



中国认可
国际互认
检测
TESTING
CNAS L6451



Guangdong Dongdian Testing Service Co., Ltd.

Test Report

Applicant	:	XGIMI Technology Co., Ltd.
Address of applicant	:	Building No.4, Zone A, No.1129, Shijicheng Road, Chengdu High-tech Zone, Sichuan Pilot Free Trade Zone, China.
Equipment under Test	:	Projector
Model No.	:	XR06B, XR03B, XR08B, XR03E, XR04E, XR06E, XR07E, XR08E, XR09E, XR08G, XR09G, XR10G, XR06H, XR07H, XR08H
Trademark	:	N/A
Manufacturer	:	XGIMI Technology Co., Ltd.
Address of manufacture	:	Building No.4, Zone A, No.1129, Shijicheng Road, Chengdu High-tech Zone, Sichuan Pilot Free Trade Zone, China.
Test Standards:	:	EN 18031-1:2024

Issued By: Guangdong Dongdian Testing Service Co., Ltd.

Add: Unit 2,Building 1,No.17,Zongbu 2nd Road, Songshan Lake Park,
Dongguan,Guangdong, China, 523808

Tel: +86-0769-38826678, E-mail: ddt@dgddt.com, <http://www.dgddt.com>

REPORT

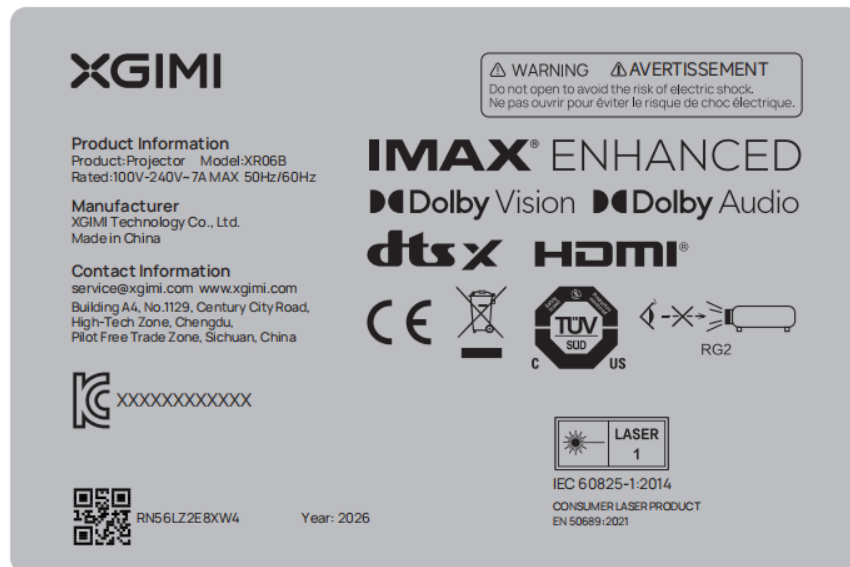
TEST REPORT EN 18031-1:2024 Common security requirements for radio equipment - Part 1: Internet connected radio equipment	
Report No.:	DDT-RE25111708-1F02
Tested by (+ signature)	Aston Xie
Approved by (+ signature).....	Hami Zeng
Date of issue	2026/01/28
Total number of pages.....	118
Testing Laboratory.....	Guangdong Dongdian Testing Service Co., Ltd.
Testing location/Address	Unit 2,Building 1,No.17,Zongbu 2nd Road, Songshan Lake Park, Dongguan,Guangdong, China, 523808
Applicant.....	XGIMI Technology Co., Ltd.
Address.....	Building No.4, Zone A, No.1129, Shijicheng Road, Chengdu High-tech Zone, Sichuan Pilot Free Trade Zone, China.
Manufacturer.....	XGIMI Technology Co., Ltd.
Address.....	Building No.4, Zone A, No.1129, Shijicheng Road, Chengdu High-tech Zone, Sichuan Pilot Free Trade Zone, China.
Test specification:	
Standards	EN 18031-1:2024
Model differences:	
Models XR06B, XR03B, XR08B, XR03E, XR04E, XR06E, XR07E, XR08E, XR09E, XR08G, XR09G, XR10G, XR06H, XR07H, and XR08H adopt the same cyber security mechanism. The differences lie in the Wi-Fi modules, Bluetooth modules, firmware versions, hardware versions and interfaces of different models. However, these differences do not affect the evaluation and test results of Article 3.3 of the EU RED. Therefore, the test was conducted on the main test model of the Projector, XR06B.	
We Declare:	
The equipment described above is tested by Guangdong Dongdian Testing Service Co., Ltd. and in the configuration tested the equipment complied with the standards specified above. The test results are contained in this test report and Guangdong Dongdian Testing Service Co., Ltd. is assumed of full responsibility for the accuracy and completeness of these tests.	
Test item description.....	Projector
Trade Mark(s)	N/A



Model/Type reference.....:	XR06B, XR03B, XR08B, XR03E, XR04E, XR06E, XR07E, XR08E, XR09E, XR08G, XR09G, XR10G, XR06H, XR07H, XR08H
Human user interfaces.....:	Buttons, LEDs, IR/BT remote control, On-screen display (OSD) menu
Communication interfaces	Wi-Fi, Bluetooth, Ethernet (LAN), RS-232 (serial control)
Local interfaces.....:	AC IN, SERVICE, USB 2.0, USB 3.0, REMOTE, AUDIO, RS232 IN, HDMI1/eARC, HDMI2, LAN, OPTICAL
Android IoT app versions.....:	N/A
iOS IoT app versions	N/A
Firmware/software versions	V2.0.8
Hardware versions.....:	11-000109-001
Possible test case verdicts:	
- test case was not evaluated	N/A
- test object meets the requirement:	P (Pass)
- test object does not meet the requirement.....:	F (Fail)
Testing:	
Date of receipt of test item.....:	2025-12-09
Start date of performance of tests .:	2025-12-09
Completion date of performance of tests	2025-01-23
Summary of testing:	
The equipment evaluation is carried out based on the relevant documents and samples provided by the manufacturer.	
This product has been evaluated and tested in accordance with the requirements of Standard EN 18031 - 1:2024. The results are as follows:	
Pass: 22	
Fail: 0	
N/A: 11	
The evaluation and testing of this product meet the requirements of RED 3.3 (d). It can protect the security assets and network assets from common cybersecurity threats and will not be exploited by security vulnerabilities that are publicly known.	
The evaluation results are limited to the samples under test.	

Product information:**Copy of the marking plate(Label):**

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

**Picture of the product:****Test Sample SN: XZD9R169ZYXX**

1. Summary of test results

No.	Test items	Verdict
1	[ACM] Access control mechanism	
1.1	[ACM-1] Applicability of access control mechanisms	Pass
1.2	[ACM-2] Appropriate access control mechanisms	Pass
2	[AUM] Authentication mechanism	
2.1	[AUM-1] Applicability of authentication mechanisms	
2.1.1	[AUM-1-1] Requirement network interface	Pass
2.1.2	[AUM-1-2] Requirement user interface	N/A
2.2	[AUM-2] Appropriate authentication mechanisms	Pass
2.3	[AUM-3] Authenticator validation	Pass
2.4	[AUM-4] Changing authenticators	Pass
2.5	[AUM-5] Password strength	
2.5.1	[AUM-5-1] Requirement for factory default passwords	N/A
2.5.2	[AUM-5-2] Requirement for non-factory default passwords	N/A
2.6	[AUM-6] Brute force protection	Pass
3	[SUM] Secure update mechanism	
3.1	[SUM-1] Applicability of update mechanisms	Pass
3.2	[SUM-2] Secure updates	Pass
3.3	[SUM-3] Automated updates	Pass
4	[SSM] Secure storage mechanism	
4.1	[SSM-1] Applicability of secure storage mechanisms	N/A

No.	Test items	Verdict
4.2	[SSM-2] Appropriate integrity protection for secure storage mechanisms	N/A
4.3	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	N/A
5	[SCM] Secure communication mechanism	
5.1	[SCM-1] Applicability of secure communication mechanisms	Pass
5.2	[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	Pass
5.3	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	Pass
5.4	[SCM-4] Appropriate replay protection for secure communication mechanisms	Pass
6	[RLM] Resilience mechanism	
6.1	[RLM-1] Applicability and appropriateness of resilience mechanisms	Pass
7	[NMM] Network monitoring mechanism	
7.1	[NMM-1] Applicability and appropriateness of network monitoring mechanisms	N/A
8	[TCM] Traffic control mechanism	
8.1	[TCM-1] Applicability of and appropriate traffic control mechanisms	N/A
9	[CCK] Confidential cryptographic keys	
9.1	[CCK-1] Appropriate CCKs	Pass
9.2	[CCK-2] CCK generation mechanisms	Pass
9.3	[CCK-3] Preventing static default values for preinstalled CCKs	N/A
10	[GEC] General equipment capabilities	
10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	Pass

No.	Test items	Verdict
10.2	[GEC-2] Limit exposure of services via related network interfaces	Pass
10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces	Pass
10.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces	N/A
10.5	[GEC-5] No unnecessary external interfaces	Pass
10.6	[GEC-6] Input validation	Pass
11	[CRY] Cryptography	
11.1	[CRY-1] Best practice cryptography	N/A

2. Test environment

2.1 Test software and hardware items

No.	Hardware environment		Software environment
	Name/Model	Configuration (CPU/RAM/HDD)	
1	Lenovo Laptop/ Xiaoxin Pro16/ DDT-ZC04156	CPU main frequency:2.50GHz RAM:16GB HDD:512GB	1. Windows 11 Professional Edition/ Client Operating System; 2. VMware Workstation Pro 17/ Virtual Machine; 3. Kali Linux v2024.3/ Penetration testing tool; 4. Wireshark 4.2.4/ packet capture tool; 5. Zenmap 7.95 / port scanning tool; 6. Hping3 / network analysis tool; 7. binwalk v2.4.3 / tool for firmware reverse engineering and data analysis; 8. Btscanner 2.0/ Bluetooth scanning tool; 9. blueman-manager 2.4.3/ Bluetooth management tool; 10. bluetoothctl 5.79/ An interactive command-line tool for controlling Bluetooth devices; 11. Wireless Protocol Suite 2.50/ Bluetooth protocol analysis tool;

			12. ssllscan 2.1.5 / A command-line tool used to scan and test the SSL/TLS security configurations of network services; 13. Nessus 10.8.3/ Vulnerability Scanning Tool. 14. OKScan 2.0.327 (Vulnerability Database Version: 2.0.327.11301708)/ vulnerability scanning tool.
Network environment: The Internet.			

