TEST REPORT

CYBERSECURITY ASSESSMENT TEST REPORT

LYNS-TCi - CYBER-ETSI-EN-303 645

Version: 2022-9-12

Prepared by: **(Responsible for Testing)**	**Boeing Huang**
Approved by: **(Responsible for accreditation scope)**	**Lukes Lin**
Test report Nº.	**HC2407190100GC03**
Issued date	**2024-12-11**

ACCREDITED
Certificate # 5200.02

Test report number........................:	**HC2407190100GC03**
Date of issue..................................:	2024-12-11
Total number of pages..........….....:	197
Testing laboratory ....:	**Lyns-tci Technology Guangdong Co., Ltd.**
Address...:	Room 1201, Unit 2, Building 18, No. 7, Science and Technology Boulevard, Houjie Town, Dongguan City, Guangdong, 523960 P.R. China
Testing location / address...............:	Same as above
Applicant's name ....:	EAST Group Co., Ltd.
Address...:	No.6 Northern Industry Road, Songshan Lake Sci. & Tech. Industrial Park, Dongguan City, Guangdong Province, China
Test specification	
Standard ....:	ETSI EN 303 654, Cyber Security for Consumer Internet of Things: Baseline Requirements ETSI TS 103 701 Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
Test report form number..............:	1.1
Test report form(s) originator..........:	Lyns-tci Technology Guangdong Co., Ltd.
Master TRF....................................:	TRF_Cyber
Test item description ....:	Device Category: **Inverter** Device Type: **Converter (Hybrid Inverter with storage battery system)**
Trademark ....:	EAST
Model / Type reference...................:	EAHI-6000-SL-S
Technical data ....:	See section 6 assessment results
Dates of testing...............................:	2024-11-15 to 2024-12-02

Tested / Report prepared by	Approved by
Boeing	
Boeing Huang	Lukes Lin
(Test engineer)	(Project manager)

LYNS-TCi TECHNOLOGY
LYNS-TCi

Contents

1 REPORT HISTORY

1.1 Report Revision History

Test Report No	Date	Change Description	Validity
HC2407190100GC03	2024-12-10	Final	Valid

1.2 Report Template Revision History

Date	Version	Comments	Changed by	Approved by
2024/05/22	Rev1	Creation	Boeing Huang	Lukes Lin

2 Terms and Conditions

The test results presented in this report relate only to the object tested.

This report is for the exclusive use of Lyns-tci Technology Guangdong Co., Ltd. (abbreviation: Lyns-tci) Client and is provided pursuant to the agreement between Lyns-tci and its Client. This report shall not be reproduced, except in full, without the written approval of Lyns-tci. Test reports without seal and signature are not valid.

Lyns-tci responsibility and liability are limited to the terms and conditions of the agreement. Lyns-tci assumes no liability to any party, other than to the Client in accordance with the agreement, for any loss, expense or damage occasioned using this report.

Information on derived or extended models of the range as provided by the applicant (if any) is included in this report for information purposes only. Lyns-tci shall not be liable for any incorrect results due to unclear, incorrect, incomplete, misleading or false information provided by client.

3 INTRODUCTION

3.1 Scope & Methodology

This test report documents the cybersecurity assessment performed by Lyns-tci Technology Guangdong Co., Ltd.

The assessment is based on the Lyns-tci Technology Guangdong Co., Ltd Consumer Products Services Cybersecurity Assessment Methodology for ETSI EN 303 645 (CYBER-ETSI-EN-303 645).

The cybersecurity assessment of IoT devices is intended to verify and confirm that the Device under Test is in conformance with the baseline provisions as specified by ETSI in EN 303 645.

The assessment fully applies the procedures and methodology defined by ETSI in TS 103 701.

Due to the generic character of these ETSI documents some amendments are necessary for the performance of a conformance assessment. Lyns-tci Technology Guangdong Co., Ltd follows and applies the specific amendments as published by the German Federal Office for Information Security (BSI - Bundesamt für Sicherheit in der Informationstechnik) in BSI TR-03173.

The versions of referenced documents applied for this assessment are specified in the following table.

3.2 References

Document	Date	Version	Comments
ETSI EN 303 645	2020-06	V2.1.1	Cyber Security for Consumer Internet of Things: Baseline Requirements
ETSI TS 103 701	2021-08	V1.1.1	Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements
BSI TR-03173	2022-04-27	V1.0	Amendments for Conformance Assessments based on ETSI EN 303 645/TS 103 701

4 TARGET OF EVALUATION

The target of evaluation for this assessment is the IoT device including it’s interfaces and interactions with associated services.

As input to the assessment the manufacturer has provided information in the form of an Implementation Conformance Statement (ICS) and eXtra Information for Testing (IXIT). The proforma is defined by ETSI.

Additionally samples of the Device under Test (DUT) have been provided by the manufacturer to the Bureau Veritas.

4.1 Manufacturer Contact Information

Information	Manufacturer
Company Name	EAST Group Co., Ltd.
Address	No.6 Northern Industry Road, Songshan Lake Sci. & Tech. Industrial Park, Dongguan City, Guangdong Province, China
Contact Person	zhangjunfeng
E-Mail address	psirt@eastups.com
Phone Number	8613138038110

4.2 Vendor Questionnair (ICS&IXIT)

Filename of the ICS/IXIT provided by the manufacturer	Date/Version
ETSI_ICS_IXIT_v2024-11-13_EAST	2024-11-13

4.3 Device Under Test (DUT)

Information	Manufacturer
Product Name	Converter (Hybrid Inverter)
Type or Model	EAHI-6000-SL-S
Serial Number(s)	HI06CS2404220001
Software Version(s)	MCU:1035,DSP:1037/Version 1.3.709
Intended Use	smart home system is a 6kW solar storage charging system
Date of receipt	2024-11-12

Foto(s) of the DUT
See appendix Annex 1 - Photo of the unit on page 193

Foto(s) of the Marking Plate
/

Foto(s) of Architecture
/

4.4 Auxilliary Equipment

The following additional equipment and devices were used during the assessment but they are not included in the device under test. (e.g. used to bring the DUT into operation). Auxilliary Equipment is typically provided by the manufacturer.

Auxiliiary Equipment				
Component	**Function**	**Manufacturer**	**Model/Version**	**Serial Number**
Smartphone	Commissioning steps with DUT sample	(Google) Pixel 5	Android Original	/

5 TEST SETUP

The test setup consists of the DUT, auxiliary equipment, test equipment and test software tools. It is operated by the test lab and provides the environment in which the DUT is assessed.

The test equipment and test software tools are provided, maintained and are used by the test lab to execute the test procedures.

Foto(s) of the Test Setup
/

5.1 Test Equipment

Test Equipment used during the assessment				
Device Name	**Function**	**Manufacturer**	**Serial Number**	**Version**
Desktop computer	Windows11	lenovo	/	Vostro

5.2 Test Software Tools

Test Software Tools used during the assessment			
Tool/Script Name	**Function**	**Developer**	**Version**
Nessus	Vulnerability scanning	/	/
Wireshark	Network Protocol Analysis	/	/
Burp Suite Community Edition	Application Testing	/	/
Postman	interface authentication forensics	/	/
Nmap - Zenmap	Port scanning and operating system detection	/	/
mqttfx	Testing and Simulating MQTT Messaging	/	/

6 ASSESSMENT RESULTS

The assessment results relate only to the items tested.

First day of testing	Last day of testing
2024-11-18	2024-12-02

6.1 Overview

- The column "**Reference**" provides the Provision as defined in ETSI EN 303 645
- The column "**Status**" provides information, if the provision is mandatory (M) or recommended (R) and if it depends on a condition (C) as defined in ETSI TS 103 701 Annex A
- The column "**Support**" contains the declaration provided by the manufacturer in the ICS, if the provision is supported (Y) or not supported (N) by the DUT. Or N/A when the provision is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the DUT)
- The column "**Detail**" contains the information provided by the manufacturer in the ICS with explanations about the implementation or with reasons why "Support" is set to N or N/A.
- The column "**Conceptual**" contains the assessment of the test lab for the test cases marked as "conceptual" in ETSI TS 103 701
- The column "**Functional**" contains the assessment of the test lab for the test cases marked as "functional" in ETSI TS 103 701

- "**PASS**" verdict is assigned when the required elements for the test case performance are present; and the criteria for pass defined for each test step in the "Assignment of Verdict" are fulfilled.
- "**FAIL**" verdict is assigned when the required elements for the test case performance are present; and the criteria for fail defined for one of the test steps in the "Assignment of Verdict" are fulfilled.
- "**INCON**" = "Inconclusive" verdict is assigned when the required elements (e.g. evaluation tools and IXIT information) for the test case performance are not present or are not sufficient to allow a proper execution of the test case and therefore no meaningful pass or fail verdict can be assigned.
- "**N/E**" is assigned when the tester lab has **not evaluated** the requirement. This can be the case if the manufacturer answered in the ICS the Support = Not supported (N) or Not applicable (N/A).
- "**-**" means no test case for this category is specified by the standard.

Reference	Status	Support	Detail
Provision 4-1 A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the consumer IoT device.	M	Y	**PASS**
Provision 5.1-1 Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.	M C (1)	Y	**PASS**
Provision 5.1-2 Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.	M C (2)	N/A	**PASS**
Provision 5.1-3 Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.	M C (8)	Y	**PASS**
Provision 5.1-4 Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.	M C (8)	Y	**PASS**
Provision 5.1-5 When the device is not a constrained device, it shall have a mechanism available which makes brute force attacks on authentication mechanisms via via network interfaces impracticable.	M C (5)	Y	**PASS**
Provision 5.2-1 The manufacturer shall make a vulnerability disclosure policy publicly available.	M	Y	**PASS**
Provision 5.2-2 Disclosed vulnerabilities should be acted on in a timely manner	R	Y	**PASS**
Provision 5.2-3 Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.	R	Y	**PASS**
Provision 5.3-1 All software components in consumer IoT devices should be securely updateable.	R	Y	**PASS**
Provision 5.3-2 When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.	M C (5)	Y	**PASS**

Reference	Status	Support	Detail
Provision 5.3-3 An update shall be simple for the user to apply.	M C (12)	Y	**PASS**
Provision 5.3-4 Automatic mechanisms should be used for software updates.	R C (12)	N/A	**FAIL**
Provision 5.3-5 The device should check after initialization, and then periodically, whether security updates are available.	R C (12)	N/A	**FAIL**
Provision 5.3-6 If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.	R C (9, 12)	N/A	**FAIL**
Provision 5.3-7 The device shall use best practice cryptography to facilitate secure update mechanisms.	M C (12)	Y	**PASS**
Provision 5.3-8 Security updates shall be timely.	M C (12)	Y	**PASS**
Provision 5.3-9 The device should verify the authenticity and integrity of software updates.	R C (12)	Y	**PASS**
Provision 5.3-10 Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.	M (11, 12)	Y	**PASS**
Provision 5.3-11 The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.	R C (12)	Y	**N/A**
Provision 5.3-12 The device should notify the user when the application of a software update will disrupt the basic functioning of the device.	R C (12)	Y	**N/A**
Provision 5.3-13 The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.	M	Y	**PASS**
Provision 5.3-14 For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.	R C (3, 4)	N/A	**N/A**

Reference	Status	Support	Detail
Provision 5.3-15 For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.	R C (3, 4)	N/A	PASS
Provision 5.3-16 The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.	M	Y	PASS
5.4 Securely store sensitive security parameters	-		
Provision 5.4-1 Sensitive security parameters in persistent storage shall be stored securely by the device.	M C (14)	Y	PASS
Provision 5.4-2 Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.	M C (10)	N/A	PASS
Provision 5.4-3 Hard-coded critical security parameters in device software source code shall not be used.	M	Y	PASS
Provision 5.4-4 Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.	M C (15)	Y	PASS
5.5 Communicate securely	-		
Provision 5.5-1 The consumer IoT device shall use best practice cryptography to communicate securely.	M	Y	PASS
Provision 5.5-2 The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.	R	Y	PASS
Provision 5.5-3 Cryptographic algorithms and primitives should be updateable	R	Y	FAIL
Provision 5.5-4 Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.	R C (16)	Y	PASS
Provision 5.5-5 Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication.	M C (17)	Y	PASS

Reference	Status	Support	Detail
The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate			
Provision 5.5-6 Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.	R C (18)	Y	PASS
Provision 5.5-7 The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.	M C (19)	Y	PASS
Provision 5.5-8 The manufacturer shall follow secure management processes for critical security parameters that relate to the device.	M C (20)	Y	PASS
5.6 Minimize exposed attack surfaces	-		
Provision 5.6-1 All unused network and logical interfaces shall be disabled.	M	Y	PASS
Provision 5.6-2 In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.	M	Y	PASS
Provision 5.6-3 Device hardware should not unnecessarily expose physical interfaces to attack.	R	N/A	PASS
Provision 5.6-4 Where a debug interface is physically accessible, it shall be disabled in software.	M C (13)	N/A	PASS
Provision 5.6-5 The manufacturer should only enable software services that are used or required for the intended use or operation of the device.	R	Y	PASS
Provision 5.6-6 Code should be minimized to the functionality necessary for the service/device to operate.	R	Y	PASS
Provision 5.6-7 Software should run with least necessary privileges, taking account of both security and functionality.	R	Y	PASS
Provision 5.6-8 The device should include a hardware-level access control mechanism for memory.	R	Y	PASS
Provision 5.6-9 The manufacturer should follow secure development processes for software deployed on the device.	R	Y	FAIL
5.7 Ensure software integrity	-		

Reference	Status	Support	Detail
Provision 5.7-1 The consumer IoT device should verify its software using secure boot mechanisms.	R	N	N/A
Provision 5.7-2 If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.	R	N	N/A
5.8 Ensure that personal data is secure	-		
Provision 5.8-1 The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.	R C (21)	N/A	PASS
Provision 5.8-2 The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage	M C (22)	N/A	PASS
Provision 5.8-3 All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.	M C (23)	N/A	PASS
5.9 Make systems resilient to outages	-		
Provision 5.9-1 Resilience should be built in to consumer IoT devices and services, taking into account the possibility of outages of data networks and power.	R	Y	PASS
Provision 5.9-2 Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.	R	Y	PASS
Provision 5.9-3 The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.	R	Y	PASS
5.10 Examine system telemetry data	-		
Provision 5.10-1 If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.	R C (6)	N/A	FAIL
5.11 Make it easy for users to delete user data	-		

Reference	Status	Support	Detail
Provision 5.11-1 The user shall be provided with functionality such that user data can be erased from the device in a simple manner.	M C (24)	Y	FAIL
Provision 5.11-2 The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.	R C (25)	Y	FAIL
Provision 5.11-3 Users should be given clear instructions on how to delete their personal data.	R C (26)	Y	N/A
Provision 5.11-4 Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.	R C (26)	Y	N/A
5.12 Make installation and maintenance of devices easy	-		
Provision 5.12-1 Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.	R	Y	PASS
Provision 5.12-2 The manufacturer should provide users with guidance on how to securely set up their device.	R	Y	FAIL
Provision 5.12-3 The manufacturer should provide users with guidance on how to check whether their device is securely set up.	R	Y	FAIL
5.13 Validate input data	-		
Provision 5.13-1 The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.	M C (27)	Y	PASS
6 Data protection provisions for consumer IoT	-		
Provision 6-1 The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.	M C (28)	Y	FAIL
Provision 6-2 Where personal data is processed on the basis of consumers'	M C (7)	Y	PASS

Reference	Status	Support	Detail
consent, this consent shall be obtained in a valid way.			
Provision 6-3 Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.	M C (7)	Y	**FAIL**
Provision 6-4 If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.	R C (6)	N/A	**FAIL**
Provision 6-5 If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.	M C (6)	N/A	**PASS**

6.2 Overview 1

Provision	Description	Verdict
Reporting implementation		
4-1-1	ICS reporting implementation	PASS (M)
No universal default passwords		
5.1-1	Unique per device passwords	PASS (M)
5.1-2	Pre-installed password randomness	N/E (M)
5.1-3	Authentication mechanism cryptography	PASS (M)
5.1-4	Ability to change authentication value	PASS (M)
5.1-5	Network interface brute force protection	PASS (M)
Implement a means to manage reports of vulnerabilities		
5.2-1	Means to report vulnerabilities	PASS (M)
5.2-2	Acting on disclosed vulnerabilities	N/E
5.2-3	Company monitoring, vulnerability identifying and rectifying	N/E
Keep software update		
5.3-1	Securely updateable	N/E
5.3-2	Secure installation of updates	PASS (M)
5.3-3	Ease of updating	PASS (M)
5.3-4	Automatic update	N/E
5.3-5	Timeliness of security updates	N/E
5.3-6	Software update mechanism modification	N/E
5.3-7	Cryptography in update mechanism	PASS (M)
5.3-8	Security updates shall be timely	PASS (M)
5.3-9	Authenticity and integrity of updates	N/E
5.3-10	Network cryptography in update mechanism	PASS (M)
5.3-11	Security update information	N/E
5.3-12	Disruption of basic functionality	N/E
5.3-13	Product support	PASS (M)
5.3-14	Period and method of hardware replacement support	N/E
5.3-15	Hardware isolation and replacement	N/E
5.3-16	Informing of model number	PASS (M)
Securely store sensitive security parameters		
5.4-1	Sensitive security parameters storage	PASS (M)
5.4-2	Hard coded unique id tamper protection	N/E
5.4-3	Hard coded critical security parameters	PASS (M)
5.4-4	Unique resistant critical security parameters	PASS (M)
Communicate securely		
5.5-1	Cryptography in communication	PASS (M)
5.5-2	Usage of reviewed or evaluated implementations	N/E

5.5-3	Cryptoagility	N/E
5.5-4	Network access in initialized state before authentication	N/E
5.5-5	Security relevant changes through network access before authentication	PASS (M)
5.5-6	Encryption of critical security parameters in transit	N/E
5.5-7	Confidentiality of critical security parameters in transit	PASS (M)
5.5-8	Critical security parameters management	PASS (M)
Minimize exposed attack surface		
5.6-1	Justification concerning interfaces exposure	PASS (M)
5.6-2	Unauthenticated exposure in the initialized state through network	PASS (M)
5.6-3	Exposure of physical interfaces	N/E
5.6-4	Software setting for debug interfaces	N/E
5.6-5	Unnecessary software services	N/E
5.6-6	Code attack surface	N/E
5.6-7	Least necessary privilege	N/E
5.6-8	Memory access control	N/E
5.6-9	Secure development training	N/E
Ensure software integrity		
5.7-1	Secure boot implementation	N/E
5.7-2	Unauthorized access alert	N/E
Ensure that personal data is secure		
5.8-1	Cryptography used for personal data communication	N/E
5.8-2	Cryptography used for sensitive personal communication	N/E
5.8-3	Data protection and privacy	N/E
Make system resilient to outages		
5.9-1	Resilience against power/network outages	N/E
5.9-2	Basic function during outage and clean recover	N/E
5.9-3	Stable (re)connection	N/E
Examine system telemetry data		
5.10-1	Telemetry data examination	N/E
Make it easy for users to delete user data		
5.11-1	Ease of personal data deletion from device	PASS (M)
5.11-2	Ease of personal data deletion from services	N/E
5.11-3	Instructions on deletion of personal data	N/E
5.11-4	Confirmation of deletion	N/E
Make installation and maintenance of devices easy		
5.12-1	Ease and security of installation and maintenance	N/E
5.12-2	Guidance on securing the device	N/E
5.12-3	Guidance on checking security	N/E

Validate input data		
5.13-1	Input data validation	PASS (M)
Data protection for consumer IoT		
6-1	Personal data usage	PASS (M)
6-2	Obtaining consumer consent	PASS (M)
6-3	Consumer consent withdrawal	PASS (M)
6-4	Confidentiality of personal data	N/E
6-5	Confidentiality of sensitive personal data	N/E

6.3 Test Case Assessments

The test case assessment has been executed according the test procedures described in ETSI TS 103 701.

6.3.1 Reporting implementation

Test Case 4.1-1	
PROVISION 4.1	A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the consumer IoT device.
Applicability	Mandatory
Type of Assessment	Conceptual
Assignment of verdict	The verdict **PASS** is assigned if: - a justification is given for every recommendation that is considered to be not applicable for the DUT; AND - a justification is given for every recommendation that is considered to be not fulfilled by the DUT. The verdict **FAIL** is assigned otherwise.

Test Result
PASS

Note:

Conformity statement are decided in accordance with ILAC-G8:09/2019 Binary Statement for Simple Acceptance Rule, unless otherwise normatively specified or contractually agreed.

6.4 No universal default passwords

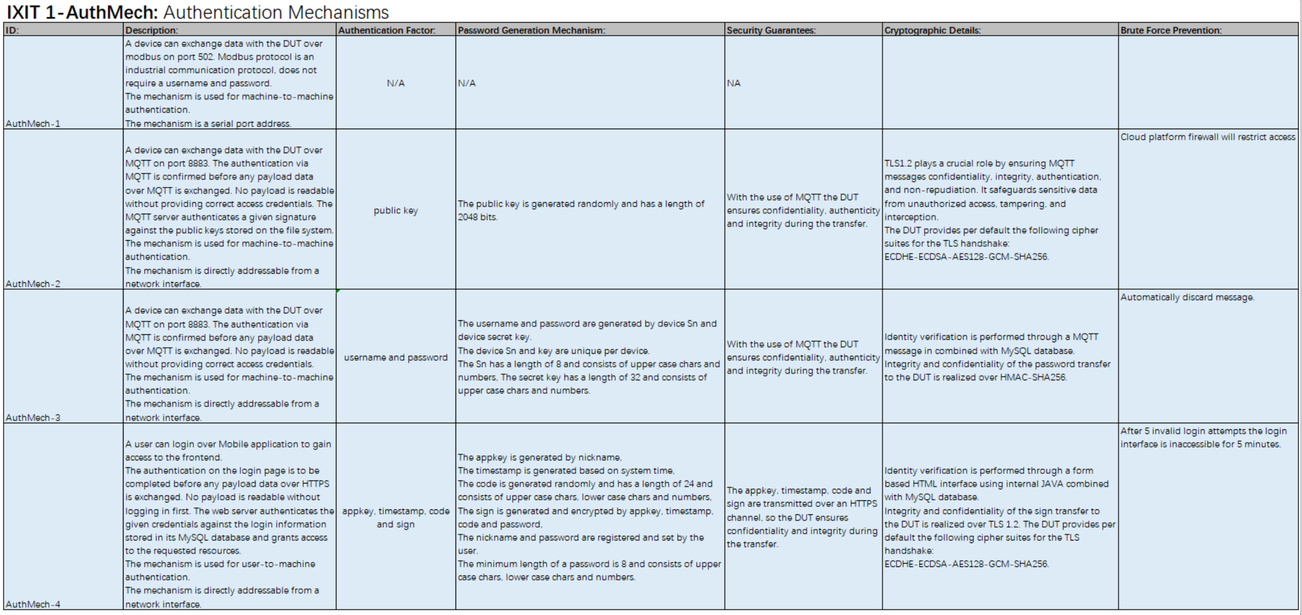
6.4.1.1 Unique per device

Test Case 5.1-1-1	
PROVISION 5.1-1	Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.
Applicability	M C(1) = Mandatory Conditional C(1) = Where passwords are used.
Type of Assessment	Conceptual
Assignment of verdict	The verdict **PASS** is assigned if: - Each password of a password-based authentication mechanism being used in any state other than the factory default, that is not defined by the user, is unique per device. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 1-AuthMech: Authentication Mechanisms

ID:	Description:	Authentication Factor:	Password Generation Mechanism:	Security Guarantees:	Cryptographic Details:	Brute Force Prevention:
AuthMech-1	A device can exchange data with the DUT over modbus on port 502. Modbus protocol is an industrial communication protocol, does not require a username and password. The mechanism is used for machine-to-machine authentication. The mechanism is a serial port address.	N/A	N/A	NA		
AuthMech-2	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The MQTT server authenticates a given signature against the public keys stored on the file system. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	public key	The public key is generated randomly and has a length of 2048 bits.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	TLS1.2 plays a crucial role by ensuring MQTT messages confidentiality, integrity, authentication, and non-repudiation. It safeguards sensitive data from unauthorized access, tampering, and interception. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	Cloud platform firewall will restrict access
AuthMech-3	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	username and password	The username and password are generated by device Sn and device secret key. The device Sn and key are unique per device. The Sn has a length of 8 and consists of upper case chars and numbers. The secret key has a length of 32 and consists of upper case chars and numbers.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	Identity verification is performed through a MQTT message in combined with MySQL database. Integrity and confidentiality of the password transfer to the DUT is realized over HMAC-SHA256.	Automatically discard message.
AuthMech-4	A user can login over Mobile application to gain access to the frontend. The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its MySQL database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	appkey, timestamp, code and sign	The appkey is generated by nickname, The timestamp is generated based on system time, The code is generated randomly and has a length of 24 and consists of upper case chars, lower case chars and numbers, The sign is generated and encrypted by appkey, timestamp, code and password, The nickname and password are registered and set by the user. The minimum length of a password is 8 and consists of upper case chars, lower case chars and numbers.	The appkey, timestamp, code and sign are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Identity verification is performed through a form based HTML interface using internal JAVA combined with MySQL database. Integrity and confidentiality of the sign transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	After 5 invalid login attempts the login interface is inaccessible for 5 minutes.

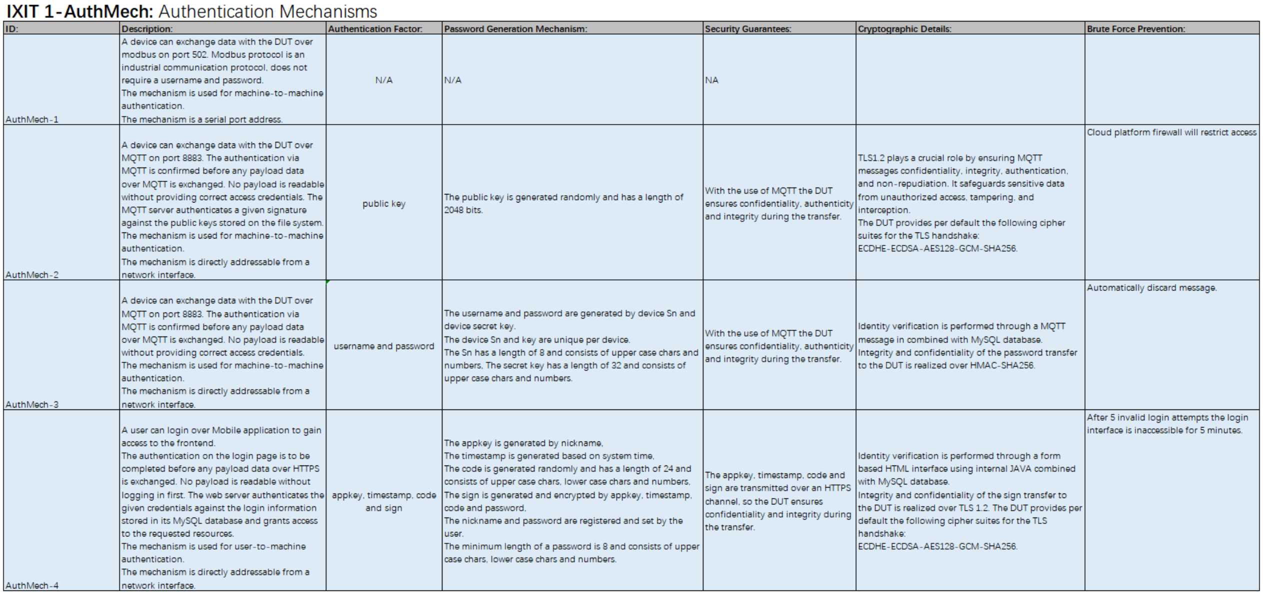
According to the information provided by IXIT 1-AuthMe, the device has two types of connectivity. in AuthMech-2 the connection is made via MQTTs, using account password authentication, where the username and password are generated from the device serial number and the device number, and the user password is 32 in length and consists of alphanumeric characters; and in AuthMech-4 the connection is made to the device via an app, where the username and password are generated by the user registration, the minimum length of user password is 8 and consists of letters and numbers.

Therefore, this test case is considered passed.

Test Case 5.1-1-2	
PROVISION 5.1-1	Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

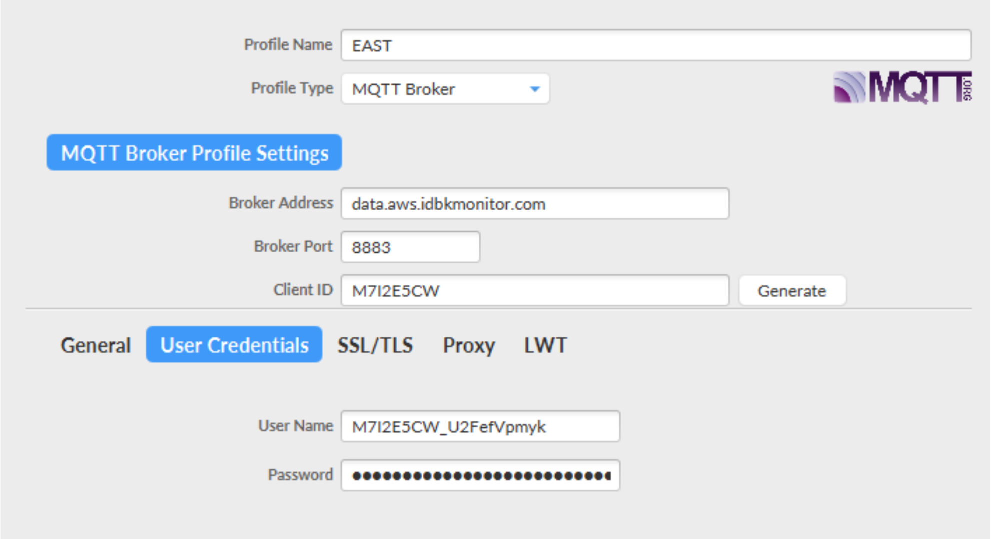
Applicability	M C(1) =Mandatory Conditional C(1) = Where passwords are used.
Type of Assessment	Conceptual
Assignment of verdict	The verdict **PASS** is assigned if: • Every discovered password-based authentication mechanism is documented in the IXIT; **AND** • The user is required to define all passwords before being used, that are stated as defined by the user in the IXIT **AND** • There is no indication that the generation of a not user-defined password of the DUT used in any state other than the factory default differs from the generation mechanism described in the IXIT. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 1-AuthMech: Authentication Mechanisms

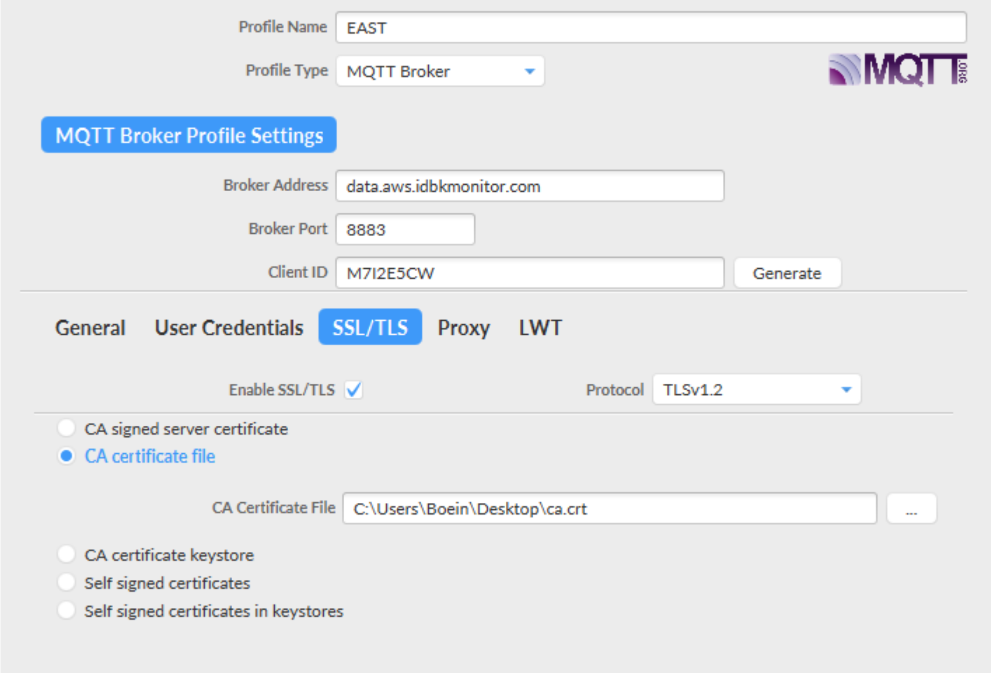
ID:	Description:	Authentication Factor:	Password Generation Mechanism:	Security Guarantees:	Cryptographic Details:	Brute Force Prevention:
AuthMech-1	A device can exchange data with the DUT over modbus on port 502. Modbus protocol is an industrial communication protocol, does not require a username and password. The mechanism is used for machine-to-machine authentication. The mechanism is a serial port address.	N/A	N/A	NA		
AuthMech-2	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The MQTT server authenticates a given signature against the public keys stored on the file system. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	public key	The public key is generated randomly and has a length of 2048 bits.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	TLS1.2 plays a crucial role by ensuring MQTT messages confidentiality, integrity, authentication, and non-repudiation. It safeguards sensitive data from unauthorized access, tampering, and interception. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	Cloud platform firewall will restrict access
AuthMech-3	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	username and password	The username and password are generated by device Sn and device secret key. The device Sn and key are unique per device. The Sn has a length of 8 and consists of upper case chars and numbers, The secret key has a length of 32 and consists of upper case chars and numbers.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	Identity verification is performed through a MQTT message in combined with MySQL database. Integrity and confidentiality of the password transfer to the DUT is realized over HMAC-SHA256.	Automatically discard message.
AuthMech-4	A user can login over Mobile application to gain access to the frontend. The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its MySQL database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	appkey, timestamp, code and sign	The appkey is generated by nickname, The timestamp is generated based on system time, The code is generated randomly and has a length of 24 and consists of upper case chars, lower case chars and numbers, The sign is generated and encrypted by appkey, timestamp, code and password, The nickname and password are registered and set by the user. The minimum length of a password is 8 and consists of upper case chars, lower case chars and numbers.	The appkey, timestamp, code and sign are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Identity verification is performed through a form based HTML interface using internal JAVA combined with MySQL database. Integrity and confidentiality of the sign transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	After 5 invalid login attempts the login interface is inaccessible for 5 minutes.



Profile Name: EAST
Profile Type: MQTT Broker

Broker Address: data.aws.idbkmonitor.com
Broker Port: 8883
Client ID: M7I2E5CW

User Name: M7I2E5CW_U2FefVpmyk
Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●



Profile Name: EAST
Profile Type: MQTT Broker

Broker Address: data.aws.idbkmonitor.com
Broker Port: 8883
Client ID: M7I2E5CW

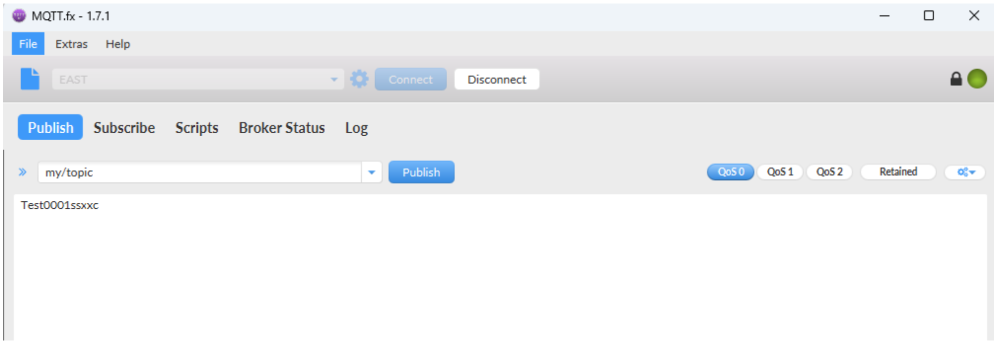
Enable SSL/TLS ✓
Protocol: TLSv1.2

○ CA signed server certificate
● CA certificate file

CA Certificate File: C:\Users\Boein\Desktop\ca.crt

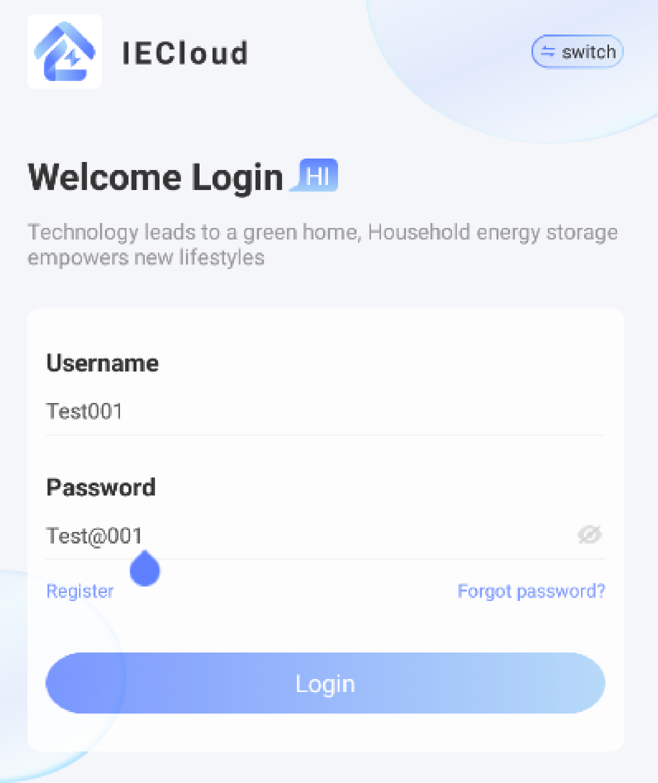
○ CA certificate keystore
○ Self signed certificates
○ Self signed certificates in keystores

Based on AuthMech-2 and AuthMech-3 in IXIT 1-AuthMech, the tester logs in to the client on port 8883 and needs to log in using an account password, which is made up of the device serial number and the device number and is encrypted by sha256. The integrity and authenticity verification of the communication is done through key pairs.



my/topic

Test0001ssxxc



Technology leads to a green home, Household energy storage empowers new lifestyles

Username
Test001

Password
Test@001

The tester needs to register the account password first, and then use the registered account password to log into the app. complexity checks were done on the username and user password, and both met the complexity requirements.

This test, passes.

Test Case 5.1-2-1

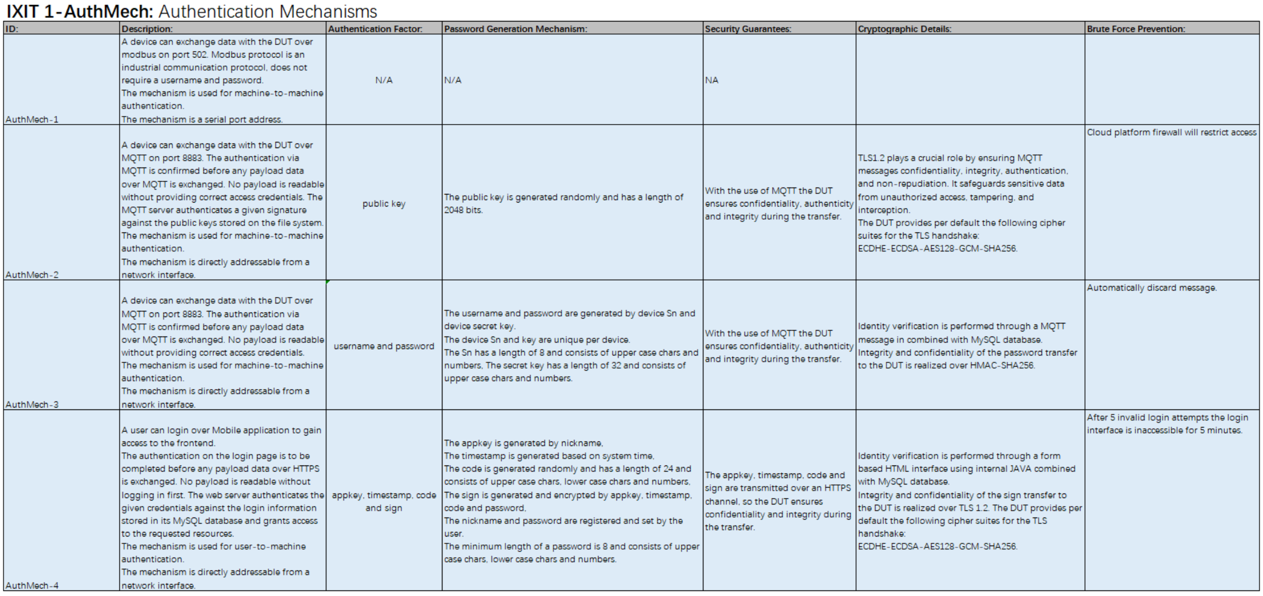
PROVISION 5.1-2	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
Applicability	M C(2) =Mandatory Conditional C(2) = Where pre-installed passwords are used.
Type of Assessment	Conceptual

Assignment of verdict	The verdict **PASS** is assigned if: - No obvious regularities in pre-installed passwords is found; **AND** - No common strings or other common patterns in pre-installed passwords is found; **AND** - The generation mechanisms for pre-installed passwords do not induce passwords, That are related in an obvious - way to public information; **AND** - The generation mechanisms for pre-installed passwords are considered appropriate in terms of complexity The verdict **FAIL** is assigned otherwise

Test Result

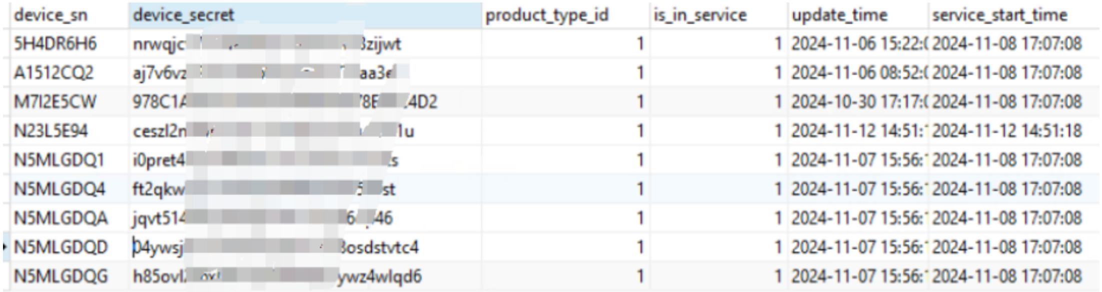
PASS

Testlab Comments



IXIT 1-AuthMech: Authentication Mechanisms

ID:	Description:	Authentication Factor:	Password Generation Mechanism:	Security Guarantees:	Cryptographic Details:	Brute Force Prevention:
AuthMech-1	A device can exchange data with the DUT over modbus on port 502. Modbus protocol is an industrial communication protocol, does not require a username and password. The mechanism is used for machine-to-machine authentication. The mechanism is a serial port address.	N/A	N/A	NA		
AuthMech-2	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The MQTT server authenticates a given signature against the public keys stored on the file system. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	public key	The public key is generated randomly and has a length of 2048 bits.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	TLS1.2 plays a crucial role by ensuring MQTT messages confidentiality, integrity, authentication, and non-repudiation. It safeguards sensitive data from unauthorized access, tampering, and interception. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	Cloud platform firewall will restrict access
AuthMech-3	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	username and password	The username and password are generated by device Sn and device secret key. The device Sn and key are unique per device. The Sn has a length of 8 and consists of upper case chars and numbers, The secret key has a length of 32 and consists of upper case chars and numbers.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	Identity verification is performed through a MQTT message in combined with MySQL database. Integrity and confidentiality of the password transfer to the DUT is realized over HMAC-SHA256.	Automatically discard message.
AuthMech-4	A user can login over Mobile application to gain access to the frontend. The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its MySQL database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	appkey, timestamp, code and sign	The appkey is generated by nickname, The timestamp is generated based on system time, The code is generated randomly and has a length of 24 and consists of upper case chars, lower case chars and numbers, The sign is generated and encrypted by appkey, timestamp, code and password, The nickname and password are registered and set by the user. The minimum length of a password is 8 and consists of upper case chars, lower case chars and numbers.	The appkey, timestamp, code and sign are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Identity verification is performed through a form based HTML interface using internal JAVA combined with MySQL database. Integrity and confidentiality of the sign transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	After 5 invalid login attempts the login interface is inaccessible for 5 minutes.



device_sn	device_secret	product_type_id	is_in_service	update_time	service_start_time
5H4DR6H6	nrwqjc[redacted]3zijwt	1	1	2024-11-06 15:22:(	2024-11-08 17:07:08
A1512CQ2	aj7v6vz[redacted]aa3e	1	1	2024-11-06 08:52:(	2024-11-08 17:07:08
M7I2E5CW	978C1A[redacted]4D2	1	1	2024-10-30 17:17:(	2024-11-08 17:07:08
N23L5E94	ceszl2n[redacted]1u	1	1	2024-11-12 14:51:1	2024-11-12 14:51:18
N5MLGDQ1	i0pret4[redacted]s	1	1	2024-11-07 15:56:1	2024-11-08 17:07:08
N5MLGDQ4	ft2qkw[redacted]st	1	1	2024-11-07 15:56:1	2024-11-08 17:07:08
N5MLGDQA	jqvt514[redacted]46	1	1	2024-11-07 15:56:1	2024-11-08 17:07:08
N5MLGDQD	b4ywsj[redacted]3osdstvtc4	1	1	2024-11-07 15:56:1	2024-11-08 17:07:08
N5MLGDQG	h85ovl[redacted]ywz4wlqd6	1	1	2024-11-07 15:56:1	2024-11-08 17:07:08

According to the information provided in AuthMech-2 in IXIT 1-AuthMech, referenced in 5.1-1-2, the device login password is compliant with the strength, and by searching the database, there is no apparent pattern in the password, which is consistent with randomness.

The user password in AuthMech-4 is user-set and conforms to the complexity requirements in IXIT.

Therefore, this test case is considered passed.

Test Case 5.1-2-2

PROVISION 5.2-1	Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.
Applicability	M C(2) =Mandatory Conditional C(2) = Where pre-installed passwords are used.
Type of Assessment	Conceptual
Assignment of verdict	The verdict **PASS** is assigned if: - for each pre-installed password there is no indication, that its generation differs from the generation mechanism described in the IXIT. The verdict **FAIL** is assigned otherwise.

Test Result
PASS

Testlab Comments
Refer to Test Case 5.1-2-1 above.

6.4.1.2 Provision 5.1-3

M (8): Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.

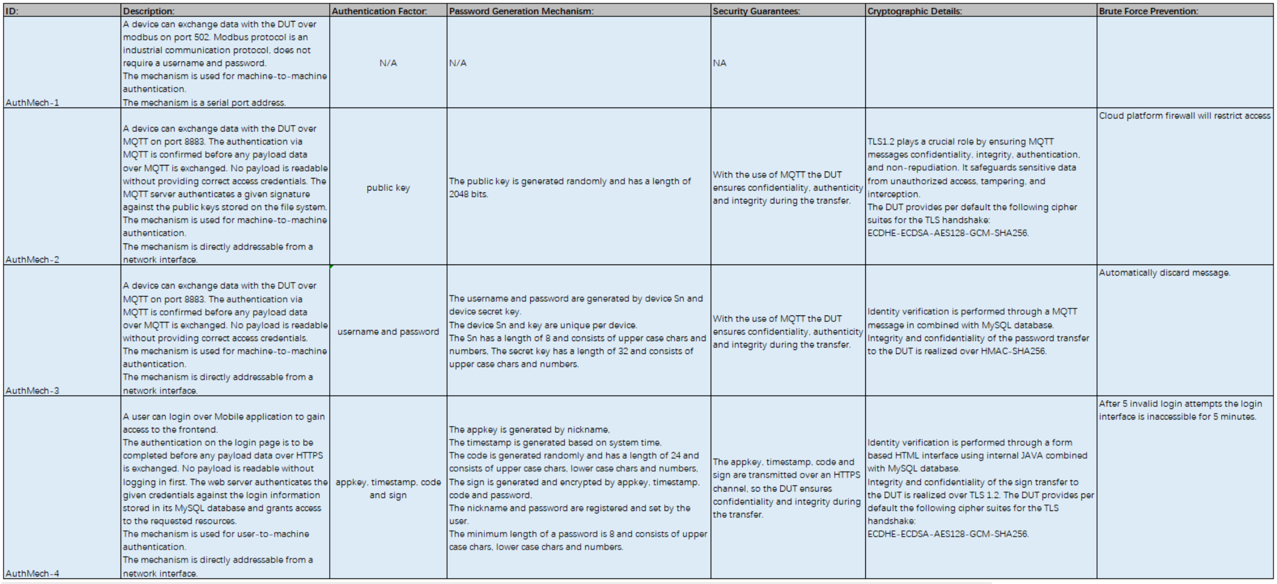
This provision relates to the cryptography usage of the device in authentication mechanisms, both in terms of protocols and algorithms. They have to be appropriate as define by the risk analysis done during preliminary tasks.

TC_UNIVERSAL_PASSWORDS#5 / Test case 5.1.3-1	
Security requirement	PROVISION 5.1-3
Type of work	IXIT analysis
Applicability	Conditional (the device allowing user authentication)
Documentation analysis objectives	Verify that the device does not implement insecure or obsolete authentication mechanisms
Evaluation inputs	- Collected authentication management from **IXIT 1-AuthMech**
Documentation analysis procedure	a) For each authentication mechanism in **IXIT 1-AuthMech** used to authenticate users against the DUT, tester assess whether the **Security Guarantees** are appropriate for the use case of user authentication, at least integrity and authenticity are required to be fulfilled. b) For each authentication mechanism in **IXIT 1-AuthMech** used to authenticate users against the DUT, assess whether the mechanism according to **Description** is appropriate to achieve the **Security Guarantees**. c) For each authentication mechanism in **IXIT 1-AuthMech** used to authenticate users against the DUT, tester assess whether the **Cryptographic Details** are considered as best practice cryptography for the use case of user authentication based on a reference catalogue. General reference catalogues of best practice cryptography are available, for example: SOGIS Agreed Cryptographic Mechanisms (https://www.sogis.eu). For other cases please refer to ETSI 701 details d) For each authentication mechanism in **IXIT 1-AuthMech** used to authenticate users against the DUT, tester assess whether the **Cryptographic Details** are not known to be vulnerable to a feasible attack for the desired security property on the base of the **Security Guarantees** by reference to competent cryptanalytic reports.
Verdict	The verdict **PASS** is assigned if for all user authentication mechanisms: - The security guarantees are appropriate for the use case of user authentication; **AND** - The mechanism is appropriate to achieve the security guarantees with respect to the use case; **AND** - All used cryptographic details are considered as best practice for the use case; **AND** - All used cryptographic details are not known to be vulnerable to a feasible attack for the desired security property. The verdict **FAIL** is assigned otherwise.

