testing location/ address.....:** | | | |
| **Tested by (name + signature).....:** | | | |
| **Witnessed by (name, function, signature) .:** | | | |
| **Approved by (name, function, signature)...:** | | | |
| ☐ | **Testing procedure: CTF Stage 3:** | | |
| ☐ | **Testing procedure: CTF Stage 4:** | | |
| **Testing location/ address.....:** | | | |
| **Tested by (name, function, signature).....:** | | | |
| **Witnessed by (name, function, signature) .:** | | | |

| | | |
|---|---|---|
| **Approved by (name, function, signature)...:** | | |
| **Supervised by (name, function, signature) :** | | |
| | | |

| |
|---|
| **List of Attachments (including a total number of pages in each attachment):**<br>N/A |
| **Summary of compliance with National Differences (List of countries addressed):**<br>N/A |

**Copy of marking plate:**

**The artwork below may be only a draft. The use of certification marks on a product must be authorized by the respective NCBs that own these marks.**

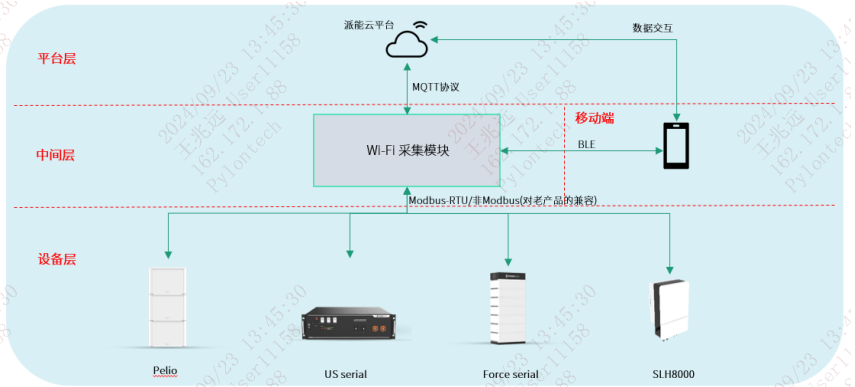


| | |
|---|---|
| **POSSIBLE TEST CASE VERDICTS:** | |
| - test case does not apply to the test object..... : | N/A |
| - test object does meet the requirement ..... : | P (Pass) |
| - test object does not meet the requirement ..... : | F (Fail) |
| **TESTING:** | |
| Date of receipt of test item..... : | See cover page |
| Date (s) of performance of tests..... : | See cover page |
| **GENERAL REMARKS:** | |
| **"(See Enclosure #)" refers to additional information appended to the report.**<br>**"(See appended table)" refers to a table appended to the report.**<br>**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.**<br>**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<br>Jiangsu Pylon Battery Co., Ltd.<br>No.7, Keyan 3rd Road, Yizheng Economic Development Zone Yangzhou JIANGSU P.R.CHINA<br><br>Factory 2<br>Anhui Pylon Technologies Co., Ltd.<br>Intersection of Daqianshan Road and Gaocheng Road, Economic Development Zone, Feixi County ,<br>Hefei, ANHUI P.R.CHINA |

## GENERAL PRODUCT INFORMATION:

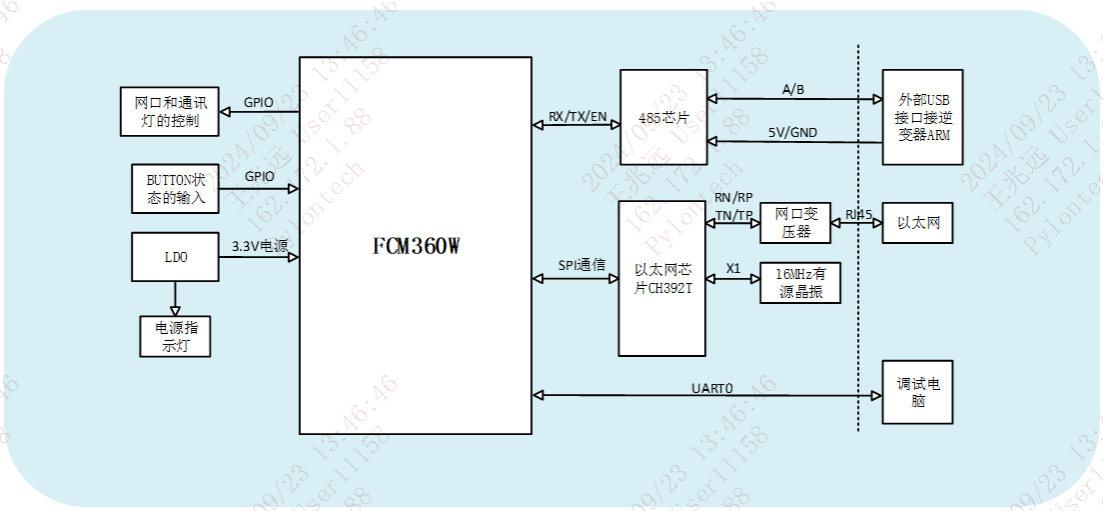
The Pylon Wi-Fi Stick is an insertable external device. One end is inserted into the device to be collected via USB, while the other end connects to the cloud through Wi-Fi (or LAN). It also enables near-field communication via Bluetooth. This device facilitates the uploading of data from the underlying device, the upgrading of various modules of the underlying device, and remote control functions.