3. Common security requirements for radio equipment

3.1 [ACM] Access control mechanism

3.1.1 [ACM-1] Applicability of access control mechanisms

--Conceptual assessment--

Identifier [ACM-1]-S01	[E.Info.ACM-1.SecurityAsset]: SecurityAsset-1.1: HTTPS certificate SecurityAsset-1.2: Wi-Fi password SecurityAsset-1.3: The AES-CCM-128 encryption key used in the Bluetooth 5.2 protocol is generated through negotiation during the first pairing process and then stored in the device's flash memory. SecurityAsset-1.4: Public Key for OTA Signature Verification		
Decision node	Decision		Justification
	[E.Info.DT.ACM-1]		[E.Just.DT.ACM-1]
DT.ACM-1.DN-2	Yes (√)	No	[E.Info.ACM-1.SecurityAsset.Access]: The asset is stored inside the device, protected by its outer casing, with no interface available for accessing the asset. [E.Info.ACM-1.SecurityAsset.Environment]: The asset is stored inside the device, protected by its outer casing, with no interface available for accessing the asset.
Assignment of verdict:	N/A		

Identifier [ACM-1]-S02	[E.Info.ACM-1.SecurityAsset]: SecurityAsset-2.1: The DUT connects to the server via Wi-Fi. SecurityAsset-2.2: The DUT connects to the server via Ethernet. SecurityAsset-2.3: Perform over-the-air (OTA) firmware updates for devices via the OTA server.		
Decision node	Decision		Justification
	[E.Info.DT.ACM-1]		[E.Just.DT.ACM-1]
DT.ACM-1.DN-4	Yes (√)	No	[E.Info.ACM-1.SecurityAsset.Access]: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity

			verification and key exchange mechanisms are employed to establish an encrypted connection for authentication. [E.Info.ACM-1.SecurityAsset.ACM]: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.
Assignment of verdict:	Pass		

Identifier [ACM-1]-S03	[E.Info.ACM-1.SecurityAsset]: SecurityAsset-3.1: Bluetooth pairing code.		
Decision node	Decision [E.Info.DT.ACM-1]	Justification [E.Just.DT.ACM-1]	
DT.ACM-1.DN-2	Yes (√)	No	[E.Info.ACM-1.SecurityAsset.Access] The device adopts authentication-based access control measures to restrict the acquisition and use of the Bluetooth pairing code to authorized entities only. The user shall manually confirm the pairing code displayed on the device screen, and input the same code on the paired terminal to complete the access authorization. [E.Info.ACM-1.SecurityAsset.Environment] In the equipment's targeted operational environment, the Bluetooth pairing code is not transmitted in plaintext and is only displayed locally on the device screen for a limited time. Unauthorized entities cannot obtain the pairing code through non-physical contact or eavesdropping, thus ensuring the confidentiality of the security asset in the deployment environment.
Assignment of verdict:	N/A		

Identifier [ACM-1]-S04	[E.Info.ACM-1.SecurityAsset]: SecurityAsset-4.1: Reset the Device. SecurityAsset-4.2: Local Upgrade via USB.		
Decision node	Decision [E.Info.DT.ACM-1]	Justification [E.Just.DT.ACM-1]	
DT.ACM-1.DN-2	Yes (√)	No	[E.Info.ACM-1.SecurityAsset.Access]: Physical access to the DUT itself is required to access this asset. [E.Info.ACM-1.SecurityAsset.Environment]: Physical access to the DUT itself is required to access this asset.
Assignment of verdict:	N/A		

Identifier [ACM-1]-N01	[E.Info.ACM-1.NetworkAsset]: NetworkAsset-1.1: Bluetooth Connection Function NetworkAsset-1.2: Wi-Fi Connection Function		
---------------------------	--	--	--

	NetworkAsset-1.3: WLAN Wireless Client Function		
Decision node	Decision		Justification
	[E.Info.DT.ACM-1]		[E.Just.DT.ACM-1]
DT.ACM-1.DN-2	Yes (√)	No	[E.Info.ACM-1.NetworkAsset.Access]: Physical access to the DUT itself is required to access this asset. [E.Info.ACM-1.NetworkAsset.Environment]: Physical access to the DUT itself is required to access this asset.
Assignment of verdict:	N/A		

Identifier [ACM-1]-N02	[E.Info.ACM-1.NetworkAsset]: NetworkAsset-2.1: IP address/MAC address		
Decision node	Decision		Justification
	[E.Info.DT.ACM-1]		[E.Just.DT.ACM-1]
DT.ACM-1.DN-1	Yes (√)	No	[E.Info.ACM-1.NetworkAsset.Access]: The asset can be viewed on the device's network configuration page. [E.Info.ACM-1.NetworkAsset.PublicAccess]: The asset can be viewed on the device's network configuration page.
Assignment of verdict:	N/A		

Identifier [ACM-1]-N03	[E.Info.ACM-1.NetworkAsset]: NetworkAsset-3.1: The device can create its own hotspot, allowing mobile phones to connect and access the internet.		
Decision node	Decision		Justification
	[E.Info.DT.ACM-1]		[E.Just.DT.ACM-1]
DT.ACM-1.DN-2	Yes (√)	No	[E.Info.ACM-1.NetworkAsset.Access]: The device adopts credential-based access control measures to restrict the connection to the built-in AP hotspot to authorized entities only. The AP hotspot is disabled by default at factory settings and must be manually enabled by the user on the device before use. The user shall manually obtain the AP hotspot SSID and access password displayed locally on the device, and input the correct password on the client terminal to complete the network access authentication. Unauthorized entities without valid credentials cannot establish a connection to the AP hotspot. [E.Info.ACM-1.NetworkAsset.Environment]: In the equipment's targeted operational environment, the AP hotspot's access password is not transmitted in plaintext during the authentication process. The SSID and password are only displayed locally on the device for a limited time. The data transmitted through the AP hotspot is encrypted via the WPA3 protocol, preventing unauthorized eavesdropping or tampering of data in the wireless environment.
Assignment of verdict:	N/A		

Identifier	[E.Info.ACM-1.NetworkAsset]:
------------	------------------------------

[ACM-1]-N04		NetworkAsset-4.1: RS232 Physical Interface	
Decision node	Decision		Justification
	[E.Info.DT.ACM-1]		[E.Just.DT.ACM-1]
DT.ACM-1.DN-2	Yes (√)	No	[E.Info.ACM-1.NetworkAsset.Access]: The device restricts the access permission of the RS232 physical interface to authorized maintenance personnel only. The operator shall obtain valid operation authorization and use dedicated serial communication equipment to connect to the RS232 interface for local debugging, configuration modification, and log export. Unauthorized personnel cannot access the interface due to physical isolation and authorization management. [E.Info.ACM-1.NetworkAsset.Environment]: The RS232 interface is typically used for short-distance serial communication between two devices (such as computers and modems, or industrial controllers and peripherals), transmitting data in a single-ended manner with relatively limited transmission distance and noise immunity. Physical access via wiring or connectors is required to enable its signal transmission and device control functions.
Assignment of verdict:	N/A		

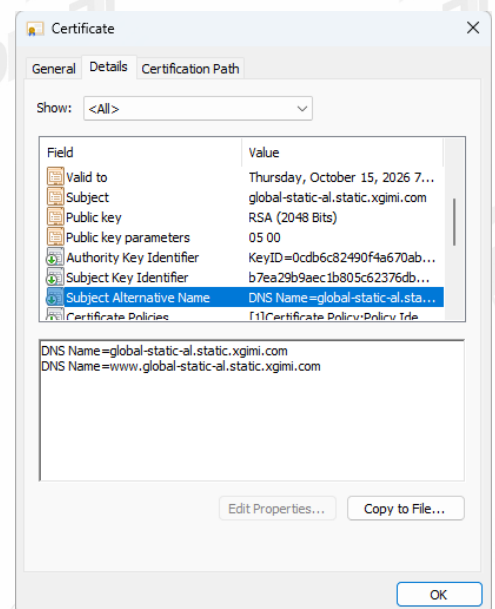
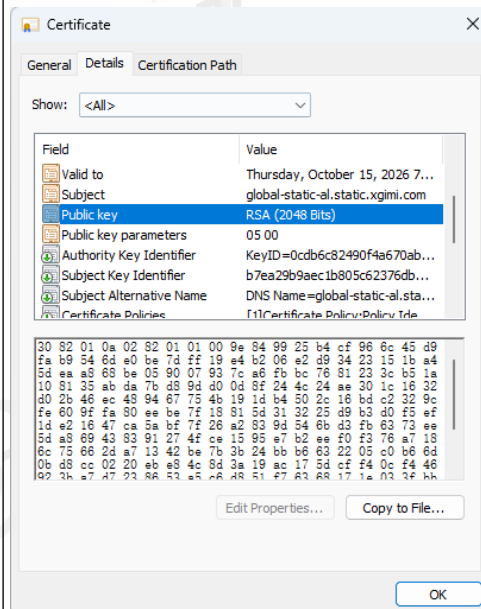
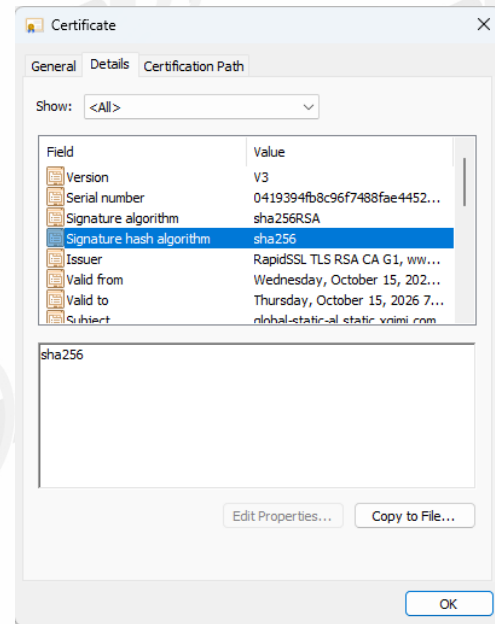
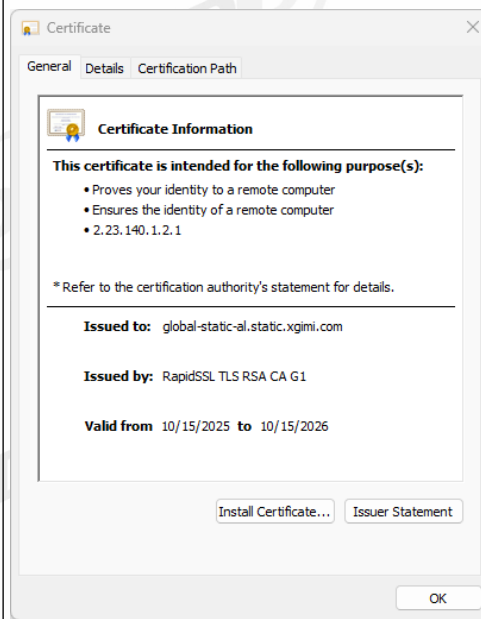
Identifier [ACM-1]-N05		[E.Info.ACM-1.NetworkAsset]: NetworkAsset-5.1: Paired Devices Access Rights NetworkAsset-5.2: Saved Wi-Fi Networks NetworkAsset-5.3: Network configuration parameters	
Decision node	Decision		Justification
	[E.Info.DT.ACM-1]		[E.Just.DT.ACM-1]
DT.ACM-1.DN-2	Yes (√)	No	[E.Info.ACM-1.NetworkAsset.Access]: Physical contact with the device is required to access this asset. [E.Info.ACM-1.NetworkAsset.Environment]: Physical contact with the device is required to access this asset.
Assignment of verdict:	N/A		