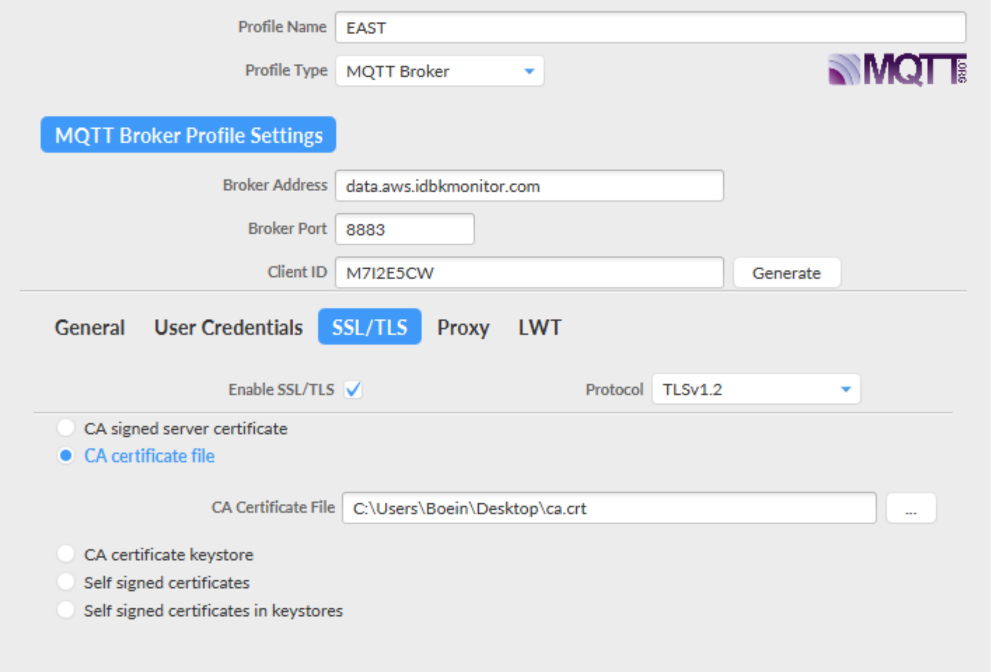
Test Result
PASS

Testlab Comments

IXIT 1-AuthMech: Authentication Mechanisms



ID:	Description:	Authentication Factor:	Password Generation Mechanism:	Security Guarantees:	Cryptographic Details:	Brute Force Prevention:
AuthMech-1	A device can exchange data with the DUT over modbus on port 502. Modbus protocol is an industrial communication protocol, does not require a username and password. The mechanism is used for machine-to-machine authentication. The mechanism is a serial port address.	N/A	N/A	NA		
AuthMech-2	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The MQTT server authenticates a given signature against the public keys stored on the file system. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	public key	The public key is generated randomly and has a length of 2048 bits.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	TLS1.2 plays a crucial role by ensuring MQTT messages confidentiality, integrity, authentication, and non-repudiation. It safeguards sensitive data from unauthorized access, tampering, and interception. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	Cloud platform firewall will restrict access
AuthMech-3	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	username and password	The username and password are generated by device Sn and device secret key. The device Sn and key are unique per device. The Sn has a length of 8 and consists of upper case chars and numbers, The secret key has a length of 32 and consists of upper case chars and numbers.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	Identity verification is performed through a MQTT message in combined with MySQL database. Integrity and confidentiality of the password transfer to the DUT is realized over HMAC-SHA256.	Automatically discard message.
AuthMech-4	A user can login over Mobile application to gain access to the frontend. The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its MySQL database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	appkey, timestamp, code and sign	The appkey is generated by nickname, The timestamp is generated based on system time, The code is generated randomly and has a length of 24 and consists of upper case chars, lower case chars and numbers, The sign is generated and encrypted by appkey, timestamp, code and password, The nickname and password are registered and set by the user. The minimum length of a password is 8 and consists of upper case chars, lower case chars and numbers.	The appkey, timestamp, code and sign are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Identity verification is performed through a form based HTML interface using internal JAVA combined with MySQL database. Integrity and confidentiality of the sign transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	After 5 invalid login attempts the login interface is inaccessible for 5 minutes.



Profile Name: EAST

Profile Type: MQTT Broker

MQTT Broker Profile Settings

Broker Address: data.aws.idbkmonitor.com

Broker Port: 8883

Client ID: M7I2E5CW

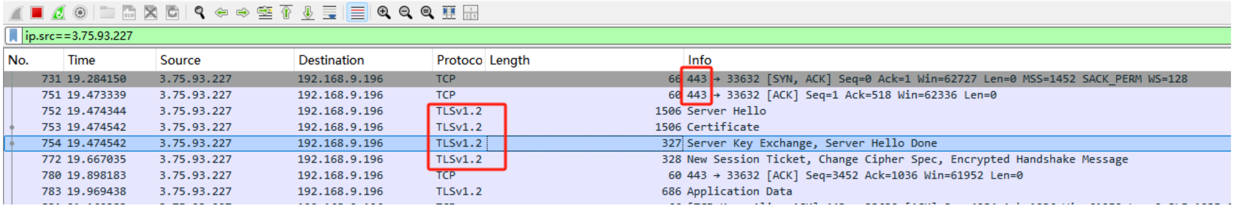
Enable SSL/TLS ☑ Protocol: TLSv1.2

○ CA signed server certificate
● CA certificate file

CA Certificate File: C:\Users\Boein\Desktop\ca.crt

○ CA certificate keystore
○ Self signed certificates
○ Self signed certificates in keystores

Based on the description of IXIT 1-AuthMech, the MQTT connection method in AuthMech-2/3, the tester performed login verification and confirmed that the TLS1.2 protocol, certificate, and user password login authentication were used, in accordance with the documentation information.



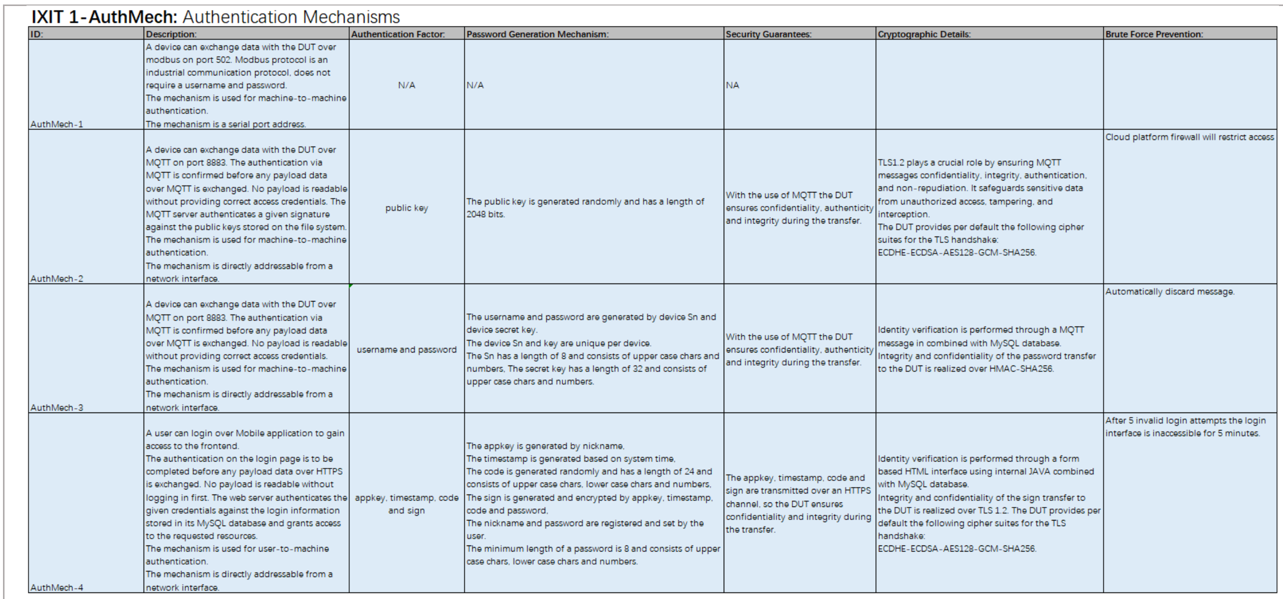
```
ip.src==3.75.93.227

No.   Time       Source       Destination   Protoco Length  Info
  731 19.284150  3.75.93.227  192.168.9.196 TCP         66  443 → 33632 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1452 SACK_PERM WS=128
  751 19.473339  3.75.93.227  192.168.9.196 TCP         60  443 → 33632 [ACK] Seq=1 Ack=518 Win=62336 Len=0
  752 19.474344  3.75.93.227  192.168.9.196 TLSv1.2   1506  Server Hello
  753 19.474542  3.75.93.227  192.168.9.196 TLSv1.2   1506  Certificate
  754 19.474542  3.75.93.227  192.168.9.196 TLSv1.2    327  Server Key Exchange, Server Hello Done
  772 19.667035  3.75.93.227  192.168.9.196 TLSv1.2    328  New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  780 19.898183  3.75.93.227  192.168.9.196 TCP         60  443 → 33632 [ACK] Seq=3452 Ack=1036 Win=61952 Len=0
  783 19.969438  3.75.93.227  192.168.9.196 TLSv1.2    686  Application Data
```

The application connection method in AuthMech-4, with tester login verification, confirms that the service uses the https+tls1.2 protocol and conforms to the documented information.
The test passed.

TC_UNIVERSAL_PASSWORDS#6 / Test case 5.1.3-2	
Security requirement	PROVISION 5.1-3
Type of work	Test CAB
Applicability	Conditional (the device allowing user authentication)
Test objectives	Functional evaluation of the authentication mechanisms
Evaluation inputs	- At least one device suitable for testing - Collected authentication management from **IXIT 1-AuthMech**
Test scenario	**Precondition:** - The devices shall be operating under normal conditions. - Test plan for authentication mechanisms after usage analysis **Test sequence:** a) For each authentication mechanism in **IXIT 1-AuthMech** used to authenticate users against the DUT, tester assess whether the described **Cryptographic Details** are used by the DUT. **Expected result:** ✓ Functional status of authentication mechanisms
Verdict	The verdict **PASS** is assigned if: - There is no indication that any used cryptographic setting differs from its IXIT documentation. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 1-AuthMech: Authentication Mechanisms

ID:	Description:	Authentication Factor:	Password Generation Mechanism:	Security Guarantees:	Cryptographic Details:	Brute Force Prevention:
AuthMech-1	A device can exchange data with the DUT over modbus on port 502. Modbus protocol is an industrial communication protocol, does not require a username and password. The mechanism is used for machine-to-machine authentication. The mechanism is a serial port address.	N/A	N/A	NA		
AuthMech-2	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The MQTT server authenticates a given signature against the public keys stored on the file system. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	public key	The public key is generated randomly and has a length of 2048 bits.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	TLS1.2 plays a crucial role by ensuring MQTT messages confidentiality, integrity, authentication, and non-repudiation. It safeguards sensitive data from unauthorized access, tampering, and interception. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	Cloud platform firewall will restrict access
AuthMech-3	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	username and password	The username and password are generated by device Sn and device secret key. The device Sn and key are unique per device. The Sn has a length of 8 and consists of upper case chars and numbers, The secret key has a length of 32 and consists of upper case chars and numbers.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	Identity verification is performed through a MQTT message in combined with MySQL database. Integrity and confidentiality of the password transfer to the DUT is realized over HMAC-SHA256.	Automatically discard message.
AuthMech-4	A user can login over Mobile application to gain access to the frontend. The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its MySQL database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	appkey, timestamp, code and sign	The appkey is generated by nickname, The timestamp is generated based on system time, The code is generated randomly and has a length of 24 and consists of upper case chars, lower case chars and numbers, The sign is generated and encrypted by appkey, timestamp, code and password, The nickname and password are registered and set by the user. The minimum length of a password is 8 and consists of upper case chars, lower case chars and numbers.	The appkey, timestamp, code and sign are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Identity verification is performed through a form based HTML interface using internal JAVA combined with MySQL database. Integrity and confidentiality of the sign transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	After 5 invalid login attempts the login interface is inaccessible for 5 minutes.

According to the information provided by IXIT 1-AuthMe, the device has two connection methods.

In AuthMech-2 /3, the connection is made via MQTT, using account password authentication, the username and password are generated from the device serial number and the device number, and the user password has a length of 32 and consists of alphanumeric characters. In conjunction with 5.1-1-2, this encryption method is consistent with the IXIT documentation.

In AuthMech-4, the connection to the device is made through the application, the username and password are generated from the user registration, and the minimum length of the user password is 8, consisting of alphanumeric characters. In conjunction with 5.1-1-2, this encryption method is compliant with the IXIT documentation.

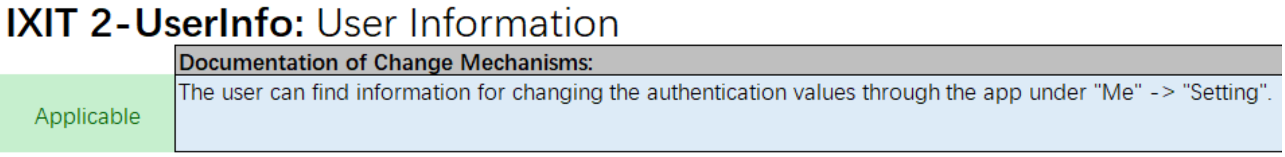
Therefore, the test case is considered passed.

6.4.1.3 Provision 5.1-4

M C (8): where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication values used

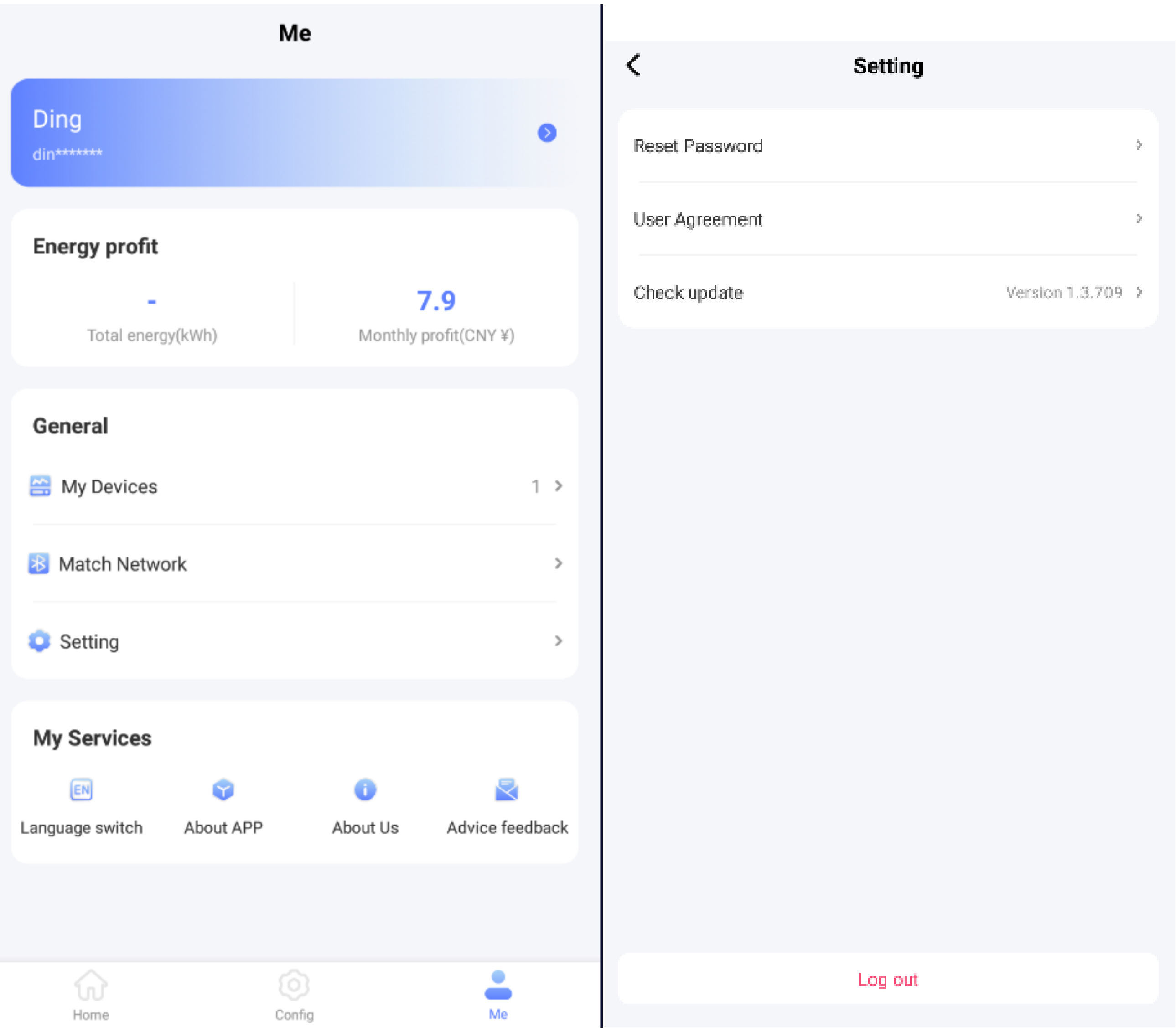
TC_UNIVERSAL_PASSWORDS#7 / Test case 5.1.4-1	
Security requirement	PROVISION 5.1-4
Type of work	Test CAB
Applicability	Conditional (the device allowing user authentication)
Test objectives	Check if means provided by the manufacturer to change authentication values is simple for a common user
Evaluation inputs	- At least one device / User Guide / list of change authentication mechanism - Collected authentication management from **IXIT 1-AuthMech** - Documentation of Change Mechanisms from **IXIT 2-UserInfo**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence**: a) Tester assess whether for every authentication mechanism in **IXIT 1-AuthMech** where **Description** indicates that the mechanism is used for user authentication, the resource of **Documentation of Change Mechanisms** in **IXIT 2-UserInfo** considers the mechanism and describes how to change the authentication value for the mechanism in a manner that is understandable for a user with limited technical knowledge (cf. Annex D.3 of ETSI EN 103 701). **Expected result:** ✓ Benchmark of the simplicity for a common user to change authentication value
Verdict	The verdict PASS is assigned if: - For all user based authentication mechanisms the published resource describes how to change the authentication value with a simple mechanism. The verdict FAIL is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 2-UserInfo: User Information

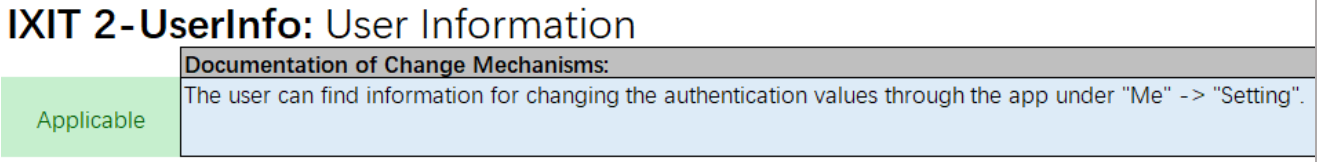
	Documentation of Change Mechanisms:
Applicable	The user can find information for changing the authentication values through the app under "Me" -> "Setting".



According to IXIT 2-UserInfo, the user can make changes to the user password on the app.
The tester views the app and refers to the guidance provided in the documentation to perform a change operation on the user's password.
The test, passed.

TC_UNIVERSAL_PASSWORDS#8: / Test case 5.1.4-2	
Security requirement	PROVISION 5.1-4
Type of work	Test CAB
Applicability	Conditional (the device allowing user authentication)
Test objectives	Check if authentication values modification mechanisms provided by the manufacturer works like expected
Evaluation inputs	- At least one device - Collected authentication management from **IXIT 1-AuthMech** - Documentation of Change Mechanisms from **IXIT 2-UserInfo**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) Tester perform a change of the authentication values for all user authentication mechanisms in **IXIT 1-AuthMech** as documented in the resource from **Documentation of Change Mechanism** in **IXIT 2-UserInfo**. b) Tester assess whether all changes of user authentication values are successful. **Expected result:** ✓ Modification of authentication values successes (old ones are no longer valid, and the new ones are valid after change)
Verdict	The verdict **PASS** is assigned if: - All mechanisms for the user to change authentication values for user authentication mechanisms work as described. The verdict **FAIL** is assigned otherwise.

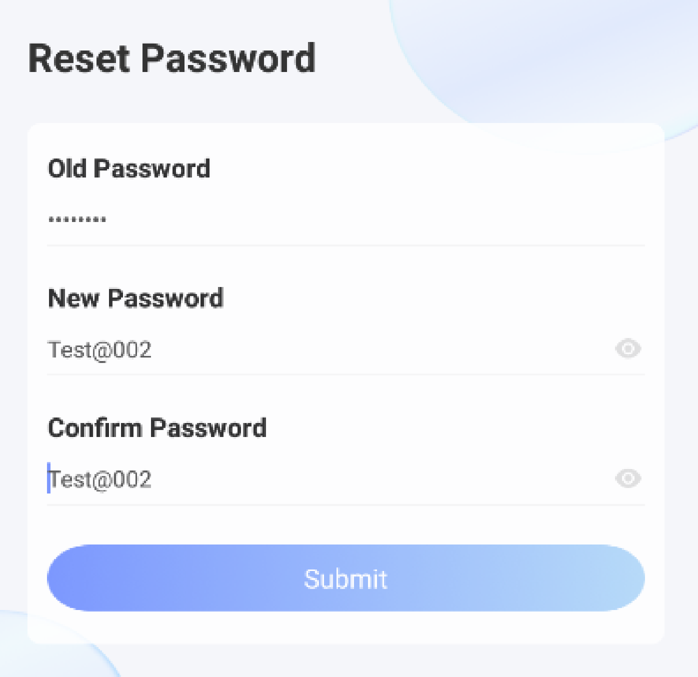
Test Result
PASS
Testlab Comments



IXIT 2-UserInfo: User Information

	Documentation of Change Mechanisms:
Applicable	The user can find information for changing the authentication values through the app under "Me" -> "Setting".

Users can change your password by going to “Me-Setting-Reset Password” in the app.



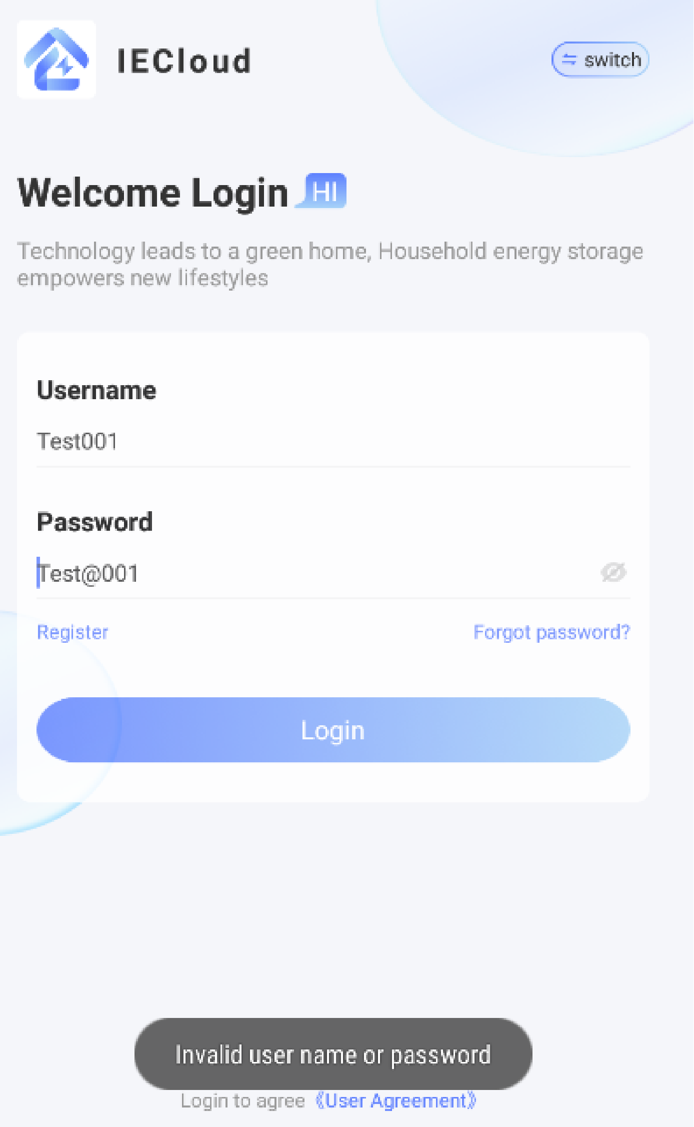
Reset Password

Old Password: ••••••••

New Password: Test@002

Confirm Password: Test@002

The tester conducts a change password test, changing the original password “Test@001” to a new password “Test@002”, which requires verification of the old password, and the strength of the new password is also verified.


IECloud
switch
Welcome Login HI
Technology leads to a green home, Household energy storage empowers new lifestyles
Username
Test001
Password
Test@001
Register
Forgot password?
Login
Invalid user name or password
Login to agree 《User Agreement》

After the tester changed the password, the old password login test was performed and the old password was no longer available.
This test, passed.

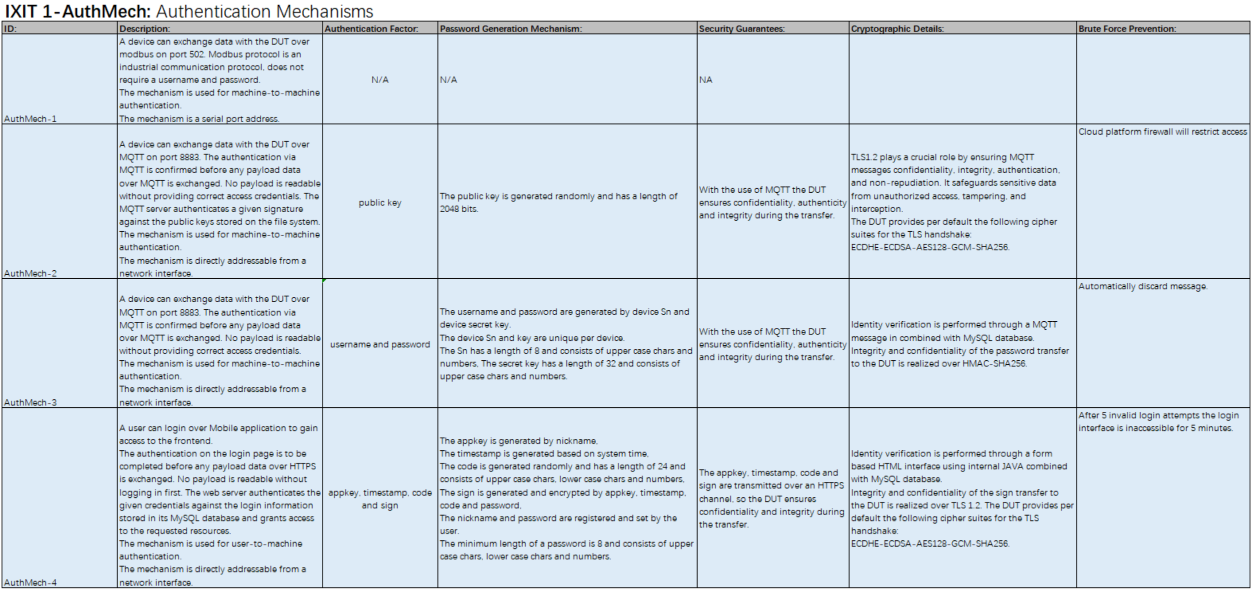
6.4.1.4 Provision 5.1-5

M.C (5): When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.

This provision relates to counter-measures to avoid brute force attacks through network interfaces.

TC_UNIVERSAL_PASSWORDS#9 / Test case 5.1.5-1	
Security requirement	PROVISION 5.1-5
Type of work	Doc
Applicability	Conditional (the device is not contrained)
Documentation analysis objectives	Verify that the device does not allow brute force authentication mechanisms
Evaluation inputs	- Collected authentication management from **IXIT 1-AuthMech**
Documentation analysis procedure	a) Tester assess whether for each authentication mechanism in **IXIT 1-AuthMech**, where **Description** indicates that the mechanism is directly addressable via a network interface, the mechanism in **Brute Force Prevention** makes brute force attacks via network interfaces impracticable.
Verdict	The verdict **PASS** is assigned if: - The documented mechanisms make brute force attacks via network interfaces impracticable. The verdict **FAIL** is assigned otherwise.

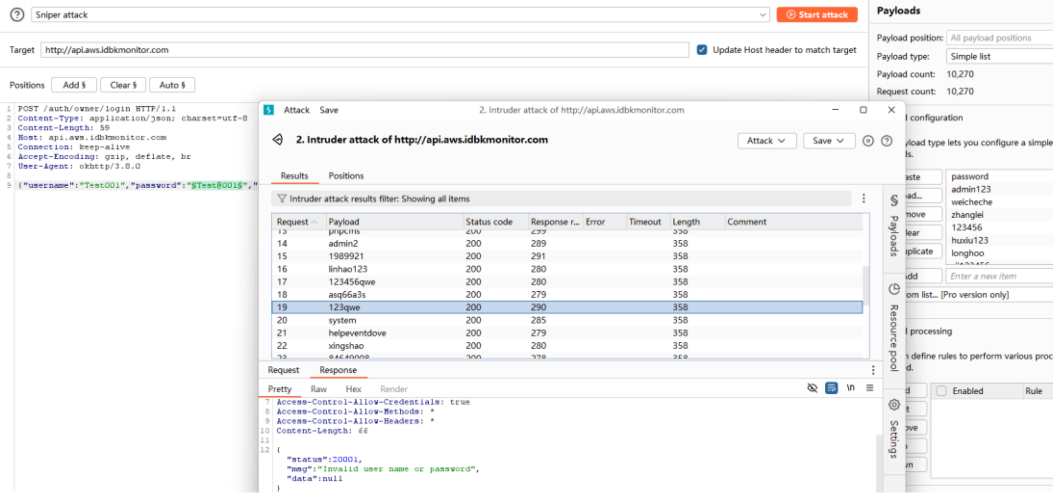
Test Result
PASS
Testlab Comments



IXIT 1-AuthMech: Authentication Mechanisms

ID:	Description:	Authentication Factor:	Password Generation Mechanism:	Security Guarantees:	Cryptographic Details:	Brute Force Prevention:
AuthMech-1	A device can exchange data with the DUT over modbus on port 502. Modbus protocol is an industrial communication protocol, does not require a username and password. The mechanism is used for machine-to-machine authentication. The mechanism is a serial port address.	N/A	N/A	NA		
AuthMech-2	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The MQTT server authenticates a given signature against the public keys stored on the file system. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	public key	The public key is generated randomly and has a length of 2048 bits.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	TLS1.2 plays a crucial role by ensuring MQTT messages confidentiality, integrity, authentication, and non-repudiation. It safeguards sensitive data from unauthorized access, tampering, and interception. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	Cloud platform firewall will restrict access
AuthMech-3	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	username and password	The username and password are generated by device Sn and device secret key. The device Sn and key are unique per device. The Sn has a length of 8 and consists of upper case chars and numbers. The secret key has a length of 32 and consists of upper case chars and numbers.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	Identity verification is performed through a MQTT message in combined with MySQL database. Integrity and confidentiality of the password transfer to the DUT is realized over HMAC-SHA256.	Automatically discard message.
AuthMech-4	A user can login over Mobile application to gain access to the frontend. The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its MySQL database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	appkey, timestamp, code and sign	The appkey is generated by nickname, The timestamp is generated based on system time, The code is generated randomly and has a length of 24 and consists of upper case chars, lower case chars and numbers, The sign is generated and encrypted by appkey, timestamp, code and password, The nickname and password are registered and set by the user. The minimum length of a password is 8 and consists of upper case chars, lower case chars and numbers.	The appkey, timestamp, code and sign are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Identity verification is performed through a form based HTML interface using internal JAVA combined with MySQL database. Integrity and confidentiality of the sign transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	After 5 invalid login attempts the login interface is inaccessible for 5 minutes.

According to the description in IXIT 1-AuthMech, the service is deployed on Amazon, whose PAAS platform provides hosted DDoS protection services.



Target: http://api.aws.idbkmonitor.com

☑ Update Host header to match target

```
POST /auth/owner/login HTTP/1.1
Content-Type: application/json; charset=utf-8
Content-Length: 59
Host: api.aws.idbkmonitor.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/3.8.0

{"username":"Test001","password":"§Test@001§","
```

Payload position: All payload positions
Payload type: Simple list
Payload count: 10,270
Request count: 10,270

password
admin123
weicheche
zhanglei
123456
huxiu123
longhoo

Enter a new item

om list... [Pro version only]

2. Intruder attack of http://api.aws.idbkmonitor.com

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response r...	Error	Timeout	Length	Comment
14	admin2	200	289			358	
15	1989921	200	291			358	
16	linhao123	200	280			358	
17	123456qwe	200	280			358	
18	asq66a3s	200	279			358	
19	123qwe	200	290			358	
20	system	200	285			358	
21	helpeventdove	200	279			358	
22	xingshao	200	280			358	

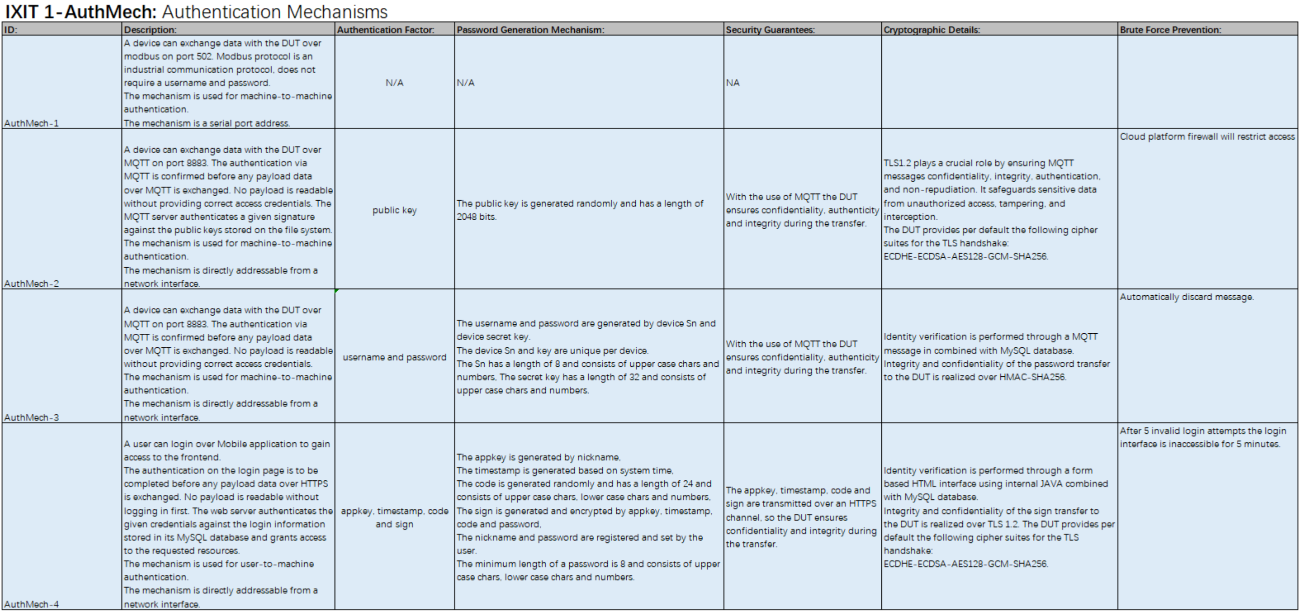
```
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Length: 66

{
  "status":20001,
  "msg":"Invalid user name or password",
  "data":null
}
```

Testers conducted a brute-force attack test on the login interface, which was unsuccessful.
This test, passed.

TC_UNIVERSAL_PASSWORDS#10 / Test case 5.1.5-2	
Security requirement	PROVISION 5.1-5
Type of work	Test CAB
Applicability	Conditional (the device is not contrained)
Test objectives	Assess that brute force attacks are impracticable
Evaluation inputs	- At least one device - Collect authentication management from **IXIT 1-AuthMech**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) Tester assess whether there exist further network-based authentication mechanisms, that are not listed in **IXIT 1-AuthMech**. b) Tester attempt to brute force every network-based authentication mechanisms described in **IXIT 1-AuthMech**. **Expected result:** ✓ Result authentication mechanisms
Verdict	The verdict **PASS** is assigned if: - Ever discovered network-based authentication mechanism is documented in the IXIT; **AND** - For all authentication mechanism via network interfaces there is no indication that the implementation of brute force prevention differs from its IXIT documentation. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 1-AuthMech: Authentication Mechanisms

ID:	Description:	Authentication Factor:	Password Generation Mechanism:	Security Guarantees:	Cryptographic Details:	Brute Force Prevention:
AuthMech-1	A device can exchange data with the DUT over modbus on port 502. Modbus protocol is an industrial communication protocol, does not require a username and password. The mechanism is used for machine-to-machine authentication. The mechanism is a serial port address.	N/A	N/A	NA		
AuthMech-2	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The MQTT server authenticates a given signature against the public keys stored on the file system. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	public key	The public key is generated randomly and has a length of 2048 bits.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	TLS1.2 plays a crucial role by ensuring MQTT messages confidentiality, integrity, authentication, and non-repudiation. It safeguards sensitive data from unauthorized access, tampering, and interception. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	Cloud platform firewall will restrict access
AuthMech-3	A device can exchange data with the DUT over MQTT on port 8883. The authentication via MQTT is confirmed before any payload data over MQTT is exchanged. No payload is readable without providing correct access credentials. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	username and password	The username and password are generated by device Sn and device secret key. The device Sn and key are unique per device. The Sn has a length of 8 and consists of upper case chars and numbers, The secret key has a length of 32 and consists of upper case chars and numbers.	With the use of MQTT the DUT ensures confidentiality, authenticity and integrity during the transfer.	Identity verification is performed through a MQTT message in combined with MySQL database. Integrity and confidentiality of the password transfer to the DUT is realized over HMAC-SHA256.	Automatically discard message.
AuthMech-4	A user can login over Mobile application to gain access to the frontend. The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its MySQL database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	appkey, timestamp, code and sign	The appkey is generated by nickname, The timestamp is generated based on system time, The code is generated randomly and has a length of 24 and consists of upper case chars, lower case chars and numbers, The sign is generated and encrypted by appkey, timestamp, code and password, The nickname and password are registered and set by the user. The minimum length of a password is 8 and consists of upper case chars, lower case chars and numbers.	The appkey, timestamp, code and sign are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Identity verification is performed through a form based HTML interface using internal JAVA combined with MySQL database. Integrity and confidentiality of the sign transfer to the DUT is realized over TLS 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256.	After 5 invalid login attempts the login interface is inaccessible for 5 minutes.

Based on IXIT 1-AuthMech, has provided various authentication methods of brute force breaking defense mechanism.
Testers using tools to violently break and inject were unsuccessful.
This test is judged to have passed.

6.5 Implement a means to manage reports of vulnerabilities

6.5.1 IXIT Data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 2-UserInfo: User Information:

The completed IXIT lists documentations, publications and information provided to users.

Publication of Vulnerability Disclosure Policy:	Description of the way the vulnerability disclosure policy is published, including all information to access the publication.

IXIT 3-VulnTypes: Relevant Vulnerabilities

The completed IXIT lists all types of vulnerabilities that are relevant for the DUT.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the kind of vulnerability that is relevant for the DUT. **NOTE**: *Hardware, software and firmware are possible kinds of vulnerabilities. If all vulnerabilities are covered by a single process a separation is not necessary.*
Action:	Description of the way of acting on this kind of vulnerability in case of a vulnerability disclosure including all entities and responsibilities. **NOTE**: *Rolling out patches and publishing advisories are possible actions in this case.*
Time Frame:	Targeted time frame in which the given steps of the action in case of a vulnerability are scheduled. **EXAMPLE**: *5 days for initial response and 90 days until publication of the patch.*

IXIT 4-Conf: Confirmations

The completed IXIT lists confirmations for the establishment of processes.

Confirmation of Vulnerability Actions (Yes/No):	Confirmation that for every "**Action**" described in **IXIT 3- VulnTypes** the required infrastructure is in place and operators are briefed in order to achieve the targeted "**Time Frame**".
Confirmation of Vulnerability Monitoring (Yes/No):	Confirmation that for every vulnerability monitoring, identifying and rectifying described in **IXIT 4-VulnMon** the required infrastructure is in place and operators are briefed.

IXIT 5-VulnMon: Vulnerability Monitoring

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Description of the way security vulnerabilities are monitored, identified and rectified in products and services. **NOTE**: Procedures for identifying vulnerabilities commonly include assessments whether a potential vulnerability is relevant for a certain product, responsible persons, an approach to gather information and a workflow to perform in case a vulnerability is discovered.

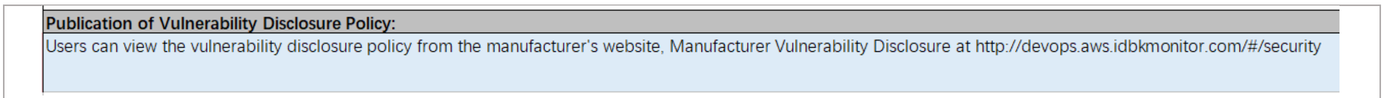
6.5.2 Evaluation tasks

6.5.2.1 Provision 5.2-1

- **M:** The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum:
  - Contact information for reporting issues; and
  - All Information's related to disclosure policy must be publicly available, which means that anyone has access to it.

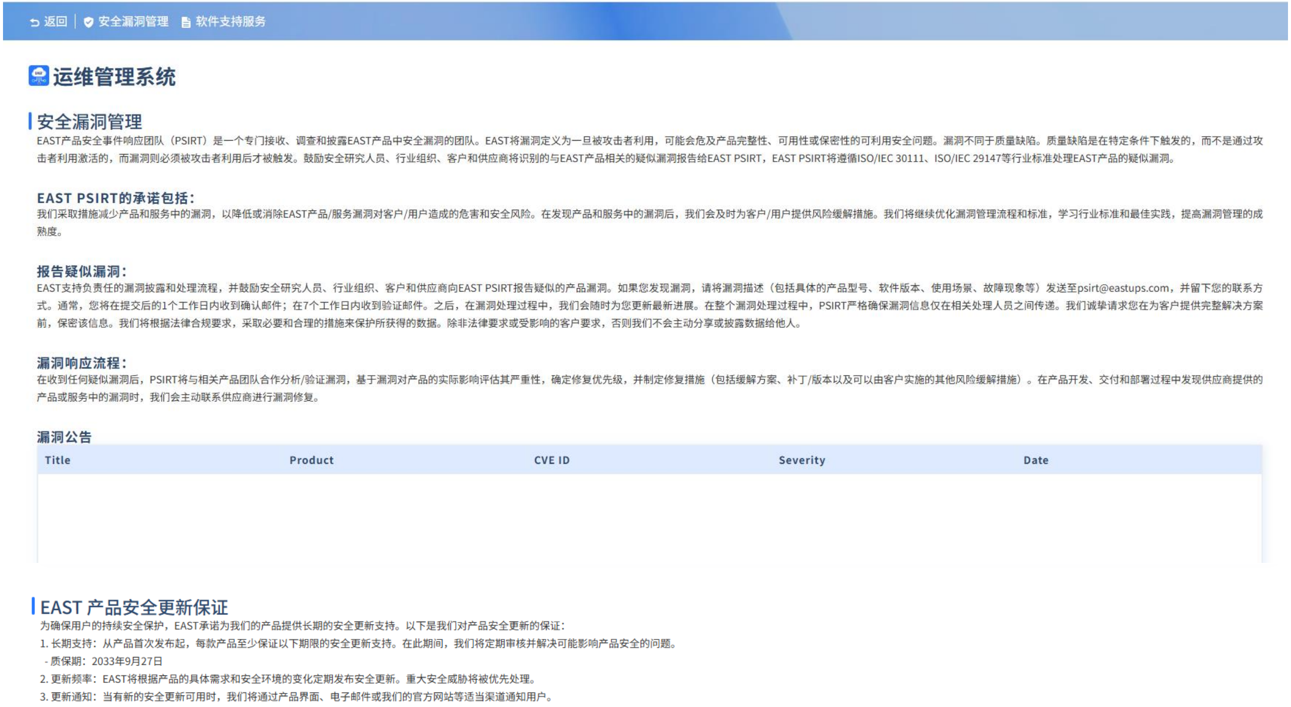
TC_VULNERABILITY_REPORTING#1 / Test case 5.2-1-1	
Security requirement	PROVISION 5.2-1
Type of work	Doc
Applicability	Always
Documentation analysis objectives	Verify that vulnerability disclosure policy publication is available to anybody
Evaluation inputs	**"Publication of vulnerability disclosure"** in **IXIT 2-UserInfo**
Documentation analysis procedure	Do a short analysis of the vulnerability disclosure policy publication (for instance referring to ISO/IEC 29147). a) Tester access to the publication as described in "**Publication of Vulnerability Disclosure Policy**" in **IXIT 2-UserInfo** is possible without meeting criteria such as user account, i.e. whether anybody can access the documentation.
Verdict	The verdict **PASS** is assigned if: - Publication of the vulnerability disclosure policy is available to anybody The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



Publication of Vulnerability Disclosure Policy:
Users can view the vulnerability disclosure policy from the manufacturer's website, Manufacturer Vulnerability Disclosure at http://devops.aws.idbkmonitor.com/#/security

Based on the Publication of Vulnerability Disclosure Policy in IXIT 2-UserInfo, the manufacturer's vulnerability disclosure policy is available at http://devops.aws.idbkmonitor.com/#/security.



运维管理系统

安全漏洞管理

EAST产品安全事件响应团队（PSIRT）是一个专门接收、调查和披露EAST产品中安全漏洞的团队。EAST将漏洞定义为一旦被攻击者利用，可能会危及产品完整性、可用性或保密性的可利用安全问题。漏洞不同于质量缺陷。质量缺陷是在特定条件下触发的，而不是通过攻击者利用激活的，而漏洞则必须被攻击者利用后才被触发。鼓励安全研究人员、行业组织、客户和供应商将识别的与EAST产品相关的疑似漏洞报告给EAST PSIRT，EAST PSIRT将遵循ISO/IEC 30111、ISO/IEC 29147等行业标准处理EAST产品的疑似漏洞。

EAST PSIRT的承诺包括：

我们采取措施减少产品和服务中的漏洞，以降低或消除EAST产品/服务漏洞对客户/用户造成的危害和安全风险。在发现产品和服务中的漏洞后，我们会及时为客户/用户提供风险缓解措施。我们将继续优化漏洞管理流程和标准，学习行业标准和最佳实践，提高漏洞管理的成熟度。

报告疑似漏洞：

EAST支持负责任的漏洞披露和处理流程，并鼓励安全研究人员、行业组织、客户和供应商向EAST PSIRT报告疑似的产品漏洞。如果您发现漏洞，请将漏洞描述（包括具体的产品型号、软件版本、使用场景、故障现象等）发送至psirt@eastups.com，并留下您的联系方式。通常，您将在提交后的1个工作日内收到确认邮件；在7个工作日内收到验证邮件。之后，在漏洞处理过程中，我们会随时为您更新最新进展。在整个漏洞处理过程中，PSIRT严格确保漏洞信息仅在相关处理人员之间传递。我们诚挚请求您在为客户提供完整解决方案前，保密该信息。我们将根据法律合规要求，采取必要和合理的措施来保护所获得的数据。除非法律要求或受影响的客户要求，否则我们不会主动分享或披露数据给他人。

漏洞响应流程：

在收到任何疑似漏洞后，PSIRT将与相关产品团队合作分析/验证漏洞，基于漏洞对产品的实际影响评估其严重性，确定修复优先级，并制定修复措施（包括缓解方案、补丁/版本以及可以由客户实施的其他风险缓解措施）。在产品开发、交付和部署过程中发现供应商提供的产品或服务中的漏洞时，我们会主动联系供应商进行漏洞修复。

漏洞公告

Title	Product	CVE ID	Severity	Date

EAST 产品安全更新保证

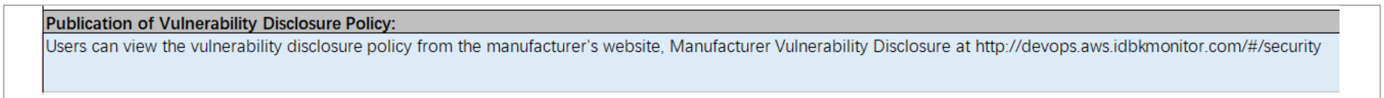
为确保用户的持续安全保护，EAST承诺为我们的产品提供长期的安全更新支持。以下是我们对产品安全更新的保证：

1. 长期支持：从产品首次发布起，每款产品至少保证以下期限的安全更新支持。在此期间，我们将定期审核并解决可能影响产品安全的问题。
   - 质保期：2033年9月27日
2. 更新频率：EAST将根据产品的具体需求和安全环境的变化定期发布安全更新。重大安全威胁将被优先处理。
3. 更新通知：当有新的安全更新可用时，我们将通过产品界面、电子邮件或我们的官方网站等适当渠道通知用户。

Testers can see that the manufacturer manages security vulnerabilities from the manufacturer's security vulnerability slip-up site, which allows every user to view and submit questions.
This test, passed.

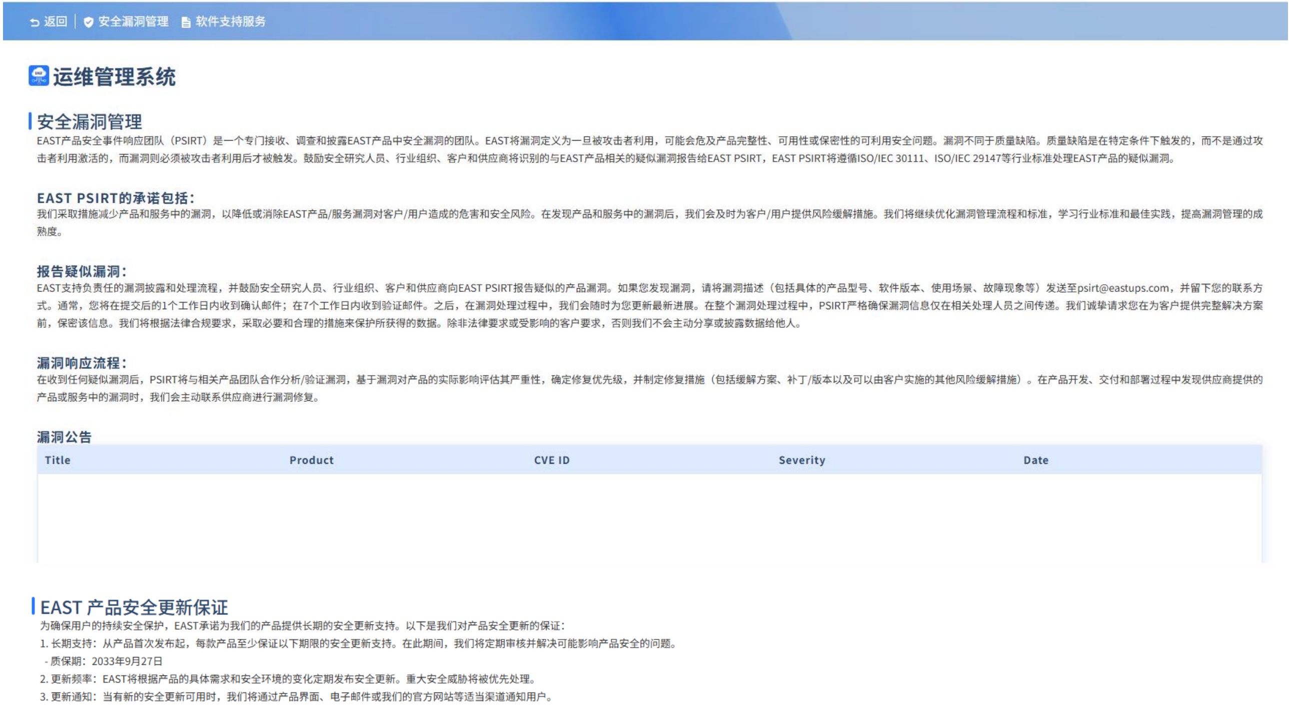
TC_VULNERABILITY_REPORTING #2 / Test case 5.2-1-2	
Security requirement	PROVISION 5.2-1
Type of work	Doc
Applicability	Always
Documentation analysis objectives	Verify that vulnerability disclosure policy publication contains contact information and information about timelines regarding acknowledgement of receipt and status updates.
Evaluation inputs	**"Publication of Vulnerability Disclosure Policy"** in **IXIT 2-UserInfo**
Documentation analysis procedure	a) Tester assess whether the vulnerability disclosure policy is publicly accessible as described in **"Publication of Vulnerability Disclosure Policy" in IXIT 2-UserInfo** b) Tester do a short analysis of the **vulnerability disclosure policy publication** Tester check whether in the user manual and in the information's bonded to the device that vulnerability disclosure policy contains - Contact information - Information about timelines regarding acknowledgement of receipt and status updates
Verdict	The verdict **PASS** is assigned if: - The vulnerability disclosure policy is publicly accessible; **AND** - The vulnerability disclosure policy contains contact information and information on timelines regarding acknowledgement of receipt and status updates. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



Publication of Vulnerability Disclosure Policy:
Users can view the vulnerability disclosure policy from the manufacturer's website, Manufacturer Vulnerability Disclosure at http://devops.aws.idbkmonitor.com/#/security

Based on the Publication of Vulnerability Disclosure Policy in IXIT 2-UserInfo, the manufacturer's vulnerability disclosure policy is available at http://devops.aws.idbkmonitor.com/#/security.