The Wi-Fi stick serves as the central hub in a three-tiered IoT architecture, bridging field devices to cloud services. The structure is organized into three distinct layers:



1. **Platform Layer**: Interfaces with the *Enable Cloud Platform* via MQTT protocol for bidirectional data exchange and remote management. Additionally, it maintains BLE-based communication with mobile devices (e.g., smartphones) for real-time monitoring and configuration.
2. **Middleware Layer**: The Wi-Fi stick acts as the core data aggregator, processing signals from downstream devices and translating protocols (e.g., Modbus-RTU to MQTT) for upstream cloud integration. It ensures backward compatibility with legacy systems through hybrid protocol support (*Modbus-RTU/non-Modbus*).
3. **Device Layer**: Directly connects to other Pylon equipment (e.g., *Pelio, US serial, Force serial, SLH8000*) via wired interfaces. This layer handles raw data collection and local signal conditioning before transmission to the middleware.

The Wi-Fi stick acquisition module is built around the FCM360W core chip. The internal topology of the Wi-Fi stick is shown as figure below. On the left side, GPIO pins manage network/communication indicator lights and button state inputs, while a 3.3V LDO stabilizes power input and drives a dedicated power status LED. The right side integrates an RS-485 chip connected to the FCM360W's RX/TX/EN pins for serial communication with external devices via a USB-to-serial converter (ARI). The CH392T Ethernet controller interfaces with the FCM360W through SPI protocol, linking to an Ethernet transformer for network connectivity. A 16MHz crystal oscillator ensures timing precision, while a UART port at the bottom enables direct debugging with a computer.




The basic parameters of the Wi-Fi stick are shown in the table below.

| Category | Parameter | Parameter Specification |
|---|---|---|
| **Wireless Parameters** | Operating Frequency | 2400MHz ~ 2483.5MHz |
| | Transmit Power | 802.11b: +17dBm ± 2.0dBm @1Mbps, 11Mbps |
| | | 802.11g: +15dBm ± 2.0dBm (@6Mbps/54Mbps) |

| | | |
|---|---|---|
| | | 802.11n: +14dBm ± 2.0dBm (@HT20/HT40, MCS0/MCS7) |
| | | 802.11ax: +14dBm ± 2.0dBm (@HT20, MCS0/MCS7) |
| **Bluetooth** | Antenna Option | Built-in: On-board antenna |
| | Wireless Standard | BLE 5.1 |
| | Frequency Range | 2400MHz ~ 2483.5MHz |
| **Hardware Parameter** | Transmit Power | 6dBm ± 2dBm |
| | Operating Voltage | DC 5V |
| | Operating Power | <2W (Steady-state 0.5W) |
| | Indicator Lights | 1x Signal light (connected to device/BMS/PCS) |
| | | 1x Network status light |
| | | 1x Power light |
| | Data Storage | Default configuration: 8MBYTE FLASH |
| | Operating Temperature | -30℃ ~ +75℃ |
| | Operating Humidity | 5% ~ 95% RH (Non-condensing) |
| | Storage Temperature | -40℃ ~ +80℃ |
| | Storage Humidity | 5% ~ 95% RH |
| | External Interfaces | USB, LAN |
| | Connected Device Quantity | 1 unit |
| | Dimensions | 160×46×30mm |
| | Serial Port Rate | 115200bps |

| | | |
|---|---|---|
| **Software Parameters** | User Configuration | Remote server & App configuration |
| | Firmware Upgrade | Remote OTA upgrade |
| | Other Features | Real-time control, Breakpoint resume |