--Completeness testing--

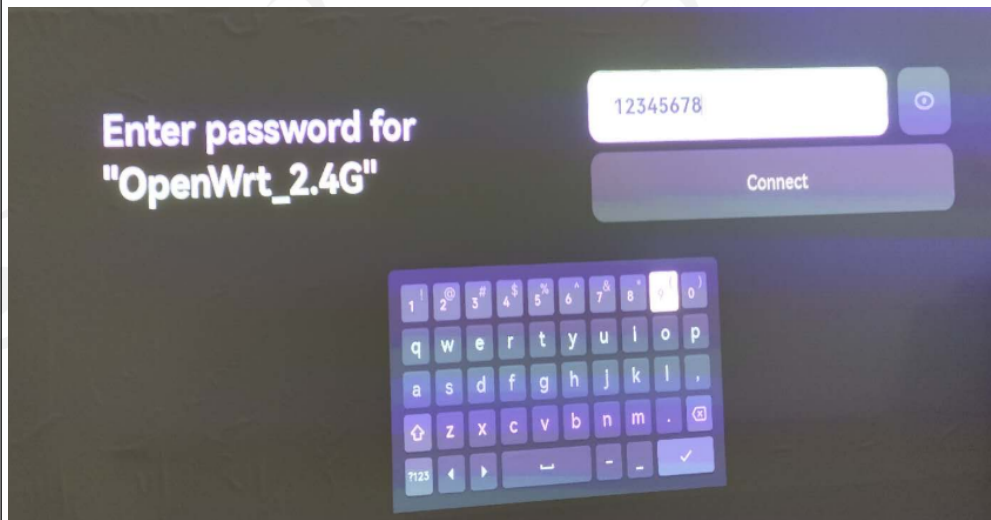
Assessment purpose:	The purpose of the functional assessment is to verify that all the security assets and network assets that are accessible by entities, are documented in [E.Info.ACM-1.NetworkAsset] or [E.Info.ACM-1.SecurityAsset].
Preconditions:	The equipment is in an operational state.
Operation steps:	Functionally assess whether there are security assets, that are accessible by entities, in the equipment, which are not documented in [E.Info.ACM-1.SecurityAsset] and whether there are network assets, that are accessible by entities, in the equipment, which are not documented in [E.Info.ACM-1.NetworkAsset], e.g. by inspecting all parts of the software such as built-in software, installed applications and interfaces for connected peripherals.
Result:	All discovered security assets are recorded in [E.Info.ACM-1.SecurityAsset], and all discovered

network assets are recorded in [E.Info.ACM-1.NetworkAsset].

SecurityAsset-1.1: HTTPS certificate



SecurityAsset-1.2: Wi-Fi password



SecurityAsset-1.3: AES-CCM-128 encryption key

Frame 1,431: (Central) Len=30

- Baseband:
 - LMP:
 - Link: 2
 - Role: Central
 - Address: 1
 - Opcode: LMP_encryption_key_size_req
 - Transaction ID: Initiated by central
 - Key Size: 16 bytes

Decode Device Database

Bluetooth Security

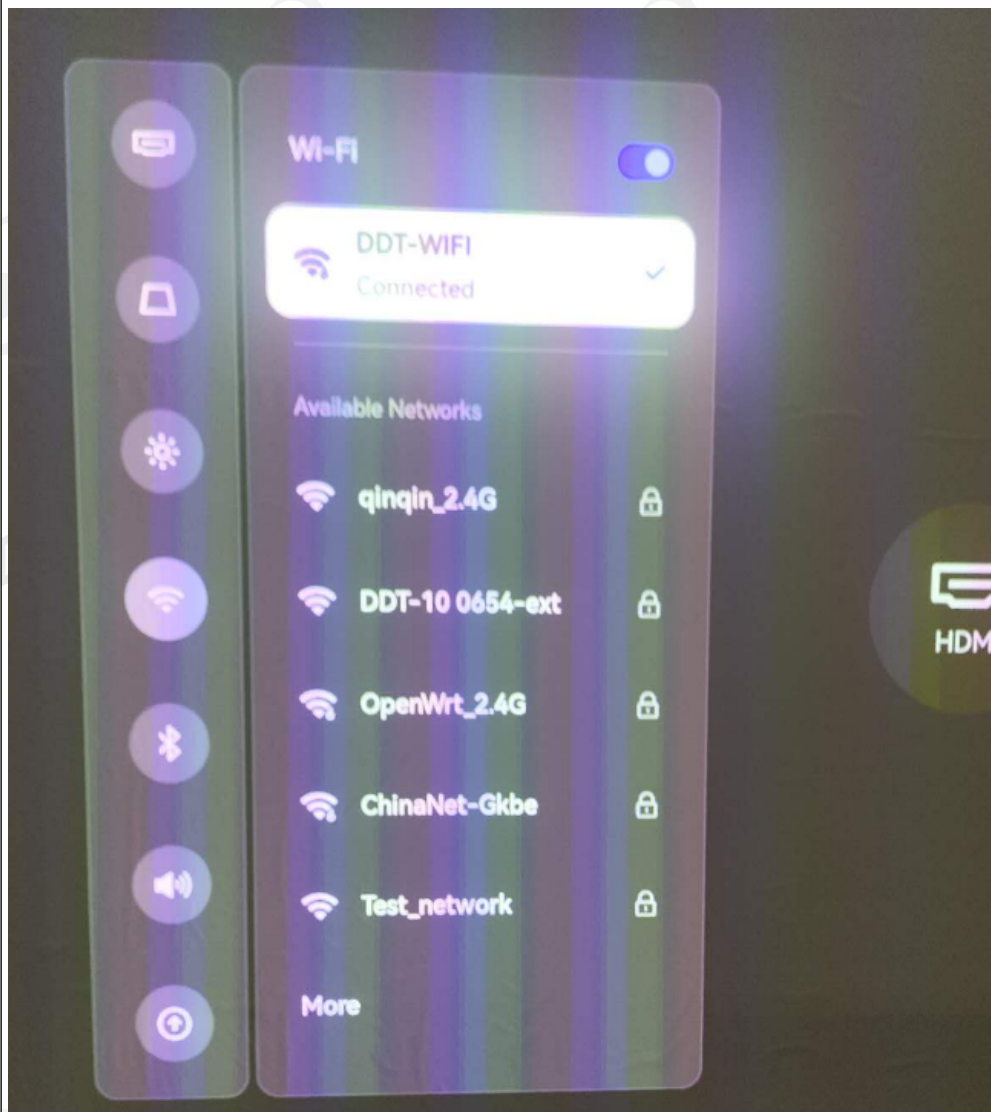
Show: All Security Events ▼

Time	Central & Peripheral
1/4/2026 9:32:07.53515...	DC:EC:4F:27:5A:68
...	"KENWOOD GLASS Core" 5C:8E:8B:9C:7A:13