运维管理系统

安全漏洞管理

EAST产品安全事件响应团队（PSIRT）是一个专门接收、调查和披露EAST产品中安全漏洞的团队。EAST将漏洞定义为一旦被攻击者利用，可能会危及产品完整性、可用性或保密性的可利用安全问题。漏洞不同于质量缺陷。质量缺陷是在特定条件下触发的，而不是通过攻击者利用激活的，而漏洞则必须被攻击者利用后才被触发。鼓励安全研究人员、行业组织、客户和供应商将识别的与EAST产品相关的疑似漏洞报告给EAST PSIRT，EAST PSIRT将遵循ISO/IEC 30111、ISO/IEC 29147等行业标准处理EAST产品的疑似漏洞。

EAST PSIRT的承诺包括：

我们采取措施减少产品和服务中的漏洞，以降低或消除EAST产品/服务漏洞对客户/用户造成的危害和安全风险。在发现产品和服务中的漏洞后，我们会及时为客户/用户提供风险缓解措施。我们将继续优化漏洞管理流程和标准，学习行业标准和最佳实践，提高漏洞管理的成熟度。

报告疑似漏洞：

EAST支持负责任的漏洞披露和处理流程，并鼓励安全研究人员、行业组织、客户和供应商向EAST PSIRT报告疑似的产品漏洞。如果您发现漏洞，请将漏洞描述（包括具体的产品型号、软件版本、使用场景、故障现象等）发送至psirt@eastups.com，并留下您的联系方式。通常，您将在提交后的1个工作日内收到确认邮件；在7个工作日内收到验证邮件。之后，在漏洞处理过程中，我们会随时为您更新最新进展。在整个漏洞处理过程中，PSIRT严格确保漏洞信息仅在相关处理人员之间传递。我们诚挚请求您在为客户提供完整解决方案前，保密该信息。我们将根据法律合规要求，采取必要和合理的措施来保护所获得的数据。除非法律要求或受影响的客户要求，否则我们不会主动分享或披露数据给他人。

漏洞响应流程：

在收到任何疑似漏洞后，PSIRT将与相关产品团队合作分析/验证漏洞，基于漏洞对产品的实际影响评估其严重性，确定修复优先级，并制定修复措施（包括缓解方案、补丁/版本以及可以由客户实施的其他风险缓解措施）。在产品开发、交付和部署过程中发现供应商提供的产品或服务中的漏洞时，我们会主动联系供应商进行漏洞修复。

漏洞公告

Title	Product	CVE ID	Severity	Date

EAST 产品安全更新保证

为确保用户的持续安全保护，EAST承诺为我们的产品提供长期的安全更新支持。以下是我们对产品安全更新的保证：

1. 长期支持：从产品首次发布起，每款产品至少保证以下期限的安全更新支持。在此期间，我们将定期审核并解决可能影响产品安全的问题。
   - 质保期：2033年9月27日
2. 更新频率：EAST将根据产品的具体需求和安全环境的变化定期发布安全更新。重大安全威胁将被优先处理。
3. 更新通知：当有新的安全更新可用时，我们将通过产品界面、电子邮件或我们的官方网站等适当渠道通知用户。

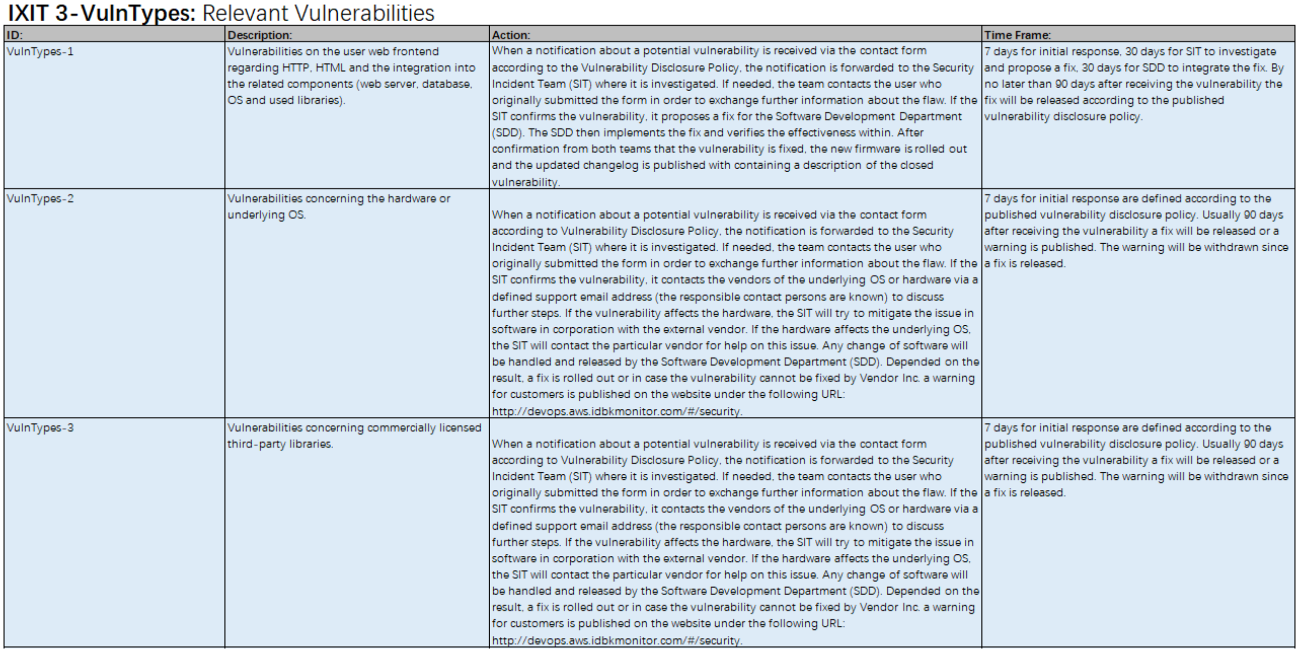
Testers can see that the manufacturer manages security vulnerabilities from the manufacturer's security vulnerability slip-up site, which allows every user to view and submit questions.
The site provides a complete vulnerability management process, an email address for submitting vulnerabilities, and a response time for receiving vulnerability questions.
This test, passed.

6.5.2.2 Provision 5.2-2

R: Disclosed vulnerabilities should be acted on in a timely manner

TC_VULNERABILITY_REPORTING# 3 / Test case 5.2-2-1	
Security requirement	PROVISION 5.2-2
Type of work	Doc
Applicability	Always
Documentation analysis objectives	Assess declaration from manufacturer on the way he manages vulnerability disclosure, and whether is done in a timely manner
Evaluation inputs	- **“Action”** & **“Time Frame”** from I**XIT 3-Vulntypes** - **“Publication of vulnerability disclosure policy”** from **IXIT 2-UserInfo** - **“Confirmation of vulnerability actions”** from **IXIT 4- Conf**
Documentation analysis procedure	a) Assess whether the "**Action**" and the "**Time Frame**" of each disclosed vulnerability in **IXIT 3-VulnTypes** facilitate that vulnerabilities are acted on in a timely manner under consideration of the vulnerability disclosure policy according to "**Publication of Vulnerability Disclosure Policy**" in **IXIT 2-UserInfo.** b) Assess whether **“Confirmation of vulnerability actions”** in **IXIT 4-Confirmations** states a confirmation
Verdict	The verdict **PASS** is assigned if: • There is no indication that any described kind of vulnerability is not acted on timely; **AND** • A confirmation for the implementation is given. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 3-VulnTypes: Relevant Vulnerabilities

ID:	Description:	Action:	Time Frame:
VulnTypes-1	Vulnerabilities on the user web frontend regarding HTTP, HTML and the integration into the related components (web server, database, OS and used libraries).	When a notification about a potential vulnerability is received via the contact form according to the Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it proposes a fix for the Software Development Department (SDD). The SDD then implements the fix and verifies the effectiveness within. After confirmation from both teams that the vulnerability is fixed, the new firmware is rolled out and the updated changelog is published with containing a description of the closed vulnerability.	7 days for initial response, 30 days for SIT to investigate and propose a fix, 30 days for SDD to integrate the fix. By no later than 90 days after receiving the vulnerability the fix will be released according to the published vulnerability disclosure policy.
VulnTypes-2	Vulnerabilities concerning the hardware or underlying OS.	When a notification about a potential vulnerability is received via the contact form according to Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it contacts the vendors of the underlying OS or hardware via a defined support email address (the responsible contact persons are known) to discuss further steps. If the vulnerability affects the hardware, the SIT will try to mitigate the issue in software in corporation with the external vendor. If the hardware affects the underlying OS, the SIT will contact the particular vendor for help on this issue. Any change of software will be handled and released by the Software Development Department (SDD). Depended on the result, a fix is rolled out or in case the vulnerability cannot be fixed by Vendor Inc. a warning for customers is published on the website under the following URL: http://devops.aws.idbkmonitor.com/#/security.	7 days for initial response are defined according to the published vulnerability disclosure policy. Usually 90 days after receiving the vulnerability a fix will be released or a warning is published. The warning will be withdrawn since a fix is released.
VulnTypes-3	Vulnerabilities concerning commercially licensed third-party libraries.	When a notification about a potential vulnerability is received via the contact form according to Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it contacts the vendors of the underlying OS or hardware via a defined support email address (the responsible contact persons are known) to discuss further steps. If the vulnerability affects the hardware, the SIT will try to mitigate the issue in software in corporation with the external vendor. If the hardware affects the underlying OS, the SIT will contact the particular vendor for help on this issue. Any change of software will be handled and released by the Software Development Department (SDD). Depended on the result, a fix is rolled out or in case the vulnerability cannot be fixed by Vendor Inc. a warning for customers is published on the website under the following URL: http://devops.aws.idbkmonitor.com/#/security.	7 days for initial response are defined according to the published vulnerability disclosure policy. Usually 90 days after receiving the vulnerability a fix will be released or a warning is published. The warning will be withdrawn since a fix is released.

Based on the Publication of Vulnerability Disclosure Policy in IXIT 2-UserInfo, describes the actions and timeframe when a potential security vulnerability is identified. Users who report the issue through the correct channels can expect to receive an initial response from the security team on the matter within 7 days. Later, within 30 days, the security team may contact the researcher for additional details or evidence to validate the issue. If the issue is confirmed, the next 90 days or so will be spent by the software development department developing and integrating a solution.

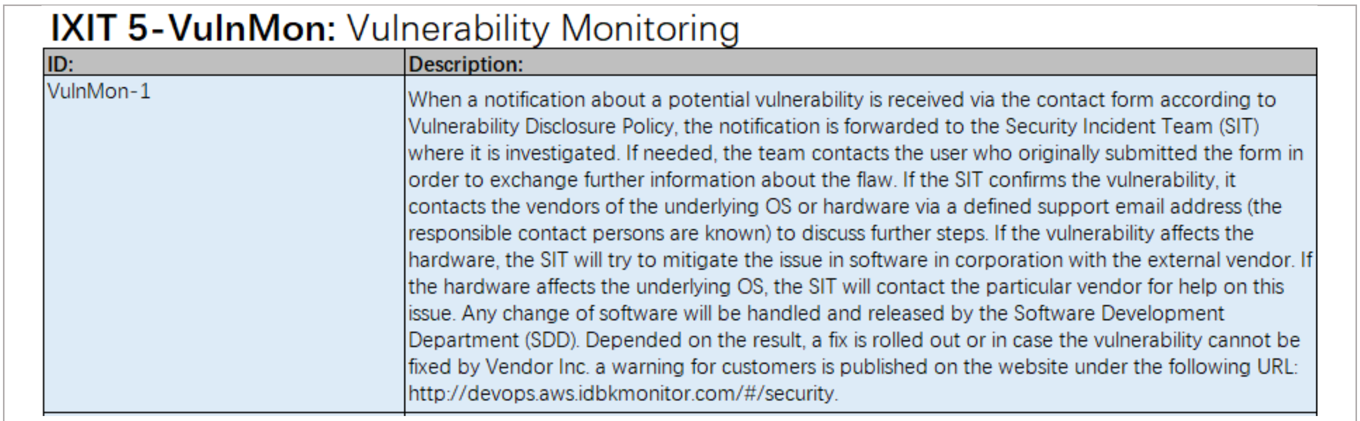
This test, passed.

6.5.2.3 Provision 5.2-3

R: Manufacturer should continually monitor for, identify, and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.

TC_VULNERABILITY_REPORTING#4 / Test case 5.2-3-1	
Security requirement	PROVISION 5.2-3
Type of work	Doc
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of continuous monitoring, identifying and rectifying security vulnerabilities concerning the described procedures **(a-c)** and the confirmation that the preconditions for the implementation are ensured **(d).**
Evaluation inputs	- Information about vulnerabiliy monitoring procedures described in **IXIT 5-VulnMon** - Information about vulnerability identification procedure described in **IXIT 5-VulnMon** - Information about vulnerability mitigation procedure described in **IXIT 5-VulnMon** - **“Confirmation of vulnerability monitoring”** in **IXIT 4-Conf**
Documentation analysis procedure	a. Assess whether the way of continuously monitoring for security vulnerabilities documented in **IXIT 5- VulnMon** is suited to systematically gather information about security vulnerabilities that potentially can affect the DUT. b. Assess whether the way of identifying security vulnerabilities documented in I**XIT 5-VulnMon** is suited to determine if and how a security vulnerability can affect the DUT. c. Assess whether the way of rectifying security vulnerabilities documented in **IXIT 5-VulnMon** is suited to address and mitigate the susceptibility of a DUT against a security vulnerability. d. Assess check whether **"Confirmation of Vulnerability Monitoring"** in **IXIT 4-Conf** states a confirmation.
Verdict	The verdict **PASS** is assigned if: • The described way is suited for continuously monitoring for security vulnerabilities; **AND** • The described way is suited for **identifying** security vulnerabilities; **AND** • The described way is suited for **rectifying** security vulnerabilities; **AND** • A confirmation for the implementation is given. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 5-VulnMon: Vulnerability Monitoring

ID:	Description:
VulnMon-1	When a notification about a potential vulnerability is received via the contact form according to Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it contacts the vendors of the underlying OS or hardware via a defined support email address (the responsible contact persons are known) to discuss further steps. If the vulnerability affects the hardware, the SIT will try to mitigate the issue in software in corporation with the external vendor. If the hardware affects the underlying OS, the SIT will contact the particular vendor for help on this issue. Any change of software will be handled and released by the Software Development Department (SDD). Depended on the result, a fix is rolled out or in case the vulnerability cannot be fixed by Vendor Inc. a warning for customers is published on the website under the following URL: http://devops.aws.idbkmonitor.com/#/security.

Based on IXIT 5- VulnMon, the manufacturer provides a security vulnerability monitoring and remediation process.
Vulnerability feedback submitted by the security team or user vulnerability disclosure URLs/emails are used to detect emerging vulnerabilities and provide appropriate remediation recommendations. The manufacturer also has a clear process in place to ensure that each time a vulnerability is found, it is verified to confirm that the issue has been resolved.
This test, passed.

6.6 Keep software update

6.6.1 IXIT data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 2-UserInfo: User Information

The completed IXIT lists documentations, publications and information provided to users. The pro forma contains the following entries, which are independent from each other, and is typically filled out in form of a list.

Documentation of Replacement:	If the DUT is not updatable: Description of the way the guidance to isolate the DUT and the hardware replacement plan is documented for the user, including all information to access the documentation.
Support Period:	Time during which the product or service is maintained by the manufacturer, e.g. in terms of updates.
Publication of Support Period:	Description of the way the defined "Support Period" is published and documented to the user, including all information to access the publication.
Publication of Non-Updatable:	If the DUT is not updatable: Description of the way the rationale for the absence of software updates is published, including all information to access the publication.

IXIT 6-SoftComp: Software Components

The completed IXIT lists all software components of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the software component.
Update Mechanism:	Reference to update mechanisms in IXIT 7-UpdMech that are used for updating the software component. An empty list of update mechanisms

	indicates the absence of updates for the software component and in this case a justification is provided.
Cryptographic Usage:	Indicates, if the software component makes use of cryptographic algorithms or primitives (Yes/No) and if so, it is included additionally, whether side effects of updating those algorithms and primitives are considered by the manufacturer (Yes/No).

IXIT 7- UpdMech: Update Mechanisms

The completed IXIT lists all software components of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the update mechanism including its major characteristics. It is indicated additionally whether the delivery of an update is network-based.
Security Guarantees:	Description of the realized security objectives and the threats the mechanism is protected against. For authenticity and integrity is indicated additionally whether the security guarantee is given by the DUT itself.
Cryptographic Details:	Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the update mechanism considering key management, and to facilitate the described "Security Guarantees".
Initiation and Interaction:	Brief description of the procedure an update is initiated and a brief description of the user interaction, which is necessary to initiate and apply an update.
Configuration:	Brief description of how automation and notification of software updates can be configured by the user and which options the user can choose from. The default configuration is indicated additionally.
Update Checking:	Brief description of the mechanism and the schedule for querying for security updates. It is indicated additionally whether the availability check is performed by the DUT itself.
User Notification:	Brief description of how the user is informed about an available update and about disruptions caused by the update mechanism, e.g. limited availability of certain features. It is indicated additionally which information are contained in the notification and if the notification is realized by the DUT itself.

IXIT 8-UpdProc: Update Procedures

The completed IXIT lists all software components of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the procedure for deploying security updates including all entities and responsibilities.
Time Frame:	Targeted time frame for completing the procedure.

IXIT 9-ReplSup: Replacement Support

The completed IXIT lists information about the isolation and hardware replacement of the DUT. The pro forma contains the following entries, which are independent from each other, and is typically filled out in form of a list.

Isolation:	Description of the method and its including steps to isolate the DUT.
Hardware Replacement:	Description of the method and its including steps to replace the hardware of the DUT.

6.6.2 Evaluation tasks

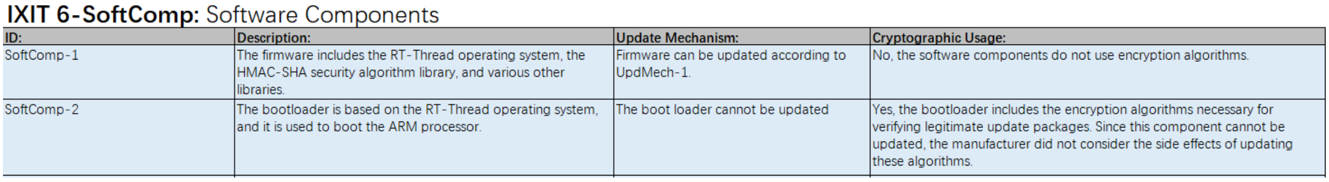
6.6.2.1 Provision 5.3-1

R: All software components in consumer IoT devices should be securely updateable

This provision requires that adequate measures exist to prevent any misuses by an attacker of the update mechanisms.

TC_SOFTWARE_UPDATE_#1 / Test case 5.3-1-1	
Security requirement	PROVISION 5.3-1
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the updatability of software components concerning the absence of software updates and the update mechanisms.
Evaluation inputs	Update Mechanism in **IXIT 6-SoftComp**
Documentation analysis procedure	✓ a) For each software component in **IXIT 6-SoftComp** with an empty list of **"Update Mechanisms",** the tester shall assess whether the implementation of software updates is beyond practicability or for a security reason as described in the justification for the absence of software updates. ✓ b) The tester shall apply all test units as specified in the **Test case 5.3-2-1** to every referenced **"Update Mechanism"** in **IXIT 6-SoftComp**.
Verdict	The verdict **PASS** is assigned if: - For all software components without the ability for software updates, a software update is not possible for practicability reasons or security reasons **AND** - No update mechanism can be misused by an attacker. The verdict **FAIL** is assigned otherwise.

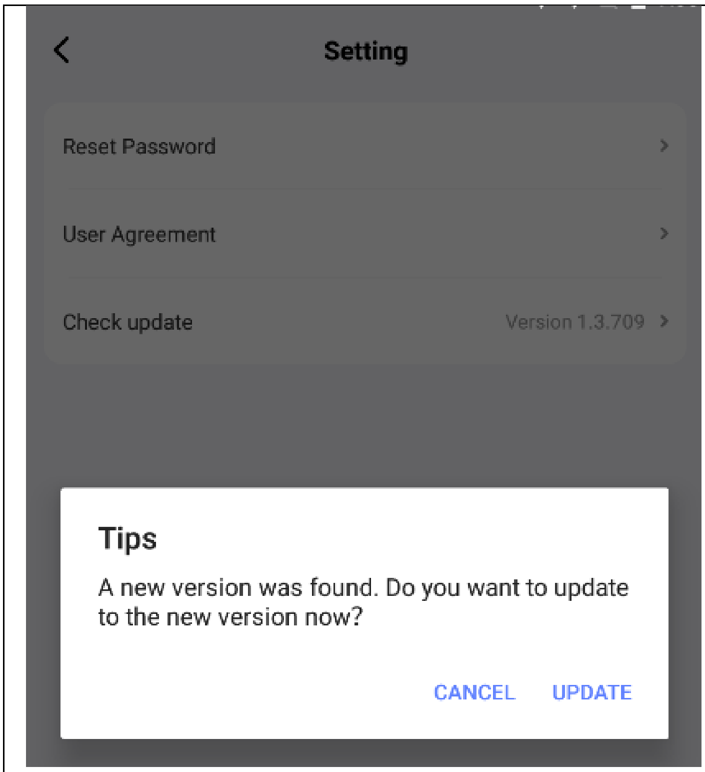
Test Result
PASS
Testlab Comments



IXIT 6-SoftComp: Software Components

ID:	Description:	Update Mechanism:	Cryptographic Usage:
SoftComp-1	The firmware includes the RT-Thread operating system, the HMAC-SHA security algorithm library, and various other libraries.	Firmware can be updated according to UpdMech-1.	No, the software components do not use encryption algorithms.
SoftComp-2	The bootloader is based on the RT-Thread operating system, and it is used to boot the ARM processor.	The boot loader cannot be updated	Yes, the bootloader includes the encryption algorithms necessary for verifying legitimate update packages. Since this component cannot be updated, the manufacturer did not consider the side effects of updating these algorithms.

Based on the content of IXIT 6-SoftComp, it can be confirmed that there is a software update function in the APP that provides the device with support for OTA updates, which is triggered by the user clicking on the view and performing the update.



Setting

Reset Password

User Agreement

Check update Version 1.3.709

Tips

A new version was found. Do you want to update to the new version now?

The installer downloads the package and asks whether to install it, the tester confirms the installation and then automatically completes the installation and finishes the update.

Update failure test:

After the download of the update package is completed, cancel the update, the app functions normally.

Update package download, change the download parameters, prompt download failure, return to the original state, app function is normal.

The tester tested the updated app, the functions are normal, check the latest version, prompted that it is the latest version.

This test, passed.

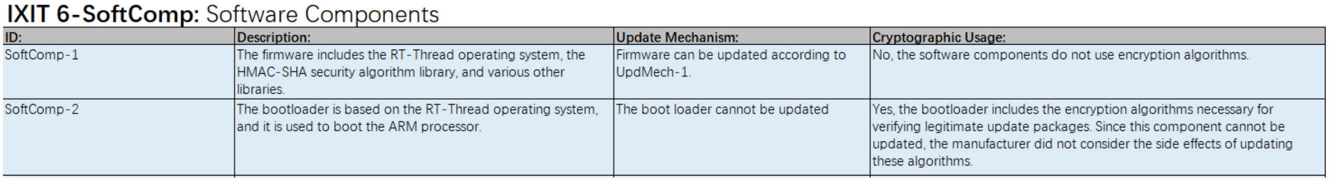
TC_SOFTWARE_UPDATE_#2 / Test Case 5.3-1-2

Security requirement	PROVISION 5.3-1
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the effectiveness of the update mechanisms to avoid misuse.
Evaluation inputs	Update Mechanism in **IXIT 6-SoftComp**
Test scenario	✓ a) The tester shall apply all test units as specified in the **Test case 5.3-2-2** to every referenced **"Update Mechanism"** in **IXIT 6-SoftComp**.
Verdict	The verdict PASS is assigned if: - There is no indication that a misuse of any update mechanism is possible. The verdict FAIL is assigned otherwise.

Test Result

PASS

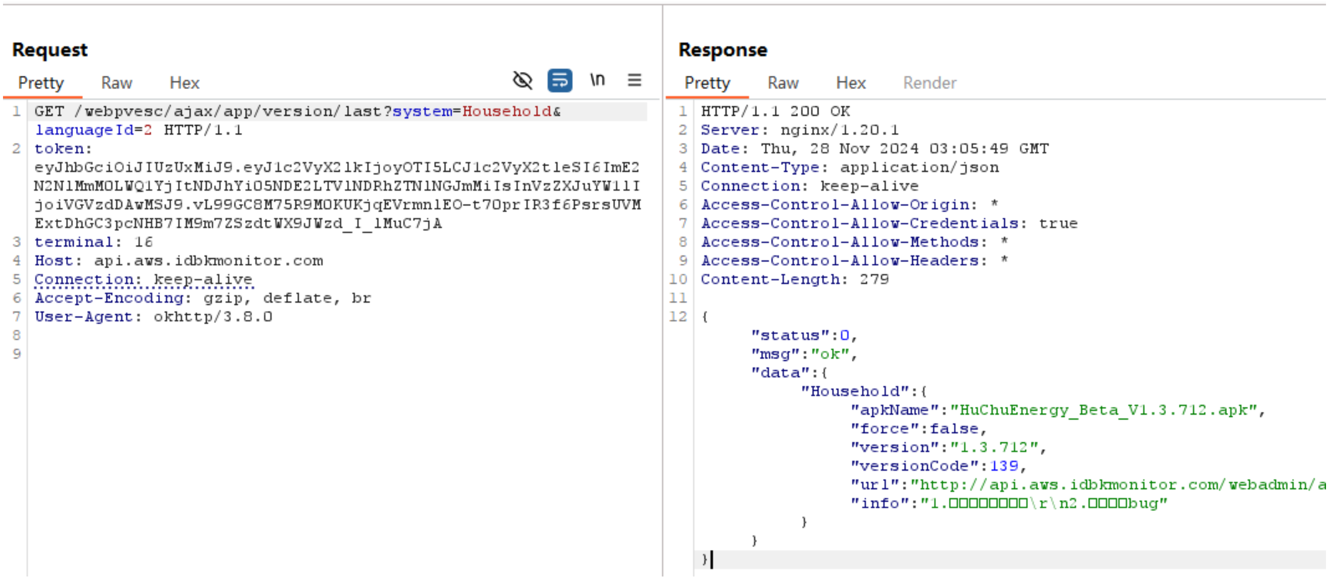
Testlab Comments



IXIT 6-SoftComp: Software Components

ID:	Description:	Update Mechanism:	Cryptographic Usage:
SoftComp-1	The firmware includes the RT-Thread operating system, the HMAC-SHA security algorithm library, and various other libraries.	Firmware can be updated according to UpdMech-1.	No, the software components do not use encryption algorithms.
SoftComp-2	The bootloader is based on the RT-Thread operating system, and it is used to boot the ARM processor.	The boot loader cannot be updated	Yes, the bootloader includes the encryption algorithms necessary for verifying legitimate update packages. Since this component cannot be updated, the manufacturer did not consider the side effects of updating these algorithms.

Based on the content of IXIT 6-SoftComp, it can be confirmed that there is a software update function in the APP that provides the device with support for OTA updates, which is triggered by the user clicking on the view and performing the update.



```
GET /webpvesc/ajax/app/version/last?system=Household&
languageId=2 HTTP/1.1
token:
eyJhbGciOiJIUzUxMiJ9.eyJ1c2VyX21kIjoyOTI5LCJ1c2VyX2tleSI6ImE2
N2N1MmMOLWQ1YjItNDJhYi05NDE2LTV1NDRhZTN1NGJmMiIsInVzZXJuYW11I
joiVGVzdDAwMSJ9.vL99GC8M75R9MOKUKjqEVrmn1EO-t7OprIR3f6PsrsUVM
ExtDhGC3pcNHB7IM9m7ZSzdtWX9JWzd_I_1MuC7jA
terminal: 16
Host: api.aws.idbkmonitor.com
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
User-Agent: okhttp/3.8.0
```

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Thu, 28 Nov 2024 03:05:49 GMT
Content-Type: application/json
Connection: keep-alive
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Methods: *
Access-Control-Allow-Headers: *
Content-Length: 279