Model difference:

N/A

**Additional application considerations – (Considerations used to test a component) –**

N/A

| EN 18031-1 | | | |
|---|---|---|---|
| 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 network assets, except for access to security assets or network assets where:<br>- public accessibility is the equipment's intended functionality; or<br>- physical or logical measures in the equipment's targeted operational environment limit their accessibility to authorized entities; or<br>- legal implications do not allow for access control mechanisms. | [E.Info.ACM-1.SecurityAsset] and [E.Info.ACM-1.NetworkAsset] are provided. | P |
| **6.1.2** | **[ACM-2] Appropriate access control mechanisms** | **Implementation category(ies):**<br>[IC.ACM-2.DAC] | P |
| | Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets. | [E.Info.ACM-2.SecurityAsset] and [E.Info.ACM-2.NetworkAsset] are provided. | P |

| | | | |
|---|---|---|---|
| **6.2** | **[AUM] Authentication mechanism** | | **P** |
| **6.2.1** | **[AUM-1] Applicability of authentication mechanisms** | | **P** |
| 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:<br>— read confidential network function configuration or confidential security parameters; or<br>— modify sensitive network function configuration or sensitive security parameters; or<br>— use network functions or security functions, except for access:<br>— to network functions or network function configuration where the absence of authentication is required for the equipment's intended functionality; or<br>— 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. | P |

| EN 18031-1 | | | |
|---|---|---|---|
| Clause | Requirement + Test | Result - Remark | Verdict |
| **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:<br>— read confidential network function configuration or confidential security parameters; or<br>— modify sensitive network function configuration or sensitive security parameters; or<br>— use network functions or security functions,<br>except for access:<br>— where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorized entities;<br>and except for read only access to network functions or network functions configuration where access without authentication is needed:<br>— to enable the intended equipment functionality; or<br>— because legal implications do not allow for authentication mechanisms. | [E.Info.AUM-1-2.ACM] is provided. | P |
| **6.2.2** | **[AUM-2] Appropriate authentication mechanisms** | | **P** |
| | 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.AuthenticationMechanism] is provided. | P |
| **6.2.3** | **[AUM-3] Authenticator validation** | **Implementation category(ies):**<br>[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. | 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. | P |
| **6.2.5** | **[AUM-5] Password strength** | | **N/A** |

| EN 18031-1 | | | |
|---|---|---|---|
| Clause | Requirement + Test | Result - Remark | Verdict |

| | | | |
|---|---|---|---|
| **6.2.5.1** | **[AUM-5-1] Requirement for factory default passwords** | **Implementation category(ies):** | **N/A** |
| | If factory default passwords are used by an authentication mechanism that is required per AUM-1-1 or AUM-1-2, they shall:<br>— be unique per equipment; and<br>— follow best practice concerning strength;<br>or<br>— be enforced to be changed by the user before or on first use. | | N/A |
| **6.2.5.2** | **[AUM-5-2] Requirement for non-factory default passwords** | **Implementation category(ies):**<br>**[IC.AUM-5-2.SettingFirstUse]** | **P** |
| | If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall:<br>— be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or<br>— be defined by an authorized entity within a network where access is limited to authorised entities; or<br>— 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. | P |
| **6.2.6** | **[AUM-6] Brute force protection** | **Implementation category(ies):** | **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. | P |

| | | | |
|---|---|---|---|
| **6.3** | **[SUM] Secure update mechanism** | | **P** |
| **6.3.1** | **[SUM-1] Applicability of update mechanisms** | | **P** |
| | The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or network assets, except for software:<br>— where functional safety implications do not allow updatability; or<br>— which is immutable; or<br>— where alternative measures protect the affected security assets and/or network assets during the entire lifecycle of the equipment. | [E.Info.SUM-1.PartOfSoftw] is provided. | P |