SecurityAsset-1.4: Public Key for OTA Signature Verification

```
L$ openssl x509 -in otacert.cer -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            d0:19:71:b3:8a:35:de:b8
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=SHICHUAN, L=CHENGDU, O=XGIMI_CO_LTD, OU=XGIMI, CN=XGIMI, emailAddress=www.xgimi.com
        Validity
            Not Before: Sep 28 07:43:04 2018 GMT
            Not After : Feb 13 07:43:04 2046 GMT
        Subject: C=CN, ST=SHICHUAN, L=CHENGDU, O=XGIMI_CO_LTD, OU=XGIMI, CN=XGIMI, emailAddress=www.xgimi.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:ba:11:71:12:02:7d:19:a7:56:cd:5b:b9:14:67:
                60:82:da:36:1b:c1:b2:95:e1:88:00:0f:0a:35:09:
                84:63:b1:9e:c4:1c:1e:d7:eb:da:2d:e0:9d:81:3c:
                0c:c3:46:07:d7:16:7a:0c:ab:4a:b2:ae:ba:9d:90:
                92:11:e8:4d:a8:8b:cb:4c:42:c1:b7:c4:73:fe:41:
                df:1d:b9:62:8d:c4:b0:ba:a9:56:57:be:2c:ed:b5:
                c5:47:9e:e3:4d:f6:ba:53:79:81:02:0e:e8:60:54:
                fd:21:5a:78:71:5e:ad:d3:a8:b5:b2:ec:d6:2a:a7:
                a4:e1:f1:48:ba:6e:af:db:b8:6c:15:2e:96:f2:ad:
                8b:3b:3c:54:7a:2d:b1:df:0f:cd:d6:d9:8e:68:83:
                6c:f2:2c:b6:09:42:ea:29:9b:7d:e1:f2:ba:8d:97:
                5d:66:8e:34:57:26:78:c2:e9:18:91:f3:9f:87:e8:
                12:9d:4f:dd:4b:e2:6d:81:3a:a3:a2:65:3f:9d:04:
                ad:19:b6:ee:02:ba:71:65:af:4a:2a:ed:6f:8e:81:
                e7:96:7b:ae:69:60:a2:fb:fb:94:d0:ae:7d:97:ba:
                aa:00:7a:4b:dd:66:0d:f7:ac:72:bc:28:45:2e:a6:
                b8:93:26:5f:99:64:1e:eb:e8:93:1c:da:07:d1:f9:
                da:b9
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                15:35:18:20:72:26:8D:84:03:C0:B2:E3:71:56:9C:E1:07:D0:E5:4D
            X509v3 Authority Key Identifier:
                15:35:18:20:72:26:8D:84:03:C0:B2:E3:71:56:9C:E1:07:D0:E5:4D
            X509v3 Basic Constraints: critical
                CA:TRUE
        Signature Algorithm: sha256WithRSAEncryption
        Signature Value:
            9c:0d:b4:ad:3d:12:bc:79:45:32:72:d1:d8:38:3e:a0:aa:f9:
            f8:3f:84:9a:55:9a:05:ae:e8:87:d2:b2:e8:b1:c1:03:9b:a8:
            91:2a:e7:ae:fb:49:36:38:12:5a:e3:17:12:52:a4:79:e4:ac:
            3b:e6:ab:a3:2b:fd:66:3d:72:d7:4c:1b:7e:0d:de:87:a6:b6:
            8d:00:34:48:a4:95:ec:f3:a6:76:7a:66:6d:7c:4b:ad:f6:84:
            04:91:cd:93:ad:23:28:f7:1c:49:d8:82:da:0d:01:de:ac:44:
            1b:1a:61:e7:37:44:8d:f2:a9:c1:2c:bb:82:4f:d0:5c:81:b4:
```

SecurityAsset-2.1: The DUT connects to the server via Wi-Fi.



securityAsset-2.2: The DUT connects to the server via Ethernet.

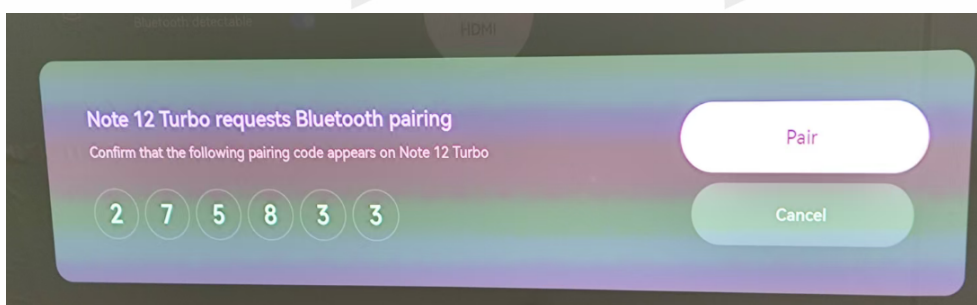


SecurityAsset-2.2: Perform over-the-air (OTA) firmware updates for devices via the OTA server.

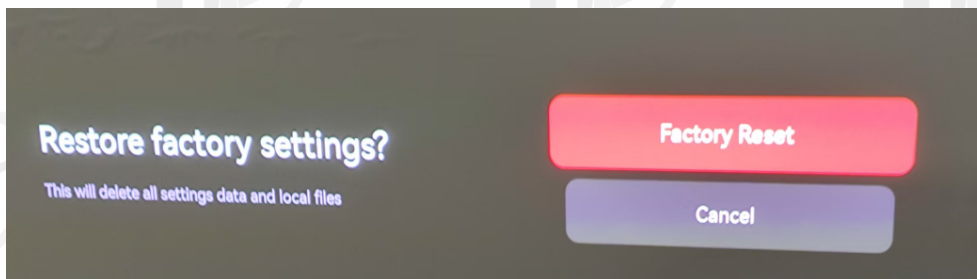
356	49.581956	222.217.94.16	192.168.137.7	TLSv1.3	1514	Application Data
373	49.610833	192.168.137.7	222.217.94.17	TLSv1.3	618	Client Hello (SHI=global-static-al.static.xgimi.com)
404	49.686563	222.217.94.17	192.168.137.7	TLSv1.3	1514	Server Hello, Change Cipher Spec, Application Data
408	49.767946	222.217.94.17	192.168.137.7	TLSv1.3	1514	Application Data
409	49.768046	222.217.94.17	192.168.137.7	TLSv1.3	251	Application Data, Application Data
412	49.808821	192.168.137.7	222.217.94.17	TLSv1.3	118	Change Cipher Spec, Application Data
413	49.887222	222.217.94.17	192.168.137.7	TLSv1.3	365	Application Data
414	49.888438	222.217.94.17	192.168.137.7	TLSv1.3	365	Application Data

> Ethernet II, Src: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1), Dst: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1)
> Internet Protocol Version 4, Src: 192.168.137.7, Dst: 222.217.94.17
> Transmission Control Protocol, Src Port: 36888, Dst Port: 443, Seq: 1, Ack: 1, Len: 564
▼ Transport Layer Security
 [Stream index: 8]
 ▼ TLSv1.3 Record Layers: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.0 (0x0301)
 Length: 559
 ▼ Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 555
 > Version: TLS 1.2 (0x0303)
 Random: c0673901c52b8fdacald1399b6c9065a3f997b5d63bb687d80d2d70020dc8a
 Session ID Length: 32
 Session ID: 90cefa15de2911bf76b1dba64f1e2e411967ebca510a94dda91a3ad8df9607
 Cipher Suites Length: 30
 > Cipher Suites (15 suites)
 Compression Methods Length: 1
 > Compression Methods (1 method)
 Extensions Length: 452
 > Extension: server_name (len=38) name=global-static-al.static.xgimi.com

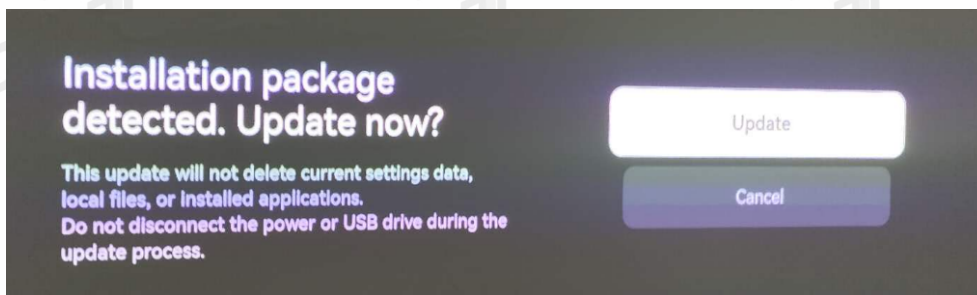
SecurityAsset-3.1: Bluetooth pairing code