{
	"status":0,
	"msg":"ok",
	"data":{
		"Household":{
			"apkName":"HuChuEnergy_Beta_V1.3.712.apk",
			"force":false,
			"version":"1.3.712",
			"versionCode":139,
			"url":"http://api.aws.idbkmonitor.com/webadmin/a
			"info":"1.□□□□□□□□\r\n2.□□□□bug"
		}
	}
}
```

The tester has tested and confirmed that the update interface has been authenticated and transmitted using the https protocol, taking into account secure transmission and data integrity, as described in IXIT 6-SoftComp.

This test, passed.

6.6.2.2 Provision 5.3-2

<u>M.C.(5):</u> When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.

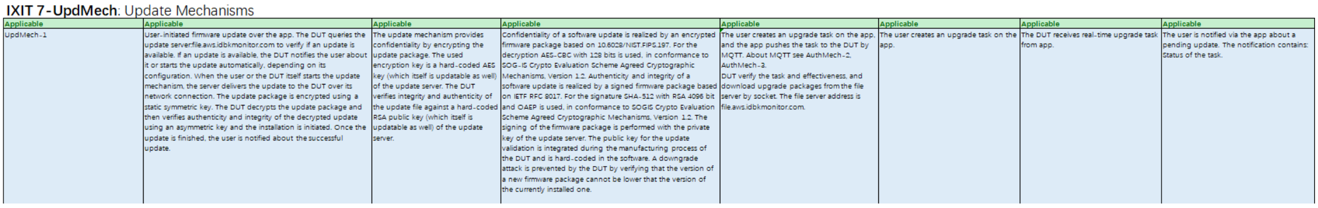
The provision requires the implementation of at least one update mechanism for not constrained devices.

TC_SOFTWARE_UPDATE_#3 / Test case 5.3-2-1

Security requirement	PROVISION 5.3-2
Type of work	IXIT analysis
Applicability	Conditional (only if the device is not a contrained device)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the update installation mechanism concerning adequate measures to prevent an attacker misusing the update installation on the DUT.
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech**
Documentation analysis procedure	✓ a) For each update mechanism in **IXIT 7-UpdMech**, the tester shall assess whether the design of the update mechanism prevents misuse from an attacker according to the **"Security Guarantees",** the corresponding **"Description"**, **"Cryptographic Details"** and **"Initiation and Interaction"**.
Verdict	The verdict **PASS** is assigned if: - One update mechanism of the DUT cannot be misused by an attacker. The verdict **FAIL** is assigned otherwise.

Test Result
PASS

Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

The test results meet the safety requirements as described in IXIT 7-UpdMech in conjunction with 5.3-1-2.

Test passed.

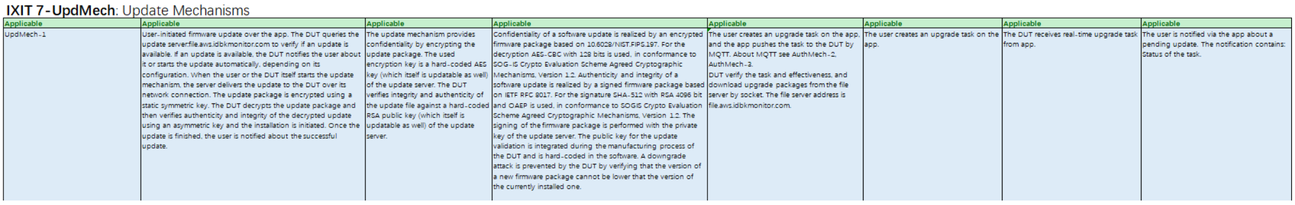
TC_SOFTWARE_UPDATE_#4 / Test case 5.3-2-2

Security requirement	PROVISION 5.3-2
Type of work	Test CAB
Applicability	Conditional (only if the device implements software updates and is not constraint device)
Test objectives	The purpose of this test case is the functional assessment of the effectiveness of the update mechanism to avoid misuse.
Evaluation inputs	Update mechanism in **IXIT 7-UpdMech**
Test scenario	✓ a) For each update mechanism in **IXIT 7-UpdMech**, the tester shall devise functional attacks to misuse the update mechanism based on the **"description"**. ✓ b) The tester shall attempt to misuse each update mechanism on the base of the devised adverse actions and assess whether the design of the mechanism (see "**Description"**, the **"Cryptographic Details"** and **"Initiation and Interaction"**) effectively prevents the misuse of software updates as described in the **"Security Guarantees"**.
Verdict	The verdict PASS is assigned if: - There is no indication that a misuse of one update mechanism of the DUT is possible. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

Testers made parameter modifications to the update interface, injected and other tests, and the update download interface prompted a download failure.

Testers made changes to the downloaded installation package, the installation shows installation failure.

This test passed.

6.6.2.3 Provision 5.3-3

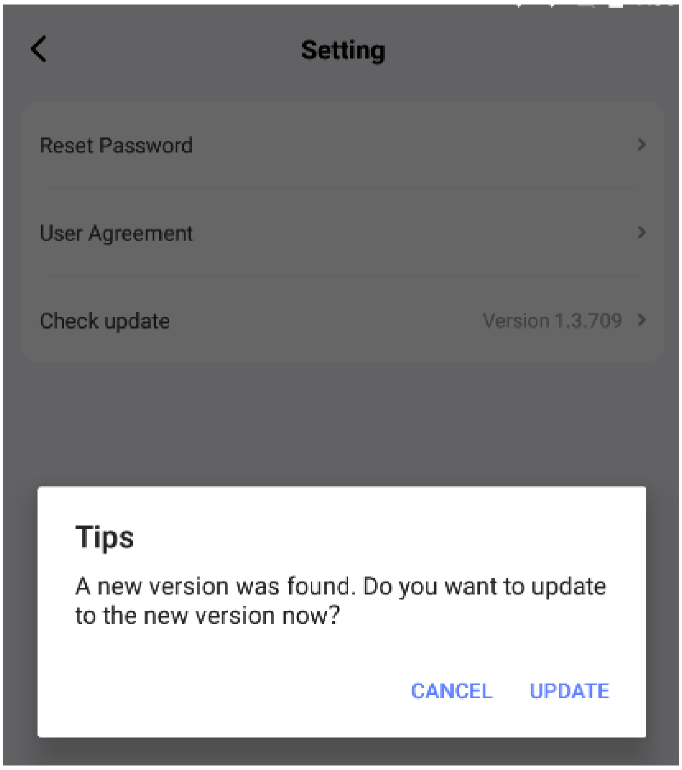
M.C.(12): An update shall be simple for the user to apply

This provision requires the simplicity for the user. Here simplicity means.

- Automatically without requiring to apply
- Doable through a service
- No technical skills required
- Easy access through web interface for instance.

TC_SOFTWARE_UPDATE_#5 / Test case 5.3-3-1	
Security requirement	PROVISION 5.3-3
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Test objectives	The purpose of this test case is the conceptual assessment of the update mechanisms concerning simplicity for the user to apply an update.
Evaluation inputs	Each software component in **IXIT 6-SoftComp** and **"Initiation and Interaction"** in **IXIT 7-UpdMech**
Test scenario	✓ a) For each software component in **IXIT 6-SoftComp**, tester shall assess whether at least one **"Update Mechanism"** is described, which is simple for the user to apply according to "Initiation and Interaction" in I**XIT 7-UpdMech** based on the following factors: *- The software update is automatically applied without requiring any user interaction* ***OR*** *- The software update is initiated via an associated service* ***OR*** *- The software update is initiated via a web interface on the device* ***OR*** *- The software update uses a comparable approach which is applicable for the user with limited technical knowledge.*
Verdict	The verdict **PASS** is assigned if: • Each software component is covered by at least one update mechanism, which is simple for the user to apply. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



Setting

Reset Password

User Agreement

Check update Version 1.3.709

Tips

A new version was found. Do you want to update to the new version now?

Based on the description of Update Mechanism in IXIT 6-SoftComp, the testers checked the update function of the application, the entrance is in “My-Settings-Check for Updates”, the display is clear, the update is triggered by the user's click to view, the user's consent is asked for, and the installation is completed automatically, which is intuitive and easy to understand. It is intuitive and easy to understand.

This test is passed.

6.6.2.4 Provision 5.3-4

R.C.(12): Automatic mechanisms should be used for software updates

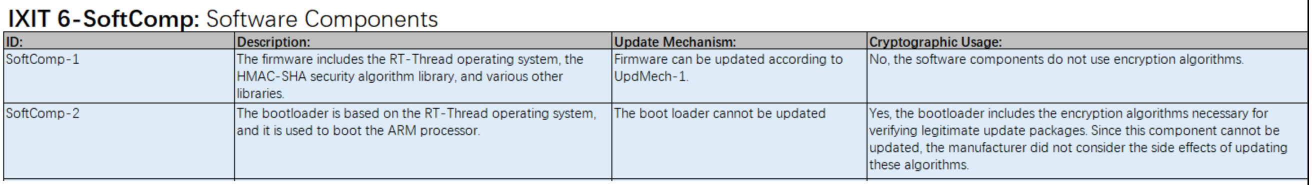
The provision requires that automatic mechanisms exist for software updates. It means:

- ✓ No user interaction to perform the update or to check the availability.

TC_SOFTWARE_UPDATE_#6 / Test case 5.3-4-1	
Security requirement	PROVISION 5.3-4
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the update mechanisms concerning automatic mechanisms.
Evaluation inputs	Each software component in **IXIT 6-SoftComp** and **"Update Mechanism"** in **IXIT 7-UpdMech**
Documentation analysis procedure	✓ For each software component in **IXIT 6-SoftComp**, the tester shall assess whether at least one **"Update Mechanism"** is described in **IXIT 7-UpdMech**, that allows • The performance of updates without requiring any user interaction according to "Initiation and Interaction" ***AND*** • The "Update Checking" without requiring any user interaction. ✓ For each software component in **IXIT 6-SoftComp** covered by an **"Update Mechanism"** in **IXIT 7-UpdMech** with the capability to configure the automation according to **"Configuration"**, the tester shall check whether at least one of the automatic mechanisms is enabled by default.
Verdict	The verdict PASS is assigned if: • Each software component is covered by at least one update mechanism that does not require any user interaction for performing an update and for checking the availability of an update **AND** • For each software component covered by an configurable update mechanism at least one of the automatic mechanisms is enabled by default. The verdict FAIL is assigned otherwise.

Test Result
FAIL

Testlab Comments



IXIT 6-SoftComp: Software Components

ID:	Description:	Update Mechanism:	Cryptographic Usage:
SoftComp-1	The firmware includes the RT-Thread operating system, the HMAC-SHA security algorithm library, and various other libraries.	Firmware can be updated according to UpdMech-1.	No, the software components do not use encryption algorithms.
SoftComp-2	The bootloader is based on the RT-Thread operating system, and it is used to boot the ARM processor.	The boot loader cannot be updated	Yes, the bootloader includes the encryption algorithms necessary for verifying legitimate update packages. Since this component cannot be updated, the manufacturer did not consider the side effects of updating these algorithms.

Based on the Update Mechanism in IXIT 6-SoftComp, which does not provide a description of automatic software updates, the tester checked the update function for the application, and after testing and confirmation from the manufacturer, the application does not have an automatically detected update function, and requires the user to check the version and manually trigger an update.

This test, failed.

6.6.2.5 Point 1 Provision 5.3-5

R.C.(12): The device should check after initialization, and then periodically, whether security updates are available.

TC_SOFTWARE_UPDATE_#7 / Test case 5.3-5-1	
Security requirement	PROVISION 5.3-5
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the update mechanisms concerning the checks for available security updates.
Evaluation inputs	Each software component in IXIT 6-SoftComp
Documentation analysis procedure	a) For each software component in **IXIT 6-SoftComp**, the tester shall assess whether at least one **"Update Mechanism"** is described in **IXIT 7-UpdMech**, that checks the availability of security updates according to the schedule for querying for security updates in **"Update Checking":** - *After initialization of the DUT **AND*** - *Periodically* **Note**: A daily security update check at a randomized time can be appropriate depending on the type of device
Verdict	The verdict **PASS** is assigned if every software component is covered by at least one update mechanism, where: • The checking of the availability of software updates is triggered by the DUT itself **AND** • The availability of software updates is checked after initialization of the DUT **AND** • The availability of software updates is checked periodically. The verdict **FAIL** is assigned otherwise.

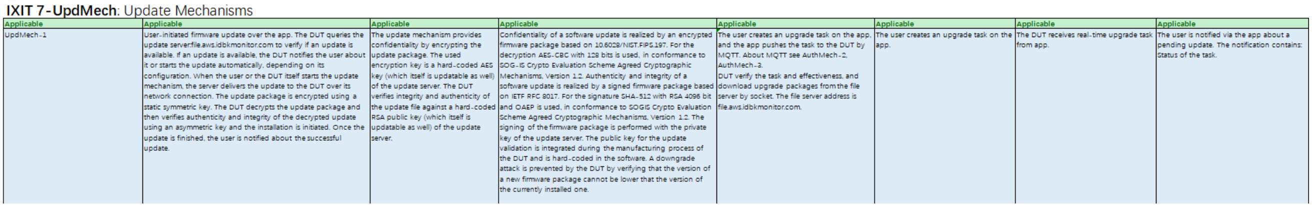
Test Result
FAIL
Testlab Comments
Testers logged in using the old version of the installation and were not prompted for a new version that needed to be updated. Restarted the old version of the installed app, no indication that there is a new version that needs to be updated. Reboot the device and open the old version of the app, no indication that a new version needs to be updated. This test, the software automatic update detection mechanism, failed.

6.6.2.6 Provision 5.3-6

R.C.(9, 12): If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.

TC_SOFTWARE_UPDATE_#8 / Test case 5.3-6-1	
Security requirement	PROVISION 5.3-6
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented) Conditional (the device supports automatic updates and/or update notifications)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the configuration of automatic updates (**a-c**) and update notifications (**d-e**).
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech**
Documentation analysis procedure	a) The tester shall apply all test units as specified in the **Test case 5.3-4-1** to identify all automatic update mechanisms in **IXIT 7-UpdMech**. b) For each update mechanism in **IXIT 7-UpdMech** that provides automatic software updates, the tester shall check whether it provides the user with the ability to: ⇨ Enable, **OR** disable **OR** postpone the automatic installation of security updates according to **"Configuration"** in **IXIT 7-UpdMech.** c) For each update mechanism in **IXIT 7-UpdMech** that provides automatic software updates, the tester shall check whether automatic software updates are enabled in the initialized state according to **"Configuration".** d) For each update mechanism in **IXIT 7-UpdMech** that provides update notifications according to "User Notification" the tester shall check whether it provides the user with the ability to: ⇨ Enable, **OR** disable **OR** postpone update notifications according to **“Configuration”** in **IXIT 7-UpdMech.** e) For each update mechanism in **IXIT 7-UpdMech** that provides update notifications according to **“User Notification”,** the tester shall check whether update notifications are enabled in the initialized state according to “Configuration”.
Verdict	The verdict **PASS** is assigned if: • The DUT supports automatic updates and for all update mechanisms the user is provided with the ability to enable, disable or postpone automatic installation of security updates and automatic updates are enabled in the initialized state; or the DUT does not support automatic updates **AND** • The DUT supports update notifications and for all update mechanisms the user is provided with the ability to enable, disable or postpone update notifications and update notifications are enabled in the initialized state; or the DUT does not support update notifications. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL
Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

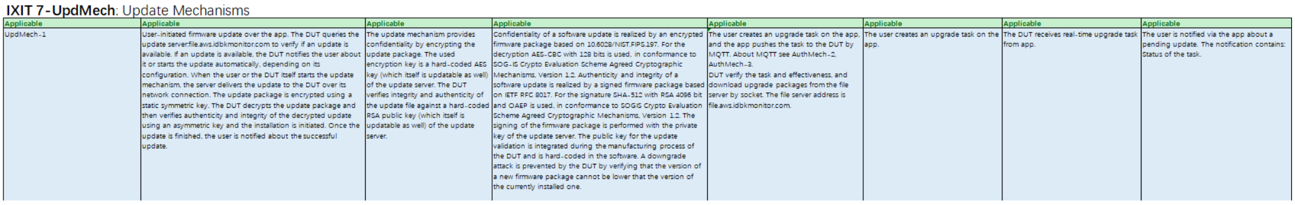
Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

Based on IXIT 7-UpdMech, there is no description of the automatic update mechanism. The tester tested the app, and there is no configurable item for the update mechanism, and there is no automatic detection of the update mechanism.

This test fails.

TC_SOFTWARE_UPDATE_#9 / Test case 5.3-6-2	
Security requirement	PROVISION 5.3-6
Type of work	Test CAB
Applicability	Conditional (an update mechanism is implemented) Conditional (the device supports automatic updates and/or update notifications)
Test objectives	The purpose of this test case is the functional assessment of the configuration of automatic updates and update notifications.
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech**
Test scenario	a) For each update mechanism in **IXIT 7-UpdMech** that provides automatic software updates (compare identification in Test case 5.3-6-1) the tester shall functionally assess whether automatic updates are configured to be enabled in the initialized state of the DUT. *b)* For each update mechanism in **IXIT 7-UpdMech** that provides automatic software updates (compare identification in Test case 5.3-6-1) the tester shall perform a modification of the configuration of automatic update as described in "Configuration" and assess whether the user is provided with the ability to : ⇨ *Enable **OR** disable **OR** postpone automatic installation of security updates.* c) For each update mechanism in **IXIT 7-UpdMech** that provides update notifications according to "User Notification" the tester shall functionally assess whether update notifications are configured to be enabled in the initialized state of the DUT. d) For each update mechanism in **IXIT 7-UpdMech** that provides update notifications according to "User Notification" the tester shall perform a modification of the configuration of update notifications as described in "Configuration" and assess whether the user is provided with the ability to: ⇨ Enable **OR** disable **OR** postpone update notifications.
Verdict	The verdict **PASS** is assigned if: • The DUT supports automatic updates and the configuration of automatic updates is enabled in the initialized state and can be modified by the user as described; or the DUT does not support automatic updates **AND** • The DUT supports update notifications and the configuration of update notifications is enabled in the initialized state and can be modified by the user as described; or the DUT does not support update notifications. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL
Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

Based on IXIT 7-UpdMech, there is no description of the automatic update mechanism. The tester tested the app, and there is no configurable item for the update mechanism, and there is no automatic detection of the update mechanism.

This test fails.

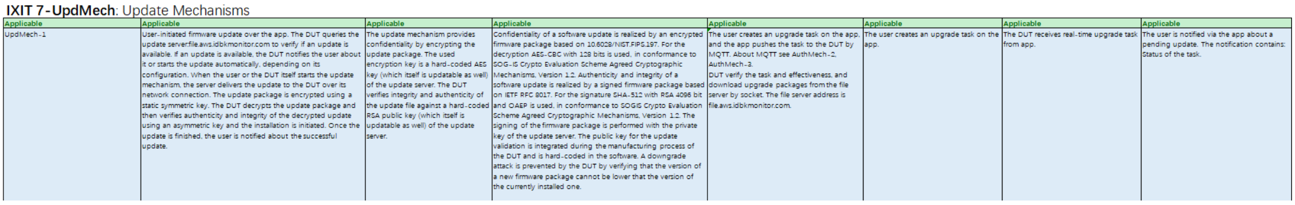
6.6.2.7 Provision 5.3-7

M.C.(12): The device shall use best practice cryptography to facilitate secure update mechanisms

The provision requires that the device use best practice cryptography protocols and algorithms to implement the secure update. The cryptography protocols and algorithms used must be appropriate. In particular, the potential of attacker must be estimated with regards to the risk analysis and the usage of the device.

TC_SOFTWARE_UPDATE_#10 / Test case 5.3-7-1	
Security requirement	PROVISION 5.3-7
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the cryptography used for the update mechanisms concerning the use of best practice cryptography and the vulnerability to a feasible attack.
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech**
Documentation analysis procedure	a) For each update mechanism in **IXIT 7-UpdMech**, the tester shall assess whether the "**Security Guarantees"** are appropriate for the use case of secure updates, at least integrity and authenticity are required to be fulfilled. b) For each update mechanism in **IXIT 7-UpdMech,** the tester shall assess whether the mechanism according to "Description" is appropriate to achieve the **"Security Guarantees".** c) For each update mechanism in **IXIT 7-UpdMech**, the tester shall assess whether the **"Cryptographic Details"** are considered as best practice cryptography for the use case of secure updates based on a reference catalogue. If **"Cryptographic Details"** are not included in a reference catalogue for the corresponding use case (e.g. novel cryptography), the SO shall provide evidences, e.g. a risk analysis, to justify the cryptography is appropriate as best practice for the use case. In such case the tester shall assess whether the evidence is appropriate and reliable for the use case. d) For each update mechanism in **IXIT 7-UpdMech**, the tester shall assess whether the **"Cryptographic Details"** are not known to be vulnerable to a feasible attack for the desired security property on the base of the **"Security Guarantees"** by reference to competent cryptanalytic reports.
Verdict	The verdict **PASS** is assigned if for all update mechanisms: • The security guarantees are appropriate for the use case of secure updates **AND** • The mechanism is appropriate to achieve the security guarantees with respect to the use case **AND** • All used cryptographic details are considered as best practice for the use case **AND** • All used cryptographic details are not known to be vulnerable to a feasible attack for the desired security property. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

Based on IXIT 7-UpdMech, the update package uses the AES algorithm for encryption and the RSA algorithm for integrity checking. Testers tested the interface, which uses the https and TLS1.2 protocols to ensure transmission security.

This test, passed.

6.6.2.8 Provision 5.3-8

M.C.(12): Security updates shall be timely

The provision requires that the secure updates happens timely and with established procedures, like for instance:

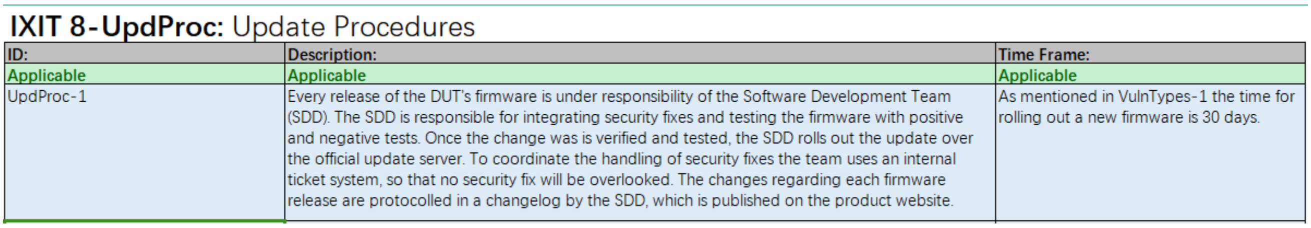
- ✓ Management of vulnerabilities (disclosure, corrections, deployment of patches)
- ✓ Scheduling of updates

TC_SOFTWARE_UPDATE_#11 / Test case 5.3-8-1	
Security requirement	PROVISION 5.3-8
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the manner in which security updates are deployed and the confirmation that the preconditions for the implementation are ensured.
Evaluation inputs	Each security update procedure in **IXIT 8-UpdProc**
Documentation analysis procedure	a) The tester shall assess whether the **"Description"** and the **"Time Frame"** of each security update procedure in **IXIT 8-UpdProc** facilitate that security updates are deployed in a timely manner. b) The tester shall check whether **"Confirmation of Update Procedures"** in **IXIT 5-Conf** states a confirmation.
Verdict	The verdict **PASS** is assigned if: • There is an indication that the described management procedure allows a timely deployment of security updates **AND** • A confirmation for the implementation is given. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 8-UpdProc: Update Procedures

ID:	Description:	Time Frame:
Applicable	Applicable	Applicable
UpdProc-1	Every release of the DUT's firmware is under responsibility of the Software Development Team (SDD). The SDD is responsible for integrating security fixes and testing the firmware with positive and negative tests. Once the change was is verified and tested, the SDD rolls out the update over the official update server. To coordinate the handling of security fixes the team uses an internal ticket system, so that no security fix will be overlooked. The changes regarding each firmware release are protocolled in a changelog by the SDD, which is published on the product website.	As mentioned in VulnTypes-1 the time for rolling out a new firmware is 30 days.

Based on the description in IXIT 8-UpdProc, The Software Development Team (SDD) is responsible for the release of the DUT firmware.The SDD is in charge of fixing issues and conducting tests. Once the new firmware has been thoroughly tested, the SDD rolls out the update via the official update server. The specific changes for each firmware version are documented by the SDD and published on the product website.

This test, passed.

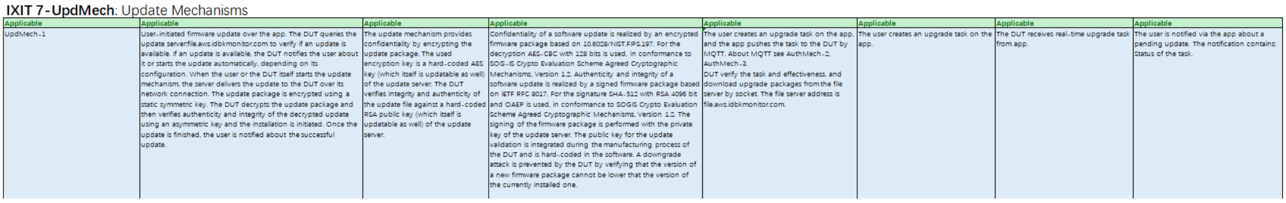
6.6.2.9 Provision 5.3-9

R.C.(12): The device should verify the authenticity and integrity of software updates.

Implicitly this provision is close to 5.3.7 or at least in some cases the correct implementation of 5.7 implies the correct implementation of 5.3.9

TC_SOFTWARE_UPDATE_#12 / Test case 5.3-9-1	
Security requirement	PROVISION 5.3-9
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the verification of software updates concerning authenticity, integrity and the performing entity.
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech.**
Documentation analysis procedure	a) For each update mechanism in **IXIT 7-UpdMech,** the tester shall assess whether the authenticity of software updates is suitably verified according to **“Security Guarantees”** and the corresponding **“Cryptographic Details”,** including, in particular, the originality of the software update in regard to its source (manufacturer) and target (DUT) prior to the installation. b) For each update mechanism in **IXIT 7-UpdMech**, the tester shall assess whether the integrity of software updates is suitably verified according to **“Security Guarantees”** and the corresponding **“Cryptographic Details”.** c) For each update mechanism in **IXIT 7-UpdMech**, the tester shall check whether the authenticity verification is performed by the DUT itself according to **“Security Guarantees”**. d) For each update mechanism in **IXIT 7-UpdMech**, the tester shall check whether the integrity verification is performed by the DUT itself according to **“Security Guarantees”.**
Verdict	The verdict **PASS** is assigned if: • Each update mechanism is effective for the verification of authenticity of software updates **AND** • Each update mechanism is effective for the verification of integrity of software updates **AND** • The verification of authenticity and integrity of software updates is performed by the DUT itself. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

Based on IXIT 7-UpdMech, the update package uses the AES algorithm for encryption and the RSA algorithm for integrity checking. Testers tested the interface, which uses the https and TLS1.2 protocols to ensure transmission security.

This test, passed.

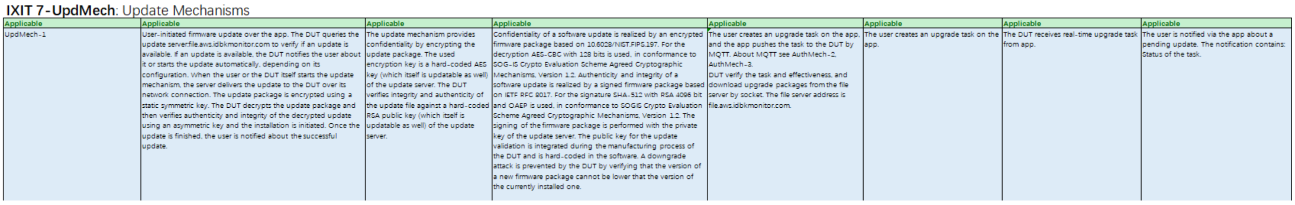
6.6.2.10 Provision 5.3-10

M.(11, 12): Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.

The provision requires a network interface.

TC_SOFTWARE_UPDATE_#13 / Test case 5.3-10-1	
Security requirement	PROVISION 5.3-10
Type of work	IXIT analysis / test CAB
Applicability	- Conditional (updates are delivered over a network interface) - Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the verification of software updates via a trust relationship concerning authenticity and integrity and the performing entity, and the functional assessment of the completeness of the IXIT documentation
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech.**
Documentation analysis procedure	a) The tester shall apply the test units a-b as specified in the **Test case 5.3-9-1.** b) For each network based update mechanism in **IXIT 7-UpdMech,** the tester shall assess whether the verification of integrity and authenticity relies on a valid trust relationship according to **“Description”** and **“Security Guarantees”.** A valid trust relationship includes: - Authenticated communication channels **OR** - Presence on a network that requires the device to possess a critical security parameter or password to join **OR** - Digital signature based verification of the update **OR** - Confirmation by the user **OR** - A comparable secure functionality. c) The tester shall functionally assess whether update mechanisms that are not documented in **IXIT 7-UpdMech** are available via a network interface on the DUT.
Verdict	The verdict **PASS** is assigned if: • Each update mechanism is effective for the verification of authenticity of software updates **AND** • Each update mechanism is effective for the verification of integrity of software updates **AND** • The verification of authenticity and integrity of software updates is based on a valid trust relationship **AND** • Every discovered network-based update mechanism is documented in the IXIT. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

Based on IXIT 7-UpdMech, the update package uses the AES algorithm for encryption and the RSA algorithm for integrity checking. Testers tested the interface, which uses the https and TLS1.2 protocols to ensure transmission security.

This test, passed.

6.6.2.11 Provision 5.3-11

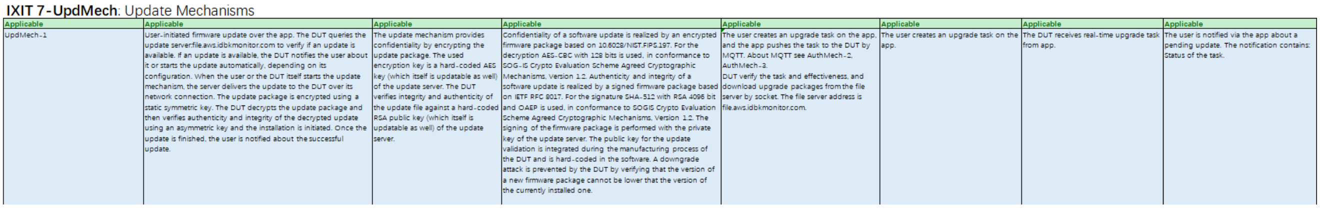
R.C.(12): The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update.

TC_SOFTWARE_UPDATE_#14 / Test case 5.3-11-1	
Security requirement	PROVISION 5.3-11
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the method and content of information for the user about required security updates.
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech.**
Documentation analysis procedure	a) For each update mechanism in **IXIT 7-UpdMech** the tester shall assess whether the method to inform the user about the availability of required security updates is recognizable and apparent according to **"User Notification".** b) For each update mechanism in **IXIT 7-UpdMech** the tester shall assess whether the user notification on required security updates includes information about the risks mitigated by the update according to **"User Notification".**
Verdict	The verdict **PASS** is assigned if for all update mechanisms: • The method to inform the user about required security updates is recognizable and apparent **AND** • The notification on required security updates includes information about the risks mitigated by the update. The verdict **FAIL** is assigned otherwise.

Test Result

N/A

Testlab Comments



IXIT 7-UpdMech: Update Mechanisms

Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
UpdMech-1	User-initiated firmware update over the app. The DUT queries the update server:file.aws.idbkmonitor.com to verify if an update is available. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration. When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded AES key (which itself is updatable as well) of the update server. The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and OAEP is used, in conformance to SOGIS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower that the version of the currently installed one.	The user creates an upgrade task on the app, and the app pushes the task to the DUT by MQTT. About MQTT see AuthMech-2, AuthMech-3. DUT verify the task and effectiveness, and download upgrade packages from the file server by socket. The file server address is file.aws.idbkmonitor.com.	The user creates an upgrade task on the app.	The DUT receives real-time upgrade task from app.	The user is notified via the app about a pending update. The notification contains: Status of the task.

Based on the description of IXIT 7-UpdMech, firmware updates are triggered by the user's initiative, and the user's consent is sought before the update is performed.

Testers tested and did not find any active notification to the user of the update function.

This test, not applicable.

6.6.2.12 Provision 5.3-12

R.C.(12): The device should notify the user when the application of a software update will disrupt the basic functioning of the device.

NOTE: When the basic functioning of the DUT is never disrupted by a software update, no user notification is necessary. In such a situation the test cases of this test group are fulfilled.

TC_SOFTWARE_UPDATE_#15 / Test case 5.3-12-1	
Security requirement	PROVISION 5.3-12
Type of work	IXIT analysis
Applicability	Conditional (an update mechanism is implemented)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of user notifications in case of disruptive software updates.
Evaluation inputs	Each update mechanism in **IXIT 7-UpdMech.**
Documentation analysis procedure	The tester shall check whether each update mechanism in **IXIT 7-UpdMech** supports user notification in case of disruptive software updates according to **“User Notification”** and it is indicated as realized on the DUT itself.
Verdict	The verdict **PASS** is assigned if for each update mechanism: • The user is appropriately notified about the disruption of basic functioning during the software update **AND** • The user notification is realized on the DUT itself. The verdict **FAIL** is assigned otherwise.

Test Result
NA

Testlab Comments
According to the information provided by the vendor regarding IXIT 7-UpdMech, it is mentioned in the User Notification field that the DUT does not possess update notification functionality. Therefore, this test item is deemed not applicable.

6.6.2.13 Provision 5.3-13

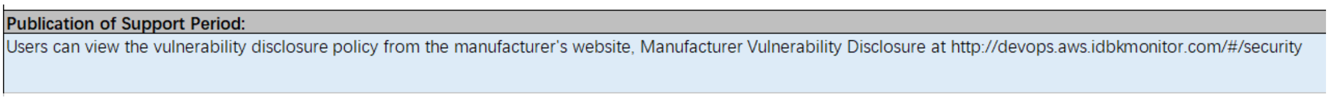
M: The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.

TC_SOFTWARE_UPDATE_#16 / Test case 5.3-13-1	
Security requirement	PROVISION 5.3-13
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the publication of the defined support period.
Evaluation inputs	IXIT 2-UserInfo
Documentation analysis procedure	The tester shall assess whether access to the **“Publication of Support Period”** in **IXIT 2-UserInfo** is understandable and comprehensible for a user with limited technical knowledge.
Verdict	The verdict **PASS** is assigned if: • The publication of software update support period is understandable and comprehensible for a user with limited technical knowledge. The verdict **FAIL** is assigned otherwise.

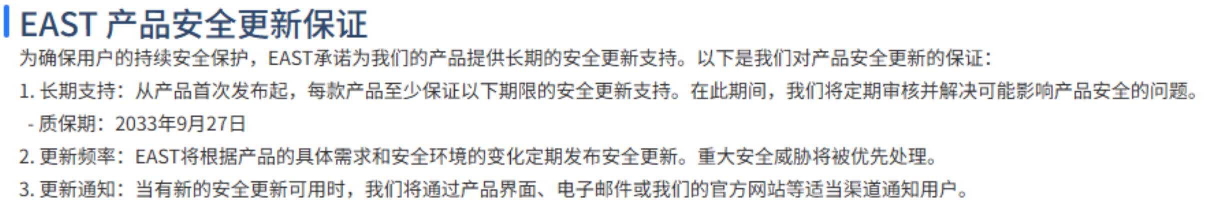
Test Result

PASS

Testlab Comments



Publication of Support Period:
Users can view the vulnerability disclosure policy from the manufacturer's website, Manufacturer Vulnerability Disclosure at http://devops.aws.idbkmonitor.com/#/security



EAST 产品安全更新保证

为确保用户的持续安全保护，EAST承诺为我们的产品提供长期的安全更新支持。以下是我们对产品安全更新的保证：

1. 长期支持：从产品首次发布起，每款产品至少保证以下期限的安全更新支持。在此期间，我们将定期审核并解决可能影响产品安全的问题。

 - 质保期：2033年9月27日

2. 更新频率：EAST将根据产品的具体需求和安全环境的变化定期发布安全更新。重大安全威胁将被优先处理。

3. 更新通知：当有新的安全更新可用时，我们将通过产品界面、电子邮件或我们的官方网站等适当渠道通知用户。

Based on the vulnerability disclosure URL provided in IXIT 2-UserInfo, testers could find a description of the support period for the vulnerability on the website.

This test passed.

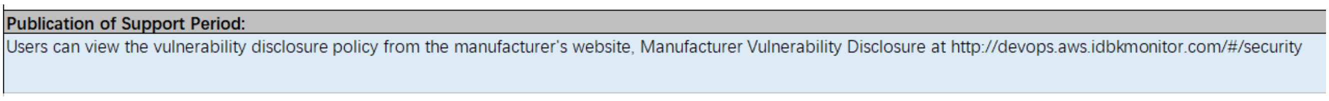
TC_SOFTWARE_UPDATE_#17 / Test case 5.3-13-2

Security requirement	PROVISION 5.3-13
Type of work	Test CAB
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the functional assessment of the publication of the defined support period.
Evaluation inputs	**IXIT 2-UserInfo**
Documentation analysis procedure	a) The tester shall functionally check whether the user information on accessing the resource for publishing the defined support period according to **“Publication of Support Period”** in **IXIT 2-UserInfo** is provided as described. b) The tester shall functionally check whether the resource for publishing the defined support period according to **“Publication of Support Period”** in **IXIT 2-UserInfo** is accessible without restrictions (like e.g. a registration prior to the access). c) The tester shall functionally check whether the published support period according to **“Publication of Support Period”** in **IXIT 2-UserInfo** actually defines the support period with respect to the updateable software components as described in **“Support Period”** in **IXIT 2-UserInfo.**
Verdict	The verdict **PASS** is assigned if: • The access to the resource for publishing the defined support period to the user is provided as described in the IXIT **AND** • The access to the resource for publishing the defined support period is unrestricted **AND** • The defined support period is published. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

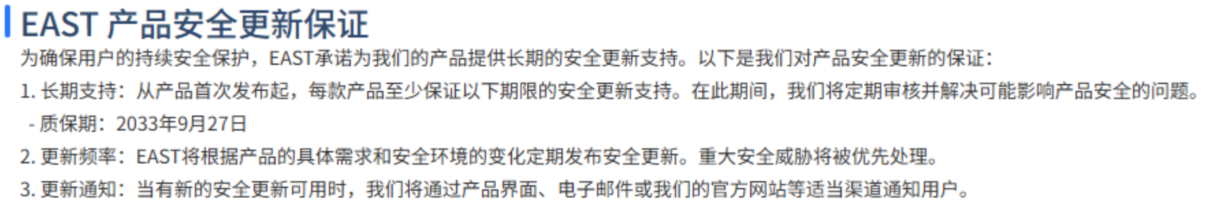
Testlab Comments



Publication of Support Period:

Users can view the vulnerability disclosure policy from the manufacturer's website, Manufacturer Vulnerability Disclosure at http://devops.aws.idbkmonitor.com/#/security

Based on the vulnerability disclosure URL provided in IXIT 2-UserInfo, testers could find a description of the support period for the vulnerability on the website.



EAST 产品安全更新保证

为确保用户的持续安全保护，EAST承诺为我们的产品提供长期的安全更新支持。以下是我们对产品安全更新的保证：

1. 长期支持：从产品首次发布起，每款产品至少保证以下期限的安全更新支持。在此期间，我们将定期审核并解决可能影响产品安全的问题。

- 质保期：2033年9月27日

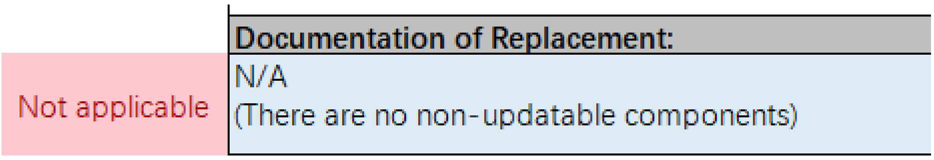
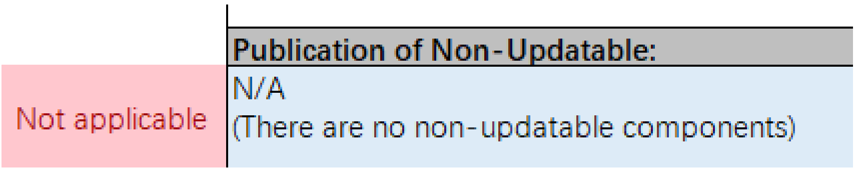
2. 更新频率：EAST将根据产品的具体需求和安全环境的变化定期发布安全更新。重大安全威胁将被优先处理。

3. 更新通知：当有新的安全更新可用时，我们将通过产品界面、电子邮件或我们的官方网站等适当渠道通知用户。

This test passed.

6.6.2.14 Provision 5.3-14

__R,C (3, 4):__ For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.

TC_SOFTWARE_UPDATE_#18 / Test case 5.3-14-1	
Security requirement	PROVISION 5.3-14
Type of work	IXIT analysis
Applicability	Conditional (Software components are not updateable) Conditional (The device is constrained)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the publication of the rationale for absence of updates and hardware replacement support.
Evaluation inputs	IXIT 2-UserInfo
Documentation analysis procedure	The tester shall assess whether the access to the **"Publication of Non-Updatable"** and **"Documentation of Replacement"** in **IXIT 2-UserInfo** is understandable for a user with limited technical knowledge.
Verdict	The verdict **PASS** is assigned if: • The publication of the rationale for absence of updates and hardware replacement support is understandable for a user with limited technical knowledge. The verdict **FAIL** is assigned otherwise.
Test Result	
N/A	
Testlab Comments	
 Not applicable Documentation of Replacement: N/A (There are no non-updatable components)  Not applicable Publication of Non-Updatable: N/A (There are no non-updatable components) Based on Publication of Non-Updatable and Documentation of Replacement in IXIT 2-UserInfo, there are no non-updatable components in the DUT. this test item is deemed not applicable.	

TC_SOFTWARE_UPDATE_#19 / Test case 5.3-14-2	
Security requirement	PROVISION 5.3-14
Type of work	Test CAB
Applicability	Conditional (Software components are not updateable) Conditional (The device is constrained)
Documentation analysis objectives	The purpose of this test case is the functional assessment of the publication of the rationale for absence of updates and hardware replacement support.
Evaluation inputs	IXIT 2-UserInfo
Documentation analysis procedure	a) The tester shall functionally check whether the user information on accessing the resource for the rationale for absence of updates and publishing the hardware replacement support according to **“Publication of Non-Updatable**” and **“Documentation of Replaceme**nt” in IXIT 2-UserInfo is provided as described. b) The tester shall functionally check whether the resource for publishing the rationale for absence of updates and hardware replacement support according to “**Publication of Non-Updatable”** and **“Documentation of Replacement”** in **IXIT 2-UserInfo** is accessible without restrictions (like e.g. a registration prior to the access). c) The tester shall functionally check whether the published rationale for absence of updates according to **“Publication of Non-Updatable”** in **IXIT 2-UserInfo** contains the rationale for the absence of software updates. d) The tester shall functionally check whether the published hardware replacement support according to **“Documentation of Replacement”** in **IXIT 2-UserInfo** contains the hardware replacement plan in terms of the period and method of hardware replacement support. e) The tester shall functionally check whether the published rationale for absence of updates according to **“Publication of Non-Updatable”** in **IXIT 2-UserInfo** contains a defined support period.
Verdict	The verdict **PASS** is assigned if: • The access to the resource for publishing the rationale for absence of updates **AND** hardware replacement support to the user is provided as described in the IXIT **AND** • The access to the resource for publishing the rationale for absence of updates **AND** hardware replacement support is unrestricted **AND** • The rationale for the absence of software updates is published **AND** • The period and method of hardware replacement support is published **AND** • A support period is published. The verdict **FAIL** is assigned otherwise.
Test Result	
N/A	
Testlab Comments	
Based on the results of the conceptual test items, this test item is deemed not applicable.	

6.6.2.15 Provision 5.3-15

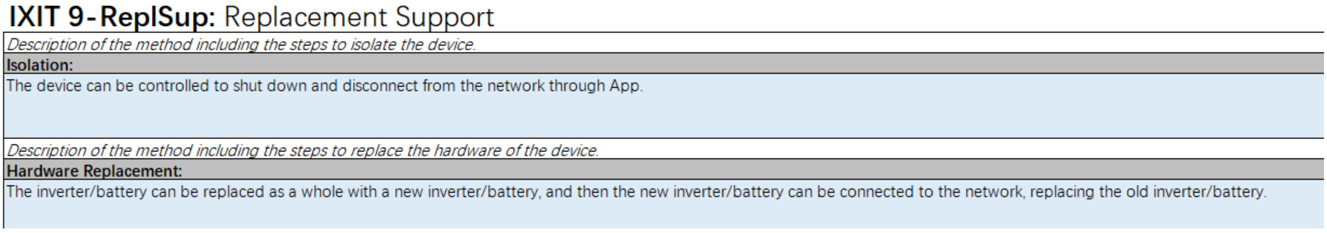
R.C. (3,4): For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.

TC_SOFTWARE_UPDATE_#20 / Test case 5.3-15-1	
Security requirement	PROVISION 5.3-15
Type of work	IXIT analysis
Applicability	Conditional (Software components are not updateable) Conditional (The device is constrained)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the isolation capabilities and hardware replacement support of the DUT.
Evaluation inputs	IXIT 9-ReplSup
Documentation analysis procedure	a) The tester shall assess whether the described method in **"Isolation"** in **IXIT 9-ReplSup** is suitable to isolate the IoT product, i.e. to remove the IoT product from the network it is connected to, or to place the IoT product in a selfcontained environment. b) The tester shall assess whether the described method in **"Hardware Replacement"** in **IXIT 9-ReplSup** is suitable to be able to replace the hardware.
Verdict	The verdict **PASS** is assigned if: • The described method is suited for the isolation of the IoT product **AND** • The described method is suited for the replacement of the hardware. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 9-ReplSup: Replacement Support

Description of the method including the steps to isolate the device.

Isolation:

The device can be controlled to shut down and disconnect from the network through App.

Description of the method including the steps to replace the hardware of the device.

Hardware Replacement:

The inverter/battery can be replaced as a whole with a new inverter/battery, and then the new inverter/battery can be connected to the network, replacing the old inverter/battery.

Based on the Isolation and Hardware Replacement descriptions in IXIT 9-ReplSup, testers can easily perform isolation operations such as disconnecting from the network or shutting down the device.

The devices are designed with replaceable batteries, and after the tester replaces the batteries, the test device still works and the software performs normally.

Each product carries a paper and electronic copy of the user manual, which allows users to easily access guidelines for hardware replacement.

This test, passed.

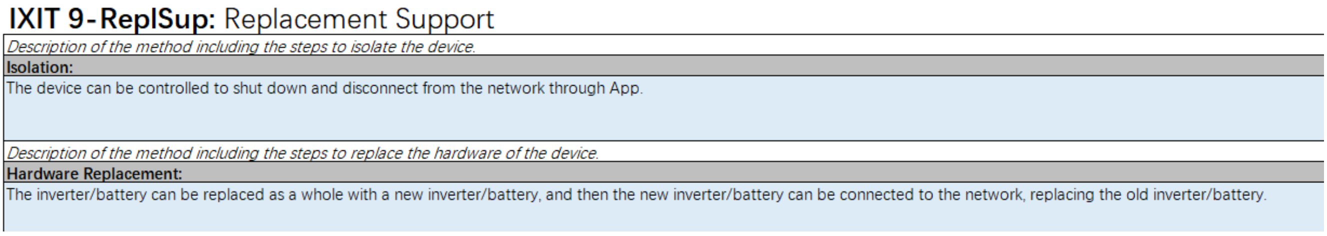
TC_SOFTWARE_UPDATE_#21 / Test case 5.3-15-2

Security requirement	PROVISION 5.3-15
Type of work	Test CAB
Applicability	Conditional (Software components are not updateable) Conditional (The device is constrained)
Documentation analysis objectives	The purpose of this test case is the functional assessment of the isolation capabilities and hardware replacement support of the DUT.
Evaluation inputs	**IXIT 9-ReplSup**
Documentation analysis procedure	a) The tester shall set up the IoT product in the intended environment. b) The tester shall perform the method described in "Isolation" in **IXIT 9-ReplSup** in order to isolate the IoT product, i.e. to remove the IoT product from the network it is connected to, or to place the IoT product in a self-contained environment, as appropriate. c) The tester shall functionally assess whether on the isolated IoT product: - In case of removing the IoT product from the network connection: any functionality loss caused is related only to that connectivity and not to the main function of the DUT, **OR** - In case of placing the IoT product in a self-contained environment - with other devices: the integrity of devices within that environment is ensured. d) The tester shall perform the method described in "Hardware Replacement" in **IXIT 9-ReplSup** in order to replace the hardware in the intended environment. e) The tester shall functionally assess whether the connectivity and associated functionality can be regained on the replaced DUT.
Verdict	The verdict PASS is assigned if: • The IoT product can be isolated successfully according to the described method for isolation. **AND** • The hardware can be replaced successfully according to the described method for hardware replacement. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 9-ReplSup: Replacement Support

Description of the method including the steps to isolate the device.

Isolation:

The device can be controlled to shut down and disconnect from the network through App.

Description of the method including the steps to replace the hardware of the device.

Hardware Replacement:

The inverter/battery can be replaced as a whole with a new inverter/battery, and then the new inverter/battery can be connected to the network, replacing the old inverter/battery.

Based on the product specification mentioned in IXIT 9-ReplSup.

Testers operating according to the product manual can easily perform isolation operations such as disconnecting from the network or shutting down the device.

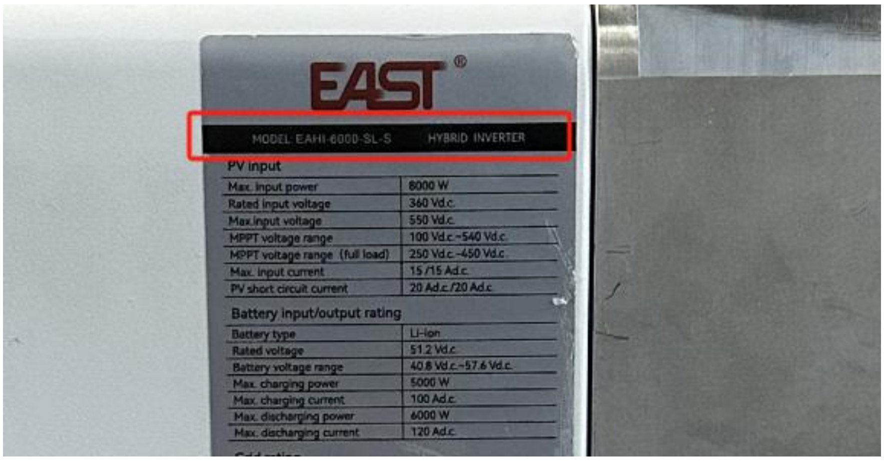
Battery replacement can be easily performed by the tester by following the product manual.

This test, passed.

6.6.2.16 Provision 5.3-16

M: The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.

TC_SOFTWARE_UPDATE_#22 / Test case 5.3-16-1	
Security requirement	PROVISION 5.3-16
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the model designation.
Evaluation inputs	IXIT 2-UserInfo
Documentation analysis procedure	The Tester **shall** assess whether the model designation of the DUT can be obtained in a clearly recognizable way, either by labelling on the DUT or via a physical interface according to **"Model Designation"** in **IXIT 2-UserInfo.**
Verdict	The verdict **PASS** is assigned if: • The model designation of the DUT can be obtained clearly recognizable by labelling on the DUT or via a physical interface. The verdict **FAIL** is assigned otherwise.
Test Result	
PASS	
Testlab Comments	



EAST®

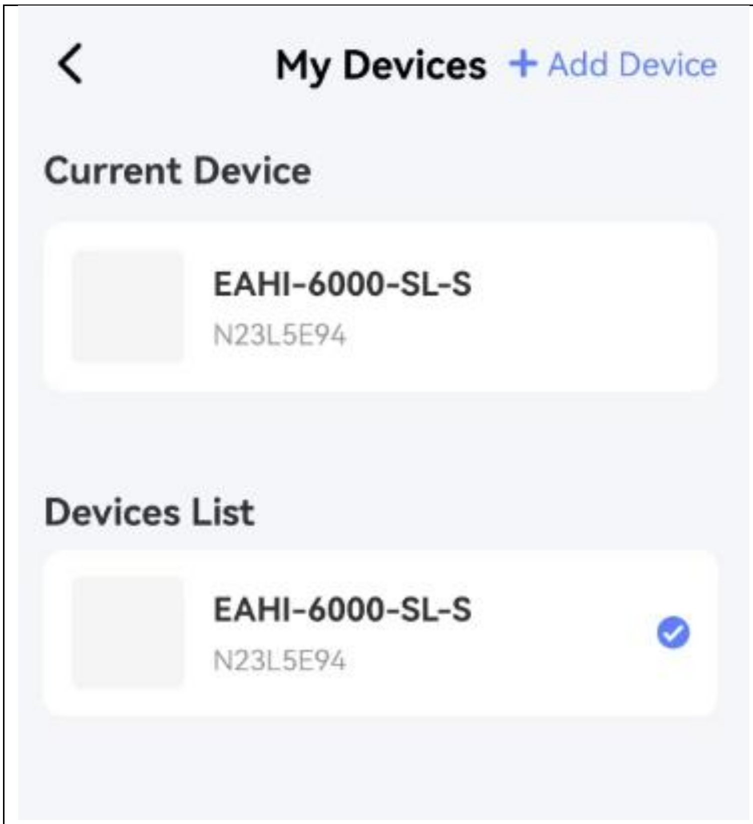
MODEL: EAHI-6000-SL-S HYBRID INVERTER

PV input

Max. input power	8000 W
Rated input voltage	360 Vd.c.
Max.input voltage	550 Vd.c.
MPPT voltage range	100 Vd.c.~540 Vd.c.
MPPT voltage range (full load)	250 Vd.c.~450 Vd.c.
Max. input current	15 /15 Ad.c.
PV short circuit current	20 Ad.c./20 Ad.c.

Battery input/output rating

Battery type	Li-ion
Rated voltage	51.2 Vd.c.
Battery voltage range	40.8 Vd.c.~57.6 Vd.c.
Max. charging power	5000 W
Max. charging current	100 Ad.c.
Max. discharging power	6000 W
Max. discharging current	120 Ad.c.



Current Device

EAHI-6000-SL-S
N23L5E94

Devices List

EAHI-6000-SL-S
N23L5E94 ✓

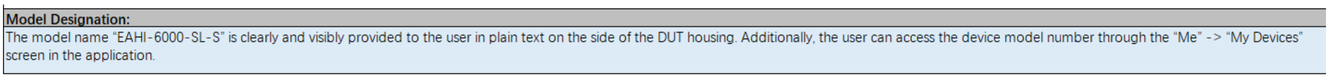
Testers can clearly see the device model number on the device casing.
The currently connected device can be viewed in the APP and the device model can be clearly displayed.
This test, passed.

TC_SOFTWARE_UPDATE_#23 / Teste case 5.3-16-2	
Security requirement	PROVISION 5.3-16
Type of work	Test CAB
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the functional assessment of the model designation.
Evaluation inputs	IXIT 2-UserInfo
Documentation analysis procedure	a) The tester shall functionally check whether the model designation of the DUT can be obtained applying the described way of recognition in **"Model Designation"** in **IXIT 2-UserInfo.** b) The tester shall functionally assess whether the obtained model designation is available in simple text and corresponds with the expected model designation described in **"Model Designation"** in **IXIT 2-UserInfo.**