| EN 18031-1 | | | |
|---|---|---|---|
| Clause | Requirement + Test | Result - Remark | Verdict |
| **6.3.2** | **[SUM-2] Secure updates** | **Implementation category(ies):** [IC.SUM-2.AuthIntVal.Sign] and [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. | P |
| **6.3.3** | **[SUM-3] Automated updates** | | **P** |
| | Each update mechanism that is required per SUM-1 shall be capable of updating the software:<br>— without human intervention at the equipment; or<br>— via scheduling the installation of an update under human approval; or<br>— 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. | P |
| **6.4** | **[SSM] Secure storage mechanism** | | **P** |
| **6.4.1** | **[SSM-1] Applicability of secure storage mechanisms** | | **P** |
| | The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets where:<br>— the physical or logical measures in the target environment ensures the security asset or network asset stored on the equipment accessibility is limited to authorized entities. | [E.Info.SSM-1.SecurityAsset] and [E.Info.SSM-1.NetworkAsset] are provided. | P |
| **6.4.2** | **[SSM-2] Appropriate integrity protection for secure storage mechanisms** | **Implementation category(ies):** [IC.SSM-2.AccessControl] and [IC.SSM-2.HardwareProtection] | **P** |
| | Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently. | [E.Info.SSM-2.SSM] is provided. | P |
| **6.4.3** | **[SSM-3] Appropriate confidentiality protection for secure storage mechanisms** | **Implementation category(ies):** [IC.SSM-3.Encryption] and [IC.SSM-3.HardwareProtection] | **P** |

| EN 18031-1 | | | |
|---|---|---|---|
| Clause | Requirement + Test | Result - Remark | Verdict |
| | Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently. | [E.Info.SSM-3.SSM] is provided. | P |
| **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 network assets with other entities via network interfaces, except for:<br>— communicating security assets or network assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that network assets or security assets are not exposed to unauthorised entities; or<br>— 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. | [E.Info.SCM-1.NetworkInterface]<br>[E.Info.SCM-1.SecurityAsset]<br>[E.Info.SCM-1.NetworkAsset]<br>[E.Info.SCM-1.SCM] are provided. | P |
| **6.5.2** | **[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms** | **Implementation category(ies):**<br>[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 network assets communicated, except for communicating security assets or network assets where:<br>— a deviation from best practice for integrity or authenticity protection is required for interoperability reasons. | [E.Info.SCM-2.SecurityAsset]<br>[E.Info.SCM-2.NetworkAsset]<br>[E.Info.SCM-2.NetworkInterface]<br>[E.Info.SCM-2.SCM] are provided. | P |
| **6.5.3** | **[SCM-3] Appropriate confidentiality protection for secure communication mechanisms** | **Implementation category(ies):**<br>[IC.SCM-3.MessageEnc] | **P** |
| | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed, except for communicating security assets or network assets where:<br>— a deviation from best practice for protecting confidentiality is required for interoperability reasons. | [E.Info.SCM-3.SecurityAsset]<br>[E.Info.SCM-3.NetworkAsset]<br>[E.Info.SCM-3.NetworkInterface]<br>[E.Info.SCM-3.SCM] are provided. | P |

| EN 18031-1 | | | |
|---|---|---|---|
| Clause | Requirement + Test | Result - Remark | Verdict |
| **6.5.4** | **[SCM-4] Appropriate replay protection for secure communication mechanisms** | **Implementation category(ies):** [IC.SCM-4.Generic] | P |
| | Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the network assets communicated against replay attacks, except for communicating security assets or network assets where:<br>— a duplicate transfer does not impose a threat of a replay attack; or<br>— a deviation from best practice for replay protection is required for interoperability reasons. | [E.Info.SCM-4.SecurityAsset]<br>[E.Info.SCM-4.NetworkAsset]<br>[E.Info.SCM-4.NetworkInterface]<br>[E.Info.SCM-4.SCM] are provided. | P |
| **6.6** | **[RLM] Resilience mechanism** | | **N/A** |
| **6.6.1** | **[RLM-1] Applicability and appropriateness of resilience mechanisms** | | **N/A** |
| | The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces and return to a defined state after the attack except for:<br>— network interfaces that are only used in a local network that do not interoperate with other networks; or<br>— network interfaces where other devices in the network provide sufficient protection against DoS attacks and loss of essential functions for network operations. | After the device completes its network configuration and connects to the internet via the home router, its resilience mechanism primarily relies on the router's configuration. | N/A |
| **6.7** | **[NMM] Network monitoring mechanism** | | **N/A** |
| **6.7.1** | **[NMM-1] Applicability and appropriateness of network monitoring mechanisms** | **Implementation category(ies):** | **N/A** |
| | If the equipment is a network equipment, the equipment shall provide network monitoring mechanism(s) to detect for indicators of DoS attacks in the network traffic between networks which it processes. | Not a network equipment. | N/A |
| **6.8** | **[TCM] Traffic control mechanism** | | **N/A** |
| **6.8.1** | **[TCM-1] Applicability of and appropriate traffic control mechanisms** | **Implementation category(ies):** | **N/A** |