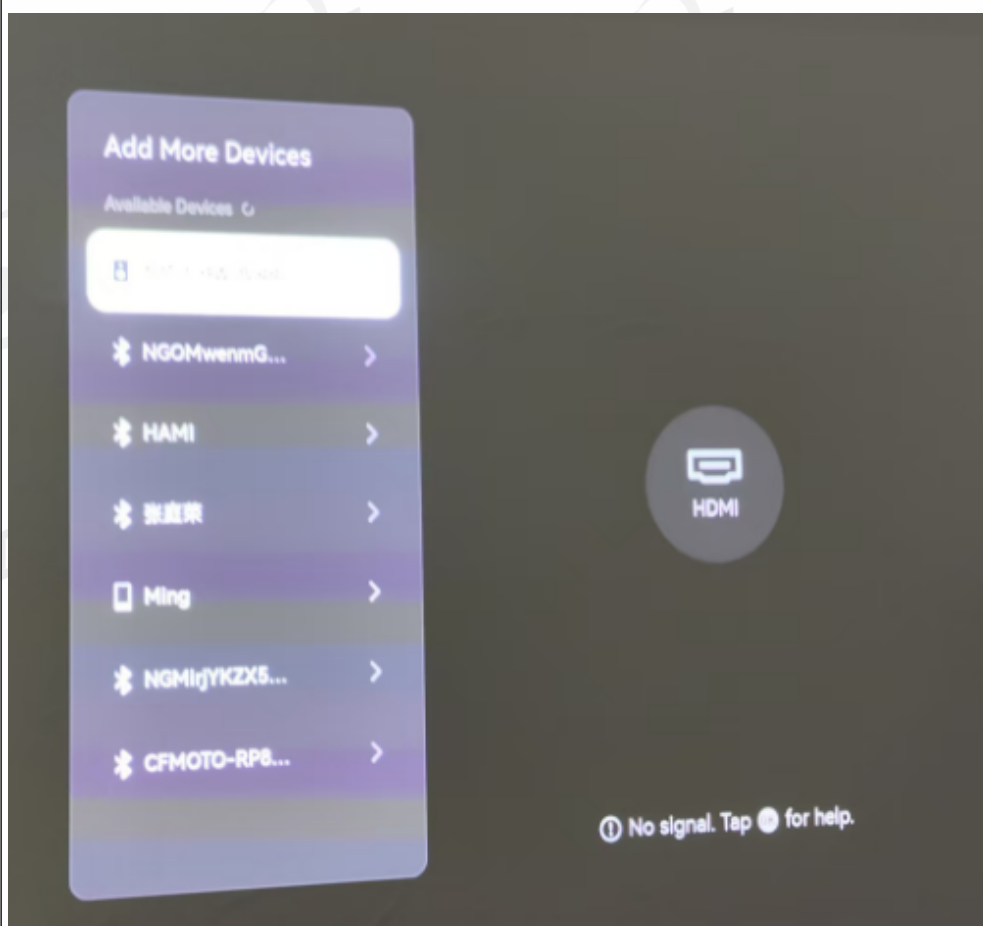
SecurityAsset-4.1: Reset the Device



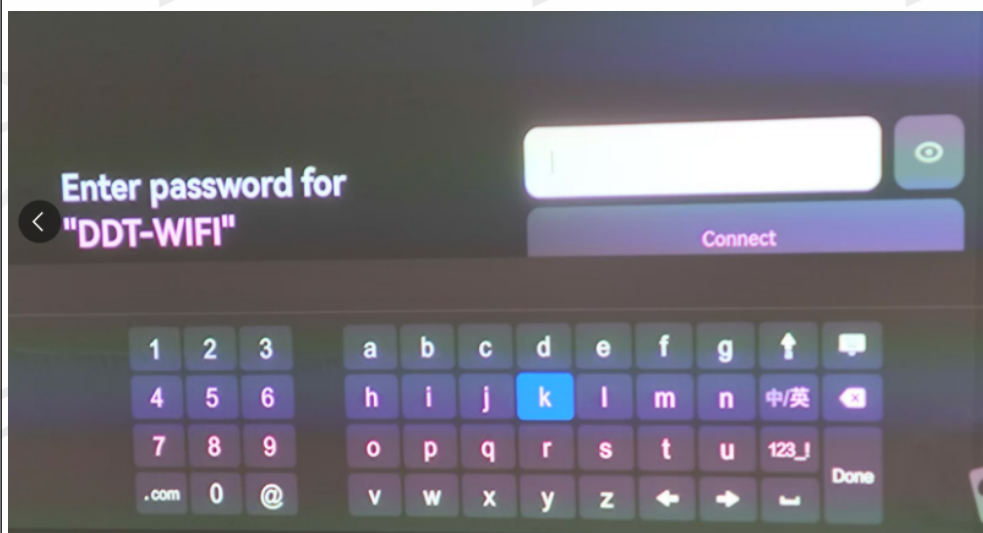
SecurityAsset-4.2: Local Upgrade via USB.



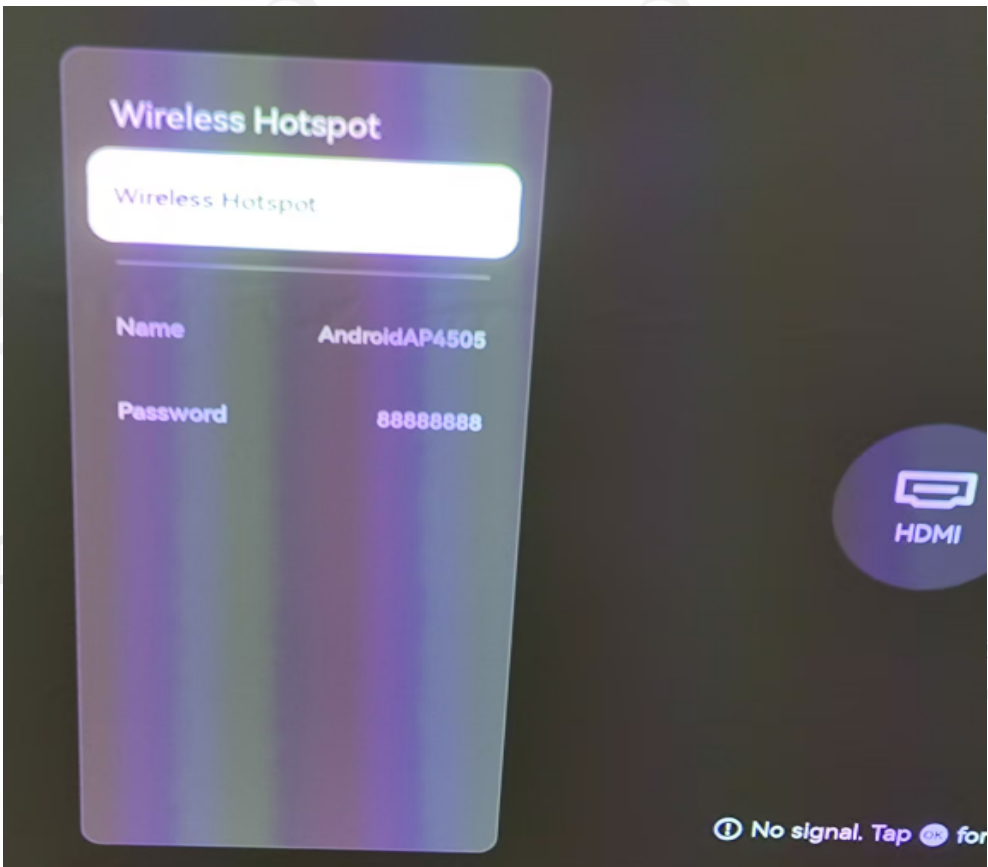
NetworkAsset-1.1: Bluetooth Connection Function



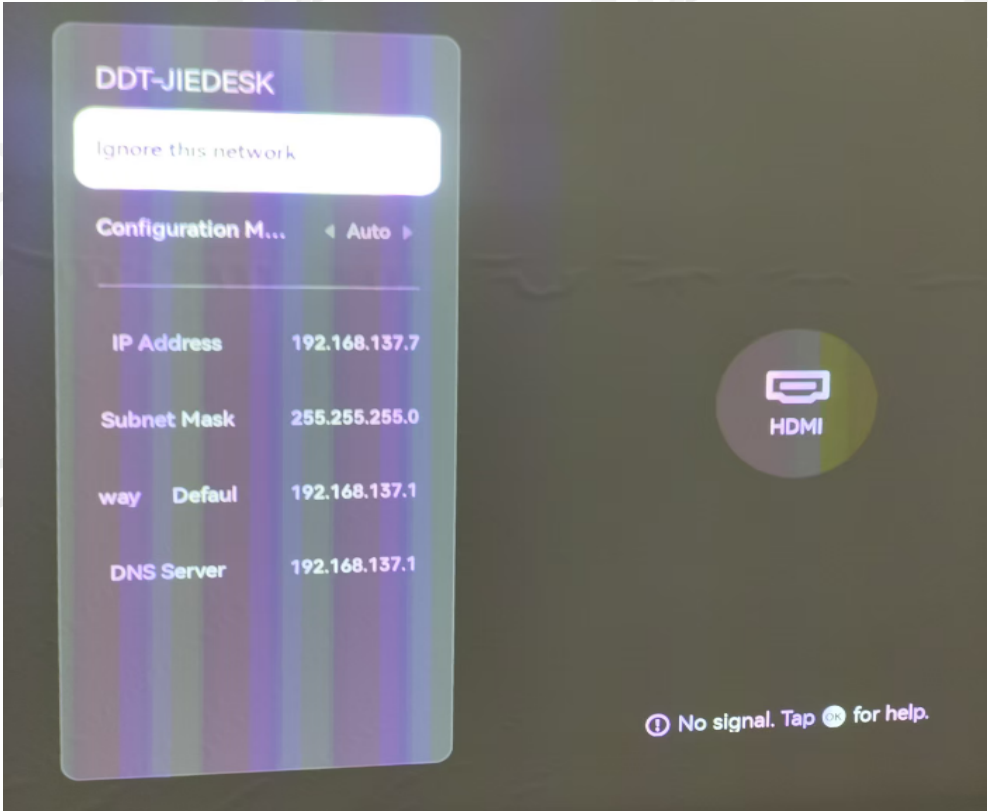
NetworkAsset-1.2: Wi-Fi Connection Function

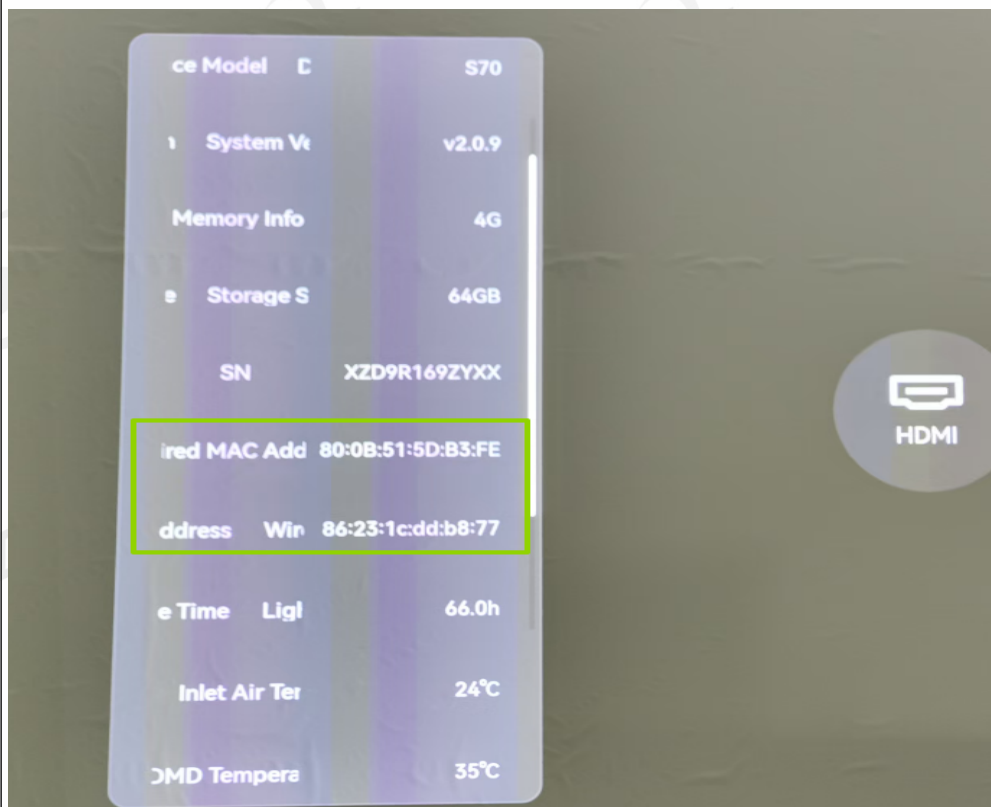


NetworkAsset-1.3: WLAN Wireless Client Function



NetworkAsset-2.1: IP address/MAC address





NetworkAsset-3.1: The device can create its own hotspot, allowing mobile phones to connect and access the internet.