Verdict	The verdict **PASS** is assigned if: • The model designation of the DUT can be extracted according to the described way of recognition **AND** • The model designation is available in simple text **AND** • The model designation is corresponding with the expected model designation according to the IXIT. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



Model Designation:

The model name "EAHI-6000-SL-S" is clearly and visibly provided to the user in plain text on the side of the DUT housing. Additionally, the user can access the device model number through the "Me" -> "My Devices" screen in the application.

Testers can clearly see the device model number on the device casing.

The currently connected device can be viewed in the APP and the device model can be clearly displayed.

The test result matches the document description and passed.

6.7 Securely store sensitive security parameters

6.7.1 IXIT data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 10-SecParam: Security Parameters

The completed IXIT lists all sensitive (public and critical) security parameters that are persistently stored on the DUT during intended usage. The pro forma contains the following entries and is typically filled out in form of a table.

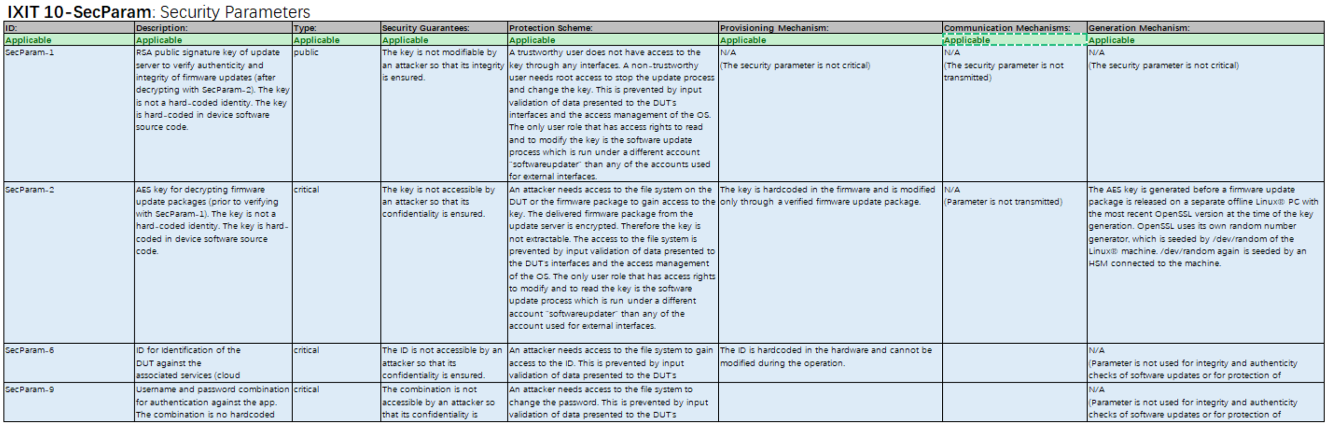
ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the security parameter, including its purpose. It is indicated additionally whether the parameter is a hard-coded unique per device identity used in a device for security purposes (hardcoded identity) and/or hard-coded in device software source code.
Type:	Indication whether the security parameter is public or critical. **Note**: *Public and critical security parameters are defined in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].*
Security Guarantees:	Description of the realized baseline security objectives and threats the security parameter is protected against during persistent storage.
Protection Scheme:	Description of the measures that are applied to achieve the Security Guarantees. This includes the principals and roles through which access to the parameter is possible, including the privileges associated to each role.
Provisioning Mechanism:	f the “Type” indicates that the parameter is critical: Description of the mechanism through which the parameter is assigned its value for the operation of the DUT. **Note1**: *Such assignment can happen during initialization or in initialized state (e.g. when a device functionality relying on the parameter is activated by the user).* **Note2**: *Persistent configuration data, runtime configuration data, protocol negotiation and assignment to a default value are potentially possible provisioning mechanisms.*
Communication Mechanisms:	Reference to communication mechanisms in **IXIT 11-ComMech** that are used for communicating the parameter and an indication whether the communication is done via remotely accessible interfaces.
Generation Mechanism:	If the **"Type"** indicates that the parameter is critical and used for integrity and authenticity checks of software updates or for protection of communication with associated services: - Description of the mechanism used to generate the values of the parameter and it is indicated additionally that the parameter is used for integrity and authenticity checks of software updates or for protection of communication with associated services. **Example**: References to a standard random number generator and applicable design documents.

6.7.2 Evaluation tasks

6.7.2.1 Provision 5.4-1

M (14): Sensitive security parameters in persistent storage shall be stored securely by the device

TC_SENSITIVE_DATA#1 / Test case 5.4-1-1	
Security requirement	PROVISION 5.4-1
Type of work	IXIT analysis
Applicability	Conditional (sensitive security parameters are stored persistently)
Documentation analysis objectives	Verify that sensitive security parameters described in user manual and public information's bonded to the device are securely stored
Evaluation inputs	- Collected sensitive security parameter from **IXIT 10-SecParam**
Documentation analysis procedure	✓ Tester assess whether the declaration in "**Type"** of each sensitive security parameter provided in **IXIT 10-SecParam** is consistent with the **Description**. ✓ Tester assess whether the "**Security Guarantees"** of each sensitive security parameter provided in **IXIT 10-SecParam** matches at least the protection needs indicated by **Type**. **NOTE 1:** *Criftical security parameter require integrity and confidentiality protection while public security parameter require integrity protection only.* ✓ Tester assess whether the "**Protection Scheme"** of each sensitive security parameter provided in **IXIT 10-SecParam** provides the claimed **Security Guarantees**. **NOTE 2:** *Consider the usage of external evidences (see clause 4.7) to (partially) cover the provision if a secure element is used.* ✓ Tester assess the completeness of the sensitive security parameters in **IXIT 10-SecParam** by considering indications for sensitive security parameters in the provided information in all other IXITs. **EXAMPLE:** If there are authentication mechanisms described in **IXIT 1-AuthMech**, the verification whether the corresponding cryptographic parameters are listed in **IXIT 10-SecParam** can be helpful tocollect indications.
Verdict	The verdict PASS is assigned if: • For every sensitive security parameter the declaration is consistent with its description; **AND** • For every sensitive security parameter the claimed security guarantees match its minimal protection needs; **AND** • Every sensitive security parameter has a suitable protection mechanism for the claimed security guarantees; **AND** • There is no indication, that the listed sensitive security parameters are incomplete. The verdict **FAIL** is assigned otherwise.
Test Result	
PASS	
Testlab Comments	



IXIT 10-SecParam: Security Parameters

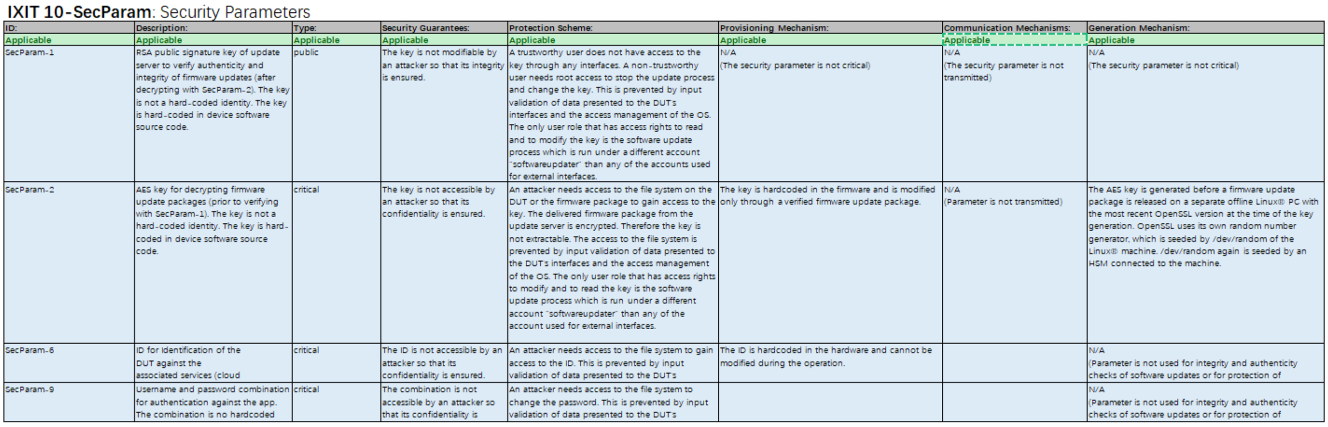
ID:	Description:	Type:	Security Guarantees:	Protection Scheme:	Provisioning Mechanism:	Communication Mechanisms:	Generation Mechanism:
Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
SecParam-1	RSA public signature key of update server to verify authenticity and integrity of firmware updates (after decrypting with SecParam-2). The key is not a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	A trustworthy user does not have access to the key through any interfaces. A non-trustworthy user needs root access to stop the update process and change the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read and to modify the key is the software update process which is run under a different account "softwareupdater" than any of the accounts used for external interfaces.	N/A (The security parameter is not critical)	N/A (The security parameter is not transmitted)	N/A (The security parameter is not critical)
SecParam-2	AES key for decrypting firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key. The delivered firmware package from the update server is encrypted. Therefore the key is not extractable. The access to the file system is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify and to read the key is the software update process which is run under a different account "softwareupdater" than any of the account used for external interfaces.	The key is hardcoded in the firmware and is modified only through a verified firmware update package.	N/A (Parameter is not transmitted)	The AES key is generated before a firmware update package is released on a separate offline Linux® PC with the most recent OpenSSL version at the time of the key generation. OpenSSL uses its own random number generator, which is seeded by /dev/random of the Linux® machine. /dev/random again is seeded by an HSM connected to the machine.
SecParam-6	ID for Identification of the DUT against the associated services (cloud	critical	The ID is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to gain access to the ID. This is prevented by input validation of data presented to the DUT's	The ID is hardcoded in the hardware and cannot be modified during the operation.		N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of
SecParam-9	Username and password combination for authentication against the app. The combination is no hardcoded	critical	The combination is not accessible by an attacker so that its confidentiality is	An attacker needs access to the file system to change the password. This is prevented by input validation of data presented to the DUT's			N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of

According to the information provided by the vendor regarding IXIT 10-SecParam. The content mentioned in the Security Guarantees section meets the requirements for ensuring confidentiality and integrity. Therefore, this test item is deemed to pass.

TC_SENSITIVE_DATA _#2 / Test case 5.4-1-2

Security requirement	PROVISION 5.4-1
Type of work	Test CAB
Applicability	Conditional (sensitive security parameters are stored persistently)
Test objectives	Verify that secure storage mechanism of sensitive security parameters works as expected
Evaluation inputs	- At least three devices suitable for testing - Collected sensitive security parameter from **IXIT 10-SecParam**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) Tester assess whether for all sensitive security parameters provided in **IXIT 10-SecParam, Protection Scheme** is implemented according to the IXIT documentation **Expected result:** ✓ Result of sensitive parameter secure storage robustness
Verdict	The verdict PASS is assigned if: - For every sensitive security parameter there is no indication that the implementation of the corresponding protection scheme differs from its IXIT documentation. The verdict FAIL is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 10-SecParam: Security Parameters

ID:	Description:	Type:	Security Guarantees:	Protection Scheme:	Provisioning Mechanism:	Communication Mechanisms:	Generation Mechanism:
Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
SecParam-1	RSA public signature key of update server to verify authenticity and integrity of firmware updates (after decrypting with SecParam-2). The key is not a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	A trustworthy user does not have access to the key through any interfaces. A non-trustworthy user needs root access to stop the update process and change the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read and to modify the key is the software update process which is run under a different account "softwareupdater" than any of the accounts used for external interfaces.	N/A (The security parameter is not critical)	N/A (The security parameter is not transmitted)	N/A (The security parameter is not critical)
SecParam-2	AES key for decrypting firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key. The delivered firmware package from the update server is encrypted. Therefore the key is not extractable. The access to the file system is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify and to read the key is the software update process which is run under a different account "softwareupdater" than any of the account used for external interfaces.	The key is hardcoded in the firmware and is modified only through a verified firmware update package.	N/A (Parameter is not transmitted)	The AES key is generated before a firmware update package is released on a separate offline Linux® PC with the most recent OpenSSL version at the time of the key generation. OpenSSL uses its own random number generator, which is seeded by /dev/random of the Linux® machine. /dev/random again is seeded by an HSM connected to the machine.
SecParam-6	ID for Identification of the DUT against the associated services (cloud	critical	The ID is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to gain access to the ID. This is prevented by input validation of data presented to the DUT's	The ID is hardcoded in the hardware and cannot be modified during the operation.		N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of
SecParam-9	Username and password combination for authentication against the app. The combination is no hardcoded	critical	The combination is not accessible by an attacker so that its confidentiality is	An attacker needs access to the file system to change the password. This is prevented by input validation of data presented to the DUT's			N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of

Based on the test results above, SecParam-1、SecParam-2、SecParam-3 and SecParam-4 are no differs from the "Protection Scheme " in the IXIT documentation. It is determined that the requirement passed.

6.7.2.2 Provision 5.4-2

<u>**M C (10):**</u> Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.

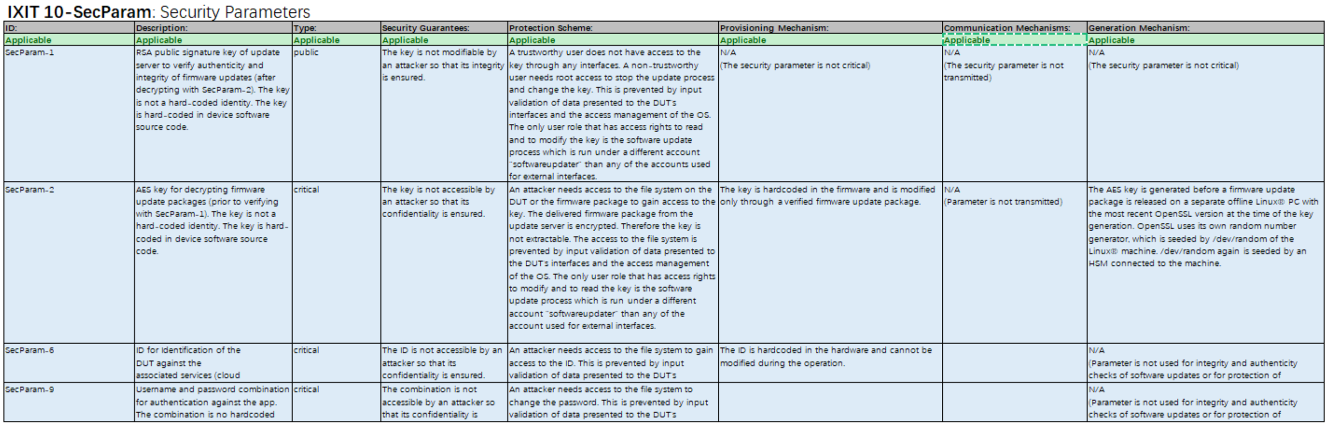
TC_SENSITIVE_DATA#3 / Test case 5.4-2-1

Security requirement	PROVISION 5.4-2
Type of work	IXIT analysis
Applicability	Conditional (a hard-coded unique per device identity is used for security purposes)
Documentation analysis objectives	Verify that sensitive security parameters described in user manual and public information's bonded to the device are securely stored
Evaluation inputs	- Collected sensitive security parameter from **IXIT 10-SecParam**
Documentation analysis procedure	a) Check whether for each sensitive security parameter in **IXIT 10-SecParam** where the **Description** indicates that it is used as an hard-coded identity, a corresponding explicit statement is provided. b) Assess whether for each hard-coded identity as indicated in **Description** in **IXIT 10-SecParam** the corresponding "Security Guarantee" provides tamper-resistance. ***<u>NOTE 1</u>:*** *Tamper-resistance addresses protection against means such as physical, electrical and software means.* ***<u>NOTE 2</u>:*** *Consider the usage of external evidences (see clause 4.7) to (partially) cover the provision if a secure element is used.* c) Assess whether the **Protection Scheme** of each hard-coded identity as indicated in **Description** in **IXIT 10-SecParam** provides the claimed **Security Guarantees** with respect to tamper-resistance.
Verdict	The verdict PASS is assigned if: - There is no indication that any hard-coded identity is not documented as such; **AND** - For all hard-coded identities the security guarantee includes tamper-resistance; **AND** - Every hard-coded identity has a suitable protection mechanism for tamper-resistance. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 10-SecParam: Security Parameters

ID:	Description:	Type:	Security Guarantees:	Protection Scheme:	Provisioning Mechanism:	Communication Mechanisms:	Generation Mechanism:
Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
SecParam-1	RSA public signature key of update server to verify authenticity and integrity of firmware updates (after decrypting with SecParam-2). The key is not a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	A trustworthy user does not have access to the key through any interfaces. A non-trustworthy user needs root access to stop the update process and change the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read and to modify the key is the software update process which is run under a different account "softwareupdater" than any of the accounts used for external interfaces.	N/A (The security parameter is not critical)	N/A (The security parameter is not transmitted)	N/A (The security parameter is not critical)
SecParam-2	AES key for decrypting firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key. The delivered firmware package from the update server is encrypted. Therefore the key is not extractable. The access to the file system is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify and to read the key is the software update process which is run under a different account "softwareupdater" than any of the account used for external interfaces.	The key is hardcoded in the firmware and is modified only through a verified firmware update package.	N/A (Parameter is not transmitted)	The AES key is generated before a firmware update package is released on a separate offline Linux® PC with the most recent OpenSSL version at the time of the key generation. OpenSSL uses its own random number generator, which is seeded by /dev/random of the Linux® machine. /dev/random again is seeded by an HSM connected to the machine.
SecParam-6	ID for Identification of the DUT against the associated services (cloud	critical	The ID is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to gain access to the ID. This is prevented by input validation of data presented to the DUT's	The ID is hardcoded in the hardware and cannot be modified during the operation.		N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of
SecParam-9	Username and password combination for authentication against the app. The combination is no hardcoded	critical	The combination is not accessible by an attacker so that its confidentiality is	An attacker needs access to the file system to change the password. This is prevented by input validation of data presented to the DUT's			N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of

Based on the sensitive parameters described in IXIT 10-SecParam, SecParam-1, SecParam-2, and SecParam-3, hardcoded in the device software, the device is not directly networked, and an attacker would need access to the file system or firmware package on the DUT to access the key. Software updates are also transmitted and encrypted using secure protocols for processing, so these two parameters are judged to be secure.

Based on the sensitive parameters described in IXIT 10-SecParam, SecParam-4, for the user account password, the application uses a secure transport and irreversible hash function to encrypt and store the cloud, and login access requires authentication forensics.

This test, passed.

TC_SENSITIVE_DATA _#4 / Test case 5.4.2-2	
Security requirement	PROVISION 5.4-2
Type of work	Test CAB
Applicability	Conditional (hard-coded unique per device identity is used for security purposes)
Test objectives	Verify that hard-coded unique per device identity could resist tampering by physical means
Evaluation inputs	- At least three devices suitable for testing - Collected sensitive security parameter from **IXIT 10-SecParam**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) Tester assess whether for all each hard-coded identity as indicated in **Description** in **IXIT 10-SecParam** the **Protection Scheme** with respect to tamper-resistance is implemented according to the IXIT documentation. **Expected result:** ✓ Result of tampering enforcement
Verdict	The verdict **PASS** is assigned if: - For every hard-coded identity, there is no indication that the implementation of any protection scheme with respect to tamper-resistance differs from its IXIT documentation. The verdict **FAIL** is assigned otherwise.

Test Result
PASS

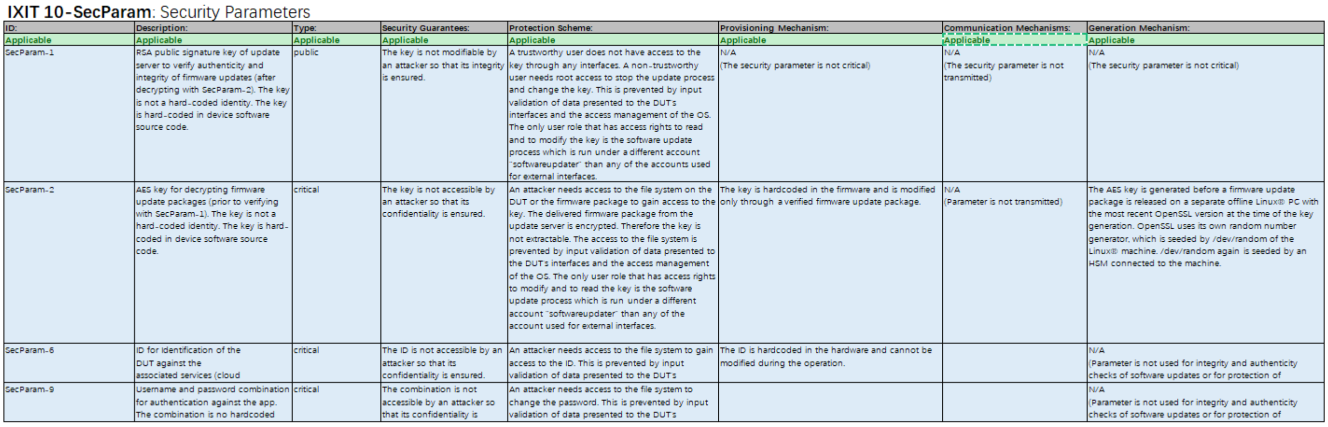
Testlab Comments
Based on the Protection Scheme description in IXIT 10-SecParam, the tester was tested for compliance. This test, passed.

6.7.2.3 Provision 5.4-3

M: Hard-coded critical security parameters in device software source code shall not be used.

TC_SENSITIVE_DATA _#5 / Test case 5.4.3-1	
Security requirement	PROVISION 5.4-3
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	Check that hard-coded security parameters defined as critical is not present inside source-code
Evaluation inputs	- Collected sensitive security parameter from **IXIT 10-SecParam**
Documentation analysis procedure	a) Check whether for all critical security parameters provided in **IXIT 10-SecParam** where **Provisioning Mechanism** indicates that it is hard coded in device software source code, the fact is reflected in **Description**. b) Assess whether for all critical security parameters in **IXIT 10-SecParam**, which are hard coded in device software source code according to **Description**, the corresponding **Provisioning Mechanism** ensures that it is not used during the operation of the DUT.
Verdict	The verdict PASS is assigned if: - There is no indication that any critical security parameter hard-coded in device software source code is not documented as such; **AND** - For all critical security parameter hard-coded in device software source code, the "**Provisioning Mechanism"** ensures that it is not used during the operation of the DUT. The verdict FAIL is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 10-SecParam: Security Parameters

ID:	Description:	Type:	Security Guarantees:	Protection Scheme:	Provisioning Mechanism:	Communication Mechanisms:	Generation Mechanism:
Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
SecParam-1	RSA public signature key of update server to verify authenticity and integrity of firmware updates (after decrypting with SecParam-2). The key is not a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	A trustworthy user does not have access to the key through any interfaces. A non-trustworthy user needs root access to stop the update process and change the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read and to modify the key is the software update process which is run under a different account "softwareupdater" than any of the accounts used for external interfaces.	N/A (The security parameter is not critical)	N/A (The security parameter is not transmitted)	N/A (The security parameter is not critical)
SecParam-2	AES key for decrypting firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key. The delivered firmware package from the update server is encrypted. Therefore the key is not extractable. The access to the file system is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify and to read the key is the software update process which is run under a different account "softwareupdater" than any of the account used for external interfaces.	The key is hardcoded in the firmware and is modified only through a verified firmware update package.	N/A (Parameter is not transmitted)	The AES key is generated before a firmware update package is released on a separate offline Linux® PC with the most recent OpenSSL version at the time of the key generation. OpenSSL uses its own random number generator, which is seeded by /dev/random of the Linux® machine. /dev/random again is seeded by an HSM connected to the machine.
SecParam-6	ID for identification of the DUT against the associated services (cloud	critical	The ID is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to gain access to the ID. This is prevented by input validation of data presented to the DUT's	The ID is hardcoded in the hardware and cannot be modified during the operation.		N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of
SecParam-9	Username and password combination for authentication against the app. The combination is no hardcoded	critical	The combination is not accessible by an attacker so that its confidentiality is	An attacker needs access to the file system to change the password. This is prevented by input validation of data presented to the DUT's			N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of

Tester testing confirmed that the RSA key hardcoded in SecParam-1 of IXIT 10-SecParam is used to verify the integrity check of the update packet, the AES key hardcoded in SecParam-2 is used to decrypt the update packet, and the ID hardcoded in SecParam-3 is used for device authentication. The above three sensitive parameters are used for updates only and are all singularized for their purpose.

The user account password for SecParam-4 in IXIT 10-SecParam is used for app login authentication, singularized usage.

This test, passed.

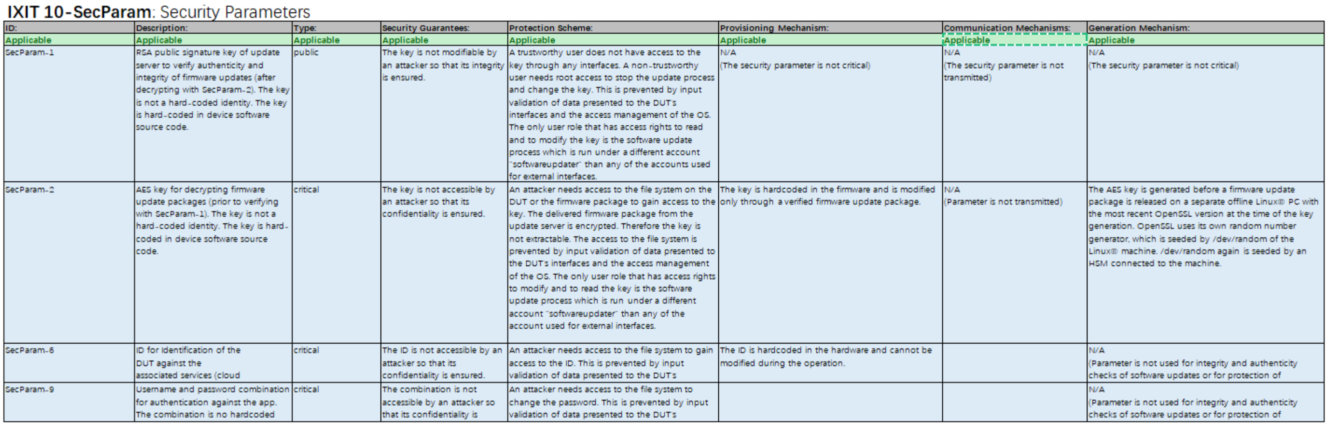
TC_SENSITIVE_DATA _#6 / Test case 5.4.3-2	
Security requirement	PROVISION 5.4-3
Type of work	Test CAB
Applicability	Always
Test objectives	Check that hard-coded security parameters defined as critical is not present inside source-code
Evaluation inputs	- At least three devices suitable for testing - Collected sensitive security parameter from **IXIT 10-SecParam**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) Tester assess whether for all critical security parameters hard-coded in device software source code documented in “**Description”** of **IXIT 10-SecParam**, the **Provisioning Mechanism** is indeed applied during the operation of the DUT. **Expected result:** ✓ Result of tampering enforcement.
Verdict	The verdict **PASS** is assigned if: - For all critical security parameter hard-coded in device software source code there is no indication that the application of the provisioning mechanism differs from its IXIT documentation. The verdict **FAIL** is assigned otherwise.
Test Result	
PASS	
Testlab Comments	
Tester testing confirms that the description in the IXIT 10-SecParam matches the actual test. This test passed.	

6.7.2.4 Provision 5.4-4

M C (15): Any critical security parameters used for integrity and authenticity checks of software update and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.

TC_SENSITIVE_DATA _#7 / Test case 5.4.4-1	
Security requirement	PROVISION 5.4-4
Type of work	IXIT analysis
Applicability	Conditional (critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist)
Documentation analysis objectives	Check that critical security parameters used for integrity and authenticity (software update and protection of communication) shall be unique per device
Evaluation inputs	- Collected sensitive security parameter from **IXIT 10-SecParam**
Documentation analysis procedure	a) Check whether all critical security parameter provided in **IXIT 10-SecParam**, where **Description** indicates that the critical security parameters are used for integrity and authenticity checks of software updates or for protection of communication with associated services are documented as such in **Generation Mechanism**. b) Assess for all critical security parameters provided in **IXIT 10-SecParam**, whether the **Generation Mechanism** ensures that the critical security parameter is unique per device and produced with a mechanism that reduces the risk of automated attacks against classes of devices.
Verdict	The verdict **PASS** is assigned if: - All critical security parameter where the purpose in **Description** indicates that the critical security parameters are used for integrity and authenticity checks of software updates or for protection of communication with associated services are documented as such in **Generation Mechanism**; **AND** - For all critical security parameters the **Generation Mechanism** ensures that the critical security parameters are unique per device and produced with a mechanism that reduces the risk of automated attacks against classes of devices. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 10-SecParam: Security Parameters

ID:	Description:	Type:	Security Guarantees:	Protection Scheme:	Provisioning Mechanism:	Communication Mechanisms:	Generation Mechanism:
Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable
SecParam-1	RSA public signature key of update server to verify authenticity and integrity of firmware updates (after decrypting with SecParam-2). The key is not a hard-coded identity. The key is hard-coded in device software source code.	public	The key is not modifiable by an attacker so that its integrity is ensured.	A trustworthy user does not have access to the key through any interfaces. A non-trustworthy user needs root access to stop the update process and change the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read and to modify the key is the software update process which is run under a different account "softwareupdater" than any of the accounts used for external interfaces.	N/A (The security parameter is not critical)	N/A (The security parameter is not transmitted)	N/A (The security parameter is not critical)
SecParam-2	AES key for decrypting firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded in device software source code.	critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key. The delivered firmware package from the update server is encrypted. Therefore the key is not extractable. The access to the file system is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify and to read the key is the software update process which is run under a different account "softwareupdater" than any of the account used for external interfaces.	The key is hardcoded in the firmware and is modified only through a verified firmware update package.	N/A (Parameter is not transmitted)	The AES key is generated before a firmware update package is released on a separate offline Linux® PC with the most recent OpenSSL version at the time of the key generation. OpenSSL uses its own random number generator, which is seeded by /dev/random of the Linux® machine. /dev/random again is seeded by an HSM connected to the machine.
SecParam-6	ID for Identification of the DUT against the associated services (cloud	critical	The ID is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system to gain access to the ID. This is prevented by input validation of data presented to the DUT's	The ID is hardcoded in the hardware and cannot be modified during the operation.		N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of
SecParam-9	Username and password combination for authentication against the app. The combination is no hardcoded	critical	The combination is not accessible by an attacker so that its confidentiality is	An attacker needs access to the file system to change the password. This is prevented by input validation of data presented to the DUT's			N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of

Based on SecParam-2 in IXIT 10-SecParam, AES keys are generated by secure random number generation.
SecParam-4 is a user setting that passes the strength check.
This test passed.

6.8 Communicate Securely

6.8.1 IXIT Data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 11-ComMech: Communication Mechanisms

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the communication mechanism, including its purpose and a description of the used protocol. For standardized protocols a reference is sufficient. It is indicated additionally whether the mechanism is remotely accessible **Note**: *A possible communication mechanism is the use of Bluetooth®, WiFi® or NFC for a local connection between an mobile application and the DUT.*
Security Guarantees:	Description of the realized security objectives and the threats the mechanism is protected against. **Note**: *The most common security guarantees to be considered include authentication of peers, authentication of origin, integrity protection, confidentiality protection, and anti-replay.*
Cryptographic Details:	Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the communication mechanism considering key management, and to facilitate the described **"Security Guarantees".** **Note**: *Cryptographic Details contain information such as: the protocol Z-Wave® with Security 2 Command Class v1 is used for the communication. The transferred data is authenticated encrypted with AES-128 CCM to facilitate confidentiality and integrity. The key exchange is based on an out-of-band mechanism.*
Resilience Measures:	Description of the measures to ensure that the connection establishment is performed in an orderly fashion including an expected, operational and stable state to achieve a stable connection. **Note**: *Resilience measures consider the sequence of the used protocol, the capability of the infrastructure, reset and initialization of the protocol and problems caused by mass reconnections*

IXIT 12-NetSecImpl: Network and Security Implementations

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the implementation of the network or security functionality, including its purpose and scope. **Note**:The kind of implementation (e.g. software library or separate microcontroller) is helpful to determine the relevant functionality for an evaluation or review.
Review/Evaluation Method:	Description of the method used to review or evaluate the implementation, including the principles it is based on (e.g. audit, peer review, automated code analysis). Additionally the implementation scope is described, that is covered by the method.
Report	Outcome of the review or evaluation or a reference to the certificate or the evaluation report that proves that the implementation has been successfully evaluated. **Note**: The outcome of the review or evaluation does not need to be a single document. For instance, it is also possible to use the documentation of bug tracking in a software management tool to demonstrate that the implementation is reviewed.

IXIT 6-SoftComp: Software Components

ID	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description	Brief description of the software component.
Update Mechanism	Reference to update mechanisms in IXIT 7-UpdMech that are used for updating the software component. An empty list of update mechanisms indicates the absence of updates for the software component and in this case a justification is provided.
Cryptographic Usage:	Indicates, if the software component makes use of cryptographic algorithms or primitives (Yes/No) and if so, it is included additionally, whether side effects of updating those algorithms and primitives are considered by the manufacturer (Yes/No).

IXIT 13-SoftServ: Software Services

ID	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description	Brief description of the service, including its purpose. It is indicated additionally whether the service is accessible via network interface and whether this is the case in the initialized state
Status:	Indication whether the service is enabled or disabled in the initialized state.
Justification:	If the service is enabled: Justification why the service is necessary for the intended use or operation of the DUT.
Allows Configuration (Yes/No):	If the service is accessible via network interface: Indication whether the service allows security-relevant changes in configuration and if so, a brief description of the possible configuration.
Authentication Mechanism:	If the service is accessible via network interface: Reference to authentication mechanisms in **IXIT 1-AuthMech** that are used for authentication prior the use of the service.

IXIT 1-AuthMech: Authentication Mechanisms

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the authentication mechanism and its corresponding authorization process. It is indicated additionally whether the mechanism is used for user or machine-to-machine authentication and whether it is directly addressable from a network interface.
Authentication Factor:	The type of attribute used for authentication. For passwords it is indicated additionally whether the password is set by the user and used in the initialized state.
Password Generation Mechanism:	If the authentication factor is a password, which is not set by the user: Description of the mechanism to generate the password. It is indicated additionally whether the password is unique per device and whether it is pre-installed. ***Note****: A detailed specification of the password generation mechanism is not necessary.It is considered as sufficient when the description explains the measures to ensure that the passwords are unique per device in any state other than the factory default and to reduce the risks of automated attacks based on obvious regularities, common strings, public available information or inappropriate complexity when used as pre- installed and unique per device password.*
Security Guarantees:	Description of the realized security objectives and the threats the mechanism is protected against.

	Example: *The mechanisms attests that the authenticated entity is in possession of a valid password. The confidentiality and integrity protection of the password during transfer is also guaranteed within the session.*
Cryptographic Details:	Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the authentication mechanism considering key management, and to facilitate the described "Security Guarantees". **Example**: *Authentication is performed via http authentication framework (IETF RFC 7235 [i.10]). Integrity and confidentiality of the password transfer to the DUT is realized with the TLS cipher suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA256.*
Brute Force Prevention:	If the authentication mechanism is directly addressable from a network interface: Description of the method to prevent an attacker from brute forcing credentials via network interfaces. **Example**: *A time delay of 5 seconds after an unsuccessful login before a new login can follow.*

IXIT 10-SecParam: Security Parameters

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the security parameter, including its purpose. It is indicated additionally whether the parameter is a hard-coded unique per device identity used in a device for security purposes (hard- coded identity) and/or hard-coded in device software source code.
Type:	Indication whether the security parameter is public or critical. **Note**: *Public and critical security parameters are defined in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].*
Security Guarantees:	Description of the realized baseline security objectives and threats the security parameter is protected against during persistent storage.
Protection Scheme:	Description of the measures that are applied to achieve the Security Guarantees. This includes the principals and roles through which access to the parameter is possible, including the privileges associated to each role.
Provisioning Mechanism:	If the **"Type"** indicates that the parameter is critical: Description of the mechanism through which the parameter is assigned its value for the operation of the DUT. **Note**: *Such assignment can happen during initialization or in initialized state (e.g. when a device functionality relying on the parameter is activated by the user).* **Note**: *Persistent configuration data, runtime configuration data, protocol negotiation and assignment to a default value are potentially possible provisioning mechanisms.*
Communication Mechanisms:	Reference to communication mechanisms in **IXIT 11-ComMech** that are used for communicating the parameter and an indication whether the communication is done via remotely accessible interfaces.
Generation Mechanism:	If the **"Type"** indicates that the parameter is critical and used for integrity and authenticity checks of software updates or for protection of communication with associated services: Description of the mechanism used to generate the values of the parameter and it is indicated additionally that the parameter is used for integrity and authenticity checks of software updates or for protection of communication with associated services. **Note**: *References to a standard random number generator and applicable design documents.*

IXIT 4-Conf: Confirmations

Confirmation of Secure Management (Yes/No):	Confirmation that the secure management processes described in **IXIT 14-SecMgmt** are established.

IXIT 14-SecMgmt: Secure Management Processes

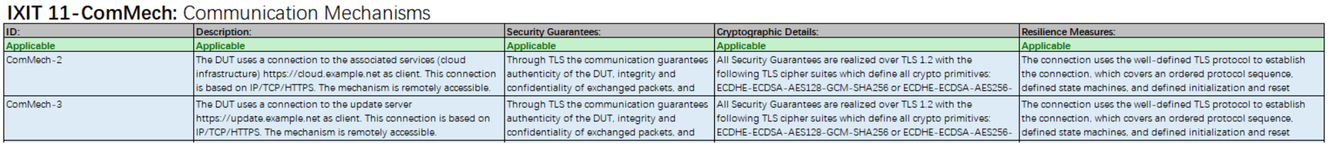
ID	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description	Brief description of the secure management process regarding the whole life cycle for critical security parameters. If an existing standard is used, a reference to the corresponding standard is provided. **Note**: The life cycle of a critical security parameters typically considers generation, provisioning, storage, updates, decommissioning, archival, destruction, processes to handle the expiration and compromise of the parameter.

6.8.2 Evaluation tasks

6.8.2.1 Provision 5.5-1

M: The consumer IoT device shall use best practice cryptography to communicate securely.

TC_COMMUNICATE_SECURELY_#1 / Test case 5.5-1-1	
Security requirement	PROVISION 5.5-1
Type of work	Doc
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the cryptography used for the communication mechanisms concerning the use of best practice cryptography **(a-c)** and the vulnerability to a feasible attack (**d).**
Evaluation inputs	List of communication mechanism in **IXIT 11-ComMech:** for each communication mechanism described in IXIT11-ComMech following information is required: - security guarantees - cryptographic details
Documentation analysis procedure	a) For each communication mechanism in **IXIT 11-ComMech,** assess whether **the "Security Guarantees"** are appropriate for the use case of the communication. b) For each communication mechanism in **IXIT 11-ComMech**, assess whether the mechanism according to **"Description**" is appropriate to achieve the **"Security Guarantees".** c) For each communication mechanism in **IXIT 11-ComMech**, assess whether the **"Cryptographic Details"** are considered as best practice cryptography for the use case of secure communication based on a reference catalogue. If **"Cryptographic Details"** are not included in a reference catalogue for the corresponding use case (e.g. novel cryptography), the SO **shall** provide evidences, e.g. a risk analysis, to justify the cryptography is appropriate as best practice for the use case. In such case the TESTER **shall** assess whether the evidence is appropriate and reliable for the use case. d) For each communication mechanism in **IXIT 11-ComMech**, the TESTER **shall** assess whether the "**Cryptographic Details"** are not known to be vulnerable to a feasible attack for the desired security property on the base of the "**Security Guarantees"** by reference to competent cryptanalytic reports.
Verdict	The verdict PASS is assigned if for all communication mechanisms: • The security guarantees are appropriate for the use case of secure communication; **AND** • The mechanism is appropriate to achieve the security guarantees with respect to the use case; **AND** • All used cryptographic details are considered as best practice for the use case; **AND** • All used cryptographic details are not known to be vulnerable to a feasible attack for the desired security property. The verdict FAIL is assigned otherwise.
Test Result	
PASS	
Testlab Comments	



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
Applicable	Applicable	Applicable	Applicable	Applicable
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset

Based on the IXIT 11-ComMech, the device has two modes of networking, one via WALA to the computer and one via the app. Testers have tested that the various interfaces of the app, which involve the transmission or display of sensitive information, have been used with the Secure Transmission Protocol and TLS1.2, and the security suite has been used.

This test, passed.

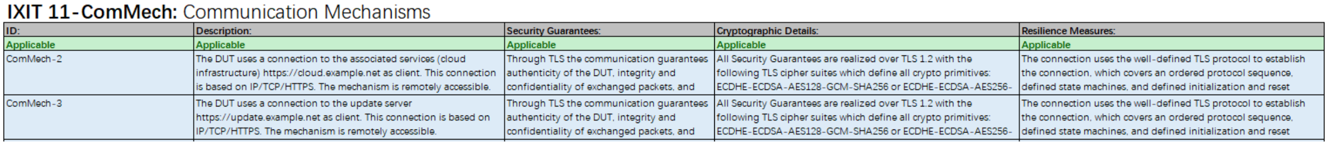
TC_COMMUNICATE_SECURELY_#2 / Test case 5.5-1-2

Security requirement	PROVISION 5.5-1
Type of work	Test CAB
Applicability	Always
Test objectives	Verify whether cryptography used for the communication mechanism by manufacturer is implemented on device
Evaluation inputs	- At least one device suitable for testing - List of communication mechanism in **IXIT 11-ComMech:** for each communication mechanism described in IXIT11-ComMech following information is required: - security guarantees - cryptographic details
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** **a)** For each communication mechanism in **IXIT 11-ComMech**, the tester functionally assess whether the described **"Cryptographic Details"** are used by the DUT. **Expected result:** ✓ Evaluation of implementation of cryptographic settings as declared on IXIT documentation
Verdict	The verdict PASS is assigned if: - There is no indication that any used cryptographic setting differs from its IXIT documentation. The verdict FAIL is assigned otherwise.

Test Result

PASS

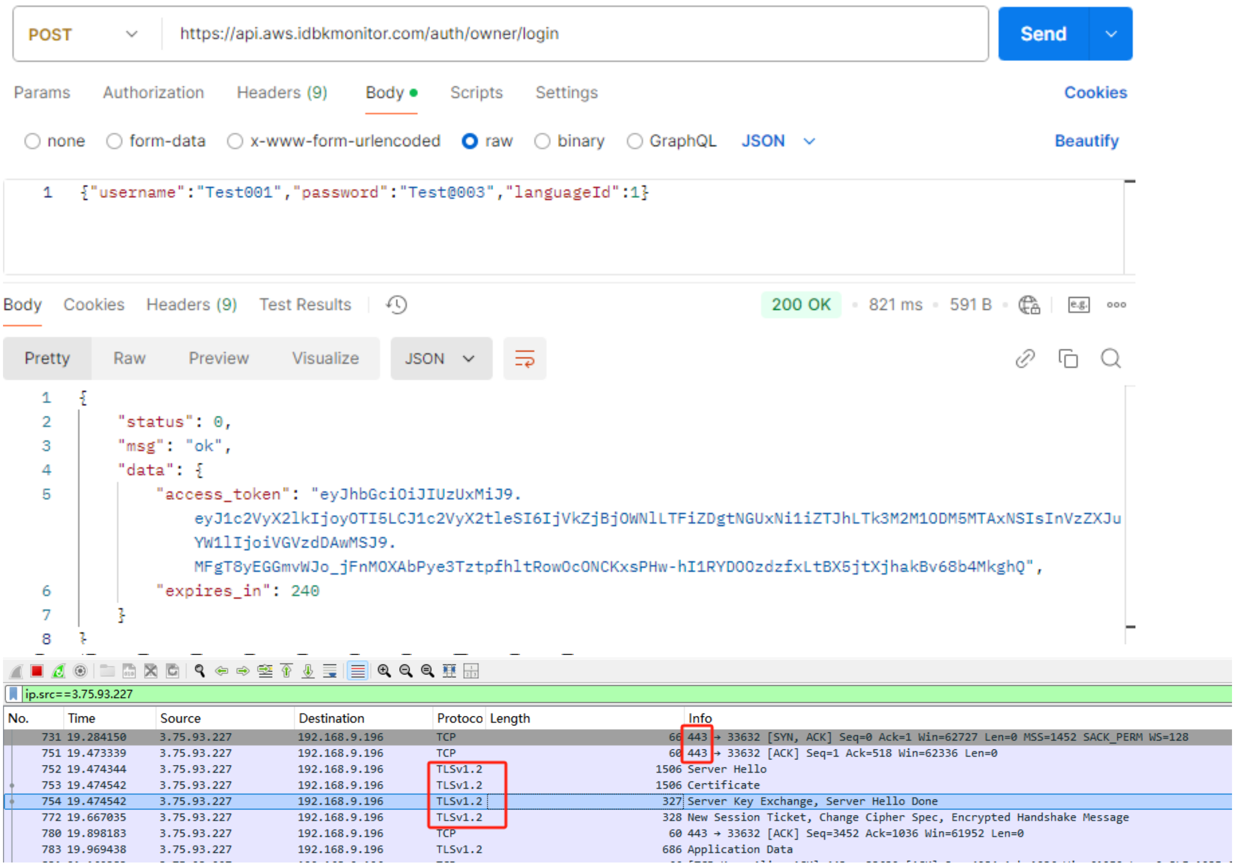
Testlab Comments



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
Applicable	Applicable	Applicable	Applicable	Applicable
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset

Based on IXIT 11-ComMech, testers have tested that the encryption settings described in the documentation are consistent with actual use.



https://api.aws.idbkmonitor.com/auth/owner/login