| EN 18031-1 | | | |
|---|---|---|---|
| Clause | Requirement + Test | Result - Remark | Verdict |
| | If the equipment is a network equipment, the equipment shall provide network traffic control mechanism(s). | Not a network equipment. | 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:<br>— 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. | P |
| **6.9.2** | **[CCK-2] CCK generation mechanisms** | | **P** |
| | The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for:<br>— 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. | 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:<br>— CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or<br>— CCKS key are shared parameters required for the equipment's intended functionality. | [E.Info.CCK-3.CCK] is provided. | P |

| | | | |
|---|---|---|---|
| **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** |

| EN 18031-1 | | | |
|---|---|---|---|
| Clause | Requirement + Test | Result - Remark | Verdict |

| | | | |
|---|---|---|---|
| | The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and network assets, except for vulnerabilities:<br>— that cannot be exploited in the specific conditions of the equipment; or<br>— that have been mitigated to an acceptable residual risk; or<br>— that have been accepted on a risk basis. | [E.Info.GEC-1.SecurityAsset]<br>[E.Info.GEC-1.NetworkAsset]<br>[E.Info.GEC-1.SoftwareDocumentation]<br>[E.Info.GEC-1.HardwareDocumentation]<br>[E.Info.GEC-1.ListOfVulnerabilities] are provided. | P |
| **6.10.2** | **[GEC-2] Limit exposure of services via related network interfaces** | | **P** |
| | In factory default state the equipment shall only expose<br>— network interfaces; and<br>— services via network interfaces<br>affecting security assets or network assets which are necessary for equipment setup or for basic operation of the equipment. | [E.Info.GEC-2.NetworkInterface.Exposure]<br>[E.Info.GEC-2.SecurityAsset]<br>[E.Info.GEC-2.NetworkAsset] are provided. | 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 network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service. | [E.Info.GEC-3.NetworkInterface.Exposure]<br>[E.Info.GEC-3.SecurityAsset]<br>[E.Info.GEC-3.NetworkAsset] are provided. | P |
| **6.10.4** | **[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces** | | **P** |
| | The equipment's user documentation shall contain a description of<br>— all exposed network interfaces; and<br>— all services exposed via network interfaces,<br>which are delivered as part of the factory default state. | [E.Info.GEC-4.UserDoc.NetworkInterface.Exposure]<br>[E.Info.GEC-4.NetworkInterface.Exposure] are provided. | 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]<br>[E.Info.GEC-5.IntFunc] are provided. | P |
| **6.10.6** | **[GEC-6] Input validation** | | **P** |

| EN 18031-1 | | | |
|---|---|---|---|
| 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 network assets. | [E.Info.GEC-6.ExternalInterface] [E.Info.GEC-6.SecurityAsset] [E.Info.GEC-6.NetworkAsset] are provided. | P |
| **6.11** | **[CRY] Cryptography** | | **P** |
| **6.11.1** | **[CRY-1] Best practice cryptography** | | **P** |
| | The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets, except for:<br>— 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.<br>Best practice for cryptography is evaluated according to SOGIS agreed Cryptographic Mechanisms V1.3. | P |

| No. | Document List | Version |
|---|---|---|
| 1 | RED Article 3.3 (d), (e) and (f) Equipment Scope Checklist | 1.0 |
| 2 | EN 18031_General Inforamtion_Assets | 3.0 |
| 3 | EN18031 – Conceptual Assessment_01B | 1.4 |

| 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 | openssl | 3.4.1 |
| 8 | sslscan | 2.1.5 |

- End of Test Report -