AndroidAP3938 network details

Connect automatically ☒


Status
Connected


Technology
Generation 4


Connection speed
144Mbps


Signal strength
Excellent


Security
WPA3-Personal


IP address
fe80::7857:e0ff:fe22:31ae
192.168.66.178

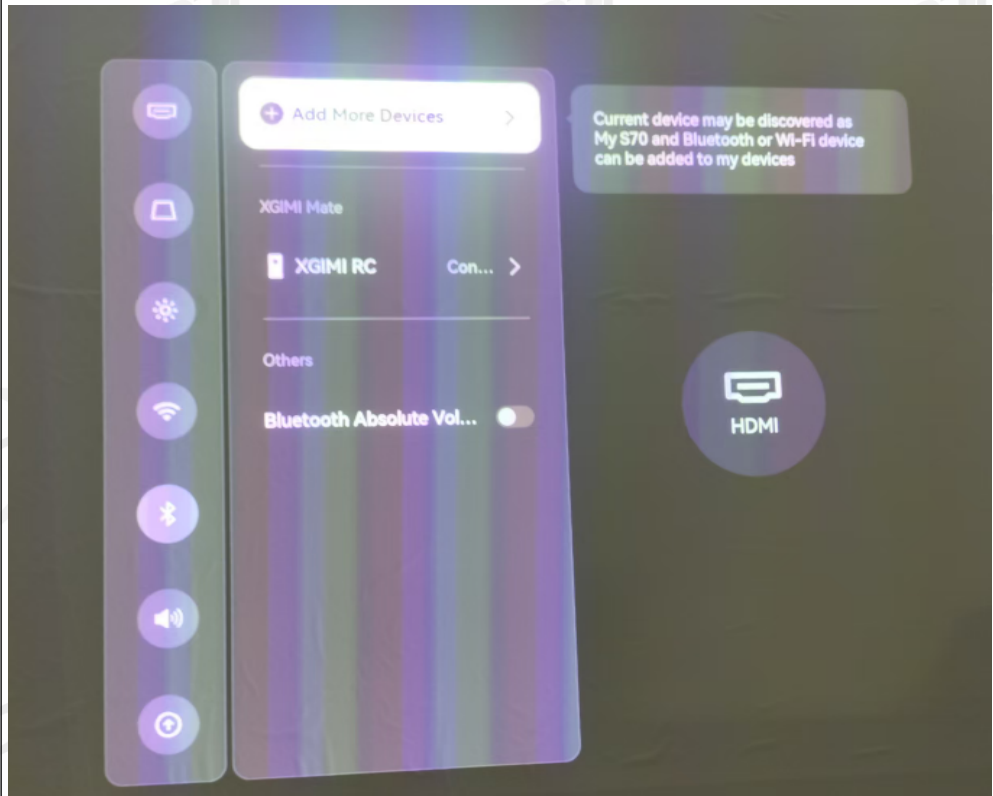

Subnet mask
255.255.255.0


Router
192.168.66.210

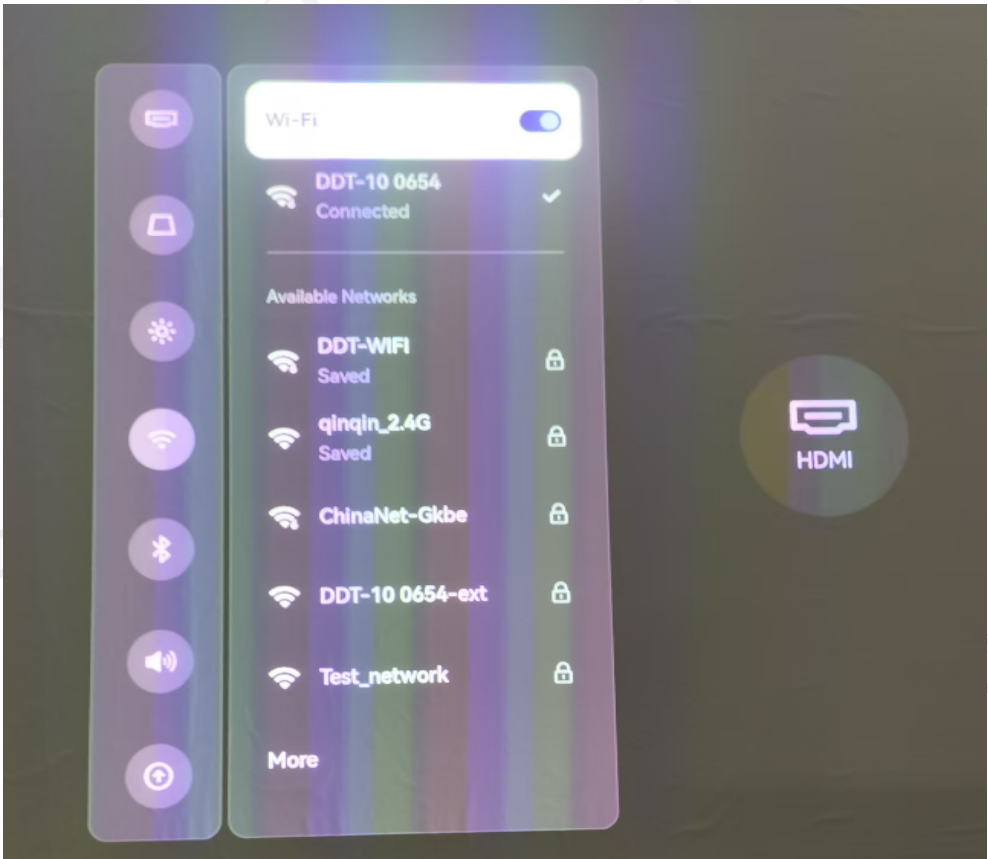
NetworkAsset-4.1: RS232 Physical interface



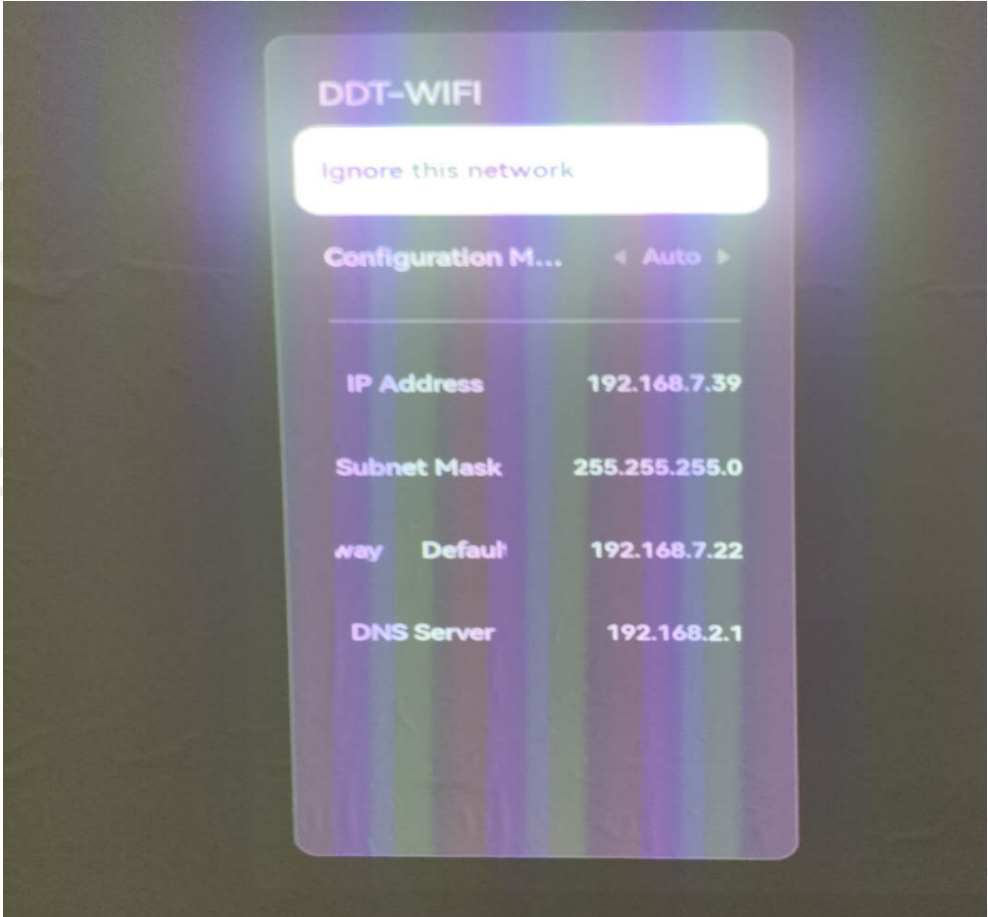
NetworkAsset-5.1: Paired Devices Access Rights



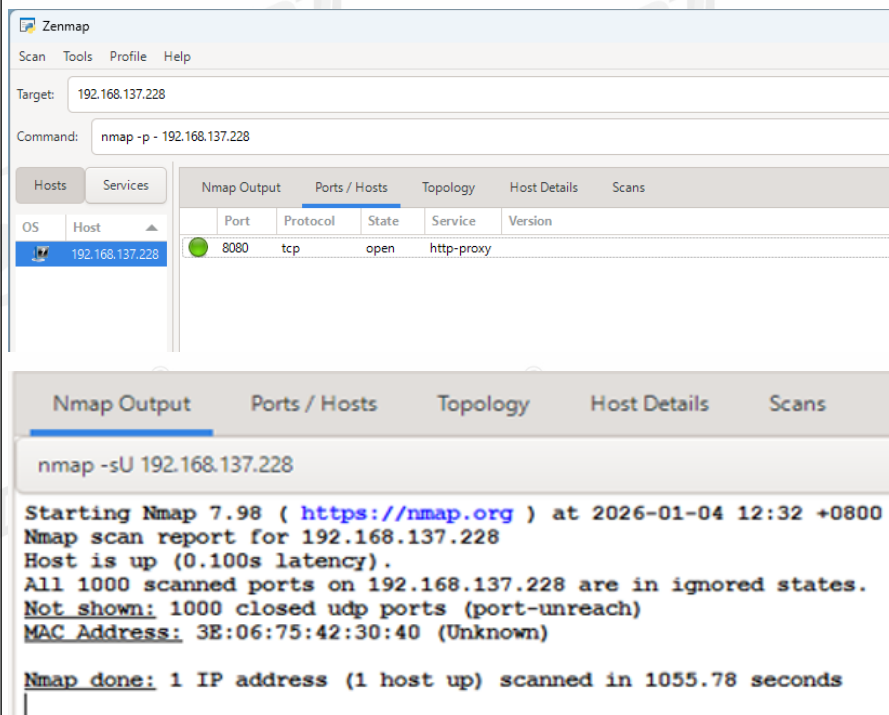
NetworkAsset-5.2: Saved Wi-Fi-Networks



NetworkAsset-5.3: Network configuration parameters



Perform a full port scan for TCP and UDP using the Zenmap tool.