```
{"username":"Test001","password":"Test@003","languageId":1}
```

200 OK · 821 ms · 591 B

```
{
    "status": 0,
    "msg": "ok",
    "data": {
        "access_token": "eyJhbGciOiJIUzUxMiJ9.
            eyJ1c2VyX2lkIjoyOTI5LCJ1c2VyX2tleSI6IjVkZjBjOWNlLTFiZDgtNGUxNi1iZTJhLTk3M2M1ODM5MTAxNSIsInVzZXJu
            YW1lIjoiVGVzdDAwMSJ9.
            MFgT8yEGGmvWJo_jFnMOXAbPye3TztpfhltRowOcONCKxsPHw-hI1RYDOOzdzfxLtBX5jtXjhakBv68b4MkghQ",
        "expires_in": 240
    }
}
```

ip.src==3.75.93.227

```
No.   Time        Source        Destination    Protoco Length  Info
  731 19.284150   3.75.93.227   192.168.9.196  TCP         66  443 → 33632 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1452 SACK_PERM WS=128
  751 19.473339   3.75.93.227   192.168.9.196  TCP         60  443 → 33632 [ACK] Seq=1 Ack=518 Win=62336 Len=0
  752 19.474344   3.75.93.227   192.168.9.196  TLSv1.2   1506  Server Hello
  753 19.474542   3.75.93.227   192.168.9.196  TLSv1.2   1506  Certificate
  754 19.474542   3.75.93.227   192.168.9.196  TLSv1.2    327  Server Key Exchange, Server Hello Done
  772 19.667035   3.75.93.227   192.168.9.196  TLSv1.2    328  New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  780 19.898183   3.75.93.227   192.168.9.196  TCP         60  443 → 33632 [ACK] Seq=3452 Ack=1036 Win=61952 Len=0
  783 19.969438   3.75.93.227   192.168.9.196  TLSv1.2    686  Application Data
```

The login interface in the application uses the https protocol, TLS 1.2 protocol, as described in IXIT 11-ComMech.

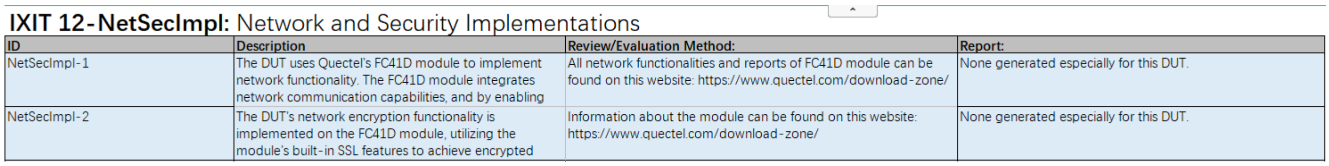
This test, passed.

6.8.2.2 Provision 5.5-2

<u>**R:**</u> The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.

TC_COMMUNICATE_SECURELY_#3 / Test case 5.5-2-1	
Security requirement	PROVISION 5.5-2
Type of work	Doc
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the implementations of network and security functionalities concerning reviews and evaluations.
Evaluation inputs	- Evaluation & Review Methods regarding on network and security functionalities on device in particular in cryptography domain **(“Review/Evaluation Method”** from **IXIT 12-NetSecImpl**) - Outcome of the review or evaluation (**“Report”** from **IXIT 12-NetSecImpl**)
Documentation analysis procedure	a) For each implementation in **IXIT 12-NetSecImpl**, assess whether it has been reviewed or evaluated according to **"Review/Evaluation Method".** b) For each review or evaluation method associated to an implementation in **IXIT 12-NetSecImpl,** assess whether the "**Review/Evaluation Method**" and its "**Report**" covers the related implementation scope as described in "**Description".**
Verdict	The verdict **PASS** is assigned if: • All implementations of network and security functionalities are reviewed or evaluated; **AND** • All review and evaluation methods cover the scope of the related implementation. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 12-NetSecImpl: Network and Security Implementations

ID	Description	Review/Evaluation Method:	Report:
NetSecImpl-1	The DUT uses Quectel's FC41D module to implement network functionality. The FC41D module integrates network communication capabilities, and by enabling	All network functionalities and reports of FC41D module can be found on this website: https://www.quectel.com/download-zone/	None generated especially for this DUT.
NetSecImpl-2	The DUT's network encryption functionality is implemented on the FC41D module, utilizing the module's built-in SSL features to achieve encrypted	Information about the module can be found on this website: https://www.quectel.com/download-zone/	None generated especially for this DUT.

Based on IXIT 12-NetSecImpl, The DUT uses Quectel's FC41D module to implement network functionality. The FC41D module integrates network communication capabilities, and by enabling the SSL service on the module, it facilitates data， Information about the module can be found on this website: https://www.quectel.com/download-zone/

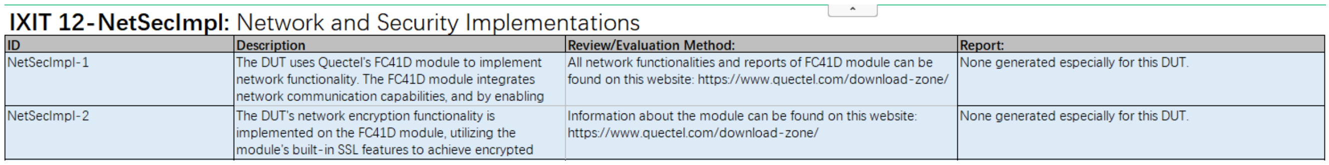
This test, passed.

TC_COMMUNICATE_SECURELY_#4 / Test case 5.5-2-2	
Security requirement	PROVISION 5.5-2
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the implementations of network and security functionalities concerning reviews and evaluations.
Evaluation inputs	- Evaluation & Review Methods regarding on network and security functionalities on device in particular in cryptography domain **(“Review/Evaluation Method”** from **IXIT 12-NetSecImpl**) - outcome of the review or evaluation (**“Report”** from **IXIT 12-NetSecImpl**)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) For each implementation associated with a review or evaluation method in **IXIT 12-NetSecImpl**, check whether the identification of the implementation (name and version) on the DUT matches the identification of the implementation provided in the **"Report".** **Expected result:** ✓ Matching between identification of the implementation (name & version) on device compare to what is provided in IXIT statement
Verdict	The verdict **PASS** is assigned if: • The name and version of every provided implementation matches the name and version provided in the related report; or • The necessary information are not obtainable, because the DUT does not provide any information on the implementation name and version. The verdict **FAIL** is assigned otherwise.

Test Result

FAIL

Testlab Comments



IXIT 12-NetSecImpl: Network and Security Implementations

ID	Description	Review/Evaluation Method:	Report:
NetSecImpl-1	The DUT uses Quectel's FC41D module to implement network functionality. The FC41D module integrates network communication capabilities, and by enabling	All network functionalities and reports of FC41D module can be found on this website: https://www.quectel.com/download-zone/	None generated especially for this DUT.
NetSecImpl-2	The DUT's network encryption functionality is implemented on the FC41D module, utilizing the module's built-in SSL features to achieve encrypted	Information about the module can be found on this website: https://www.quectel.com/download-zone/	None generated especially for this DUT.

According to IXIT 12-NetSecImpl, the DUT has two NetSecImpl.

However, the manufacturer did not provide any report of the identification of the implementation (name and version) on the DUT. The tester cannot verify that the name and version of every provided implementation matches the name and version specified in the related report. Therefore, it is determined that the requirement fails.

6.8.2.3 Provision 5.5-3

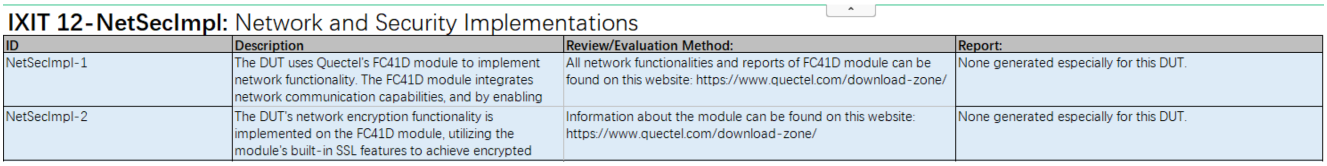
R: Cryptographic algorithms and primitives should be updateable.

TC_COMMUNICATE_SECURELY_#5 / Test case 5.5-3-1	
Security requirement	PROVISION 5.5-3
Type of work	Doc
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of implementations providing cryptographic algorithms and primitives concerning the updatability.
Evaluation inputs	For each software component**, “cryptographic Usage”** & “**Update Mechanism” from IXIT 6-SoftComp**
Documentation analysis procedure	a) For each software component in **IXIT 6-SoftComp** indicating **"Cryptographic Usage”**, assess whether an **"Update Mechanism"** to update the software component is referenced. b) For each software component in **IXIT 6-SoftComp** indicating **"Cryptographic Usage"**, assess whether side effects of updating those algorithms and primitives are considered by the manufacturer.
Verdict	The verdict PASS is assigned if: - For every software component indicating cryptographic usage an update mechanism is referenced; **AND** - Side effects of updating those algorithms and primitives are considered by the manufacturer. The verdict FAIL is assigned otherwise.

Test Result

FAIL

Testlab Comments



IXIT 12-NetSecImpl: Network and Security Implementations

ID	Description	Review/Evaluation Method:	Report:
NetSecImpl-1	The DUT uses Quectel's FC41D module to implement network functionality. The FC41D module integrates network communication capabilities, and by enabling	All network functionalities and reports of FC41D module can be found on this website: https://www.quectel.com/download-zone/	None generated especially for this DUT.
NetSecImpl-2	The DUT's network encryption functionality is implemented on the FC41D module, utilizing the module's built-in SSL features to achieve encrypted	Information about the module can be found on this website: https://www.quectel.com/download-zone/	None generated especially for this DUT.

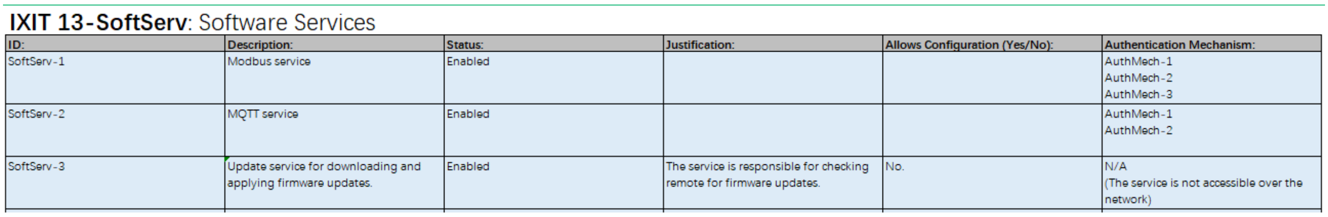
Based on the information provided by the vendor regarding IXIT 6-SoftComp, SoftComp-1 referencing Cryptographic Usage includes an Update Mechanism, while SoftComp-2, being ineligible for updates, is not applicable. Therefore, this test item is deemed to fail.

6.8.2.4 Provision 5.5-4

RC (16): Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.

TC_COMMUNICATE_SECURELY_#6 / Test case 5.5-4-1	
Security requirement	PROVISION 5.5-4
Type of work	Doc
Applicability	Conditional (access to device functionality via a network interface in the initialized state is possible)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of device functionality via a network interface in the initialized state concerning authentication and authorization.
Evaluation inputs	List of all software services (“**Authentication Mechanism”** from **IXIT 13-SoftServ**) List of all Authentication mechanism (**IXIT 1-AuthMech**)
Documentation analysis procedure	a) For each device functionality in **IXIT 13-SoftServ** indicated as accessible via network interface in the initialized state according to "**Description"**, assess whether there is at least one **"Authentication Mechanism"** referenced. b) For each **"Authentication Mechanism"** referenced in **IXIT 13-SoftServ**, assess whether the authentication mechanism described in **IXIT 1-AuthMech** allows to discriminate between multiple authentication subjects and can reject authentication attempts based on invalid identities and/or authentication factors. ***Note****: Discriminating is typically done based on unique identities and/or authentication factors.* c) For each **"Authentication Mechanism"** referenced in **IXIT 13-SoftServ,** assess whether the means protecting the authentication mechanism in **"Cryptographic Details"** in **IXIT 1-AuthMech** provide the **"Security Guarantees"** identified for the mechanism and are resistant to attempts at compromising the mechanism. d) d) For each **"Authentication Mechanism"** referenced in **IXIT 13-SoftServ**, assess whether the authorization process described in **"Description"** in **IXIT 1-AuthMech** allows authenticated subjects with proper access rights to be granted access and denies authenticated subjects with inadequate access rights or unauthenticated subjects to be granted access.
Verdict	The verdict **PASS** is assigned if: • At least one authentication mechanism is referenced for every device functionality accessible via network interface in the initialized state; **AND** • Every authentication mechanism allows to discriminate between multiple authentication subjects and to reject authentication attempts based on invalid identities **AND/OR** authentication factors; **AND** • The means used to protect an authentication mechanism provide the expected security guarantees and are resistant at attempts to compromise the mechanism; **AND** • Every authorization mechanism allows access to authenticated subjects with proper access rights; **AND** • Every authorization mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 13-SoftServ: Software Services

ID:	Description:	Status:	Justification:	Allows Configuration (Yes/No):	Authentication Mechanism:
SoftServ-1	Modbus service	Enabled			AuthMech-1 AuthMech-2 AuthMech-3
SoftServ-2	MQTT service	Enabled			AuthMech-1 AuthMech-2
SoftServ-3	Update service for downloading and applying firmware updates.	Enabled	The service is responsible for checking remote for firmware updates.	No.	N/A (The service is not accessible over the network)

Based on IXIT 13-SoftServ, the DUT offers three connection methods.

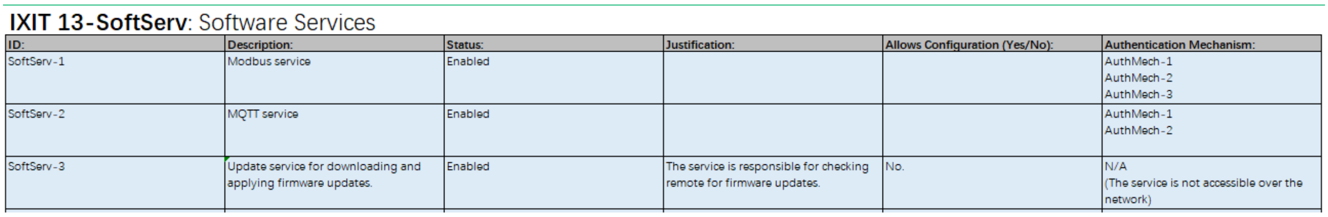
The tester connects through the application login and performs an override test, where unauthorized content cannot be viewed and this test is successful.

The tester logs in to the MQTT client and can only subscribe to public or authorized topics, cannot subscribe to unauthorized topics, etc. This test succeeds.

This test passes.

TC_COMMUNICATE_SECURELY_#7 / Test case 5.5-4-2	
Security requirement	PROVISION 5.5-4
Type of work	Test CAB
Applicability	Conditional (access to device functionality via a network interface in the initialized state is possible)
Test objectives	The purpose of this test case is the functional assessment of device functionality via a network interface in the initialized state concerning authentication and authorization.
Evaluation inputs	List of all software services (“**Authentication Mechanism”** from **IXIT 13-SoftServ**) List of all Authentication mechanism (**IXIT 1-AuthMech**)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) For each **"Authentication Mechanism"** referenced in **IXIT 13-SoftServ**, assess whether an unauthenticated subject and a subject with invalid identity **or** credentials and an authenticated subject without appropriate access rights cannot access the device functionality in the initialized state. **Note**: *This test unit cannot in principle distinguish between the authentication and the authorization step - implementation aiming at reducing information leak will not disclose which step would fail to the subject.* ✓ b) For each **"Authentication Mechanism"** referenced in **IXIT 13-SoftServ**, functionally assess whether an authenticated subject with appropriate access rights can access the device functionality in the initialized state. ✓ c) For each **"Authentication Mechanism"** referenced in **IXIT 13-SoftServ**, functionally assess whether the protection of the authentication mechanism conforms to the description in "**Security Guarantees"** and "**Cryptographic Details"** in **IXIT 1-AuthMech.** **Expected result:** ✓ a) Evaluation of software services authentication in the context of inappropriate access right ✓ b) Evaluation of software services authentication in the context of appropriate access right ✓ c) Evaluation whether protection of authentication mechanism is in conformance with IXIT statement
Verdict	The verdict **PASS** is assigned if for every device functionality accessible via network interface in the initialized state: • An unauthenticated subject, a subject with invalid identity or invalid credentials and an authenticated subject without appropriate access rights cannot access the functionality in the initialized state; **AND** • An authenticated subject with appropriate access rights can access the device functionality in the initialized state; **AND** • There is no indication that the mechanism to secure the authentication differs from its IXIT documentation. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



IXIT 13-SoftServ: Software Services

ID:	Description:	Status:	Justification:	Allows Configuration (Yes/No):	Authentication Mechanism:
SoftServ-1	Modbus service	Enabled			AuthMech-1 AuthMech-2 AuthMech-3
SoftServ-2	MQTT service	Enabled			AuthMech-1 AuthMech-2
SoftServ-3	Update service for downloading and applying firmware updates.	Enabled	The service is responsible for checking remote for firmware updates.	No.	N/A (The service is not accessible over the network)

Based on IXIT 13-SoftServ, the DUT offers three connection methods.

The tester connects through the application login and performs an override test, where unauthorized content cannot be viewed and this test is successful.

The tester logs in to the MQTT client and can only subscribe to public or authorized topics, cannot subscribe to unauthorized topics, etc. This test succeeds.

This test passes.

6.8.2.5 Provision 5.5-5

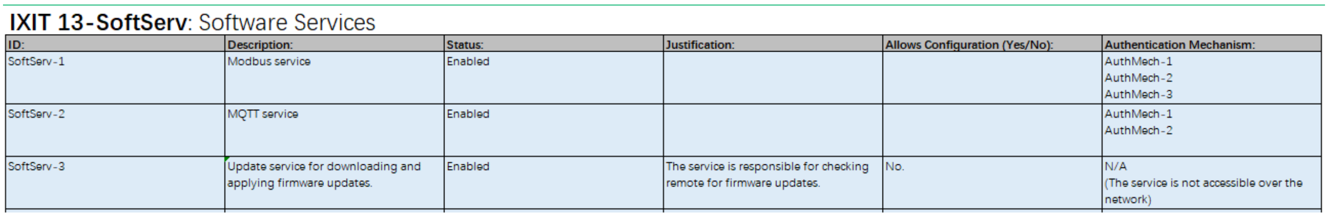
MC (17): Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device

TC_COMMUNICATE_SECURELY_#8 / Test Case 5.5.5-1	
Security requirement	PROVISION 5.5-5
Type of work	Doc
Applicability	Conditional (device functionality that allows security-relevant changes in configuration via a network interface exists)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of device functionality allowing security-relevant changes via a network interface concerning the authentication and authorization.
Evaluation inputs	List of all software services (“**Authentication Mechanism”** from **IXIT 13-SoftServ**) List of all Authentication mechanism (**IXIT 1-AuthMech**)
Documentation analysis procedure	a) Tester apply all test units as specified in the **Test case 5.5-4-1** with restriction to the functionalities that allow security-relevant changes according to **"Allows Configuration"** in **IXIT 13-SoftServ**. Network service protocols that are relied upon by the DUT and where the manufacturer cannot guarantee what configuration will be required for the DUT to operate are excluded. **Note**: *Network service protocols that are designed to enable external configuration without authentication, e.g. DHCP, are excluded in context of this provision.*
Verdict	The verdict **PASS** is assigned if: • Every authentication mechanism allows to discriminate between multiple authentication subjects and to reject authentication attempts based on invalid identities and/or authentication factors; **AND** • The means used to protect an authentication mechanism provide the expected security guarantees and are resistant at attempts to compromise the mechanism; **AND** • Every authorization mechanism allows access to authenticated subjects with proper access rights; **AND** • Every authorization mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 13-SoftServ: Software Services

ID:	Description:	Status:	Justification:	Allows Configuration (Yes/No):	Authentication Mechanism:
SoftServ-1	Modbus service	Enabled			AuthMech-1 AuthMech-2 AuthMech-3
SoftServ-2	MQTT service	Enabled			AuthMech-1 AuthMech-2
SoftServ-3	Update service for downloading and applying firmware updates.	Enabled	The service is responsible for checking remote for firmware updates.	No.	N/A (The service is not accessible over the network)

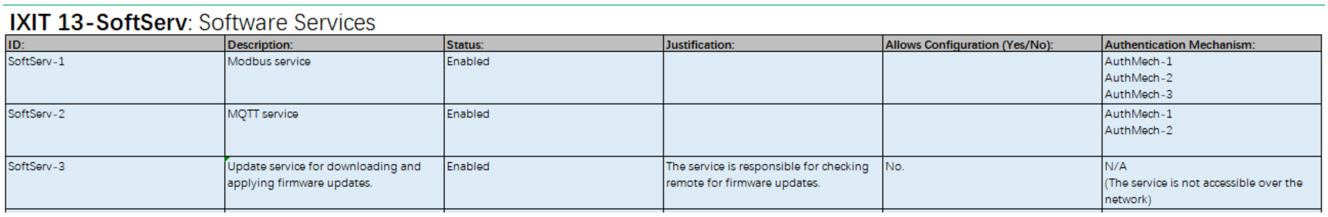
Based on IXIT 13-SoftServ, the authentication method provided by the DUT is to connect via app login, the user needs to register for an account should connect using the device's unique serial number.

The device has only one permission and requires authentication to log in and connect to the device before it can be operated.

This test, passed.

TC_COMMUNICATE_SECURELY_#9 / Test Case 5.5.5-2

Security requirement	PROVISION 5.5-5
Type of work	Test CAB
Applicability	Conditional (device functionality that allows security-relevant changes in configuration via a network interface exists)
Test objectives	The purpose of this test case is the functional assessment of device functionality allowing security-relevant changes via a network interface concerning the authentication and authorization (a) and the completeness of the IXIT documentation (b).
Evaluation inputs	- At least one device suitable for testing - List of all software services (“**Authentication Mechanism”** from **IXIT 13-SoftServ**) - List of all authentication mechanism (**IXIT 1-AuthMech**)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ Try to access security configuration functionality though network interfaces with authorized and unauthorized credentials ✓ a) Tester shall apply all test units as specified in the **Test case 5.5-4-2** for all states of the DUT with restriction to the functionalities that allow security-relevant changes according to **"Allows Configuration"** in **IXIT 13-SoftServ.** Network service protocols that are relied upon by the DUT and where the manufacturer cannot guarantee what configuration will be required for the DUT to operate are excluded. **Note**: Network service protocols that are designed to enable external configuration without authentication, e.g. DHCP, are excluded in context of this provision. ✓ b) Tester shall functionally assess whether communication mechanisms that are not documented in **IXIT 11- ComMech** are available via a network interface on the DUT. **Example**: Network scanning tools allow for discovery of network-based communication mechanisms **Expected result:** ✓ Denial or authorization access to configuration functionality
Verdict	The verdict **PASS** is assigned if: • An unauthenticated subject, a subject with invalid identity or invalid credentials **AND** • an authenticated subject without appropriate access rights cannot access the functionality; **AND** • An authenticated subject with appropriate access rights can access the device functionality; **AND** • There is no indication that the mechanism to secure the authentication differs from its IXIT documentation; **AND** • Every discovered network-based communication mechanism is documented in the IXIT. The verdict **FAIL** is assigned otherwise.
Test Result	
PASS	
Testlab Comments	



IXIT 13-SoftServ: Software Services

ID:	Description:	Status:	Justification:	Allows Configuration (Yes/No):	Authentication Mechanism:
SoftServ-1	Modbus service	Enabled			AuthMech-1 AuthMech-2 AuthMech-3
SoftServ-2	MQTT service	Enabled			AuthMech-1 AuthMech-2
SoftServ-3	Update service for downloading and applying firmware updates.	Enabled	The service is responsible for checking remote for firmware updates.	No.	N/A (The service is not accessible over the network)

Based on IXIT 13-SoftServ, the DUT offers three connection methods.

The tester connects through the application login and performs an override test, where unauthorized content cannot be viewed and this test is successful.

The tester logs in to the MQTT client and can only subscribe to public or authorized topics, cannot subscribe to unauthorized topics, etc. This test succeeds.

This test passes.

6.8.2.6 Provision 5.5-6

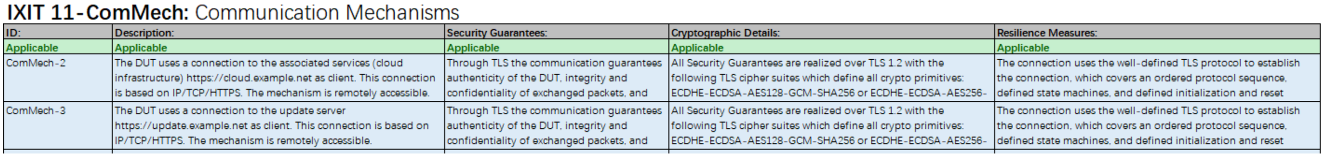
RC(18): Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.

TC_COMMUNICATE_SECURELY_#10 / Test Case 5.5-6-1	
Security requirement	PROVISION 5.5-6
Type of work	Doc
Applicability	Conditional (Critical security parameters are transmitted)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the cryptography used for communicating critical security parameters.
Evaluation inputs	List of communication mechanism **(“Communication Mechanisms”** in **IXIT 11-ComMech**) List of Security parameters (**IXIT 10-SecParam**)
Documentation analysis procedure	a) For all "**Communication Mechanisms"** in **IXIT 11-ComMech** referenced in any critical security parameter in **IXIT 10-SecParam**, tester apply all test units as specified in the **Test case 5.5-1-1** with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.
Verdict	The verdict PASS is assigned if for all communication mechanisms used for communicating critical security parameters: • The security guarantees are appropriate for the use case of secure communication; **AND** • The mechanism is appropriate to achieve the security guarantees with respect to the use case; **AND** • All used cryptographic details are considered as best practice for the use case; **AND** • All used cryptographic details are not known to be vulnerable to a feasible attack. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
Applicable	Applicable	Applicable	Applicable	Applicable
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset

Based on IXIT 13-SoftServ, reference 5.1-3-1.

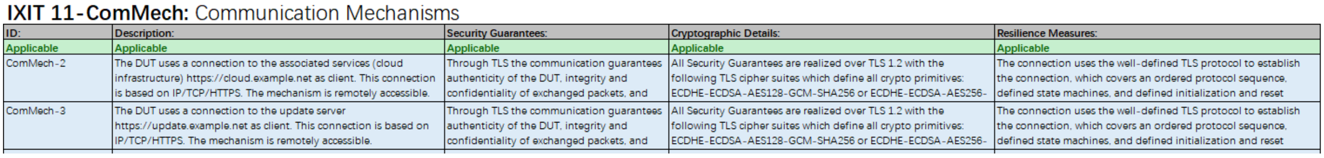
This test, passes.

TC_COMMUNICATE_SECURELY_#11 / Test Case 5.5-6-2	
Security requirement	PROVISION 5.5-6
Type of work	Test CAB
Applicability	Conditional (Critical security parameters are transmitted)
Test objectives	The purpose of this test case is the functional assessment of the cryptography used for communicating critical security parameters.
Evaluation inputs	- At least one device suitable for testing - List of communication mechanism in **IXIT 11-ComMech** - List of security parameters in **IXIT 10-SecParam**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) For all "**Communication Mechanisms"** in **IXIT 11-ComMech** referenced in any critical security parameter in **IXIT 10-SecParam**, tester apply all test units as specified in the **Test case 5.5-1-2**. **Expected result:** ✓ Implementation of secure communication in particular for critical security parameter
Verdict	The verdict PASS is assigned if for all communication mechanisms used for communicating critical security parameters: • The security guarantees are appropriate for the use case of secure communication; **AND** • The mechanism is appropriate to achieve the security guarantees with respect to the use case; **AND** • All used cryptographic details are considered as best practice for the use case; **AND** • All used cryptographic details are not known to be vulnerable to a feasible attack. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
Applicable	Applicable	Applicable	Applicable	Applicable
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset

Based on IXIT 13-SoftServ, reference 5.1-3-1.

This test, passes.

6.8.2.7 Provision 5.5-7

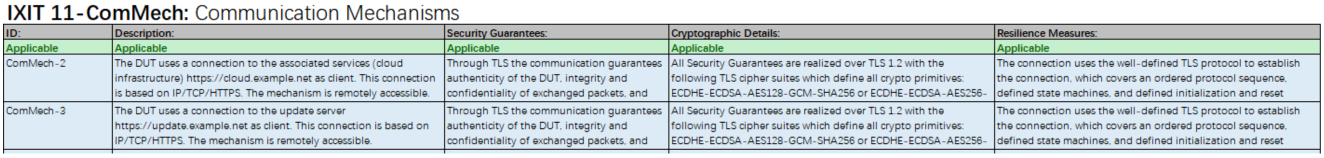
MC(19): The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.

TC_COMMUNICATE_SECURELY_#12 / Test Case 5.5-7-1	
Security requirement	PROVISION 5.5-7
Type of work	Doc
Applicability	Conditional (critical security parameters are transmitted via remotely accessible network interfaces)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the cryptography used for communicating critical security parameters via remotely accessible network interfaces.
Evaluation inputs	- List of critical security parameters (**IXIT 10-SecParam**) - List of communication mechanisms **(IXIT 11-ComMech**)
Documentation analysis procedure	a) For all **"Communication Mechanisms",** that are remotely accessible according to their **"Description"** in **IXIT 11- ComMech** referenced in any critical security parameter in **IXIT 10-SecParam,** tester shall apply all test units as specified in the **Test case 5.5-1-1** with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.
Verdict	The verdict **PASS** is assigned if for all communication mechanisms used for communicating critical security parameters via remotely accessible network interfaces: • The security guarantees are appropriate for the use case of secure communication; **AND** • The mechanism is appropriate to achieve the security guarantees with respect to the use case; **AND** • All used cryptographic details are considered as best practice for the use case; **AND** • All used cryptographic details are not known to be vulnerable to a feasible attack. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
Applicable	Applicable	Applicable	Applicable	Applicable
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset

Based on IXIT 13-SoftServ, reference 5.1-3-1.

This test, passes.

TC_COMMUNICATE_SECURELY_#13 / Test Case 5.5-7-2	
Security requirement	PROVISION 5.5-7
Type of work	Test CAB
Applicability	Conditional (critical security parameters are transmitted via remotely accessible network interfaces)
Test objectives	The purpose of this test case is the functional assessment of the cryptography used for communicating critical security parameters via remotely accessible network interfaces**.**
Evaluation inputs	- At least one device suitable for testing - List of “**Communications Mechanisms”** from **IXIT 11-ComMech** - List of critical security parameters **(IXIT 10-SecParam**)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) For all **"Communication Mechanisms",** that are remotely accessible according to their "**Description"** in **IXIT 11- ComMech** referenced in any critical security parameter in **IXIT 10-SecParam**, Tester shall apply all test units as specified in the **Test case 5.5-1-2.** **Expected result:** ✓ implementation results that cryptographic settings used for communicating critical security parameters via remotely accessible network interfaces are to those declared by manufacturer in IXIT
Verdict	The verdict PASS is assigned if: - There is no indication that any used cryptographic setting differs from its IXIT documentation. The verdict FAIL is assigned otherwise.

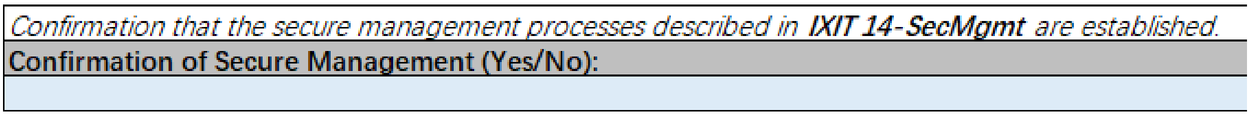
Test Result
PASS
Testlab Comments
Based on the description provided by IXIT, the tester has tested and determined that the documentation is met. This test, passed.

6.8.2.8 Provision 5.5-8

MC(20): The manufacturer shall follow secure management processes for critical security parameters that relate to the device.

TC_COMMUNICATE_SECURELY_#14 / Test Case 5.5-8-1	
Security requirement	PROVISION 5.5-8
Type of work	Doc
Applicability	Conditional (critical security parameters relating to the device exist)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the secure management processes concerning the coverage of the parameter life cycles (a) and the confirmation that the preconditions for the implementation are ensured (b).
Evaluation inputs	- **"Processes"** in IXIT **14-SecMgmt** - **"Confirmation of Secure Management"** in **IXIT 4-Conf**
Documentation analysis procedure	a) The Tester assess whether the secure management of critical security parameters covers the whole life cycle of an critical security parameter considering its: • - generation; **AND** • - provisioning; **AND** • - storage; **AND** • - updates; **AND** • - decommissioning, archival, and destruction; **AND** • - processes to handle the expiration and compromise according to the processes in **IXIT 14-SecMgmt.** b) Tester check whether **"Confirmation of Secure Management"** in **IXIT 4-Conf** states a confirmation.
Verdict	The verdict PASS is assigned if: • The secure management covers the whole life cycle of a critical security parameter according to its processes; and • A confirmation for the implementation is given. The verdict FAIL is assigned otherwise.

Test Result
FAIL
Testlab Comments



*Confirmation that the secure management processes described in **IXIT 14-SecMgmt** are established.*

Confirmation of Secure Management (Yes/No):

Based on Confirmation of Secure Management in IXIT 4-Conf, the manufacturer did not provide the information. This test, fails.

6.9 Minimize exposed attack surfaces

6.9.1 IXIT data

IXIT 4-Conf: Confirmations

The completed IXIT lists confirmations for the establishment of processes. The pro forma contains the following entries, which are independent from each other, and is typically filled out in form of a list.

Confirmation of Secure Development (Yes/No):	Confirmation that the secure development processes described in **IXIT 19-SecDev** are established.

IXIT 15-Intf: Interfaces

The completed IXIT lists all network, physical and logical interfaces of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the interface, including its purpose. For physical interfaces, it is described additionally whether the interface is always required, never required or required only in specific cases (e.g. intermittently usage), which are briefly described then.
Type:	Indication whether the interface is network, physical (includes also air interfaces), logical or several types.
Status:	Indication whether the interface is enabled or disabled in the initialized state. For enabled interfaces a justification is given.
Disclosed Information:	If the interface is a network interface: Description of the information disclosed without authentication in the initialized state and the reason for the disclosure. It is indicated additionally whether the information is security-relevant.
Debug Interface:	If the interface is a physical interface: Indication whether the interface can be used as debug interface.
Protection:	If the interface is a physical interface: Description of the protection methods necessary to limit exposure of the interface.

IXIT 13-SoftServ: Software Services

This completed IXIT lists all software services of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the service, including its purpose. It is indicated additionally whether the service is accessible via network interface and whether this is the case in the initialized state.
Status:	Indication whether the service is enabled or disabled in the initialized state.
Justification:	If the service is enabled: Justification why the service is necessary for the intended use or operation of the DUT.

IXIT 16-CodeMin: Code Minimization

The completed IXIT lists all methods for minimizing code. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

Description:	Brief description of the method used to minimize code to the necessary functionality.

IXIT 17-PrivlCtrl: Privilege Control

The completed IXIT lists all privilege control mechanisms. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the mechanism to control privileges of software on the DUT.

IXIT 18-AccCtrl: Access Control

The completed IXIT lists all access control mechanisms for memory on hardware-level. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the hardware-level access control mechanism. It is described additionally how it is supported by the operating system of the DUT.

IXIT 19-SecDev: Secure Development Processes

The completed IXIT lists all secure development processes implemented by the SO for the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the secure development process. If an existing standard is used, a reference to the corresponding standard is provided.

6.9.2 Evaluation tasks

6.9.2.1 Provision 5.6-1

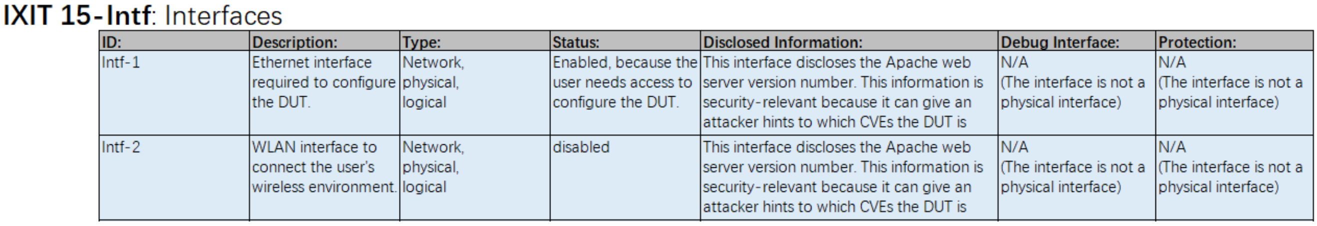
M: All unused network and logical interfaces shall be disabled

TC_ATTACK_SURFACE#1 / Test Case 5.6-1-1	
Security requirement	PROVISION 5.6-1
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the network and logical interfaces of the DUT.
Evaluation inputs	Each network and logical interface in **IXIT 15-Intf**
Documentation analysis procedure	a) For each network and logical interface in **IXIT 15-Intf** that is described as enabled according to **"Status",** the tester shall assess whether the purpose of the interface in "Description" provides a valid justification for being enabled.
Verdict	The verdict **PASS** is assigned if: • For every network or logical interface that is marked as enabled in the IXIT documentation, there is a purpose that provides a valid justification for the interface to be enabled. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 15-Intf: Interfaces

ID:	Description:	Type:	Status:	Disclosed Information:	Debug Interface:	Protection:
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)

Based on IXIT 15-Intf, the tester reviewed the interface documentation to test against the application and all application interfaces were documented in the interface documentation and there were no undisclosed or unused interfaces. The equipment was tested and the hardware interfaces were all in use.

This test, passed.

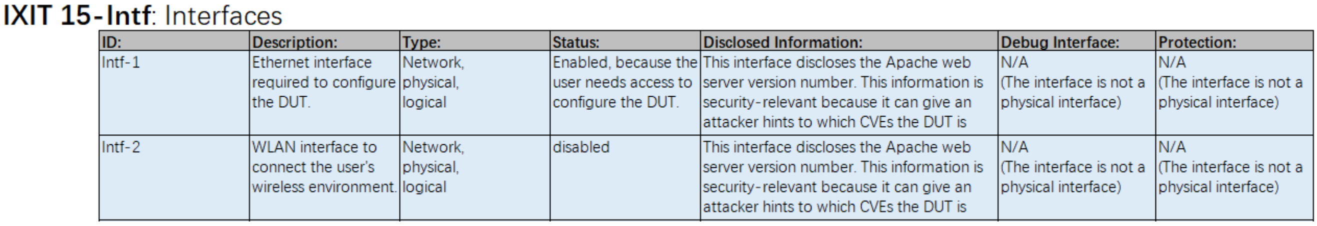
TC_ATTACK_SURFACE#2 / Test Case 5.6-1-2

Security requirement	PROVISION 5.6-1
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the network and logical interfaces of the DUT (a) and the completeness of the IXIT documentation.
Evaluation inputs	Each network and logical interface in **IXIT 15-Intf**
Test scenario	a) For each network and logical interface in **IXIT 15-Intf**, the tester shall functionally check whether the status of the interface matches the **"Status"** in the IXIT documentation. b) The tester shall functionally assess whether network or logical interfaces that are not documented in **IXIT 15-Intf** are available via a network interface on the DUT.
Verdict	The verdict PASS is assigned if: • Every documented network or logical interface that is marked as disabled in the IXIT documentation is found to be disabled or not accessible on the DUT **AND** • Every discovered network and logical interface is documented in the IXIT. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 15-Intf: Interfaces

ID:	Description:	Type:	Status:	Disclosed Information:	Debug Interface:	Protection:
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)

Based on IXIT 15-Intf, the tester reviewed the interface documentation to test against the application and all application interfaces were documented in the interface documentation and there were no undisclosed or unused interfaces. The equipment was tested and the hardware interfaces were all in use.

This test, passed.

6.9.2.2 Provision 5.6-2

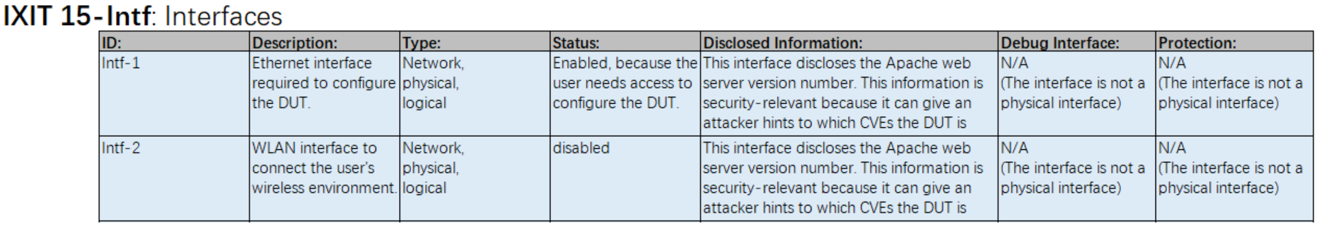
__M:__ In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security relevant information

TC_ATTACK_SURFACE#3 / Test Case 5.6-2-1	
Security requirement	PROVISION 5.6-2
Type of work	IXIT analysis
Applicability	Always
Test objectives	The purpose of this test case is the conceptual assessment of the information disclosed by network interfaces without authentication in the initialized state.
Evaluation inputs	Each network and logical interface in **IXIT 15-Intf**
Test procedure	a) For each network interface in **IXIT 15-Intf**, the tester shall assess whether the **"Disclosed Information"** disclosed by the interface without authentication in the initialized state and indicated as not security-relevant, is however security relevant. b) For each network interface in **IXIT 15-Intf**, the tester shall assess whether the **"Disclosed Information"** disclosed by the interface without authentication in the initialized state and indicated as security-relevant, is necessary for the operation of the DUT.
Verdict	The verdict **PASS** is assigned if for every network interface: • Every security-relevant information disclosed by the interface without authentication in the initialized state is documented as such **AND** • All security-relevant information disclosed by the interface without authentication in the initialized state is necessary for the operation of the DUT. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 15-Intf: Interfaces

ID:	Description:	Type:	Status:	Disclosed Information:	Debug Interface:	Protection:
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)

Based on the evaluation of the Disclosed Information description in IXIT 15-Intf, testers viewed the interface documentation to test the application, and all application interfaces were documented in the interface documentation; there were no undisclosed or unused interfaces.

Interfaces use security protocols for transmission, return information, non-essential not to return, sensitive parameters to do anonymization operations.

This test, passed.

TC_ATTACK_SURFACE#4 / Test case 5.6-2-2	
Security requirement	PROVISION 5.6-2
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the information disclosed by the network interfaces without authentication in the initialized state.
Evaluation inputs	Each network and logical interface in **IXIT 15-Intf**
Test procedure	a) For each network interface in **IXIT 15-Intf**, the tester shall functionally assess whether security-relevant information can be observed from the interface without authentication in the initialized state, that is not described in **"Disclosed Information"**.
Verdict	The verdict **PASS** is assigned if: • For every network interface, only security-relevant information can be observed that is described in the IXIT documentation. The verdict **FAIL** is assigned otherwise.

Test Result
PASS

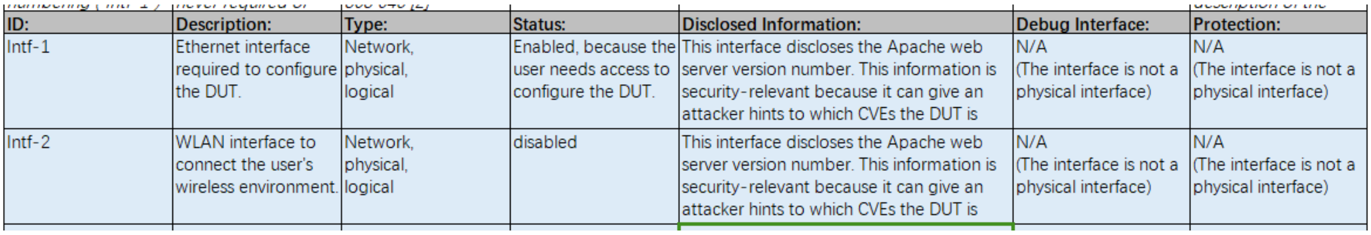
Testlab Comments
Based on the relevant information provided in IXIT 15-Intf, the tester tested the interface and it conforms to the description. This test passed.

6.9.2.3 Provision 5.6-3

R: Device hardware should not unnecessarily expose physical interfaces to attack

TC_ATTACK_SURFACE#5 / Test case 5.6-3-1	
Security requirement	PROVISION 5.6-3
Type of work	IXIT analysis
Applicability	Always
Test objectives	The purpose of this test case is the conceptual assessment of the physical interfaces of the DUT concerning interfaces that do not require exposure in general and interfaces that do not require permanent exposure.
Evaluation inputs	Each physical interface in **IXIT 15-Intf**
Test procedure	a) For each physical interface in **IXIT 15-Intf** that does not require exposure according to "Description", the TL shall assess whether the protection means of the interface in "Protection" include protection by the device casing or similar measures. *NOTE: For air interfaces it is acceptable that the antenna part remains outside of the device casing.* b) For each air interface in **IXIT 15-Intf** that does not require exposure according to **"Description",** tester shall check whether the interface is disabled according to "Status". c) For each physical interface in **IXIT 15-Intf** that does not require permanent exposure according to "Description", tester shall check whether the interface is disabled according to **"Status"** for all periods in which the use of the interface is not required.
Verdict	The verdict **PASS** is assigned if: - For every physical interface that does not require exposure, the protection means of the interface includes protection by the device casing or similar measures; **AND** - For every air interface that does not require exposure, the interface is disabled; **AND** - For every physical interface that does not require permanent exposure, the interface is disabled for all periods in which the use of the interface is not required. The verdict **FAIL** is assigned otherwise.

Test Result
PASS
Testlab Comments



ID:	Description:	Type:	Status:	Disclosed Information:	Debug Interface:	Protection:
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)

According to the IXIT documentation provided by the manufacturer, the WLAN interface was the only enabled interface, and no physical interfaces were used on the DUT. The "Intf-1" is the required air interface and it will be enabled. Therefore, it is determined that the requirement passes.

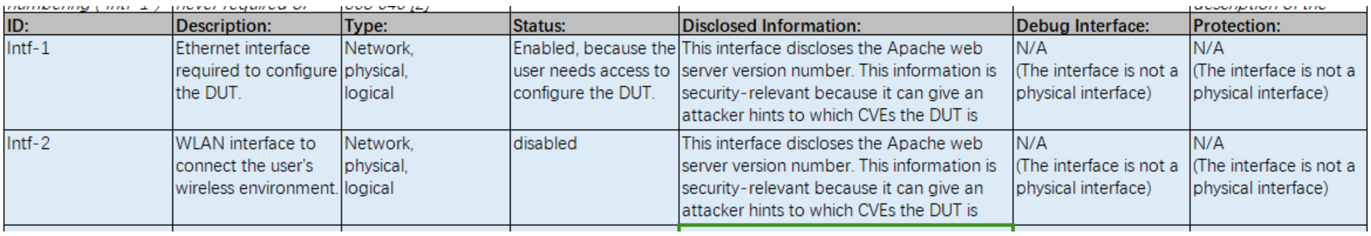
TC_ATTACK_SURFACE#6 / Test Case 5.6-3-2

Security requirement	PROVISION 5.6-3
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the physical interfaces of the DUT and the completeness of the IXIT documentation.
Evaluation inputs	Each physical interface in **IXIT 15-Intf**
Test procedure	a) For each physical interface identified on the DUT, tester shall functionally check whether exposed physical interfaces on the DUT are contained in **IXIT 15-Intf** and described as required or intermittently required in **"Description".** b) For each physical interface identified on the DUT that does not require exposure according to **"Description",** tester shall functionally assess whether physical interfaces on the DUT are protected by device casing or similar measures. ***NOTE:*** *For air interfaces it is acceptable that the antenna part remains outside of the device casing.* c) For each air interface identified on the DUT, tester shall functionally check whether it is enabled or disabled as indicated in **"Status"** in **IXIT 15-Intf.** d) For each physical interface identified on the DUT Tester shall functionally assess whether the physical interfaces that are not permanently required are disabled for all periods in which the use of the interface is not required.
Verdict	The verdict **PASS** is assigned if: - All exposed physical interfaces on the DUT are described as "required" or "intermittently required" in the IXIT documentation; **AND** - All physical interfaces that are identified as never requiring exposure in the IXIT documentation, the interface is protected by the device casing or similar measures; **AND** - All air interfaces that are enabled on the DUT are marked as "required" or "intermittently required" in the IXIT documentation; **AND** - for all physical interfaces that are marked as "intermittently required" in the IXIT documentation, the interface is disabled for all periods in which the use of the interface is not required. The verdict **FAIL** is assigned otherwise.

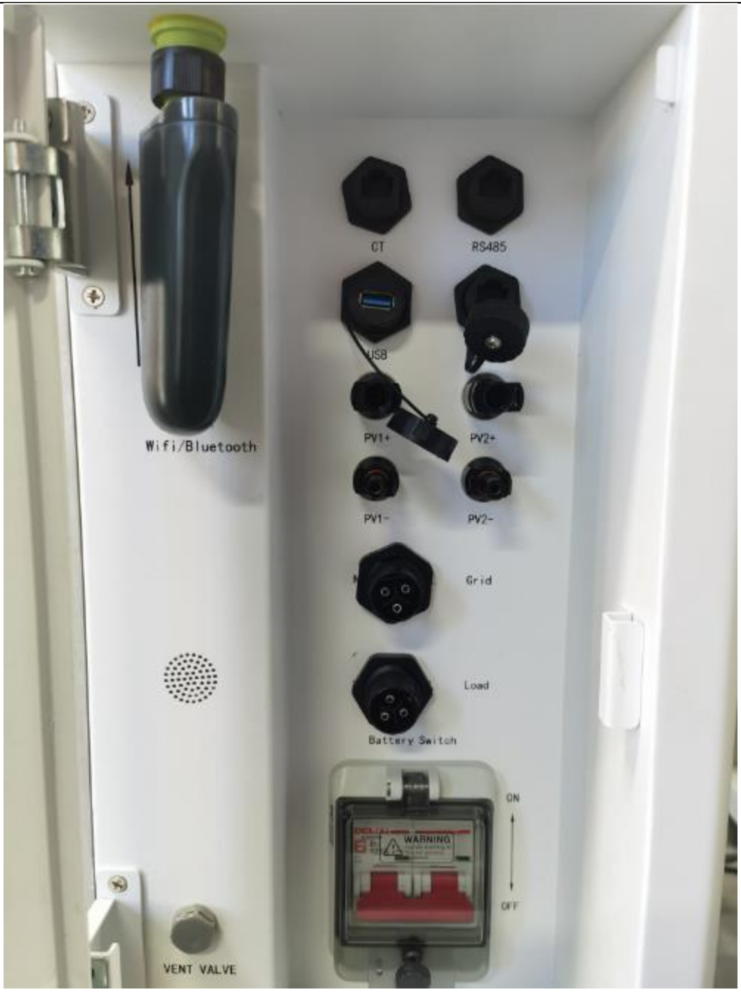
Test Result

PASS

Testlab Comments



ID:	Description:	Type:	Status:	Disclosed Information:	Debug Interface:	Protection:
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)



Testers tested the device, which is protected by covers for each of the physical interfaces when they are not enabled, and the overall exterior is protected by a security latch.

This test, passed.

6.9.2.4 Provision 5.6-4

<u>**M C (13):**</u> Where a debug interface is physically accessible, it shall be disabled in software

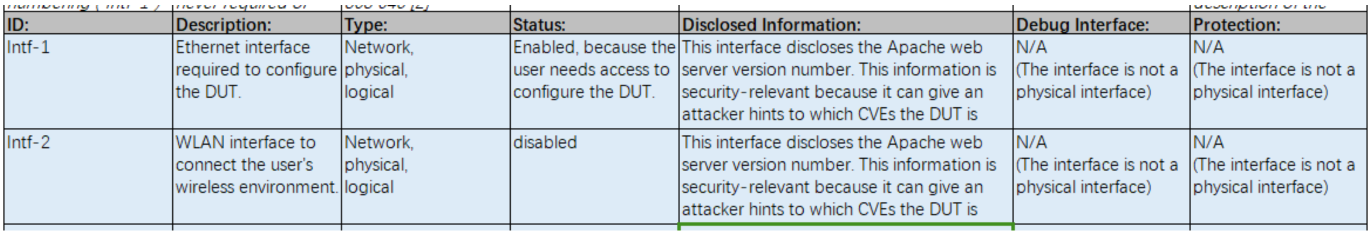
TC_ATTACK_SURFACE#7 / Test Case 5.6-4-1

Security requirement	PROVISION 5.6-4
Type of work	IXIT analysis
Applicability	Conditional (a debug interface is physically accessible)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of physically accessible debug interfaces of the DUT.
Evaluation inputs	Each physical interface in **IXIT 15-Intf**
Documentation analysis procedure	a) For each physical interface in **IXIT 15-Intf** that is described as an accessible debug interface according to **"Debug Interface",** the tester **shall** assess whether the protection means for the interface in "Protection" include a software mechanism to disable the interface. b) For each physical interface in **IXIT 15-Intf** that is described as an accessible debug interface, that is not indicated as intermittently required according to **"Description",** the tester **shall** check whether the interface is disabled permanently according to **"Status".** c) For each physical interface in **IXIT 15-Intf** that is described as an accessible debug interface, that is indicated as intermittently required according to **"Description",** the tester **shall** check whether the interface is disabled by default according to **"Status".**
Verdict	The verdict **PASS** is assigned if: • For every accessible physical debug interface, there is an software mechanism described to disable the interface **AND** • For every accessible physical debug interface that is not indicated as intermittently required, the interface is permanently disabled **AND** • For every accessible physical debug interface that is indicated as intermittently required, the interface is disabled by default. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



ID:	Description:	Type:	Status:	Disclosed Information:	Debug Interface:	Protection:
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)

The tester viewed according to intf-1 and intf-2 in IXIT 15-Intf that the Ethernet interface is enabled and the WLAN interface is disabled.

The actual test result, the device can connect to the network only in intf-1 mode, and the test result is consistent with the document description.

This test passed.

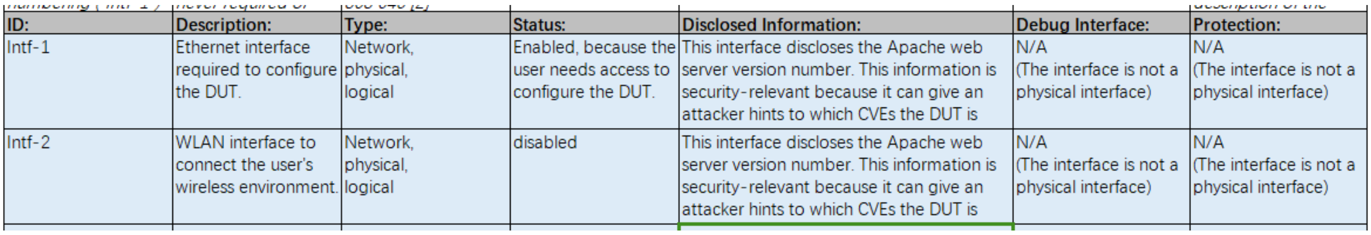
TC_ATTACK_SURFACE#8 / Test Case 5.6-4-2

Security requirement	PROVISION 5.6-4
Type of work	Test CAB
Applicability	Always
Test analysis objectives	The purpose of this test case is the functional assessment of physically accessible debug interfaces of the DUT and the completeness of the IXIT documentation
Evaluation inputs	Each accessible physical interface in **IXIT 15-Intf**
Test analysis procedure	a) For each accessible physical interface on the DUT indicated as "**Debug Interface**" **in IXIT 15-Intf,** the Tester **shall** functionally check whether the interface is disabled. b) For each accessible physical interface on the DUT the Tester **shall** functionally assess whether the interface can be used for debugging purposes although it is not indicated as "**Debug Interface**" in **IXIT 15-Intf**.
Verdict	The verdict **PASS** is assigned if: - Every accessible physical debug interface is disabled; and - Every physical debug interface is indicated as such in the IXIT. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



ID:	Description:	Type:	Status:	Disclosed Information:	Debug Interface:	Protection:
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is	N/A (The interface is not a physical interface)	N/A (The interface is not a physical interface)

The tester viewed according to intf-1 and intf-2 in IXIT 15-Intf that the Ethernet interface is enabled and the WLAN interface is disabled.

The actual test result, the device can connect to the network only in intf-1 mode, and the test result is consistent with the document description.

This test passed.

6.9.2.5 Provision 5.6-5

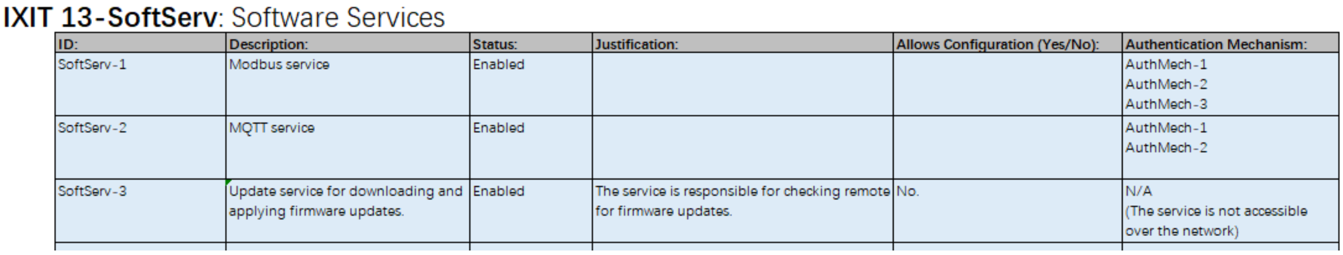
R: The manufacturer should only enable software services that are used or required for the intended use or operation of the device

TC_ATTACK_SURFACE#9 / Test Case 5.6-5-1	
Security requirement	PROVISION 5.6-5
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the enabled services concerning the intended use or operation of the DUT.
Evaluation inputs	Each software service in **IXIT 13-SoftServ**
Documentation analysis procedure	For each software service in **IXIT 13-SoftServ** that is enabled by default according to **"Status",** the tester **shall** assess whether the service is necessary for the intended use or operation of the DUT according to the purpose in **"Description"** and the **"Justification"** for enabling the service.
Verdict	The verdict PASS is assigned if: • for every enabled by default software service, the service is necessary for the intended use or operation of the DUT. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 13-SoftServ: Software Services

ID:	Description:	Status:	Justification:	Allows Configuration (Yes/No):	Authentication Mechanism:
SoftServ-1	Modbus service	Enabled			AuthMech-1 AuthMech-2 AuthMech-3
SoftServ-2	MQTT service	Enabled			AuthMech-1 AuthMech-2
SoftServ-3	Update service for downloading and applying firmware updates.	Enabled	The service is responsible for checking remote for firmware updates.	No.	N/A (The service is not accessible over the network)

Based on the information provided by the manufacturer in IXIT 13-SoftServ, after reviewing the content in the "Justification" field, the tester determined that each service is deemed necessary. Therefore, this test case is deemed to pass.

6.9.2.6 Provision 5.6-6

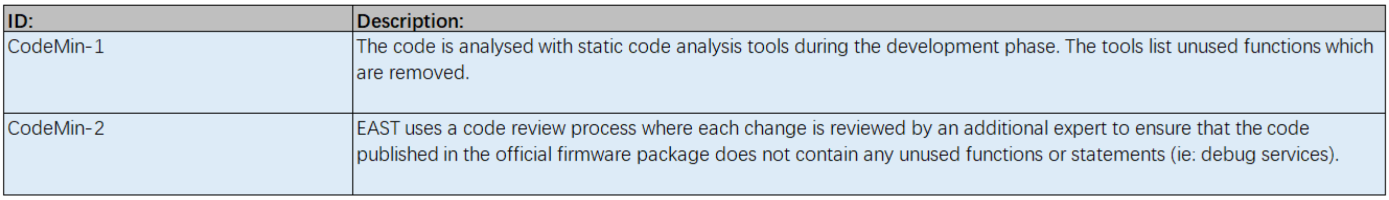
R: Code should be minimized to the functionality necessary for the service/device to operate

TC_ATTACK_SURFACE#10 / Test Case 5.6-6-1	
Security requirement	PROVISION 5.6-6
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the code minimization techniques.
Evaluation inputs	**IXIT 16-CodeMin**
Documentation analysis procedure	The tester **shall** assess whether the code minimization techniques in **IXIT 16-CodeMin** are appropriate for reducing code to the necessary functionality.
Verdict	The verdict **PASS** is assigned if: • The described code minimization techniques are appropriate for reducing code to the necessary functionality. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



ID:	Description:
CodeMin-1	The code is analysed with static code analysis tools during the development phase. The tools list unused functions which are removed.
CodeMin-2	EAST uses a code review process where each change is reviewed by an additional expert to ensure that the code published in the official firmware package does not contain any unused functions or statements (ie: debug services).

Based on the information provided by the manufacturer in IXIT 16-CodeMin, the tester reviewed and determined that the technologies used adhere to the principle of code minimization. Therefore, this test case is deemed to pass.

6.9.2.7 Provision 5.6-7

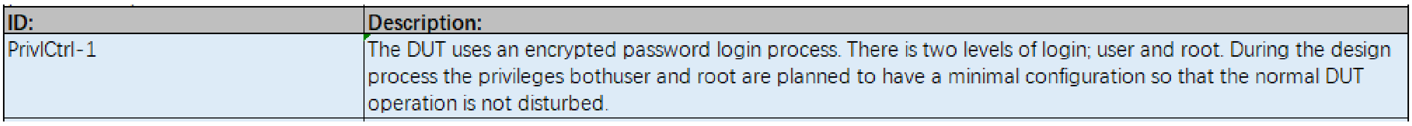
R: Software should run with least necessary privileges, taking account of both security and functionality

TC_ATTACK_SURFACE#11 / Test Case 5.6-7-1	
Security requirement	PROVISION 5.6-7
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the privilege control mechanisms of the DUT.
Evaluation inputs	**IXIT 17-PrivlCtrl**
Documentation analysis procedure	a) The tester **shall** assess whether all mechanisms to control privileges of software on the DUT in **IXIT 17-PrivlCtrl** together facilitate the principles of separation of duty, need to know and minimization of privilege.
Verdict	The verdict **PASS** is assigned if: • The described privilege control mechanisms are adequate to facilitate the principles of separation of duty, need to know and minimization of privilege. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



ID:	Description:
PrivlCtrl-1	The DUT uses an encrypted password login process. There is two levels of login; user and root. During the design process the privileges bothuser and root are planned to have a minimal configuration so that the normal DUT operation is not disturbed.

Based on the information provided by the manufacturer in IXIT 17-PrivlCtrl, the tester reviewed and determined that the role-based access control division used adheres to the principle of minimize privilege design. Therefore, this test case is deemed to pass.

6.9.2.8 Provision 5.6-8

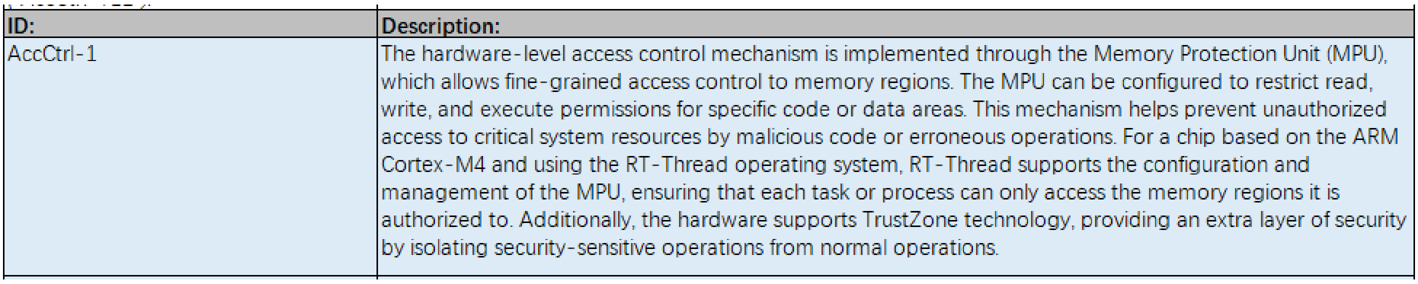
R: The device should include a hardware-level access control mechanism for memory

TC_ATTACK_SURFACE#12 / Test Case 5.6-8-1	
Security requirement	PROVISION 5.6-8
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptional assessment of the hardware-level mechanisms for access control to memory of the DUT.
Evaluation inputs	**IXIT 18-AccCtrl**
Documentation analysis procedure	a) For each hardware-level access control mechanism for memory **in IXIT 18-AccCtrl**, the tester **shall** assess whether the mechanism is implemented at the level of the hardware. b) For each hardware-level access control mechanism for memory in **IXIT 18-AccCtrl**, the tester **shall** assess whether the mechanism allows to control access to memory.
Verdict	The verdict **PASS** is assigned if: • For every hardware-level access control mechanism for memory, the mechanism is implemented at the level of the hardware AND • For every hardware-level access control mechanism for memory, the mechanism allows to control access to memory. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



ID:	Description:
AccCtrl-1	The hardware-level access control mechanism is implemented through the Memory Protection Unit (MPU), which allows fine-grained access control to memory regions. The MPU can be configured to restrict read, write, and execute permissions for specific code or data areas. This mechanism helps prevent unauthorized access to critical system resources by malicious code or erroneous operations. For a chip based on the ARM Cortex-M4 and using the RT-Thread operating system, RT-Thread supports the configuration and management of the MPU, ensuring that each task or process can only access the memory regions it is authorized to. Additionally, the hardware supports TrustZone technology, providing an extra layer of security by isolating security-sensitive operations from normal operations.

Based on the review of the IXIT 18-AccCtrl information, it has been confirmed that the hardware-level memory access control mechanisms used are implemented at the hardware level and allow control over memory access. Therefore, this test case is deemed to pass.

6.9.2.9 Provision 5.6-9

R: The manufacturer should follow secure development processes for software deployed on the device

TC_ATTACK_SURFACE#13 / Test Case 5.6-9-1	
Security requirement	PROVISION 5.6-9
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the secure development processes and the confirmation that the preconditions for the implementation are ensured.
Evaluation inputs	**IXIT 19-SecDev** and **"Confirmation of Secure Development"** in **IXIT 4-Conf**
Documentation analysis procedure	The tester **shall** assess whether the secure development of software covers: • Security training of developers • The requirement and design phases of the software • Secure coding techniques • Security tooling for the implementation phase • Security testing • Security review • Archival of assets and information relevant to maintaining security of the software • Secure deployment • Handling of third-party software providers.according to the processes in **IXIT 19-SecDev.** The tester **shall** check whether **"Confirmation of Secure Development"** in **IXIT 4-Conf states** a confirmation.
Verdict	The verdict **PASS** is assigned if the secure development covers: • Security training of developers **AND** • The requirement and design phases of the software **AND** • Secure coding techniques **AND** • Security tolling for the implementation phase **AND** • Security testing **AND** • Security reviews **AND** • Archival of assets and information relevant to maintaining security of the software **AND** • Secure deployment **AND** • If applicable, handling of third-party software providers **AND** • A confirmation for the implementation is given. The verdict **FAIL** is assigned otherwise.
Test Result	
FAIL	
Testlab Comments	
Based on IXIT 4-Conf and IXIT 19-SecDev, the tester found no description of “Secure Development”. The test failed.	

6.10 Ensure software integrity

6.10.1 IXIT Data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 20-SecBoot: Secure Boot Mechanisms

The completed IXIT lists all secure boot mechanisms of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the mechanism (including trust assumptions) used for the secure boot process of the DUT and the part of the software that is protected.
Security Guarantees:	Description of the realized security objectives of the mechanism.
Detection Mechanisms:	Description of the mechanism detecting an unauthorized change in the software of the DUT.
User Notification:	Brief description of how the user is informed about an unauthorized change in the software. It is indicated additionally which information are contained in the notification. **Note**: *Email address of a user account, communication endpoint (e.g. network address or link address) of a user device (e.g. smart phone, smart watch) or status LED are possible ways to inform the user.*
Notification Functionality:	Brief description of the network functionalities necessary to notify a user.

6.10.2 Evaluation tasks

6.10.2.1 Provision 5.7-1

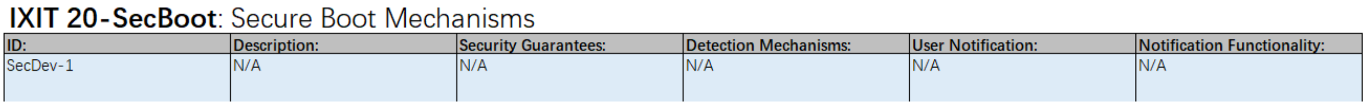
R: The consumer IoT device should verify its software using secure boot mechanisms.

TC_SOFTWARE_INTEGRITY#1 / Test Case 5.7-1-1	
Security requirement	PROVISION 5.7-1
Type of work	IXI Analysis
Applicability	Always
Documentation analysis objectives	Verify that the device implements a secure boot
Evaluation inputs	- Collected secure boot mechanism from **IXIT 20-SecBoot**
Documentation analysis procedure	a) Tester assess whether the **Security Guarantees** of each secure boot mechanism in **IXIT 20-SecBoot** provide at least verification of integrity and authenticity of device software. b) Tester assess whether for each secure boot mechanism in **IXIT 20-SecBoot** the **Description** and corresponding **Detection Mechanisms** are suitable to provide the **Security Guarantees** it is used.
Verdict	The verdict **PASS** is assigned if: - Every secure boot mechanism provides the security guarantees of integrity and authenticity of the device software; **AND** - Every secure boot mechanism and its detection mechanisms is suitable to provide the described security guarantee. The verdict **FAIL** is assigned otherwise.

Test Result

N/A

Testlab Comments



IXIT 20-SecBoot: Secure Boot Mechanisms

ID:	Description:	Security Guarantees:	Detection Mechanisms:	User Notification:	Notification Functionality:
SecDev-1	N/A	N/A	N/A	N/A	N/A

Based on the information provided by the vendor in IXIT 20-SecBoot, it is noted that the DUT does not have the Secure Boot mechanism. Therefore, this test case is deemed not applicable.

TC_SOFTWARE_INTEGRITY#2 / Test Case 5.7-1-2	
Security requirement	PROVISION 5.7-1
Type of work	Test CAB
Applicability	Always
Test objectives	Verify that the device implements a secure boot
Evaluation inputs	- At least one device suitable for testing - Collected secure boot mechanism from **IXIT 20-SecBoot**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) Tester assess whether the verification of the device software is implemented according to the information in **IXIT 20-SecBoot**. **Expected result:** ✓ List of boot fails and successes.
Verdict	The verdict PASS is assigned if: - There is no indication, that the implementation of any secure boot mechanism differs from its IXIT documentation. The verdict FAIL is assigned otherwise.

Test Result
N/A

Testlab Comments
Based on the conceptual test items, this test item is deemed not applicable.

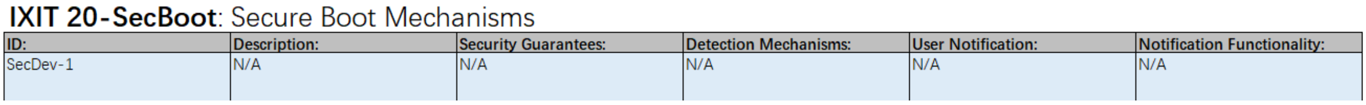
6.10.2.2 Provision 5.7-2

R: If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.

TC_SOFTWARE_INTEGRITY#3 / Test Case 5.7-2-1	
Security requirement	PROVISION 5.7.2
Type of work	IXIT Analysis
Applicability	Always
Documentation analysis objectives	Verify that the device implements mechanisms of alerts and prevents any wider networks connections in case of unauthorized changes
Evaluation inputs	- Collected secure boot mechanism from **IXIT 20-SecBoot**
Documentation analysis procedure	a) Assess whether the method for **User Notification** including its contained information is sufficient to inform the user and/or administrator about unauthorized changes in device software. b) Assess whether every **Notification Functionality** in **IXIT 20-SecBoot** is necessary for the described method of **User Notification**.
Verdict	**The verdict PASS is assigned if:** ✓ The described way of user notification is sufficient to inform the user and/or administrator about unauthorized changes in device software; **AND** ✓ Every described notification functionality is necessary for the user notification in case of detecting unauthorized software changes. **The verdict FAIL is assigned otherwise.**

Test Result
N/A

Testlab Comments



IXIT 20-SecBoot: Secure Boot Mechanisms

ID:	Description:	Security Guarantees:	Detection Mechanisms:	User Notification:	Notification Functionality:
SecDev-1	N/A	N/A	N/A	N/A	N/A

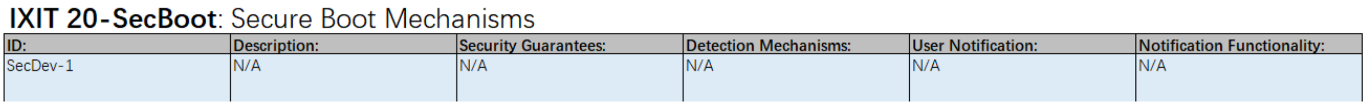
Based on the information provided by the vendor in IXIT 20-SecBoot, it is noted that the DUT does not have the Secure Boot mechanism. Therefore, this test case is deemed not applicable.

TC_SOFTWARE_INTEGRITY#4 / Test Case 5.7-2-2	
Security requirement	PROVISION 5.7-2
Type of work	Test CAB
Applicability	Access to some interfaces /tools to modify the boot
Test objectives	Verify that the device implements mechanisms of alerts and prevents any wider networks connections in case of unauthorized changes
Evaluation inputs	- At least three devices suitable for testing - Collected secure boot mechanism from **IXIT 20-SecBoot**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ Tester assess whether alerting takes place as described in **User Notification** in **IXIT 20-SecBoot** after the detection of an unauthorized change in device software. ✓ Tester assess whether the communication capabilities of the DUT to wider networks are restricted to the ones described in **Notification Functionality** in **IXIT 20-SecBoot** after the detection of an unauthorized change in device software. **Expected result:** ✓ Alert to user
Verdict	**The verdict PASS is assigned if:** - There is no indication that the implementation of any alerting mechanism of the DUT differs from its IXIT documentation; **AND** - Only communication to wider networks is detected after detection of unauthorized changes, that is described as necessary. **The verdict FAIL is assigned otherwise.**

Test Result

N/A

Testlab Comments



IXIT 20-SecBoot: Secure Boot Mechanisms

ID:	Description:	Security Guarantees:	Detection Mechanisms:	User Notification:	Notification Functionality:
SecDev-1	N/A	N/A	N/A	N/A	N/A

Based on the information provided by the vendor in IXIT 20-SecBoot, it is noted that the DUT does not have the Secure Boot mechanism. Therefore, this test case is deemed not applicable.

6.11 Ensure that personal data is secure

6.11.1 IXIT Data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 11-ComMech: Communication Mechanisms

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the communication mechanism, including its purpose and a description of the used protocol. For standardized protocols a reference is sufficient. It is indicated additionally whether the mechanism is remotely accessible **Note**: *A possible communication mechanism is the use of Bluetooth®, WiFi® or NFC for a local connection between an mobile application and the DUT.*
Security Guarantees:	Description of the realized security objectives and the threats the mechanism is protected against. **Note**: *The most common security guarantees to be considered include authentication of peers, authentication of origin, integrity protection, confidentiality protection, and anti-replay.*
Cryptographic Details:	Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the communication mechanism considering key management, and to facilitate the described **"Security Guarantees".** **Note**: *Cryptographic Details contain information such as: the protocol Z-Wave® with Security 2 Command Class v1 is used for the communication. The transferred data is authenticated encrypted with AES-128 CCM to facilitate confidentiality and integrity. The key exchange is based on an out-of-band mechanism.*
Resilience Measures:	Description of the measures to ensure that the connection establishment is performed in an orderly fashion including an expected, operational and stable state to achieve a stable connection. **Note**: *Resilience measures consider the sequence of the used protocol, the capability of the infrastructure, reset and initialization of the protocol and problems caused by mass reconnections*

IXIT 21-PersData: Personal Data

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the category of personal data processed by the DUT. ***Example:*** *Log data on the usage of the DUT, payment information, timestamped location data, audio input stream or biometric data.*
Processing Activities:	Description of how the personal data is being processed, including all involved parties. It is described additionally for what purposes the processing is done. ***Note****: Processing personal data can also include storage of such data.*
Communication Mechanisms:	Reference to communication mechanisms in **IXIT 11-ComMech** that are used for communicating the personal data and an indication whether the recipient is an associated service (Yes/No). An empty list of communication mechanisms indicates that the personal data is not transmitted.
Sensitive (Yes/No):	Indication whether the personal data is sensitive according to the definition in the provision 5.8-2 in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].
Obtaining Consent:	If the personal data is processed on the basis of consumer's consent: - Description of how the consent for the processing is obtained from the consumer.
Withdrawing Consent:	If the personal data is processed on the basis of consumer's consent: - Description of how the consumer can withdraw the consent for processing the personal data.

IXIT 2-UserInfo: User Information:

The completed IXIT lists documentations, publications and information provided to users.

Documentation of Sensors:	Description of the way the information about external sensing capabilities is documented for the user, including all information to access the documentation.

IXIT 22-ExtSens: External Sensors

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the sensing capability. ***Note:*** *Such sensing capabilities can be a microphone or camera.*

6.11.2 Evaluation tasks

6.11.2.1 Provision 5.8-1

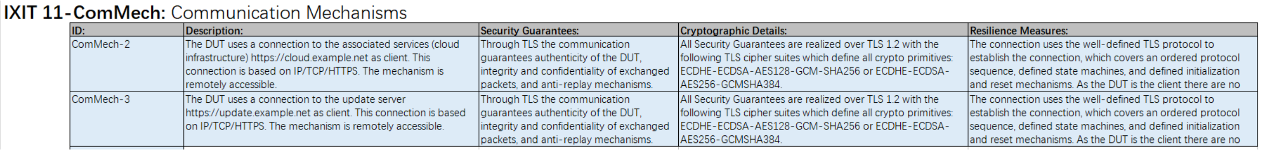
R C (21): The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.

TC_PERSONAL_DATA#1 / Test Case 5.8-1-1	
Security requirement	PROVISION 5.8-1
Type of work	Doc
Applicability	Conditional (Personal data is transmitted between a device and a service)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the cryptography used for communicating personal data between a device and a service.
Evaluation inputs	- List of communication mechanisms **(IXIT 11-ComMech**) - List of personal data (**IXIT 21-PersData**)
Documentation analysis procedure	a) For all **"Communication Mechanisms"** in **IXIT 11-ComMech** referenced in any personal data in **IXIT 21-PersData**, the thester shall apply all test units as specified in the **Test case 5.5-1-1** with restriction, that at least the security guarantee of confidentiality is required to be fulfilled. **Note**: *In this case the security guarantee "confidentiality" means confidentiality protection against unauthorized parties. This can include authenticity verification of a communication partner*.
Verdict	**The verdict PASS is assigned if for all communication mechanisms used for communicating personal data:** • The security guarantees are appropriate for the use case of communicating personal data; **AND** • The mechanism is appropriate to achieve the security guarantees with respect to the use case; **AND** • All used cryptographic details are considered as best practice for the use case; **AND** • All used cryptographic details are not known to be vulnerable to a feasible attack. **The verdict FAIL is assigned otherwise.**

Test Result

PASS

Testlab Comments



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCMSHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCMSHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no

Based on IXIT 11-ComMech and IXIT 21-PersData, the personal data involved in the DUT are user account passwords, phone numbers and email addresses.

Testers tested the relevant interfaces and used https+post to realize secure transmission, passwords were encrypted and stored using the irreversible encryption algorithm HMAC-SHA256, and the user's phone numbers and mailboxes were encrypted and stored using the AES algorithm, which realizes authentication and authentication and secure transmission.

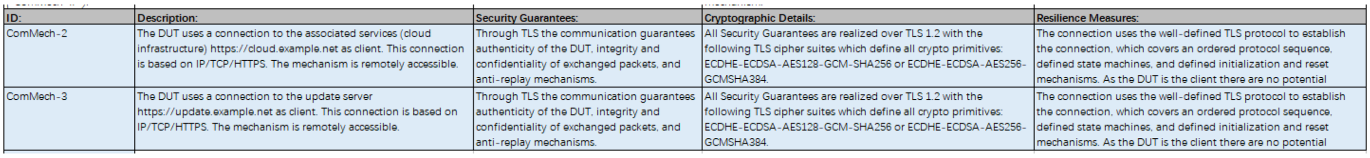
This test, passed.

TC_PERSONAL_DATA#2 / Test Case 5.8-1-2	
Security requirement	PROVISION 5.8-1
Type of work	Test CAB
Applicability	Conditional (Personal data is transmitted between a device and a service)
Test objectives	The purpose of this test case is the functional assessment of the cryptography used for communicating personal data between a device and a service.
Evaluation inputs	- At least one device suitable for testing - List of communication mechanisms **(IXIT 11-ComMech**) - List of personal data (**IXIT 21-PersData**)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ For all **"Communication Mechanisms"** in **IXIT 11-ComMech** referenced in any personal data in **IXIT 21-PersData,** tester shall apply all test units as specified in the **Test case 5.5-1-2**. **Expected result:** ✓ Secure communication on channel transmitting personal data
Verdict	**The verdict PASS is assigned if:** There is no indication that any used cryptographic setting differs from its IXIT documentation. **The verdict FAIL is assigned otherwise.**

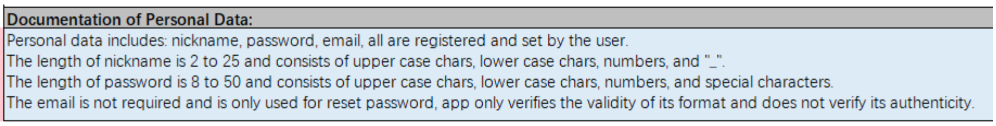
Test Result

PASS

Testlab Comments

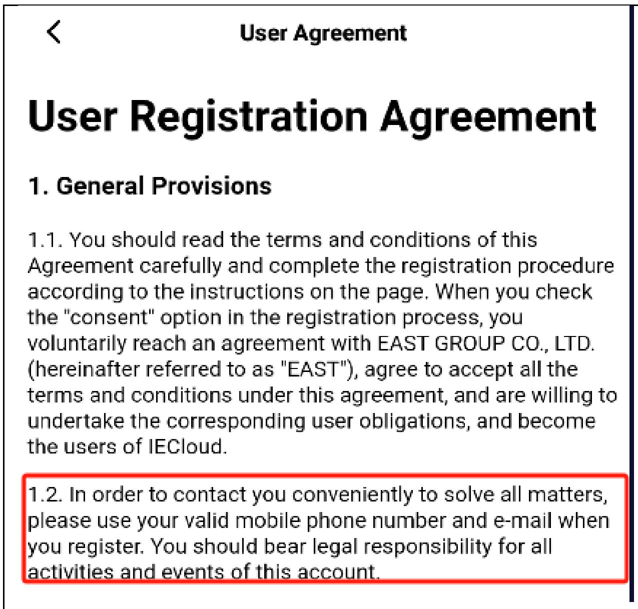


ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCMSHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no potential
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCMSHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no potential



Documentation of Personal Data:

Personal data includes: nickname, password, email, all are registered and set by the user.
The length of nickname is 2 to 25 and consists of upper case chars, lower case chars, numbers, and "_".
The length of password is 8 to 50 and consists of upper case chars, lower case chars, numbers, and special characters.
The email is not required and is only used for reset password, app only verifies the validity of its format and does not verify its authenticity.



User Agreement

User Registration Agreement

1. General Provisions

1.1. You should read the terms and conditions of this Agreement carefully and complete the registration procedure according to the instructions on the page. When you check the "consent" option in the registration process, you voluntarily reach an agreement with EAST GROUP CO., LTD. (hereinafter referred to as "EAST"), agree to accept all the terms and conditions under this agreement, and are willing to undertake the corresponding user obligations, and become the users of IECloud.

1.2. In order to contact you conveniently to solve all matters, please use your valid mobile phone number and e-mail when you register. You should bear legal responsibility for all activities and events of this account.

Based on IXIT 11-ComMech, IXIT 21-PersData, and the user manual, the tester confirmed that the personal data involved in the DUT are user account passwords, phone numbers, and email addresses.

Consistent with the documentation description.

This test, passed.

6.11.2.2 Provision 5.8-2

M C (22): The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.

Sensitive personal data definition: data whose disclosure has a high potential to cause harm to the individual
example: *video stream of a home security camera, payment information etc.*

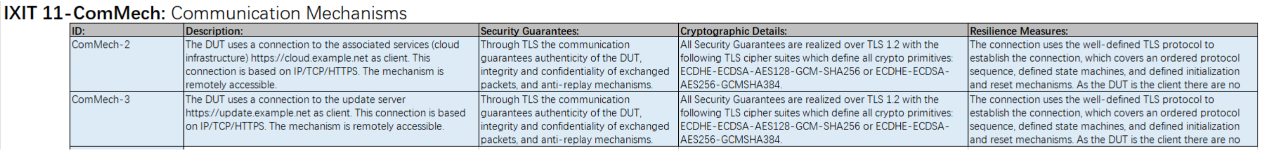
TC_PERSONAL_DATA# 3 / Test Case 5.8-2-1

Security requirement	PROVISION 5.8-2
Type of work	Doc
Applicability	Conditional (**Sensitive** personal data is transmitted between a device and a service)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the cryptography used for communicating sensitive personal data between the device and associated services.
Evaluation inputs	- List of communication mechanisms **(IXIT 11-ComMech**) - List of personal data (**IXIT 21-PersData**)
Documentation analysis procedure	a) For all **"Communication Mechanisms"** in **IXIT 11-ComMech** referenced in any sensitive personal data in **IXIT 21- Pers Data** according to **"Sensitive",** where the recipient is an associated service, Tester shall apply all test units as specified in the **Test case 5.5-1-1** with restriction, that at least the security guarantee of confidentiality is required to be fulfilled. **Note**: *In this case the security guarantee "confidentiality" means confidentiality protection against unauthorized parties. This can include authenticity verification of a communication partner.*
Verdict	**The verdict PASS is assigned if for all communication mechanisms used for communicating sensitive personal data between the device and an associated service:** • The security guarantees are appropriate for the use case of communicating sensitive personal data between the device and an associated service; **AND** • The mechanism is appropriate to achieve the security guarantees with respect to the use case; **AND** • All used cryptographic details are considered as best practice for the use case; **AND** • All used cryptographic details are not known to be vulnerable to a feasible attack. **The verdict FAIL is assigned otherwise.**

Test Result

PASS

Testlab Comments



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCMSHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCMSHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no

Based on IXIT 11-ComMech and IXIT 21-PersData, the personal data involved in the DUT are user account passwords, phone numbers and email addresses.

Testers tested the relevant interfaces and used https+post to realize secure transmission, passwords were encrypted and stored using the irreversible encryption algorithm HMAC-SHA256, and the user's phone numbers and mailboxes were encrypted and stored using the AES algorithm, which realizes authentication and authentication and secure transmission.

This test, passed.

TC_PERSONAL_DATA#4 / Test Case 5.8-2-2	
Security requirement	PROVISION 5.8-2
Type of work	Test CAB
Applicability	Conditional (**Sensitive** personal data is transmitted between a device and a service)
Test objectives	The purpose of this test case is the functional assessment of the cryptography used for communicating sensitive personal data between the device and associated services.
Evaluation inputs	- List of communication mechanisms **(IXIT 11-ComMech**) - List of personal data (**IXIT 21-PersData**)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** a) For all **"Communication Mechanisms"** in **IXIT 11-ComMech** referenced in any sensitive personal data in **IXIT 21- PersData** according to **"Sensitive",** where the recipient is an associated service, Tester shall apply all test units as specified in the **Test case 5.5-1-2.** **Expected result:** ✓ Secure communication on channel transmitting sensitive personal data
Verdict	**The verdict PASS is assigned if:** ✓ There is no indication that any used cryptographic setting differs from its IXIT documentation. **The verdict FAIL is assigned otherwise.**

Test Result
PASS

Testlab Comments
Conforms to the description in IXIT 11-ComMech and XIT 21-Pers. This test, passed.

6.11.2.3 Provision 5.8-3

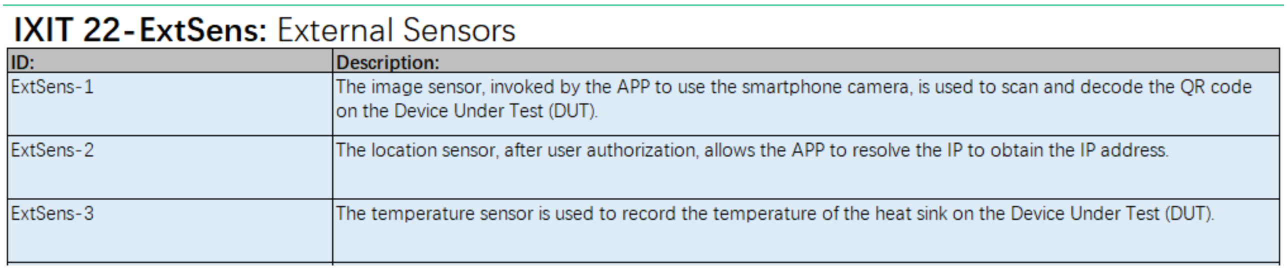
MC(23): All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.

TC_PERSONAL_DATA#5 / Test Case 5.8-3-1	
Security requirement	PROVISION 5.8-3
Type of work	Doc
Applicability	Conditional(External sensing capabilities exist)
Documentation analysis objectives	The purpose of this test case is the functional assessment of the documentation of external sensing capabilities **(a-b)** and the completeness of the IXIT documentation **(c).**
Evaluation inputs	**“Documentation of Sensors”** in **IXIT 2-UserInfo** List of external sensors **(IXIT 22-ExtSens**)
Documentation analysis procedure	a) The tester shall functionally check whether the documentation of external sensing capabilities is accessible as documented in **"Documentation of Sensors"** in **IXIT 2-UserInfo.** b) The tester shall functionally assess whether the documentation of external sensing capabilities as documented in **"Documentation of Sensors" in IXIT 2-UserInfo** is understandable for a user with limited technical knowledge (cf. ETSI EN 103 701 Annex D.3). c) The tester shall functionally assess whether all obvious sensing capabilities of the DUT are documented in **IXIT 22- ExtSens.**
Verdict	**The verdict PASS is assigned if:** • The documentation is accessible according to the IXIT; **AND** • The documentation is understandable for a user with limited technical knowledge; **AND** • Each obvious sensing capability of the DUT is documented for the user. **The verdict FAIL is assigned otherwise.**

Test Result

PASS

Testlab Comments



IXIT 22-ExtSens: External Sensors

ID:	**Description:**
ExtSens-1	The image sensor, invoked by the APP to use the smartphone camera, is used to scan and decode the QR code on the Device Under Test (DUT).
ExtSens-2	The location sensor, after user authorization, allows the APP to resolve the IP to obtain the IP address.
ExtSens-3	The temperature sensor is used to record the temperature of the heat sink on the Device Under Test (DUT).

Based on the information provided in IXIT 22- ExtSens, the device itself has the ability to sense temperature, the app has the permission to solicit location information, and the permission to solicit the camera for scanning SN numbers.

It was confirmed by the tester that it matches the description in IXIT 22-ExtSens, and that the user's consent has been solicited to use this external sensing capability.

This test, passed.

6.12 Make system resilient to outages

6.12.1 IXIT data

IXIT 23-ResMech: Resilience Mechanisms

The completed IXIT lists all resilience mechanisms for network connectivity and power outages of the DUT. The proforma contains the following entries and is typically filled in the form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Description of the mechanism that contributes to the DUT's resilience to network and/or power outages.
Purpose:	Brief description for what purpose the data is collected.
Type:	Indication whether the resilience mechanism addresses network connectivity or power outages or both.
Security Guarantees:	Description of the realised security objectives and the threats the mechanism protects against.

IXIT 11-ComMech: Communication Mechanisms

The completed IXIT lists all communication mechanisms of the DUT. The pro forma contains the following entries andis typically filled out in form of a table.

Resilience Measures:	Description of the measures to ensure that the connection establishment is performed in an orderly fashion including an expected, operational and stable state to achieve a stable connection.

6.12.2 Evaluation tasks

6.12.2.1 Provision 5.9-1

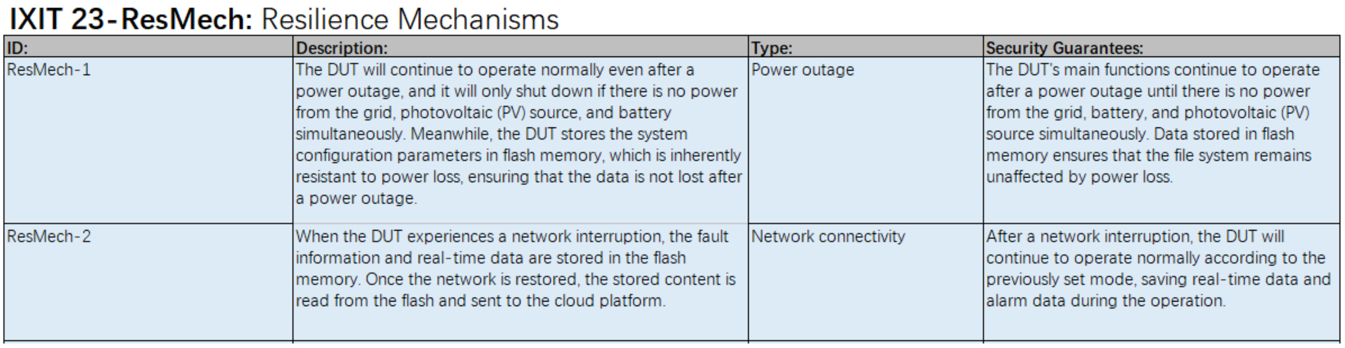
R: Resilience should be built into consumer IoT devices and services, taking into account the possibility of outages of data networks and power.

TC_RESILIENT_TO_OUTAGES#1 / Test case 5.9-1-1	
Security requirement	PROVISION 5.9-1
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the resilience mechanisms concerning outages of network and power.
Evaluation inputs	IXIT 23-ResMech
Documentation analysis procedure	a) The tester **shall** assess whether the combination of the resilience mechanisms in **IXIT 23-ResMech** are appropriate to protect against network connectivity and power outages according to the "Security Guarantees". b) For each resilience mechanism in **IXIT 23-ResMech** the tester **shall** assess whether the mechanism according to the "Description" is appropriate to achieve the **"Security Guarantees".**
Verdict	**The verdict PASS is assigned if:** • The resilience mechanisms are appropriate to protect against network connectivity and power outages **AND** • Every resilience mechanism is appropriate to achieve its security guarantees. **The verdict FAIL is assigned otherwise.**

Test Result

PASS

Testlab Comments



IXIT 23-ResMech: Resilience Mechanisms

ID:	Description:	Type:	Security Guarantees:
ResMech-1	The DUT will continue to operate normally even after a power outage, and it will only shut down if there is no power from the grid, photovoltaic (PV) source, and battery simultaneously. Meanwhile, the DUT stores the system configuration parameters in flash memory, which is inherently resistant to power loss, ensuring that the data is not lost after a power outage.	Power outage	The DUT's main functions continue to operate after a power outage until there is no power from the grid, battery, and photovoltaic (PV) source simultaneously. Data stored in flash memory ensures that the file system remains unaffected by power loss.
ResMech-2	When the DUT experiences a network interruption, the fault information and real-time data are stored in the flash memory. Once the network is restored, the stored content is read from the flash and sent to the cloud platform.	Network connectivity	After a network interruption, the DUT will continue to operate normally according to the previously set mode, saving real-time data and alarm data during the operation.

Based on IXIT 23-ResMech, it provides two resilience mechanisms in case of network and power failure.

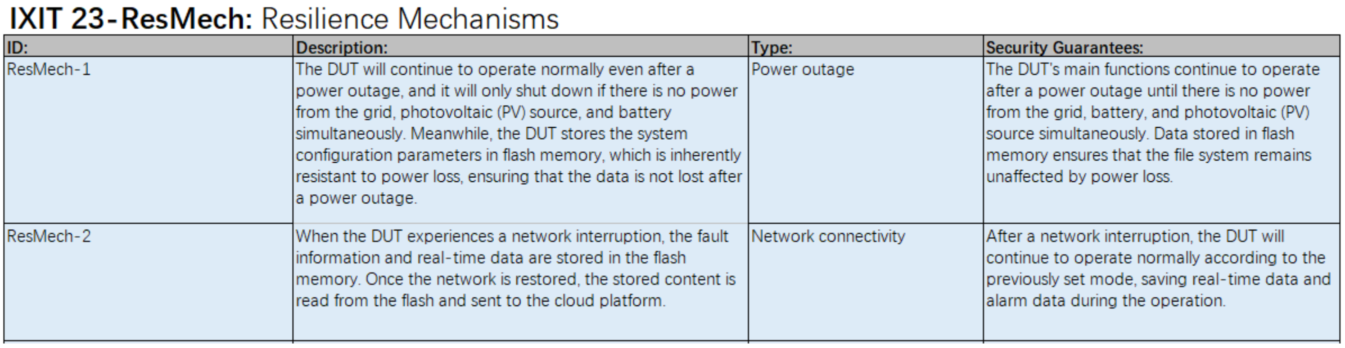
This test, passed.

TC_RESILIENT_TO_OUTAGES#2 / Test case 5.9-1-2	
Security requirement	PROVISION 5.9-1
Type of work	Test CAB
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the functional assessment of the resilience mechanisms concerning outages of network and power.
Evaluation inputs	IXIT 23-ResMech
Documentation analysis procedure	a) The tester shall interrupt the DUT's connection to the network and functionally assess whether the resilience mechanisms operate as described in **IXIT 23-ResMech**. b) The tester shall interrupt the DUT's power supply and functionally assess whether the resilience mechanisms operate as described in **IXIT 23-ResMech**.
Verdict	**The verdict PASS is assigned if:** • There is no indication that the operation of the resilience mechanisms during network connectivity and power outages differs from its IXIT documentation. **The verdict FAIL is assigned otherwise.**

Test Result

PASS

Testlab Comments



IXIT 23-ResMech: Resilience Mechanisms

ID:	Description:	Type:	Security Guarantees:
ResMech-1	The DUT will continue to operate normally even after a power outage, and it will only shut down if there is no power from the grid, photovoltaic (PV) source, and battery simultaneously. Meanwhile, the DUT stores the system configuration parameters in flash memory, which is inherently resistant to power loss, ensuring that the data is not lost after a power outage.	Power outage	The DUT's main functions continue to operate after a power outage until there is no power from the grid, battery, and photovoltaic (PV) source simultaneously. Data stored in flash memory ensures that the file system remains unaffected by power loss.
ResMech-2	When the DUT experiences a network interruption, the fault information and real-time data are stored in the flash memory. Once the network is restored, the stored content is read from the flash and sent to the cloud platform.	Network connectivity	After a network interruption, the DUT will continue to operate normally according to the previously set mode, saving real-time data and alarm data during the operation.

Based on IXIT 23-ResMech, it provides two resilience mechanisms in case of network and power failure.

This test, passed.

6.12.2.2 Provision 5.9-2

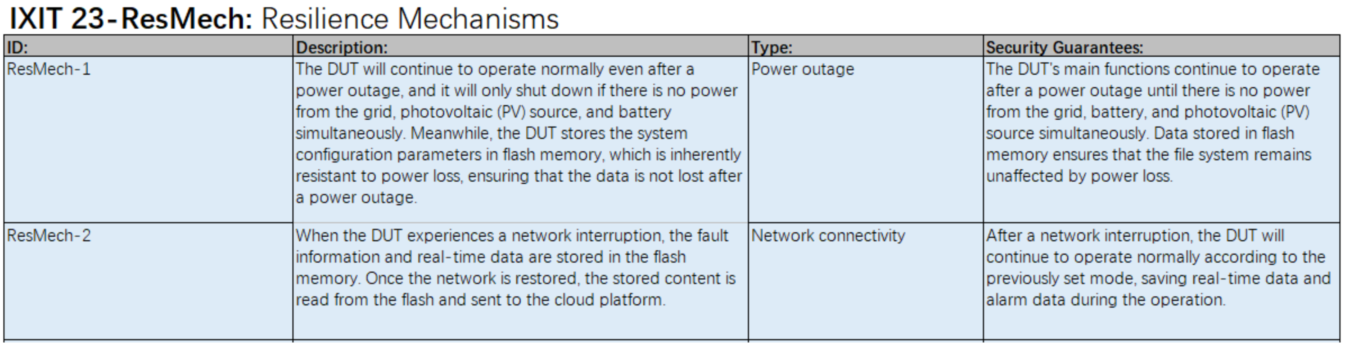
R: Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.

TC_RESILIENT_TO_OUTAGES#3 / Test case 5.9-2-1	
Security requirement	PROVISION 5.9-2
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the resilience mechanisms concerning outages of network and power and the operation during network outages and restoration after power outages.
Evaluation inputs	IXIT 23-ResMech
Documentation analysis procedure	a) The tester shall apply all test units as specified in **the Test case 5.9-1-1** for the resilience mechanisms **in IXIT 23-ResMech**. b) The tester shall assess whether the resilience mechanisms in **IXIT 23-ResMech** protecting against network connectivity outages according to **"Type"** are appropriate to ensure, that the DUT remains operating and locally functional in the case of a loss of network connectivity. c) The tester shall assess whether the resilience mechanisms in **IXIT 23-ResMech** protecting against power outages according to **"Type"** are appropriate to ensure, that the DUT resumes the connectivity and functionality after a loss of power in the same or improved state as before.
Verdict	**The verdict PASS is assigned if:** • The resilience mechanisms are appropriate to protect against network connectivity and power outages **AND** • Every resilience mechanism is appropriate to achieve its security guarantees **AND** • The resilience mechanisms are appropriate to ensure that the DUT remains operating and locally functional in the case of a loss of network connectivity **AND** • The resilience mechanisms are appropriate to ensure that the DUT recovers cleanly after a loss of power. **The verdict FAIL is assigned otherwise.**

Test Result

PASS

Testlab Comments



IXIT 23-ResMech: Resilience Mechanisms

ID:	Description:	Type:	Security Guarantees:
ResMech-1	The DUT will continue to operate normally even after a power outage, and it will only shut down if there is no power from the grid, photovoltaic (PV) source, and battery simultaneously. Meanwhile, the DUT stores the system configuration parameters in flash memory, which is inherently resistant to power loss, ensuring that the data is not lost after a power outage.	Power outage	The DUT's main functions continue to operate after a power outage until there is no power from the grid, battery, and photovoltaic (PV) source simultaneously. Data stored in flash memory ensures that the file system remains unaffected by power loss.
ResMech-2	When the DUT experiences a network interruption, the fault information and real-time data are stored in the flash memory. Once the network is restored, the stored content is read from the flash and sent to the cloud platform.	Network connectivity	After a network interruption, the DUT will continue to operate normally according to the previously set mode, saving real-time data and alarm data during the operation.

Based on IXIT 23-ResMech, it provides two resilience mechanisms in case of network and power failure.

This test, passed.

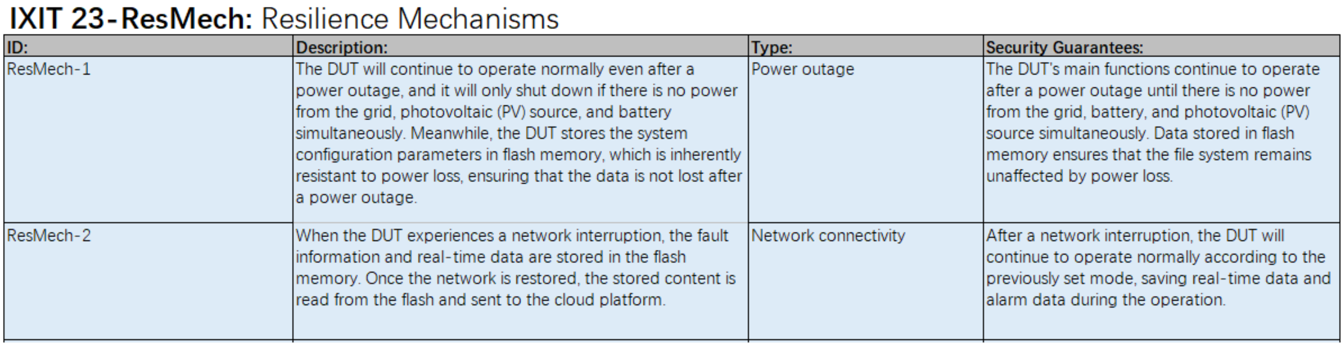
TC_RESILIENT_TO_OUTAGES#4 / Test case 5.9-2-2

Security requirement	PROVISION 5.9-2
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the resilience mechanisms concerning outages of network and power, the operation during network outages and restoration after power outages.
Evaluation inputs	**IXIT 23-ResMech**
Test scenario	a) The tester shall interrupt the DUT's connection to the network and functionally assess whether the resilience mechanisms operate as described in **IXIT 23-ResMech** and the DUT remains operating and locally functional after the loss of network connectivity. b) The tester shall interrupt the DUT's power supply and functionally assess whether the resilience mechanisms operate as described in **IXIT 23-ResMech** and the DUT resumes the connectivity and functionality after a loss of power in the same or improved state as before.
Verdict	**The verdict PASS is assigned if:** • There is no indication that the operation of the resilience mechanisms during network connectivity or power outages differs from its IXIT documentation **AND** • There is no indication that the DUT does not remain operating and locally functional after the loss of network connectivity **AND** • There is no indication that the DUT does not resume the connectivity and functionality after a loss of power in the same or improved state as before. **The verdict FAIL is assigned otherwise.**

Test Result

PASS

Testlab Comments



IXIT 23-ResMech: Resilience Mechanisms

ID:	Description:	Type:	Security Guarantees:
ResMech-1	The DUT will continue to operate normally even after a power outage, and it will only shut down if there is no power from the grid, photovoltaic (PV) source, and battery simultaneously. Meanwhile, the DUT stores the system configuration parameters in flash memory, which is inherently resistant to power loss, ensuring that the data is not lost after a power outage.	Power outage	The DUT's main functions continue to operate after a power outage until there is no power from the grid, battery, and photovoltaic (PV) source simultaneously. Data stored in flash memory ensures that the file system remains unaffected by power loss.
ResMech-2	When the DUT experiences a network interruption, the fault information and real-time data are stored in the flash memory. Once the network is restored, the stored content is read from the flash and sent to the cloud platform.	Network connectivity	After a network interruption, the DUT will continue to operate normally according to the previously set mode, saving real-time data and alarm data during the operation.

Based on IXIT 23-ResMech, it provides two resilience mechanisms in case of network and power failure.

This test, passed.

6.12.2.3 Provision 5.9-3

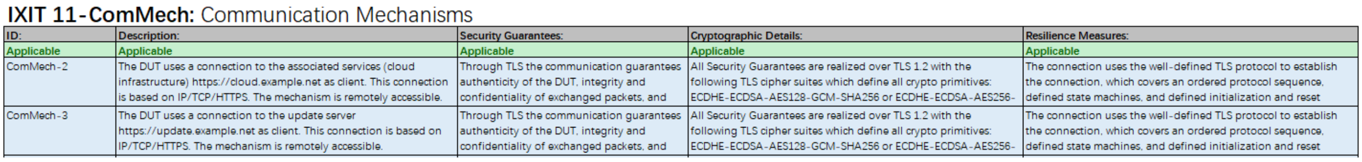
R: The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.

TC_RESILIENT_TO_OUTAGES#5 / Test case 5.9-3-1	
Security requirement	PROVISION 5.9-3
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the resilience measures for the communication mechanisms.
Evaluation inputs	Each communication mechanism in **IXIT 11-ComMech**
Documentation analysis procedure	a) For each communication mechanism in **IXIT 11-ComMech** the tester shall assess whether the **"Resilience Measures"** are appropriate to achieve a connection to a network in an orderly fashion taking the capability of the infrastructure into consideration. b) For each communication mechanism in **IXIT 11-ComMech** the tester shall assess whether the **"Resilience Measures"** are appropriate to support the operation of a stable network taking the capability of the infrastructure into consideration.
Verdict	The verdict **PASS** is assigned if: • Every communication mechanism provides appropriate measures to achieve a connection to a network in an orderly fashion **AND** • Every communication mechanism provides appropriate measures to support the operation of a stable network. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 11-ComMech: Communication Mechanisms

ID:	Description:	Security Guarantees:	Cryptographic Details:	Resilience Measures:
Applicable	Applicable	Applicable	Applicable	Applicable
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset

Based on the information provided by the manufacturer in IXIT 11-ComMech, the Resilience Measures field mentions the use of the TLS protocol to establish connections. It specifies that this protocol covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. Therefore, this test case is deemed to pass.

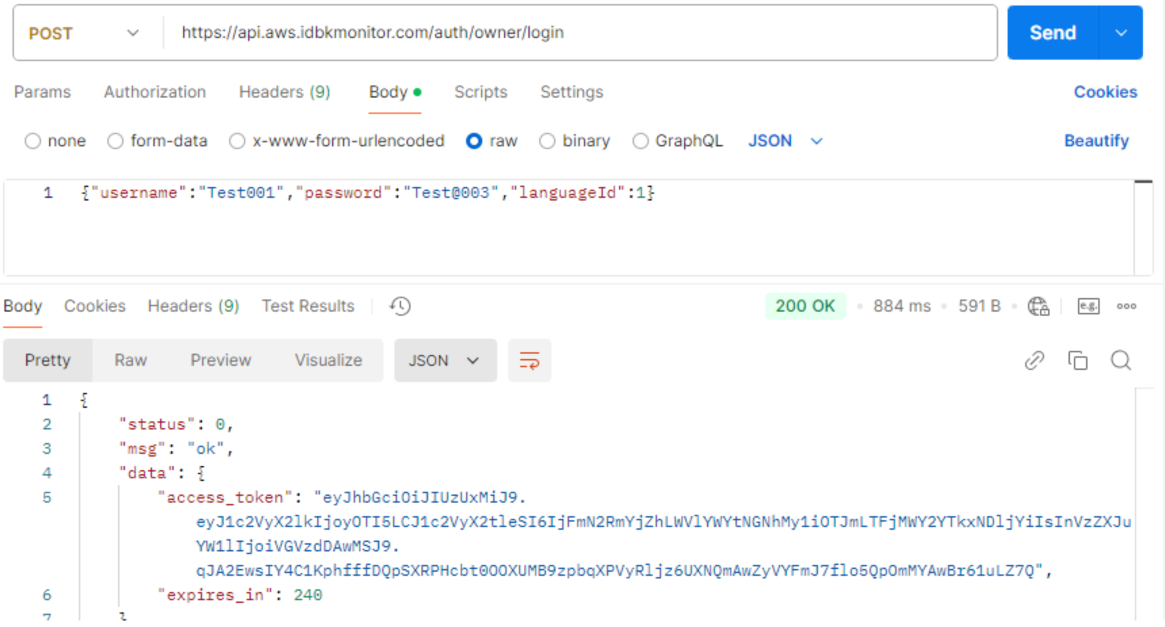
TC_RESILIENT_TO_OUTAGES#6 / Test case 5.9-3-2

Security requirement	PROVISION 5.9-3
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the resilience measures for the communication mechanisms.
Evaluation inputs	**"Resilience Measures"** for each communication method in **IXIT 11-ComMech**
Test scenario	The tester shall functionally assess whether the implemented **"Resilience Measures"** for each communication method in **IXIT 11-ComMech** are implemented as described, especially considering the protection against simultaneous mass reconnections.
Verdict	The verdict **PASS** is assigned if: - There is no indication that the operation of any implemented resilience measure differs from its IXIT documentation. The verdict **FAIL** is assigned otherwise.

Test Result

PASS

Testlab Comments



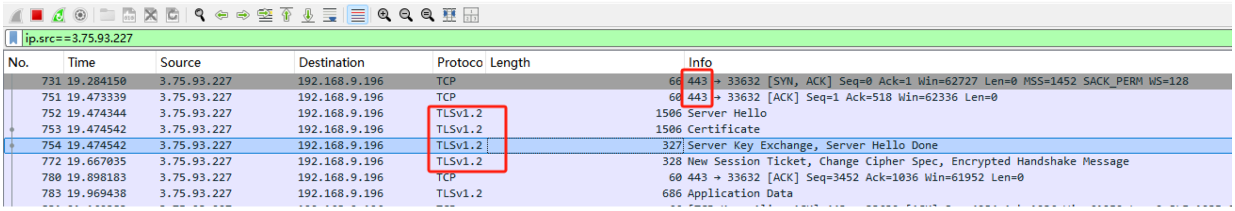
POST https://api.aws.idbkmonitor.com/auth/owner/login

○ none ○ form-data ○ x-www-form-urlencoded ● raw ○ binary ○ GraphQL JSON