Assignment of
verdict:

Pass

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether access control mechanisms are implemented when required per ACM-1.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each security asset documented in [E.Info.ACM-1.SecurityAsset] and each network asset documented in [E.Info.ACM-1.NetworkAsset] functionally confirm the existence of access control mechanisms according to [E.Info.ACM-1.SecurityAsset.ACM] or [E.Info.ACM-1.NetworkAsset.ACM] by accessing the assets following [E.Info.ACM-1.NetworkAsset.Access] and [E.Info.ACM-1.SecurityAsset.Access].
Result:	Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.

291 49.195375	192.168.137.7	222.217.94.16	TLSv1.3	655 Client Hello (SHA256-static-al.static.xgimi.com)
293 49.277047	222.217.94.16	192.168.137.7	TLSv1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295 49.306941	192.168.137.7	222.217.94.16	TLSv1.3	118 Change Cipher Spec, Application Data
296 49.375127	222.217.94.16	192.168.137.7	TLSv1.3	365 Application Data
297 49.406237	192.168.137.7	222.217.94.16	TLSv1.3	334 Application Data
298 49.487164	222.217.94.16	192.168.137.7	TLSv1.3	1468 Application Data
310 49.490389	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
334 49.564252	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data

Transmission Control Protocol, Src Port: 46050, Dst Port: 443, Seq: 1, Ack: 601, Len: 601

Transport Layer Security

[Stream Index: 7]

✓ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 596

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 592

Version: TLS 1.2 (0x0303)

Random: b6835a074b18995b92c59870a2c0ae06feccc618e634e63ed108cd4473757

Session ID Length: 32

Session ID: c25fclcccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436

Cipher Suites Length: 34

✓ Cipher Suites (17 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

291 49.195375

192.168.137.7

222.217.94.16

TLSv1.3

655 Client Hello (SHA256-static-al.static.xgimi.com)

293 49.277047

222.217.94.16

192.168.137.7

TLSv1.3

298 Server Hello, Change Cipher Spec, Application Data, Application Data

295 49.306941

192.168.137.7

222.217.94.16

TLSv1.3

118 Change Cipher Spec, Application Data

296 49.375127

222.217.94.16

192.168.137.7

TLSv1.3

365 Application Data

297 49.406237

192.168.137.7

222.217.94.16

TLSv1.3

334 Application Data

298 49.487164

222.217.94.16

192.168.137.7

TLSv1.3

1468 Application Data

310 49.490389

222.217.94.16

192.168.137.7

TLSv1.3

1514 Application Data

334 49.564252

222.217.94.16

192.168.137.7

TLSv1.3

1514 Application Data

> Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \\Device\\NPF_{A2009E98-90CA-4773-A2C0-58B161605298}, id 0

> Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1)

> Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7

> Transmission Control Protocol, Src Port: 443, Dst Port: 46050, Seq: 1, Ack: 602, Len: 244

Transport Layer Security

[Stream Index: 7]

✓ TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 128

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 124

Version: TLS 1.2 (0x0303)

Random: 0b7f1c4c9bd8732750948dea47576977cbcf2e4e91b13a40fd74127b6ec35

Session ID Length: 32

Session ID: c25fclcccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 52

> Extension: supported_versions (len=2) TLS 1.3

> Extension: key_share (len=36) x25519

> Extension: pre_shared_key (len=2)

[JA3S Fullstring: 771,4065,43-51-41]

[JA3S: fcb2d40099129227fcb1e464eeef43]

Certificate

Certificate

General Details Certification Path

 **Certificate Information**

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

* Refer to the certification authority's statement for details.

Issued to: global-static-al.static.xgimi.com

Issued by: RapidSSL TLS RSA CA G1

Valid from: 10/15/2025 to 10/15/2026

Install Certificate... Issuer Statement

OK

Certificate

General Details Certification Path

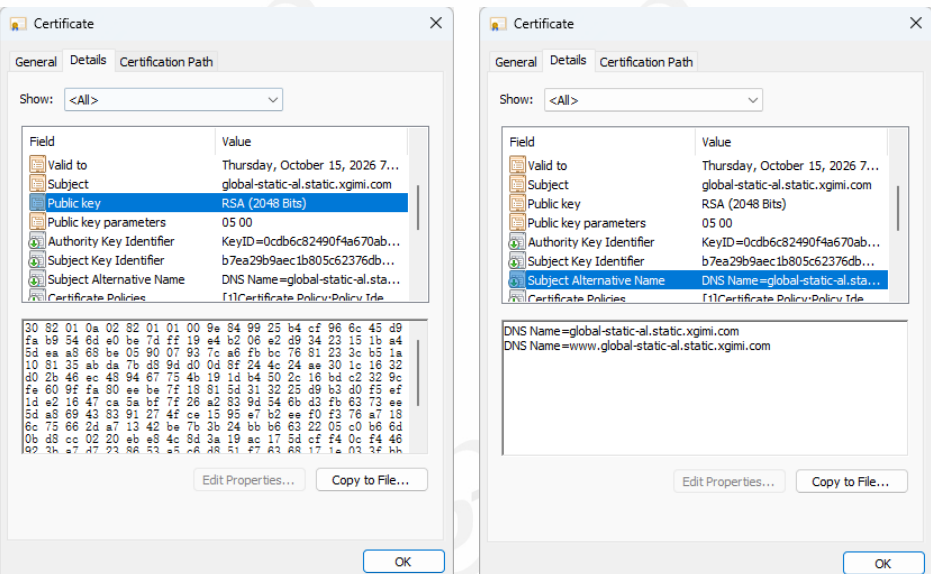
Show: <All>

Field	Value
Version	V3
Serial number	0419394fb8c96f7488fae4452...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	RapidSSL TLS RSA CA G1, ww...
Valid from	Wednesday, October 15, 202...
Valid to	Thursday, October 15, 2026 7...
Subject	global-static-al.static.xgimi.com

sha256

Edit Properties... Copy to File...

OK

	
Assignment of verdict:	Pass

3.1.2 [ACM-2] Appropriate access control mechanisms

--Conceptual assessment--

Identifier [ACM-2]-01	[E.Info.ACM-2.SecurityAsset]: SecurityAsset-2.1: The DUT connects to the server via Wi-Fi. SecurityAsset-2.2: The DUT connects to the server via Ethernet. SecurityAsset-2.3: Perform over-the-air (OTA) firmware updates for devices via the OTA server.		
Decision node	Decision [E.Info.DT.ACM-2]		Justification [E.Just.DT.ACM-2]
DT.ACM-2.DN-1	Yes (✓)	No	[E.Info.ACM-2.SecurityAsset.ACM]: [IC/ACM-2.MAC] Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.
Assignment of verdict:	Pass		

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the access control mechanism's applicability.

Therefore, the functional completeness assessment in ACM-2 is not necessary.

--Sufficiency testing--

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

Preconditions:	/
Operation steps:	[AU.ACM-2.MAC]: If the access control mechanisms documented in [E.Info.ACM-2.SecurityAsset.ACM] or [E.Info.ACM-2.NetworkAsset.ACM] belong to [IC.ACM-2.MAC], functionally confirm that: — the security asset or network asset is only accessible by authorized users after clearance was issued by the operating system and/or system administrator; and — the issuance of clearance is associated with the principle of least privileges; and — changing the operating system and/or system administrator that is responsible for the issuance of clearance to the user can only be performed by the authorized system administrator.
Result:	Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication. <pre>291 49.195375 192.168.137.7 222.217.94.16 TLSv1.3 655 Client Hello (SMI=global-static-al.static.xgimi.com) 293 49.277047 222.217.94.16 192.168.137.7 TLSv1.3 298 Server Hello, Change Cipher Spec, Application Data 295 49.306941 192.168.137.7 222.217.94.16 TLSv1.3 118 Change Cipher Spec, Application Data 296 49.375127 222.217.94.16 192.168.137.7 TLSv1.3 365 Application Data 297 49.406237 192.168.137.7 222.217.94.16 TLSv1.3 334 Application Data 298 49.487164 222.217.94.16 192.168.137.7 TLSv1.3 1468 Application Data 310 49.490389 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data 334 49.564252 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data Transmission Control Protocol, Src Port: 46050, Dst Port: 443, Seq: 1, Ack: 1, Len: 601 Transport Layer Security [Stream Index: 7] TLSv1.3 Record Layer: Handshake Protocol: Client Hello Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 596 Handshake Protocol: Client Hello Handshake Type: Client Hello (1) Length: 592 Version: TLS 1.2 (0x0303) Random: b603d5a074b18995b92c59870a2ccae0a6fecc618e6343e63ed108cd4473757 Session ID Length: 32 Session ID: c25f1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436 Cipher Suites Length: 34 Cipher Suites (17 suites) Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302) Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) Compression Methods Length: 1 291 49.195375 192.168.137.7 222.217.94.16 TLSv1.3 655 Client Hello (SMI=global-static-al.static.xgimi.com) 293 49.277047 222.217.94.16 192.168.137.7 TLSv1.3 298 Server Hello, Change Cipher Spec, Application Data 295 49.306941 192.168.137.7 222.217.94.16 TLSv1.3 118 Change Cipher Spec, Application Data 296 49.375127 222.217.94.16 192.168.137.7 TLSv1.3 365 Application Data 297 49.406237 192.168.137.7 222.217.94.16 TLSv1.3 334 Application Data 298 49.487164 222.217.94.16 192.168.137.7 TLSv1.3 1468 Application Data 310 49.490389 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data 334 49.564252 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data > Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \Device\NPF_{A2009E98-90CA-4773-A2C0-58B161605298}, id 0 > Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1) > Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7 > Transmission Control Protocol, Src Port: 443, Dst Port: 46050, Seq: 1, Ack: 602, Len: 244 Transport Layer Security [Stream Index: 7] TLSv1.3 Record Layer: Handshake Protocol: Server Hello Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 128 Handshake Protocol: Server Hello Handshake Type: Server Hello (2) Length: 124 Version: TLS 1.2 (0x0303) Random: 087f1ce4c9bd86732750948dea47576977cb8f2e4e91b13a40fd74127b6ec35 Session ID Length: 32 Session ID: c25f1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436 Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Compression Method: null (0) Extensions Length: 52 Extension: supported_versions (len=2) TLS 1.3 Extension: key_share (len=36) x25519 Extension: pre_shared_key (len=2) [JA3S Fullstring: 771,4865,43-51-41] [JA3S: fcb2d4d0991292272fcb1e464eedf4d3]</pre> Certificate