```
{"username":"Test001","password":"Test@003","languageId":1}
```

200 OK · 884 ms · 591 B

```
{
    "status": 0,
    "msg": "ok",
    "data": {
        "access_token": "eyJhbGciOiJIUzUxMiJ9.
            eyJ1c2VyX2lkIjoyOTI5LCJ1c2VyX2tleSI6IjFmN2RmYjZhLWVlYWYtNGNhMy1iOTJmLTFjMWY2YTkxNDljYiIsInVzZXJu
            YW1lIjoiVGVzdDAwMSJ9.
            qJA2EwsIY4C1KphfffDQpSXRPHcbt0OOXUMB9zpbqXPVyRljz6UXNQmAwZyVYFmJ7flo5QpOmMYAwBr61uLZ7Q",
        "expires_in": 240
    }
```



ip.src==3.75.93.227

```
No.   Time       Source       Destination   Protoco Length  Info
  731 19.284150  3.75.93.227  192.168.9.196 TCP          66 443 → 33632 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1452 SACK_PERM WS=128
  751 19.473339  3.75.93.227  192.168.9.196 TCP          60 443 → 33632 [ACK] Seq=1 Ack=518 Win=62336 Len=0
  752 19.474344  3.75.93.227  192.168.9.196 TLSv1.2    1506 Server Hello
  753 19.474542  3.75.93.227  192.168.9.196 TLSv1.2    1506 Certificate
  754 19.474542  3.75.93.227  192.168.9.196 TLSv1.2     327 Server Key Exchange, Server Hello Done
  772 19.667035  3.75.93.227  192.168.9.196 TLSv1.2     328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
  780 19.898183  3.75.93.227  192.168.9.196 TCP          60 443 → 33632 [ACK] Seq=3452 Ack=1036 Win=61952 Len=0
  783 19.969438  3.75.93.227  192.168.9.196 TLSv1.2     686 Application Data
```

Based on the resiliency measures described in IXIT 11-ComMech, testers used Postman and Wireshark and looked at the login interface to confirm that the interface used the https and Tls1.2 protocols.

This test, passed.

6.13 Examine system telemetry data

6.13.1 IXIT data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 24-TelData: Telemetry Data

The completed IXIT lists all telemetry data collected by the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the telemetry data being collected and provided to the manufacturer by the DUT.
Purpose:	Brief description for what purposes the data is collected.
Security Examination:	If the data is used for security examination: Description of how and by whom (device or associated service) the telemetry data is examined for security anomalies. **Note**: The security anomaly examination can be realized outside the DUT, i.e. by associated services. **Note**: A device telemetry service captures crash logs and data on usage (telemetry data) from the DUT in order to enable the developers to determine security flaws (security anomaly detection).
Personal Data:	Reference to personal data in **IXIT 21-PersData** that are processed in the telemetry data.

6.13.2 Evaluation tasks

6.13.2.1 Provision 5.10-1

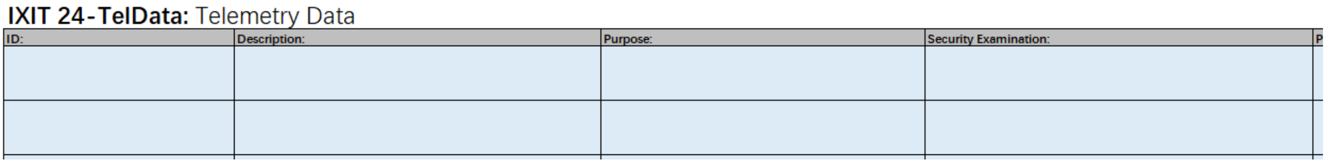
R C (6): If telemetry data are collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.

TC_TELEMETRY_DATA# 1 / Test case 5.10.1-1	
Security requirement	PROVISION 5.10-1
Type of work	IXIT analysis
Applicability	Conditional (if telemetry data is collected)
Documentation analysis objectives	Check if manufacturer have implemented a security examination process from telemetry data
Evaluation inputs	Collected telemetry data from **IXIT 24-TelData**
Documentation analysis procedure	✓ Tester check whether at least one **Security Examination** is provided in **IXIT 24-TelData** for examining for security anomalies. ✓ For each **Security Examination** of telemetry data in **IXIT 24-TelData**, tester assess whether the associated telemetry data in "Description" are suited for the described security examination and for examining the data for security anomalies.
Verdict	The verdict **PASS** is assigned if: ✓ At least one security anomaly examination is provided; **AND** ✓ Each security anomaly examination is suited for examining the associated telemetry data for a security anomaly. The verdict **FAIL** is assigned otherwise.

Test Result

FAIL

Testlab Comments



IXIT 24-TelData: Telemetry Data

ID:	Description:	Purpose:	Security Examination:	P

Based on IXIT 24-TelData, no information provided by the manufacturer.

This test, failed.

6.14 Make it easy for users to delete user data

6.14.1 IXIT Data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 2-UserInfo: User Information:

The completed IXIT lists documentations, publications and information provided to users.

Documentation of Deletion	Documentation of Deletion: Description of the way the methods for deletion of personal data documented to the user, including all information to access the documentation.

IXIT 25-DelFunc: Deletion Functionalities

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the functionality used to delete data of the user. If the "Target Type" indicates, that an associated service is addressed: The concerning associated service which is covered by the functionality is indicated additionally.
Target Type:	Indicates whether the functionality addresses user data on the device or personal data on associated services or both.
Initiation and Interaction:	Brief description of the user interaction, which is necessary to initiate and apply the deletion functionality.
Documentation:	Description of the way the deletion functionality is provided and documented to the user, including all information to access the documentation.
Confirmation:	Brief description of how the user is given indication that the addressed data has been deleted after applying the deletion functionality.

IXIT 21-PersData: Personal Data

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the category of personal data processed by the DUT. Example: Log data on the usage of the DUT, payment information, timestamped location data, audio input stream or biometric data.
Processing Activities:	Description of how the personal data is being processed, including all involved parties. It is described additionally for what purposes the processing is done. **Note**: *Processing personal data can also include storage of such data.*
Communication Mechanisms:	Reference to communication mechanisms in **IXIT 11-ComMech** that are used for communicating the personal data and an indication whether the recipient is an associated service (Yes/No). An empty list of communication mechanisms indicates that the personal data is not transmitted.
Sensitive (Yes/No):	Indication whether the personal data is sensitive according to the definition in the provision 5.8-2 in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].
Obtaining Consent:	If the personal data is processed on the basis of consumer's consent: Description of how the consent for the processing is obtained from the consumer.
Withdrawing Consent:	If the personal data is processed on the basis of consumer's consent: Description of how the consumer can withdraw the consent for processing the personal data.

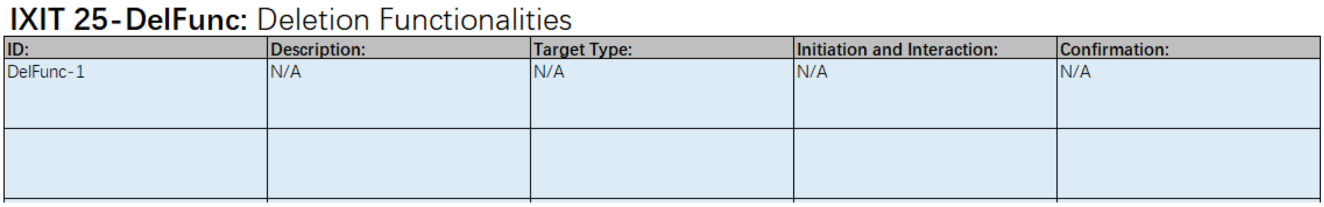
6.14.2 Evaluation tasks

6.14.2.1 Provision 5.11-1

M C(24): The user shall be provided with functionality such that user data can be erased from the device in a simple manner.

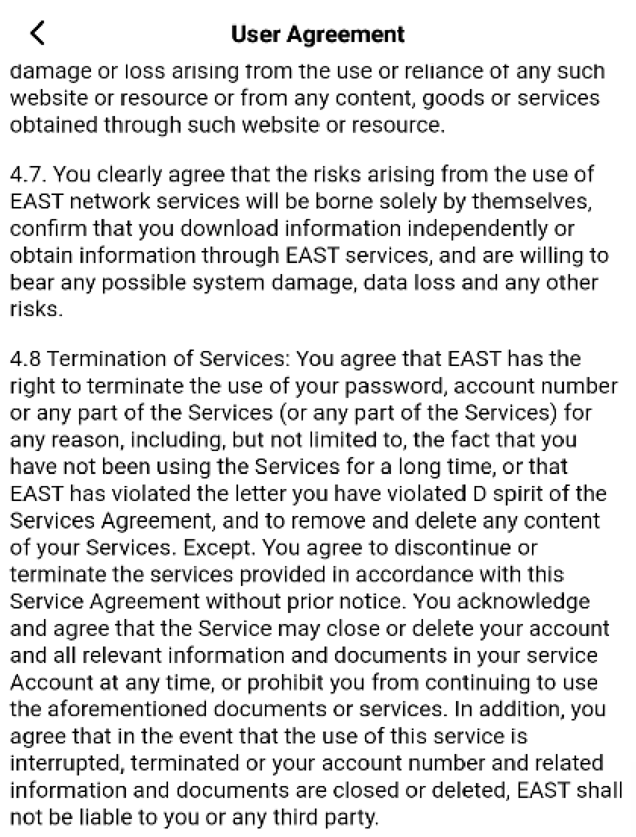
TC_USER_DELETE_DATA #1 / Test case 5.11-1	
Security requirement	PROVISION 5.11-1
Type of work	Doc
Applicability	Conditional (User data is stored on the device)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the user data erasure functionalities of the DUT.
Evaluation inputs	- List of deletion functionalities (**IXIT 25-DelFunc**)
Documentation analysis procedure	a) Tester shall assess whether at least one functionality is provided according to **IXIT 25-DelFunc**, which can be performed by the user with limited technical knowledge (cf. ETSI EN 103 701 Annex D.3) according to **“Description”** and **“Initiation and Interaction"** to erase user data from the device according to "**Target Type"**. b) Tester shall assess whether each functionality in **IXIT 25-DelFunc** is adequate to erase the targeted user data from the device. **Note**: *Erasure can be realized by overwriting with a pre-defined value or by internal irreversible blocking of all access to the data on the device.* c) Tester shall assess whether the functionalities to erase user data in **IXIT 25-DelFunc** cover personal data, user configuration and user-related cryptographic material. **Note**: *The information in **IXIT10-SecParam**, **IXIT21-PersData** and other IXITs is helpful to identify user data.* **Note**: *Cryptographic material can be user passwords or keys.*
Verdict	The verdict **PASS** is assigned if no user data is stored on the device; or: • at least one simple functionality to erase user data from the device is provided to the user; **AND** • the described functionality is adequate to erase the targeted user data from the device; **AND** • personal data, user configuration and cryptographic material is covered by the functionalities to erase user data from the device. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL
Testlab Comments



IXIT 25-DelFunc: Deletion Functionalities

ID:	Description:	Target Type:	Initiation and Interaction:	Confirmation:
DelFunc-1	N/A	N/A	N/A	N/A



User Agreement

damage or loss arising from the use or reliance of any such website or resource or from any content, goods or services obtained through such website or resource.

4.7. You clearly agree that the risks arising from the use of EAST network services will be borne solely by themselves, confirm that you download information independently or obtain information through EAST services, and are willing to bear any possible system damage, data loss and any other risks.

4.8 Termination of Services: You agree that EAST has the right to terminate the use of your password, account number or any part of the Services (or any part of the Services) for any reason, including, but not limited to, the fact that you have not been using the Services for a long time, or that EAST has violated the letter you have violated D spirit of the Services Agreement, and to remove and delete any content of your Services. Except. You agree to discontinue or terminate the services provided in accordance with this Service Agreement without prior notice. You acknowledge and agree that the Service may close or delete your account and all relevant information and documents in your service Account at any time, or prohibit you from continuing to use the aforementioned documents or services. In addition, you agree that in the event that the use of this service is interrupted, terminated or your account number and related information and documents are closed or deleted, EAST shall not be liable to you or any third party.

Based on the IXIT 25-DelFunc and the User Agreement, no information is provided in the IXIT 25-DelFunc, and the User Agreement stipulates that upon termination of the Service for reasons attributable to the User or the Service Provider, all of the User's content on the Service will be removed and deleted.

However, the tester did not find any user logout or deletion of personal data in the application.

This test failed.

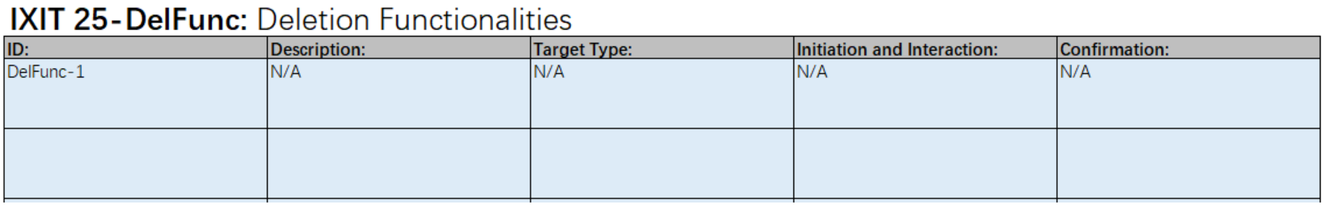
TC_USER_DELETE_DATA #2 / Test case 5.11-1-2

Security requirement	PROVISION 5.11-1
Type of work	Test CAB
Applicability	Conditional (User data is tored on the device)
Test objectives	The purpose of this test case is the functional assessment of the user data erasure functionalities of the DUT.
Evaluation inputs	- At least one device suitable for testing - List of deletion functionalities (IXIT 25-DelFunc)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) The tester shall create typical user data on the DUT with regard to the usage of the device. **Note**: *Such data can be personal data, user configuration or cryptographic material such as user passwords or keys, which differ from the standard configuration.* ✓ b) The tester shall perform each functionality to erase user data from the device according to **"Target Type"** in **IXIT 25-DelFunc** and functionally assess whether the **"Initiation and Interaction"** is consistent with the IXIT. ✓ c) The tester shall perform each functionality to erase user data from the device according to "**Target Type"** in **IXIT 25-DelFunc** and functionally assess whether the corresponding user data still exists after completing the operation. **Expected result:** ✓ Evaluation of user data erasure functionalities
Verdict	The verdict **PASS** is assigned if for any functionality to erase user data from the device: • The initiation and interaction of the user is consistent with the IXIT; **AND** • There is no indication that the corresponding user data is not erased successfully. The verdict **FAIL** is assigned otherwise.

Test Result

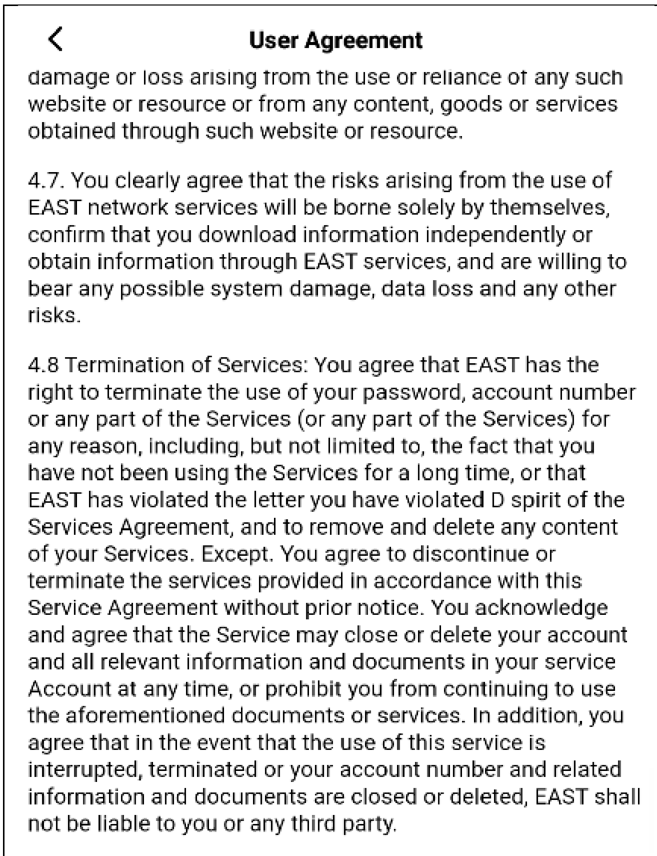
FAIL

Testlab Comments



IXIT 25-DelFunc: Deletion Functionalities

ID:	Description:	Target Type:	Initiation and Interaction:	Confirmation:
DelFunc-1	N/A	N/A	N/A	N/A



damage or loss arising from the use or reliance of any such website or resource or from any content, goods or services obtained through such website or resource.

4.7. You clearly agree that the risks arising from the use of EAST network services will be borne solely by themselves, confirm that you download information independently or obtain information through EAST services, and are willing to bear any possible system damage, data loss and any other risks.

4.8 Termination of Services: You agree that EAST has the right to terminate the use of your password, account number or any part of the Services (or any part of the Services) for any reason, including, but not limited to, the fact that you have not been using the Services for a long time, or that EAST has violated the letter you have violated D spirit of the Services Agreement, and to remove and delete any content of your Services. Except. You agree to discontinue or terminate the services provided in accordance with this Service Agreement without prior notice. You acknowledge and agree that the Service may close or delete your account and all relevant information and documents in your service Account at any time, or prohibit you from continuing to use the aforementioned documents or services. In addition, you agree that in the event that the use of this service is interrupted, terminated or your account number and related information and documents are closed or deleted, EAST shall not be liable to you or any third party.

Based on the IXIT 25-DelFunc and the User Agreement, no information is provided in the IXIT 25-DelFunc, and the User Agreement stipulates that upon termination of the Service for reasons attributable to the User or the Service Provider, all of the User's content on the Service will be removed and deleted.

However, the tester did not find any user logout or deletion of personal data in the application.

This test failed.

6.14.2.2 Provision 5.11-2

R C (25): The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.

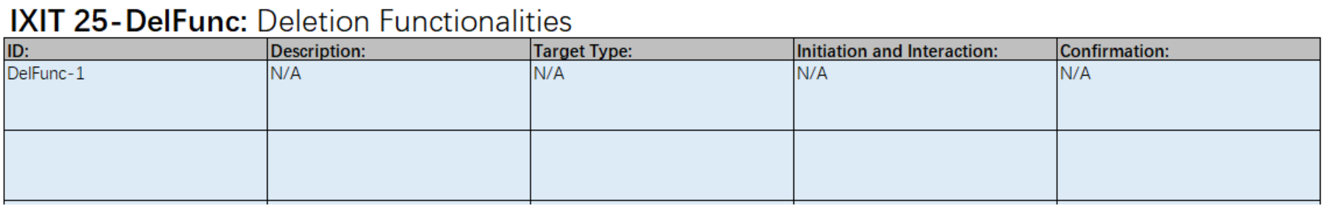
TC_USER_DELETE_DATA #3 / Test case 5.11-2-1

Security requirement	PROVISION 5.11-2
Type of work	Doc
Applicability	Conditional (Personal data is stored on accociated services.)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the personal data removal functionalities of the DUT.
Evaluation inputs	- List of deletion functionalities (**IXIT 25-DelFunc**) - List of personal data (**IXIT 21-PersData**)
Documentation analysis procedure	a) For all deletion functionalities in **IXIT 25-DelFunc** the tester shall assess whether at least one functionality is provided, which can be performed by the user with limited technical knowledge (cf. ETSI EN 103 701 Annex D.3) according to **"Description"** and **"Initiation and Interaction"** to remove all personal data stored on the associated services according to **"Target Type"**. b) The tester shall assess whether all associated services storing personal data according to **"Processing Activities"** in **IXIT 21-PersData** are covered by the combination of all deletion functionalities in **IXIT 25-DelFunc.**
Verdict	The verdict PASS is assigned if: • At least one simple functionality to remove personal data from associated services is provided to the user; **AND** • Every associated service storing personal data is covered by a simple deletion functionality. The verdict FAIL is assigned otherwise.

Test Result

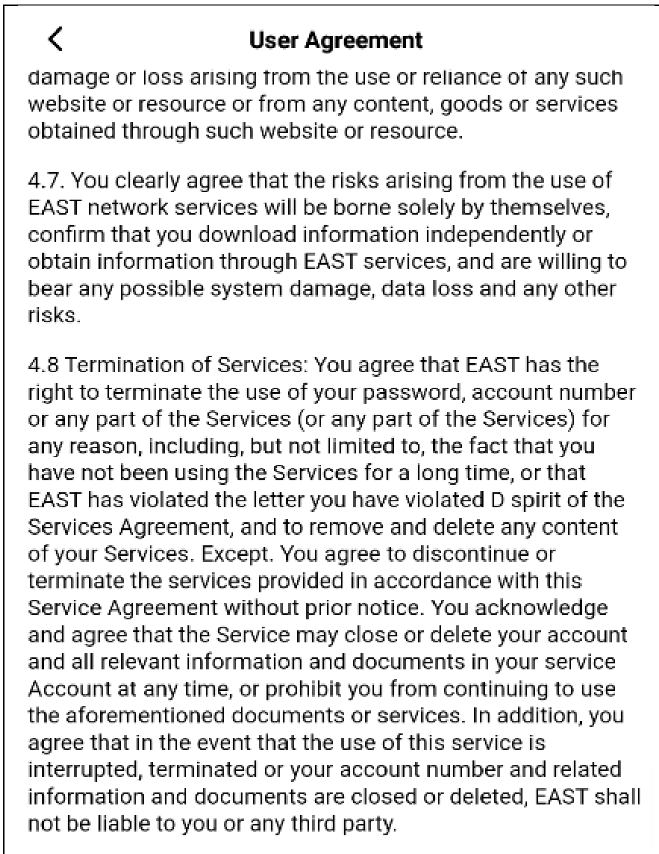
FAIL

Testlab Comments



IXIT 25-DelFunc: Deletion Functionalities

ID:	Description:	Target Type:	Initiation and Interaction:	Confirmation:
DelFunc-1	N/A	N/A	N/A	N/A



damage or loss arising from the use or reliance of any such website or resource or from any content, goods or services obtained through such website or resource.

4.7. You clearly agree that the risks arising from the use of EAST network services will be borne solely by themselves, confirm that you download information independently or obtain information through EAST services, and are willing to bear any possible system damage, data loss and any other risks.

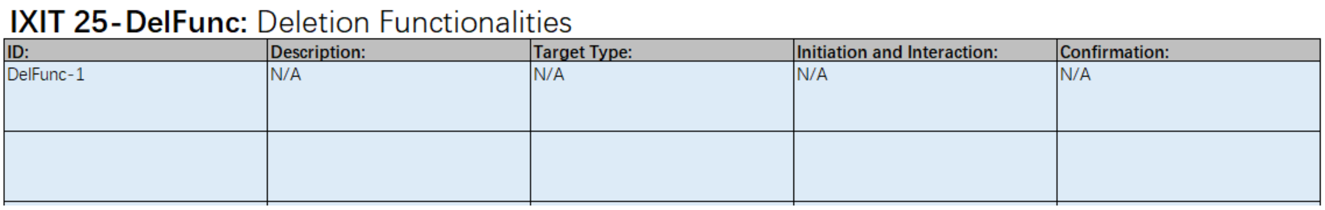
4.8 Termination of Services: You agree that EAST has the right to terminate the use of your password, account number or any part of the Services (or any part of the Services) for any reason, including, but not limited to, the fact that you have not been using the Services for a long time, or that EAST has violated the letter you have violated D spirit of the Services Agreement, and to remove and delete any content of your Services. Except. You agree to discontinue or terminate the services provided in accordance with this Service Agreement without prior notice. You acknowledge and agree that the Service may close or delete your account and all relevant information and documents in your service Account at any time, or prohibit you from continuing to use the aforementioned documents or services. In addition, you agree that in the event that the use of this service is interrupted, terminated or your account number and related information and documents are closed or deleted, EAST shall not be liable to you or any third party.

Based on the IXIT 25-DelFunc and the User Agreement, no information is provided in the IXIT 25-DelFunc, and the User Agreement stipulates that upon termination of the Service for reasons attributable to the User or the Service Provider, all of the User's content on the Service will be removed and deleted.

However, the tester did not find any user logout or deletion of personal data in the application.

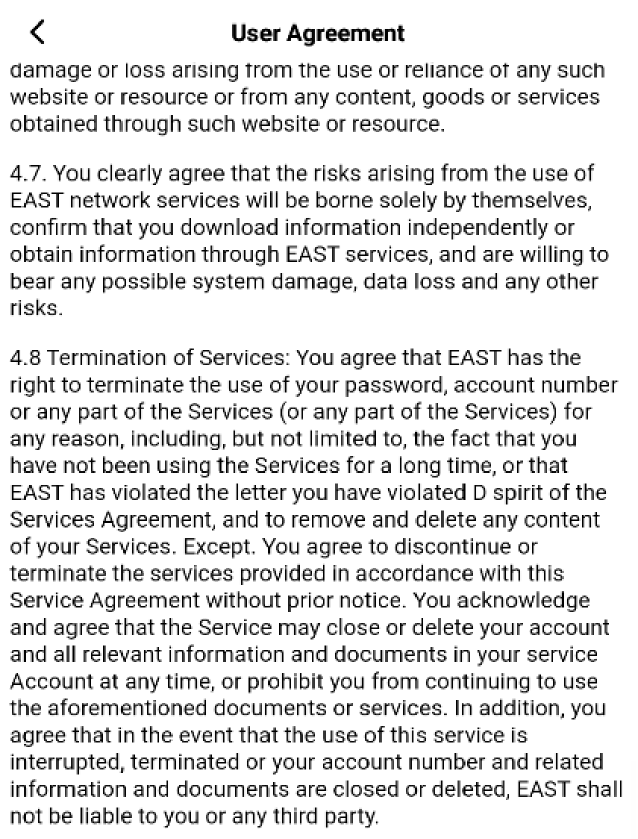
This test failed.

TC_USER_DELETE_DATA #4 / Test case 5.11-2-2	
Security requirement	PROVISION 5.11-2
Type of work	Test CAB
Applicability	Conditional (Personal data is stored on accociated services.)
Test objectives	The purpose of this test case is the functional assessment of the personal data removal functionalities of the DUT.
Evaluation inputs	- At least one device suitable for testing - List of deletion functionalities (IXIT 25-DelFunc)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) The Tester shall create typical personal data on associated services with regard to the usage of the DUT. **Note**: The information from **"Processing Activities" IXIT21-PersData** can be helpful to create personal data which are stored on associated services. ✓ b) The Tester shall perform each functionality to remove personal data according to **"Target Type"** in **IXIT 25-DelFunc** and functionally assess whether the **"Initiation and Interaction"** is consistent with in the IXIT. ✓ c) The Tester shall perform each functionality to remove personal data according to **"Target Type"** in **IXIT 25-DelFunc** and functionally assess whether the corresponding personal data still exists on the associated services after completing the operation. **Expected result:** ✓ Evaluation of user data erasure functionalities
Verdict	The verdict PASS is assigned if for any functionality to erase user data from the device: • The initiation and interaction of the user is consistent with the IXIT; **AND** • There is no indication that the corresponding user data is not erased successfully. The verdict FAIL is assigned otherwise.
Test Result	
FAIL	
Testlab Comments	



IXIT 25-DelFunc: Deletion Functionalities

ID:	Description:	Target Type:	Initiation and Interaction:	Confirmation:
DelFunc-1	N/A	N/A	N/A	N/A



damage or loss arising from the use or reliance of any such website or resource or from any content, goods or services obtained through such website or resource.

4.7. You clearly agree that the risks arising from the use of EAST network services will be borne solely by themselves, confirm that you download information independently or obtain information through EAST services, and are willing to bear any possible system damage, data loss and any other risks.

4.8 Termination of Services: You agree that EAST has the right to terminate the use of your password, account number or any part of the Services (or any part of the Services) for any reason, including, but not limited to, the fact that you have not been using the Services for a long time, or that EAST has violated the letter you have violated D spirit of the Services Agreement, and to remove and delete any content of your Services. Except. You agree to discontinue or terminate the services provided in accordance with this Service Agreement without prior notice. You acknowledge and agree that the Service may close or delete your account and all relevant information and documents in your service Account at any time, or prohibit you from continuing to use the aforementioned documents or services. In addition, you agree that in the event that the use of this service is interrupted, terminated or your account number and related information and documents are closed or deleted, EAST shall not be liable to you or any third party.

Based on the IXIT 25-DelFunc and the User Agreement, no information is provided in the IXIT 25-DelFunc, and the User Agreement stipulates that upon termination of the Service for reasons attributable to the User or the Service Provider, all of the User's content on the Service will be removed and deleted.

However, the tester did not find any user logout or deletion of personal data in the application.

This test failed.

6.14.2.3 Provision 5.11-3

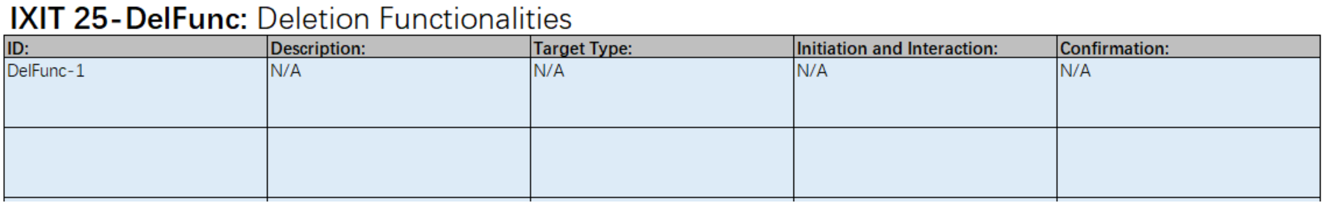
R (26): Users should be given clear instructions on how to delete their personal data.

TC_USER_DELETE_DATA #5 / Test case 5.11-3-1	
Security requirement	PROVISION 5.11-3
Type of work	Doc
Applicability	Conditional (Personal data is stored)
Documentation analysis objectives	The purpose of this test case is the functional assessment of the user documentation for the personal data deletion functionalities of the DUT.
Evaluation inputs	- At least one device suitable for testing - List of deletion functionalities & related documentation (**IXIT 25-DelFunc**)
Documentation analysis procedure	a) The tester shall create typical personal data with regard to the usage of the DUT. **Note**: *The information from "Processing Activities"* ***IXIT21-PersData*** *can be helpful to create personal data which are stored on the DUT and on associated services.* b) For each deletion functionality in **IXIT 25-DelFunc** the tester shall perform the functionality according to the **"Documentation"** and functionally assess whether it is described in a concise manner and includes all necessary steps to delete the personal data from the device or associated service according **to "Target Type".** c) The tester shall functionally assess whether all deletion functionalities in **IXIT 25-DelFunc** are covered by the **"Documentation".**
Verdict	The verdict PASS is assigned if every deletion functionality: • Is documented in a concise manner and includes the necessary steps to be taken to delete personal data; AND • Is covered by the documentation. The verdict FAIL is assigned otherwise.

Test Result

N/A

Testlab Comments



IXIT 25-DelFunc: Deletion Functionalities

ID:	Description:	Target Type:	Initiation and Interaction:	Confirmation:
DelFunc-1	N/A	N/A	N/A	N/A

According to the tester's IXIT 25-DelFunc content, the device does not provide user data deletion or user logout functionality.

However, the tester did not find the user logout or to personal data deletion functionality in the application.

This test, fails.

6.14.2.4 Provision 5.11-4

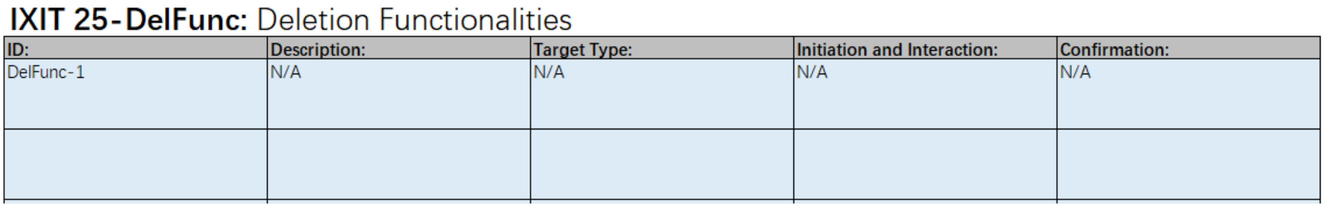
R (26): Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.

TC_USER_DELETE_DATA #6 / Test Case 5.11-4-1	
Security requirement	PROVISION 5.11-4
Type of work	Test CAB
Applicability	Conditional (Personal data is stored)
Test objectives	The purpose of this test case is the functional assessment of the personal data removal functionalities of the DUT.
Evaluation inputs	- At least one device suitable for testing - List of deletion functionalities (**IXIT 25-DelFunc**)
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) The tester shall perform each deletion functionality in **IXIT 25-DelFunc** according to **"Documentation of deletion"** in **IXIT 2-UserInfo** ✓ b) For each deletion functionality in **IXIT 25-DelFunc** the tester shall functionally assess whether the user is provided with a clear **"Confirmation"**, that the corresponding data is deleted. **Test sequence:** ✓ Availability of notification services on deletion functionality
Verdict	The verdict **PASS** is assigned if: ✓ For every deletion functionality a clear confirmation is provided, that the corresponding data is deleted. The verdict FAIL is assigned otherwise.

Test Result

N/A

Testlab Comments



IXIT 25-DelFunc: Deletion Functionalities

ID:	Description:	Target Type:	Initiation and Interaction:	Confirmation:
DelFunc-1	N/A	N/A	N/A	N/A

According to the tester's IXIT 25-DelFunc content, the device does not provide user data deletion or user logout functionality.

However, the tester did not find the user logout or to personal data deletion functionality in the application.

This test, fails.

6.15 Make installation and maintenance of devices easy

6.15.1 IXIT data

IXIT 2-UserInfo: User Information

The completed IXIT lists documentations, publications and information provided to users. The pro forma contains the following entries, which are independent from each other, and is typically filled out in form of a list.

Documentation of Secure Setup:	Description of the way the method for securely setting up the DUT is documented for the user, including all information to access the documentation.
Documentation of Setup Check:	Description of the way the method for checking the secure setup of the DUT is documented for the user, including all information to access the documentation.

IXIT 26-UserDec: User Decisions

The completed IXIT lists all decisions to be taken by the user during installation and maintenance. The pro forma contains the following entries and is typically filled in the form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Description of the decision to be taken by the user within the installation and maintenance flows. Its position within the installation or maintenance flow is additionally described.
Options:	Description of the security-relevant options the user can take and an indication for the default value.
Triggered By:	Brief description how the decision is triggered. It is indicated additionally whether the decision can be triggered by the user.

6.15.2 Evaluation tasks

6.15.2.1 Provision 5.12-1

R: Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.

TC_EASE_OF_USE#1 / Test Case 5.12-1-1	
Security requirement	PROVISION 5.12-1
Type of work	IXIT analysis
Applicability	Always
Test objectives	The purpose of this test case is the conceptual assessment of the installation and maintenance decisions to be taken by the user.
Evaluation inputs	Each decision in **IXIT 26-UserDec**
Test scenario	a) For each decision in **IXIT 26-UserDec** the tester **shall** assess whether it is necessary regarding the usage in the operational environment. b) For each decision in **IXIT 26-UserDec** the tester **shall** assess whether the default value for the decision according to **"Options"** follows security best practice.
Verdict	The verdict **PASS** is assigned if: • Every decision taken by the user is necessary regarding the usage in the operational environment **AND** • Every default value for a decision taken by the user follows security best practice. The verdict **FAIL** is assigned otherwise.
Test Result	
PASS	
Testlab Comments	
Based on IXIT 26-UserDec, user login requires a registered account password, and user passwords are tested to pass strength requirements. The application update installation process is automated and does not require user intervention. This test passed.	

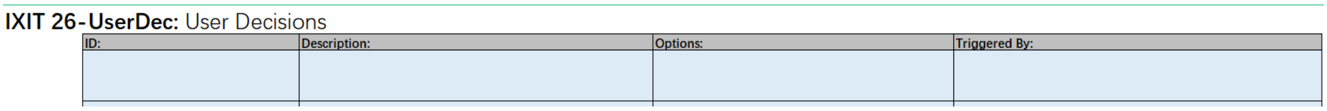
TC_EASE_OF_USE#2 / Test Case 5.12-1-2

Security requirement	PROVISION 5.12-1
Type of work	Test CAB
Applicability	Always
Test objectives	The purpose of this test case is the functional assessment of the installation and maintenance decisions to be taken by the user.
Evaluation inputs	Each decision in **IXIT 26-UserDec**
Test scenario	a) The tester shall trigger all user-based decisions in **IXIT 26-UserDec** according to **"Triggered By"**. b) For each decision in **IXIT 26-UserDec** the tester shall functionally assess whether it is prominently requested from the user during the installation and maintenance flows. c) For each decision in **IXIT 26-UserDec** the tester shall functionally assess whether the decision and its "**Options"** are understandable for a user with limited technical knowledge. d) The tester shall functionally assess whether the decisions to be taken by the user during installation and maintenance on the DUT are conformant to their **"Description"** and **"Options"** in **IXIT 26-UserDec**.
Verdict	The verdict **PASS** is assigned if: • Every decision taken by the user is prominently requested during the installation and maintenance flows **AND** • Every decision taken by the user is understandable for a user with limited technical knowledge **AND** • Every decision taken by the user during installation or maintenance on the DUT is as described in the IXIT. The verdict **FAIL** is assigned otherwise.

Test Result

FAIL

Testlab Comments



IXIT 26-UserDec: User Decisions

ID:	Description:	Options:	Triggered By:

IXIT 26-UserDec does not describe the relevant security settings.

The service does not provide guidance on application-related security settings.

This test, failed.

6.15.2.2 Provision 5.12-2

R: The manufacturer should provide users with guidance on how to securely set up their device.

TC_EASE_OF_USE#2 / Test Case 5.12-2-1	
Security requirement	PROVISION 5.12-2
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the functional assessment of the user guidance on securely setting up the DUT.
Evaluation inputs	"Documentation of Secure Setup" in **IXIT 2-UserInfo**
Documentation analysis procedure	a) The tester shall set up the DUT using the **"Documentation of Secure Setup"** described in **IXIT 2-UserInfo** b) The tester shall functionally assess whether in the **"Documentation of Secure Setup"** described in **IXIT 2-UserInfo** each security-relevant user decision is covered by the documentation. c) The tester shall functionally assess whether the **"Documentation of Secure Setup"** described in **IXIT 2-UserInfo** includes recommendations on how to take the security-relevant user decisions to achieve a secure setup.
Verdict	The verdict **PASS** is assigned if: • Every security-relevant user decision is covered by the documentation **AND** • For every security-relevant user decision a recommendation on how to achieve a secure setup is given. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL

Testlab Comments
IXIT 2-UserInfo does not describe the relevant security settings. The service does not provide guidance on application-related security settings. This test, failed.

6.15.2.3 Provision 5.12-3

R: The manufacturer should provide users with guidance on how to check whether their device is securely set up.

TC_EASE_OF_USE#3 / Test Case 5.12-3-1	
Security requirement	PROVISION 5.12-3
Type of work	IXIT analysis
Applicability	Always
Documentation analysis objectives	The purpose of this test case is the functional assessment of the user guidance on checking whether the DUT is securely set up.
Evaluation inputs	"**Documentation of Setup Check"** in **IXIT 2-UserInfo**
Documentation analysis procedure	a) The tester shall set up the DUT using an example configuration. b) The tester shall functionally assess whether in the **"Documentation of Setup Check"** described in **IXIT 2-UserInfo** each step for checking whether the DUT is securely set up is covered by the documentation. c) The tester shall functionally assess whether the check applied to the example configuration results in a reasonable outcome.
Verdict	The verdict **PASS** is assigned if: • Every step for checking the securely set up is covered by the documentation; and • The application of the check for securely set up according to the documentation results in an outcome and there is an indication that the result is reasonable. The verdict FAIL is assigned otherwise.

Test Result
FAIL

Testlab Comments
IXIT 2-UserInfo does not describe the relevant security settings. The service does not provide guidance on application-related security settings. This test, failed.

6.16 Validate input data

6.16.1 IXIT data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 11-ComMech: Communication Mechanisms:

The completed IXIT lists all communication mechanisms of the DUT. The pro forma contains the following entries and is typically filled out in form of a table.

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the communication mechanism, including its purpose and a description of the used protocol. For standardized protocols a reference is sufficient. It is indicated additionally whether the mechanism is remotely accessible. **Note**: *A possible communication mechanism is the use of Bluetooth®, WiFi® or NFC for a local connection between an mobile application and the DUT.*
Security Guarantees:	Description of the realized security objectives and the threats the mechanism is protected against. **Note**: *The most common security guarantees to be considered include authentication of peers, authentication of origin, integrity protection, confidentiality protection, and anti-replay.*
Cryptographic Details:	Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the communication mechanism considering key management, and to facilitate the described **"Security Guarantees"**. **Note**: *Cryptographic Details contain information such as: the protocol Z-Wave® with Security 2 Command Class v1 is used for the communication. The transferred data is authenticated encrypted with AES-128 CCM to facilitate confidentiality and integrity. The key exchange is based on an out-of-band mechanism.*
Resilience Measures:	Description of the measures to ensure that the connection establishment is performed in an orderly fashion including an expected, operational and stable state to achieve a stable connection. **Note**: *Resilience measures consider the sequence of the used protocol, the capability of the infrastructure, reset and initialization of the protocol and problems caused by mass reconnections.*

IXIT 27-UserIntf: User Interfaces

Description:	Brief description of the user interface enabling data input from the user. It is indicated additionally how the interface can be accessed by the user.

IXIT 28-ExtAPI: External APIs

Description:	Description of the API enabling data input from external sources of the DUT. **Note**: *External APIs are typically used for machine-to-machine communication.*

IXIT 29-InpVal: Data Input Validation

Description:	Description of the method for validating the data input via user interfaces, or transferred via APIs and between networks in services and devices including the handling of unexpected data. It is indicated additionally which of the sources for data input are addressed by the method. **Note**: *To validate the data input, it can be checked whether it is of an allowed type (format and structure), of allowed value, an allowed cardinality or an allowed ordering.*

6.16.2 Evaluation tasks

6.16.2.1 Provision 5.13-1

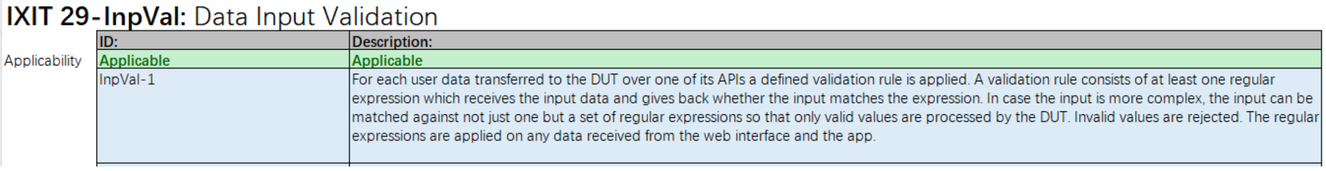
M C(27): The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices.

TC_VALIDATE_INPUT#1 / Test Case 5.13-1-1	
Security requirement	PROVISION 5.13-1
Type of work	IXIT analysis
Applicability	Conditional (data input via user interfaces or transferred via APIs or between networks in services and devices is supported)
Documentation analysis objectives	Verify that the device validates input via user interfaces
Evaluation inputs	- Collected data input validation methods in **IXIT 29-InpVal,** data input from external sources in **IXIT 28-ExtAPI,** data input from the user **in IXIT 27-UserIntf** , remotely accessible communication methods in **IXIT 11-ComMech.**
Documentation analysis procedure	✓ a) Tester assess whether the combination of data input validation methods in **IXIT 29-InpVal** covers all sources for data input including: - The user interfaces, which enable data input from the user **in IXIT 27-UserIntf**; **AND** - The application programming interfaces (APIs), which enable data input from external sources in **IXIT 28-ExtAPI**; **AND** - The network communications, which enable data input according to the corresponding remotely accessible communication methods in **IXIT 11-ComMech.** ✓ b) For each data input validation method in **IXIT 29-InpVal**, assess whether it is effective for validating the corresponding data input. **Note**: Validation typically includes checks that data input is of an allowed format and structure, of an allowed value, of an allowed cardinality and of an allowed ordering with the aim to prevent misuse.
Verdict	The verdict PASS is assigned if: - The data input validation methods cover data input via user interfaces, transmitted via APIs and between networks in services and devices; **AND** - Every described data input validation method is effective for validating the corresponding data input. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 29-InpVal: Data Input Validation

	ID:	Description:
Applicability	Applicable	Applicable
	InpVal-1	For each user data transferred to the DUT over one of its APIs a defined validation rule is applied. A validation rule consists of at least one regular expression which receives the input data and gives back whether the input matches the expression. In case the input is more complex, the input can be matched against not just one but a set of regular expressions so that only valid values are processed by the DUT. Invalid values are rejected. The regular expressions are applied on any data received from the web interface and the app.

Based on the information provided by IXIT 29-InpVal, the testers combined with the DUT inspection and confirmed that the interfaces with external injection risk are the registration interface, login interface, password change interface, interface for inputting device serial number, and interface for inputting device parameters.

For the above interfaces, authentication and authentication have been realized, security protocols have been used for transmission, and filtering and type restrictions have been applied to the input data, etc. The service is deployed on the Amazon platform, and defense measures such as brute-force cracking have been provided.

This test is passed.

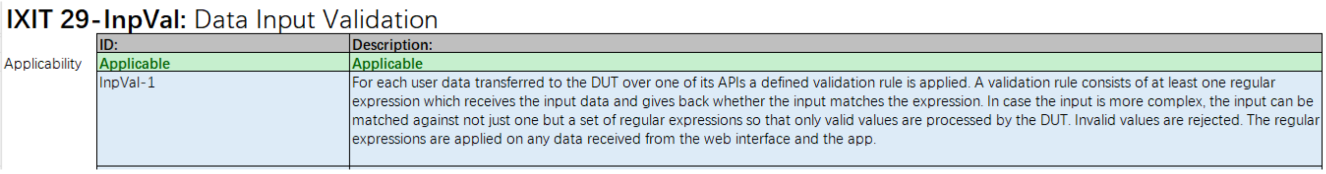
TC_VALIDATE_INPUT#2: 5.13-1-2

Security requirement	PROVISION 5.13-1
Type of work	Test CAB
Applicability	Conditional (data input via user interfaces or transferred via APIs or between networks in services and devices is supported)
Test objectives	Verify that the device validates input via user interfaces
Evaluation inputs	- At least one device suitable for testing - Collected data input validation methods in **IXIT 29-InpVal,** data input from external sources in **IXIT 28-ExtAPI,** data input from the user **in IXIT 27-UserIntf**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) Tester assess ssess whether each data input validation method in **IXIT 29-InpVal** prevents the processing of unexpected data input. NOTE 1: *The tester is free to choose a source of data input for each data input validation method.* NOTE 2: *The tester possesses all credentials of a user to attempt the misuses.* NOTE 3: *Automated tools can be used to generate unexpected data which does not suit to the expected input, e.g. in format and structure, value, cardinality or ordering.* ✓ b) Tester assess whether all user interfaces of the DUT are described in **IXIT 27-UserIntf** according to the documentation for the user, e.g. user manual. ✓ c) Tester assess whether all remotely accessible APIs of the DUT are described in **IXIT 28-ExtAPI.** **Expected result:** ✓ Device functionality.
Verdict	The verdict **PASS** is assigned if: - There is no indication that any data input validation does not protect against the processing of unexpected data input; **AND** - Every discovered user interface is documented in the IXIT; **AND** - Every discovered remotely accessible API is documented in the IXIT. The verdict FAIL is assigned otherwise.

Test Result

PASS

Testlab Comments



IXIT 29-InpVal: Data Input Validation

	ID:	Description:
Applicability	Applicable	Applicable
	InpVal-1	For each user data transferred to the DUT over one of its APIs a defined validation rule is applied. A validation rule consists of at least one regular expression which receives the input data and gives back whether the input matches the expression. In case the input is more complex, the input can be matched against not just one but a set of regular expressions so that only valid values are processed by the DUT. Invalid values are rejected. The regular expressions are applied on any data received from the web interface and the app.

Based on the information provided by IXIT 29-InpVal, the testers combined with the DUT inspection and confirmed that the interfaces with external injection risk are the registration interface, login interface, password change interface, interface for inputting device serial number, and interface for inputting device parameters.

For the above interfaces, authentication and authentication have been realized, security protocols have been used for transmission, and filtering and type restrictions have been applied to the input data, etc. The service is deployed on the Amazon platform, and defense measures such as brute-force cracking have been provided.

This test is passed.

6.17 Data protection for consumer IoT

6.17.1 IXIT Data

According annex A4 of ETSI TS 103 701, the IXIT fileds required for this family of provisions are:

IXIT 2-UserInfo: User Information:

The completed IXIT lists documentations, publications and information provided to users.

Documentation of Personal Data:	Description of the way the information about processing personal data is documented for the user, including all information to access the documentation.

IXIT 21-PersData: Personal Data

ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the category of personal data processed by the DUT. ***Example:*** *Log data on the usage of the DUT, payment information, timestamped location data, audio input stream or biometric data.*
Processing Activities:	Description of how the personal data is being processed, including all involved parties. It is described additionally for what purposes the processing is done. **Note**: *Processing personal data can also include storage of such data.*
Communication Mechanisms:	Reference to communication mechanisms in **IXIT 11-ComMech** that are used for communicating the personal data and an indication whether the recipient is an associated service (Yes/No). An empty list of communication mechanisms indicates that the personal data is not transmitted.
Sensitive (Yes/No):	Indication whether the personal data is sensitive according to the definition in the provision 5.8-2 in ETSI TS 103 645 [1]/ETSI EN 303 645 [2].
Obtaining Consent:	If the personal data is processed on the basis of consumer's consent: Description of how the consent for the processing is obtained from the consumer.
Withdrawing Consent:	If the personal data is processed on the basis of consumer's consent: Description of how the consumer can withdraw the consent for processing the personal data.

IXIT 24-TelData: Telemetry Data

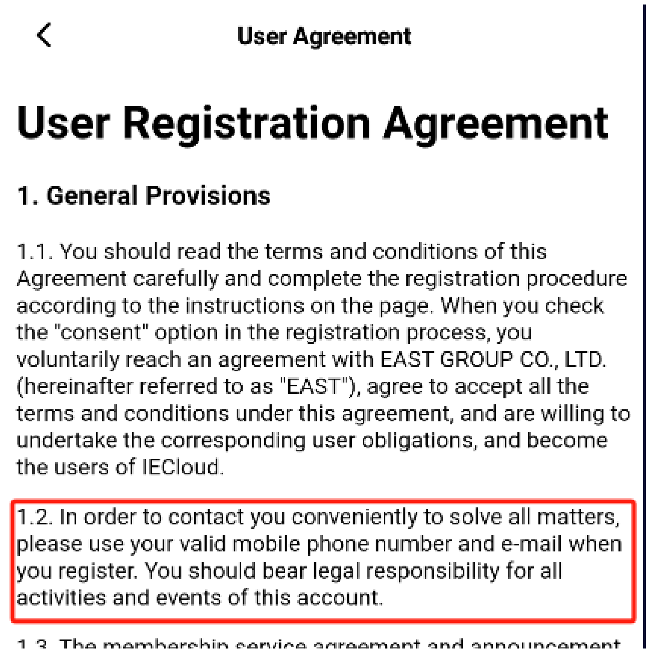
ID:	Unique per IXIT identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.
Description:	Brief description of the telemetry data being collected and provided to the manufacturer by the DUT.
Purpose:	Brief description for what purpose the data is collected.
Security Examination:	If the data is used for security examination: Description of how and by whom (device or associated service) the telemetry data is examined for security anomalies. **Note**:The security anomaly examination can be realized outside the DUT, i.e. by associated services. **Note**:A device telemetry service captures crash logs and data on usage (telemetry data) from the DUT in order to enable the developers to determine security flaws (security anomaly detection).
Personal Data:	Reference to personal data in IXIT 21-PersData that are processed in the telemetry data.

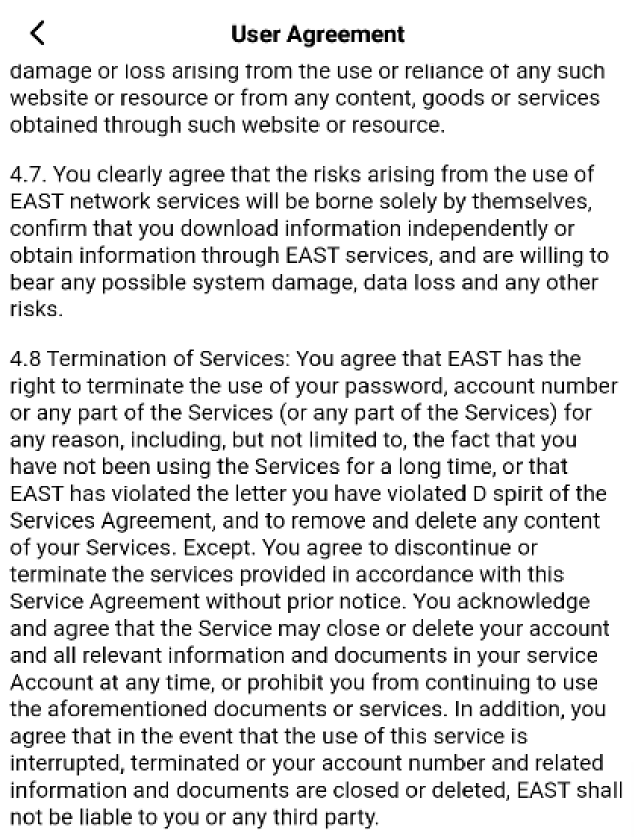
6.17.2 Evaluation tasks

6.17.2.1 Provision 6-1

M C (28): The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.

TC_DATA_PROTECTION#1 / Test Case 6-1-1	
Security requirement	PROVISION 6-1
Type of work	Doc
Applicability	Conditional (Personal data is processed)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the user information about the processing of personal data.
Evaluation inputs	Documentation related to personal data (**“Documentation of Personal Data”** in **IXIT 2-UserInfo**)
Documentation analysis procedure	a) The tester shall assess whether the **"Documentation of Personal Data"** in **IXIT 2-UserInfo** is suitable for the consumer to obtain the information about processing personal data.
Verdict	The verdict **PASS** is assigned if: ✓ The information about processing personal data is suitably provided to the consumer. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL
Testlab Comments
 User Agreement User Registration Agreement 1. General Provisions 1.1. You should read the terms and conditions of this Agreement carefully and complete the registration procedure according to the instructions on the page. When you check the "consent" option in the registration process, you voluntarily reach an agreement with EAST GROUP CO., LTD. (hereinafter referred to as "EAST"), agree to accept all the terms and conditions under this agreement, and are willing to undertake the corresponding user obligations, and become the users of IECloud. 1.2. In order to contact you conveniently to solve all matters, please use your valid mobile phone number and e-mail when you register. You should bear legal responsibility for all activities and events of this account. 1.3. The membership service agreement and announcement



User Agreement

damage or loss arising from the use or reliance of any such website or resource or from any content, goods or services obtained through such website or resource.

4.7. You clearly agree that the risks arising from the use of EAST network services will be borne solely by themselves, confirm that you download information independently or obtain information through EAST services, and are willing to bear any possible system damage, data loss and any other risks.

4.8 Termination of Services: You agree that EAST has the right to terminate the use of your password, account number or any part of the Services (or any part of the Services) for any reason, including, but not limited to, the fact that you have not been using the Services for a long time, or that EAST has violated the letter you have violated D spirit of the Services Agreement, and to remove and delete any content of your Services. Except. You agree to discontinue or terminate the services provided in accordance with this Service Agreement without prior notice. You acknowledge and agree that the Service may close or delete your account and all relevant information and documents in your service Account at any time, or prohibit you from continuing to use the aforementioned documents or services. In addition, you agree that in the event that the use of this service is interrupted, terminated or your account number and related information and documents are closed or deleted, EAST shall not be liable to you or any third party.

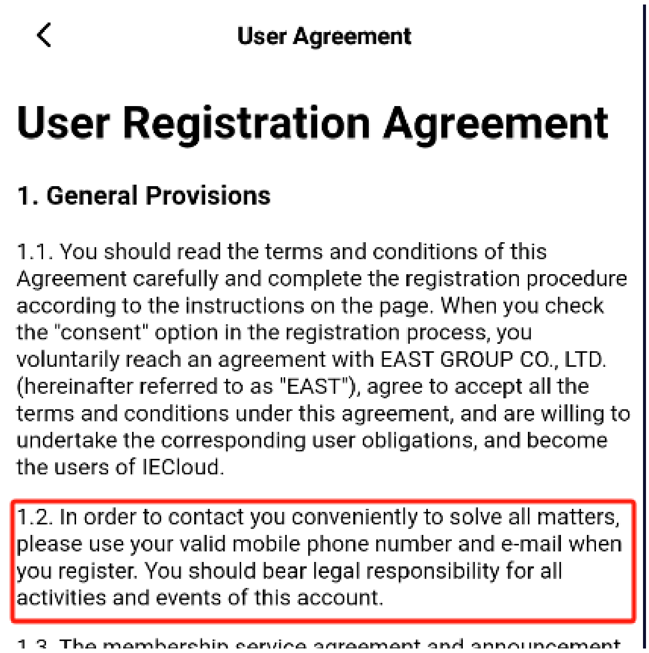
Based on the Documentation of Personal Data in IXIT 2-UserInfo, the manufacturer does not provide relevant information, and according to the user manual, there is an explanation for the collection of the user's cell phone and email address.

The User Agreement stipulates that all content of the Service will be removed and deleted upon termination of the Service by the User or the Service Provider.

However, the service does not provide the user with the function of personal data processing.

The test fails.

TC_DATA_PROTECTION#2 / Test Case 6-1-2	
Security requirement	PROVISION 6-1
Type of work	Doc
Applicability	Conditional(Personal data is processed)
Documentation analysis objectives	The purpose of this test case is the functional assessment of the user information about the processing of personal data.
Evaluation inputs	**“Documentation of Personal Data”** in **IXIT 2-UserInfo** **“Processing Activities”** in **IXIT 21-PersData**
Documentation analysis procedure	a) The tester shall functionally assess whether the provided information about processing personal data (obtained information) is consistent to the description in **"Documentation of Personal Data"** in **IXIT 2-UserInfo**. b) The tester shall functionally assess whether the obtained information about processing personal data accessing the **"Documentation of Personal Data"** in **IXIT 2-UserInfo** match their description in **"Processing Activities"** in **IXIT 21- PersData**. c) The tester shall functionally assess whether the obtained information describes what personal data is processed in a way understandable for a user with limited technical knowledge (cf. ETSI 103 701 Annex D.3). d) d) The tester shall functionally assess whether the obtained information describe how personal data is being used, by whom, and for what purposes in a way understandable for a user with limited technical knowledge (cf.ETSI 103 701 Annex D.3).
Verdict	The verdict **PASS** is assigned if: • The information about processing personal data can be obtained as described; **AND** • The obtained information about processing personal data match their description; **AND** • The personal data being processed is clearly and transparently described; **AND** • It is clearly and transparently described how personal data is being used, by whom, **AND** for what purposes. The verdict **FAIL** is assigned otherwise.
Test Result	
PASS	
Testlab Comments	



User Agreement

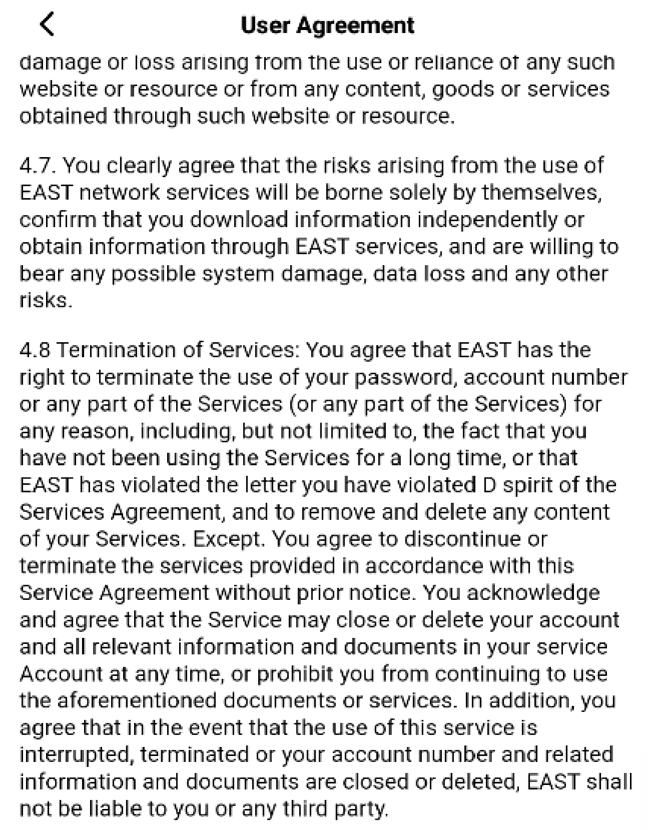
User Registration Agreement

1. General Provisions

1.1. You should read the terms and conditions of this Agreement carefully and complete the registration procedure according to the instructions on the page. When you check the "consent" option in the registration process, you voluntarily reach an agreement with EAST GROUP CO., LTD. (hereinafter referred to as "EAST"), agree to accept all the terms and conditions under this agreement, and are willing to undertake the corresponding user obligations, and become the users of IECloud.

1.2. In order to contact you conveniently to solve all matters, please use your valid mobile phone number and e-mail when you register. You should bear legal responsibility for all activities and events of this account.

1.3. The membership service agreement and announcement



User Agreement

damage or loss arising from the use or reliance of any such website or resource or from any content, goods or services obtained through such website or resource.

4.7. You clearly agree that the risks arising from the use of EAST network services will be borne solely by themselves, confirm that you download information independently or obtain information through EAST services, and are willing to bear any possible system damage, data loss and any other risks.

4.8 Termination of Services: You agree that EAST has the right to terminate the use of your password, account number or any part of the Services (or any part of the Services) for any reason, including, but not limited to, the fact that you have not been using the Services for a long time, or that EAST has violated the letter you have violated D spirit of the Services Agreement, and to remove and delete any content of your Services. Except. You agree to discontinue or terminate the services provided in accordance with this Service Agreement without prior notice. You acknowledge and agree that the Service may close or delete your account and all relevant information and documents in your service Account at any time, or prohibit you from continuing to use the aforementioned documents or services. In addition, you agree that in the event that the use of this service is interrupted, terminated or your account number and related information and documents are closed or deleted, EAST shall not be liable to you or any third party.

Based on the Documentation of Personal Data in IXIT 2-UserInfo, the manufacturer did not provide relevant information, according to the user manual, in order to have the convenience of contacting the user, the user's cell phone and email will be collected.

In addition, the application solicits location information, but confirms this with the manufacturer.

However, we confirmed with the manufacturer that the location information is used for the Bluetooth function and weather information, and no location data is stored or displayed.

This test is passed.

6.17.2.2 Provision 6-2

M C (7): Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.

TC_DATA_PROTECTION#3 / Test Case 6-2-1	
Security requirement	PROVISION 6-2
Type of work	Doc
Applicability	Conditional(Personal data is processed on the basis of consumers' consent)
Document analysis objectives	The purpose of this test case is the conceptual assessment of the consumers' consent for the processing of personal data.
Evaluation inputs	- At least one device suitable for testing - Information related to user consent **("Obtaining Consent"** in **IXIT 21-PersData**)
Document analysis procedure	personal data in **IXIT 21-PersData** that is processed on the basis of consumers' consent according to **"Obtaining Consent",** the tester shall assess whether the opt-in choice: • Is given freely; **AND** • Is given obviously; **AND** • Is given explicitly according to the description of **"Obtaining Consent".**
Verdict	The verdict **PASS** is assigned if for each category of personal data that is processed on the basis of consumers' consent: • It is described how to express consent (opt-in choice) to the processing of personal data for specific purposes; **AND** • The opt-in choice is given freely, obviously and explicitly. The verdict FAIL is assigned otherwise.

Test Result
PASS

Testlab Comments
Based on IXIT 21-PersData, it was confirmed that the user account password, phone number and email address are personal data. This information is entered by the customer during registration. In addition, the application solicits location information, but confirms this with the manufacturer. However, we confirmed with the manufacturer that the location information is used for the Bluetooth function and weather information, and no location data is stored or displayed. This test is passed.

TC_DATA_PROTECTION#4 / Test Case 6-2-2	
Security requirement	PROVISION 6-2
Type of work	Test CAB
Applicability	Conditional (Personal data is processed on the basis of consumers' consent)
Test objectives	The purpose of this test case is the functional assessment of the consumers' consent for the processing of personal data.
Evaluation inputs	- At least one device suitable for testing - Information related to user consent **(“Obtaining Consent”** in **IXIT 21-PersData**)
Test scenario	**Precondition:** ✓ The devices shall be in initial state (before commissioning step) **Test sequence:** ✓ a) For each personal data in **IXIT 21-PersData** that is processed on the basis of consumers' consent according **to "Obtaining Consent",** the tester shall functionally assess whether consumers' consent to processing personal data is obtained as described in the IXIT. - Tester shall perform commissioning step on device, often consents are asked during this step **Expected result:** ✓ Ability to device to obtain consent for personal data processing
Verdict	The verdict **PASS** is assigned if for each category of personal data that is processed on the basis of consumers' consent: • The way of obtaining consumers' consent matches the description. The verdict **FAIL** is assigned otherwise.

Test Result
PASS

Testlab Comments
Based on IXIT 21-PersData, it was confirmed that the user account password, phone number and email address are personal data. This information is entered by the customer during registration. In addition, the application solicits location information, but confirms this with the manufacturer. However, we confirmed with the manufacturer that the location information is used for the Bluetooth function and weather information, and no location data is stored or displayed. This test is passed.

6.17.2.3 Provision 6-3

M C (7): Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.

TC_DATA_PROTECTION#5 / Test Case 6-3-1	
Security requirement	PROVISION 6-3
Type of work	Doc
Applicability	Conditional (Personal data is processed on the basis of consumers’ consent)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of withdrawing consumers' consent for the processing of personal data.
Evaluation inputs	- “Withdrawing Consent” & “Obtaining consent” in **IXIT 21-PersData**
Documentation analysis procedure	a) For each personal data in **IXIT 21-PersData** that is processed on the basis of consumers' consent according to **"Obtaining Consent"**, the tester shall assess whether the information on **"Withdrawing Consent"** describes how to withdraw consent to the processing of personal data at any time by configuring IoT device and service functionality appropriately.
Verdict	The verdict **PASS** is assigned if for each category of personal data that is processed on the basis of consumers' consent: ▪ it is described how to withdraw consent to the processing of personal data at any time. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL

Testlab Comments
The service does not provide the user with personal data processing functionality. This test, failed.

TC_DATA_PROTECTION#6 / Test Case 6-3-2	
Security requirement	PROVISION 6-3
Type of work	Test CAB
Applicability	Conditional (Personal data is processed on the basis of consumers' consent)
Test objectives	The purpose of this test case is the functional assessment of withdrawing consumers' consent for the processing of personal data.
Evaluation inputs	- At least one device suitable for testing - **"Withdrawing Consent"** & **"Obtaining consent"** in **IXIT 21-PersData**
Test scenario	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) For each personal data in **IXIT 21-PersData** that is processed on the basis of consumers' consent according to **"Obtaining Consent",** the tester shall functionally assess whether consumers' consent to processing personal data can be withdrawn as described in **"Withdrawing Consent".** **Expected result:** ✓ Ability for the user to withdraw consent for the processing of its personal data
Verdict	The verdict **PASS** is assigned if for each category of personal data that is processed on the basis of consumers' consent: ✓ The way of withdrawing consumers' consent matches the description. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL

Testlab Comments
The service does not provide the user with personal data processing functionality. This test, failed.

6.17.2.4 Provision 6-4

R C (6): If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality.

TC_DATA_PROTECTION#7 / Test Case 6-4-1	
Security requirement	PROVISION 6-4
Type of work	Doc
Applicability	Conditional (if telemetry data is collected)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the processing of telemetry data.
Evaluation inputs	“Personal Data” in **IXIT 24-TelData**
Documentation analysis procedure	a) The tester shall assess whether the personal data in **IXIT 21-PersData** that are referenced in **"Personal Data"** in **IXIT 24-TelData** is necessary for the intended functionality as described in the **"Purpose"** of collecting the data. **Note**: *Telemetry data are considered to be necessary for the intended functionality if and only if they are needed for achieving the processing purposes.*
Verdict	The verdict **PASS** is assigned if for each telemetry data: ✓ Their processing is necessary for the intended functionality. The verdict **FAIL** is assigned otherwise.

Test Result
PASS

Testlab Comments
The app solicits location information from the user, however, we confirmed with the manufacturer that the location information is only used for Bluetooth functionality and weather information, that no location data is stored or displayed, and that the location information is not used for any other purpose. This test, passed.

6.17.2.5 Provision 6-5

M C (6): If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.

TC_DATA_PROTECTION#8 / Test case 6-5-1	
Security requirement	PROVISION 6-5
Type of work	Doc
Applicability	Conditional (if telemetry data is collected)
Documentation analysis objectives	The purpose of this test case is the conceptual assessment of the user information about the processing of telemetry data.
Evaluation inputs	“Documentation of Telemetry Data” in IXIT 2-UserInfo
Documentation analysis procedure	b) The tester shall assess whether the **"Documentation of Telemetry Data"** in **IXIT 2-UserInfo** is suitable for the consumer to obtain the information about processing telemetry data.
Verdict	The verdict **PASS** is assigned if: - The information about processing telemetry data is suitably provided to the consumer. The verdict FAIL is assigned otherwise.

Test Result
PASS

Testlab Comments
The app solicits location information from the user, however, we confirmed with the manufacturer that the location information is only used for Bluetooth functionality and weather information, that no location data is stored or displayed, and that the location information is not used for any other purpose. This test, passed.

TC_DATA_PROTECTION#9 / Test Case 6-5-2	
Security requirement	PROVISION 6-5
Type of work	Doc
Applicability	Conditional (Telemetry data being collected)
Document objectives	The purpose of this test case is the functional assessment of user the information about the processing of telemetry data.
Evaluation inputs	- "Documentation of Telemetry Data" in IXIT 2-UserInfo - List of telemetry data collected by DUT (IXIT 24-TelData)
Document analysis procedure	**Precondition:** ✓ The devices shall be operating under normal conditions. **Test sequence:** ✓ a) The tester shall functionally assess whether the provided information about processing telemetry data (obtained information) is consistent with the description in **"Documentation of Telemetry Data"** in **IXIT 2-UserInfo.** ✓ b) The tester shall functionally assess whether the obtained information about processing telemetry data accessing the **"Documentation of Telemetry Data"** in **IXIT 2-UserInfo** match their **"Purpose"** described in **IXIT 24-TelData.** ✓ c) The tester shall functionally check whether the obtained information describes what telemetry data is collected. ✓ d) The tester shall functionally check whether the obtained information describes how telemetry data is being used, by whom, and for what purposes.
Verdict	The verdict **PASS** is assigned if: • The information about processing telemetry data can be obtained as described; and • The obtained information about processing telemetry data match their description; and • The telemetry data being collected is described; and • Tt is completely described how telemetry data is being used, by whom, and for what purposes. The verdict **FAIL** is assigned otherwise.

Test Result
FAIL

Testlab Comments
Documentation of Telemetry Data based on IXIT 2-UserInfo, no information provided by manufacturer. So there is no description of the location information obtained by the application and the user has no way of knowing what the information is used for. This test, failed.

Annex 1 - Photo of the unit

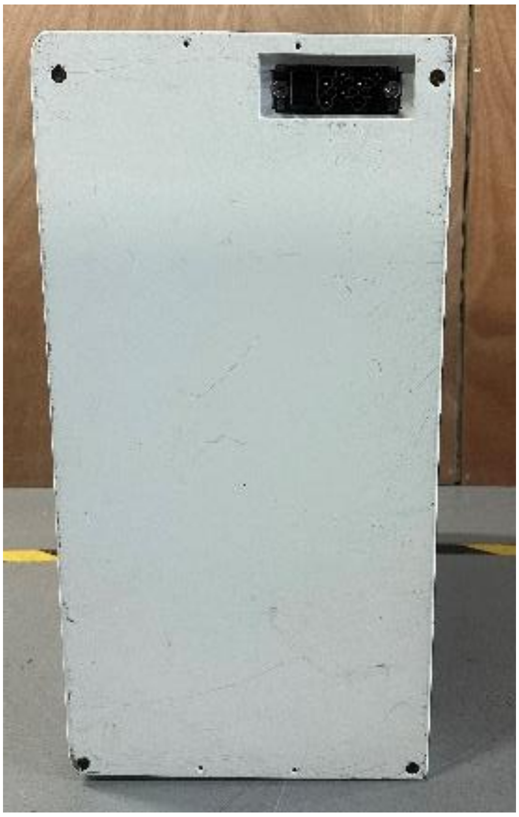
Enclosure front view

Enclosure side view-1

Enclosure side view-2

Enclosure top view

Enclosure bottom view



Enclosure rear view

»»» End of Test Report «««