Assignment of verdict:	Pass

3.2 [AUM] Authentication mechanism

3.2.1 [AUM-1] Applicability of authentication mechanisms

3.2.1.1 [AUM-1-1] Requirement network interface

--Conceptual assessment--

Identifier [AUM-1-1]-01	[E.Info.AUM-1-1.ACM]: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.	
Decision node	Decision [E.Info.DT.AUM-1-1]	Justification [E.Just.DT.AUM-1-1]

DT.AUM-1-1.DN-3	Yes (✓)	No	[E.Info.AUM-1-1.ACM.NetworkInterface]: IF-1: Connect to the Internet via Wi-Fi. IF-2: Connect to the Internet via Ethernet. [E.Info.AUM-1-1.ACM.ManagedAccessNetworkAsset]: / [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset]: SecurityAsset-2.3: Perform over-the-air (OTA) firmware updates for devices via the OTA server. [E.Info.AUM-1-1.ACM.AuthenticationMechanism]: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.
Assignment of verdict:	Pass		

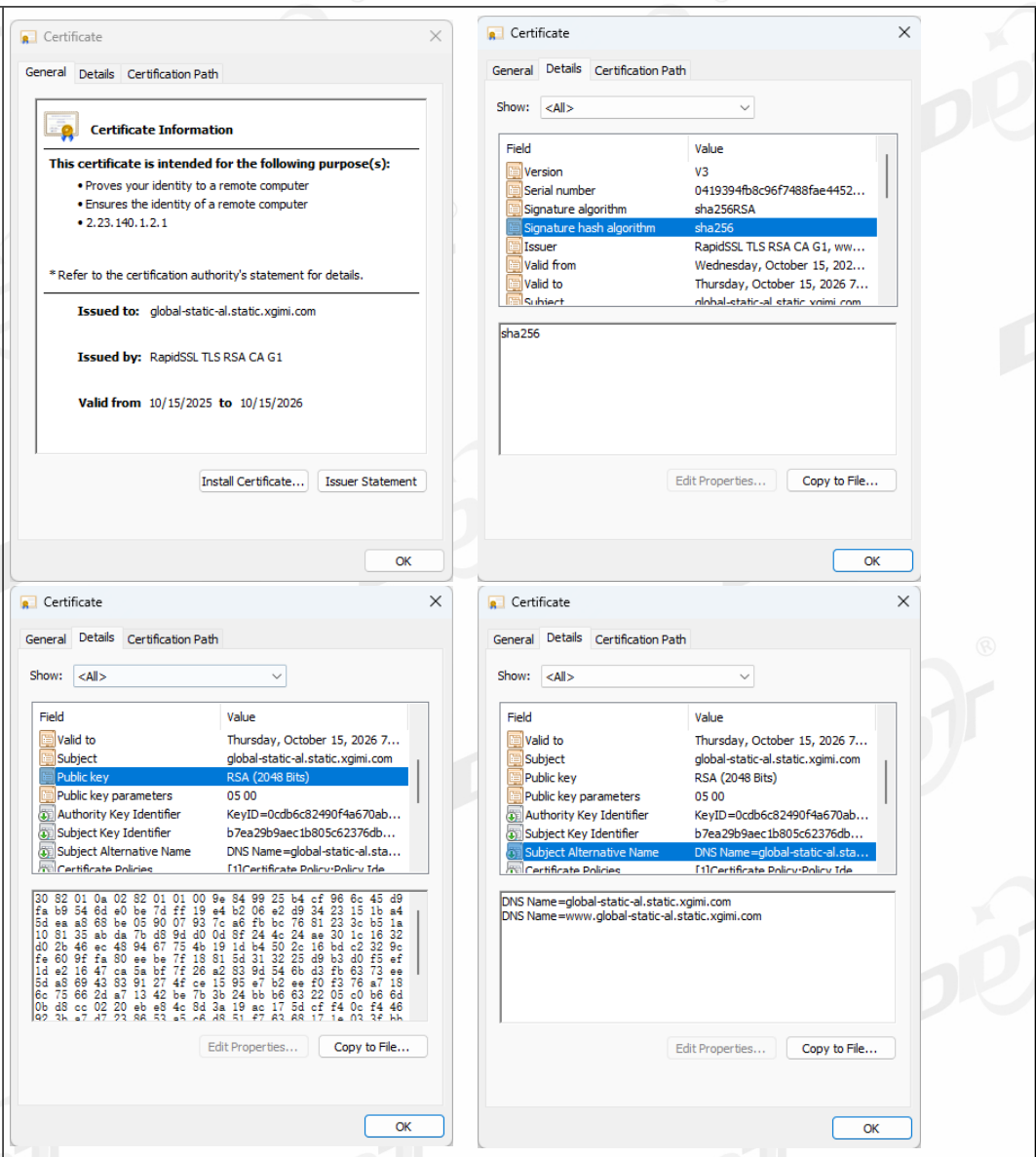
--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether there are access control mechanisms on the equipment for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions that are not described in [E.Info.AUM-1-1.ACM].
Preconditions:	The equipment is in an operational state.
Operation steps:	Functionally assess whether there are access control mechanisms required per ACM-1 for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions that are not described in [E.Info.AUM-1-1.ACM].
Result:	There is no evidence that an access control mechanism required per ACM-1 for managing entities' access over network interfaces that allow to read confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions, is found that is not documented in [E.Info.AUM-1-1.ACM].
Assignment of verdict:	Pass

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1-1 are implemented.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each access control mechanisms documented in [E.Info.AUM-1-1.ACM], each managed

	access via network interfaces to network assets documented in [E.Info.AUM-1-1.ACM.ManagedAccessNetworkAsset] and each managed access via network interfaces to security assets documented in [E.Info.AUM-1-1.ACM.ManagedAccessSecurityAsset], access the corresponding security assets or network assets and check whether the authentication mechanism is implemented.
Result:	Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication. <pre>291 49.195375 192.168.137.7 222.217.94.16 TLSv1.3 655 Client Hello (SNI=global-static-al.static.xgimi.com) 293 49.277047 222.217.94.16 192.168.137.7 TLSv1.3 298 Server Hello, Change Cipher Spec, Application Data, Application Data 295 49.306941 192.168.137.7 222.217.94.16 TLSv1.3 118 Change Cipher Spec, Application Data 296 49.375127 222.217.94.16 192.168.137.7 TLSv1.3 365 Application Data 297 49.406237 192.168.137.7 222.217.94.16 TLSv1.3 334 Application Data 298 49.487164 222.217.94.16 192.168.137.7 TLSv1.3 1468 Application Data 310 49.490389 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data 334 49.564252 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data</pre> Transmission Control Protocol, Src Port: 46058, Dst Port: 443, Seq: 1, Ack: 1, Len: 601 Transport Layer Security [Stream index: 7] ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 596 ▼ Handshake Protocol: Client Hello Handshake Type: Client Hello (1) Length: 592 ► Version: TLS 1.2 (0x0303) Random: b693d5a074b18995b92c59870a2ccae0a6feccc618e6343e3ed108cd4473757 Session ID Length: 32 Session ID: c25f1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436 Cipher Suites Length: 34 ▼ Cipher Suites (17 suites) Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302) Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc02d) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) Compression Methods Length: 1 <pre>291 49.195375 192.168.137.7 222.217.94.16 TLSv1.3 655 Client Hello (SNI=global-static-al.static.xgimi.com) 293 49.277047 222.217.94.16 192.168.137.7 TLSv1.3 298 Server Hello, Change Cipher Spec, Application Data, Application Data 295 49.306941 192.168.137.7 222.217.94.16 TLSv1.3 118 Change Cipher Spec, Application Data 296 49.375127 222.217.94.16 192.168.137.7 TLSv1.3 365 Application Data 297 49.406237 192.168.137.7 222.217.94.16 TLSv1.3 334 Application Data 298 49.487164 222.217.94.16 192.168.137.7 TLSv1.3 1468 Application Data 310 49.490389 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data 334 49.564252 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data</pre> ► Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \Device\NPF_{A2009E98-90CA-4773-A2C8-508161605298}, id 0 ► Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1) ► Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7 ► Transmission Control Protocol, Src Port: 443, Dst Port: 46058, Seq: 1, Ack: 602, Len: 244 Transport Layer Security [Stream index: 7] ▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 128 ▼ Handshake Protocol: Server Hello Handshake Type: Server Hello (2) Length: 124 ► Version: TLS 1.2 (0x0303) Random: 087f1ce4c9bd86732750948dea47576977cbc8f2e4e91b13a40fd74127b6c35 Session ID Length: 32 Session ID: c25f1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436 Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Compression Method: null (0) Extensions Length: 52 ► Extension: supported_versions (len=2) TLS 1.3 ► Extension: key_share (len=36) x25519 ► Extension: pre_shared_key (len=2) [JA3S Fullstring: 771,4865,43-51-41] [JA3S: fcb2d4d0991292272fcb1e464eedfd43]
	Certificate

	
Assignment of verdict:	Pass

3.2.1.2 [AUM-1-2] Requirement user interface

--Conceptual assessment--

Identifier [AUM-1-2]-01	/		
Decision node	Decision [E.Info.DT.AUM-1-2]	Justification [E.Just.DT.AUM-1-2]	
/	/	/	/
Assignment of verdict:	N/A The user interface of the device has no access control mechanism.		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether there are access control mechanisms on the equipment for managing entities' access over user interfaces that allow to read
---------------------	---

	confidential network function configuration or confidential security parameters; or modify sensitive network function configuration or sensitive security parameters; or use network functions or security functions that are not described in [E.Info.AUM-1-2.ACM].
Preconditions:	The equipment is in an operational state.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A The user interface of the device has no access control mechanism.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms required per AUM-1-2 are implemented.
Preconditions:	The equipment is in an operational state.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A The user interface of the device has no access control mechanism.

3.2.2 [AUM-2] Appropriate authentication mechanisms

--Conceptual assessment--

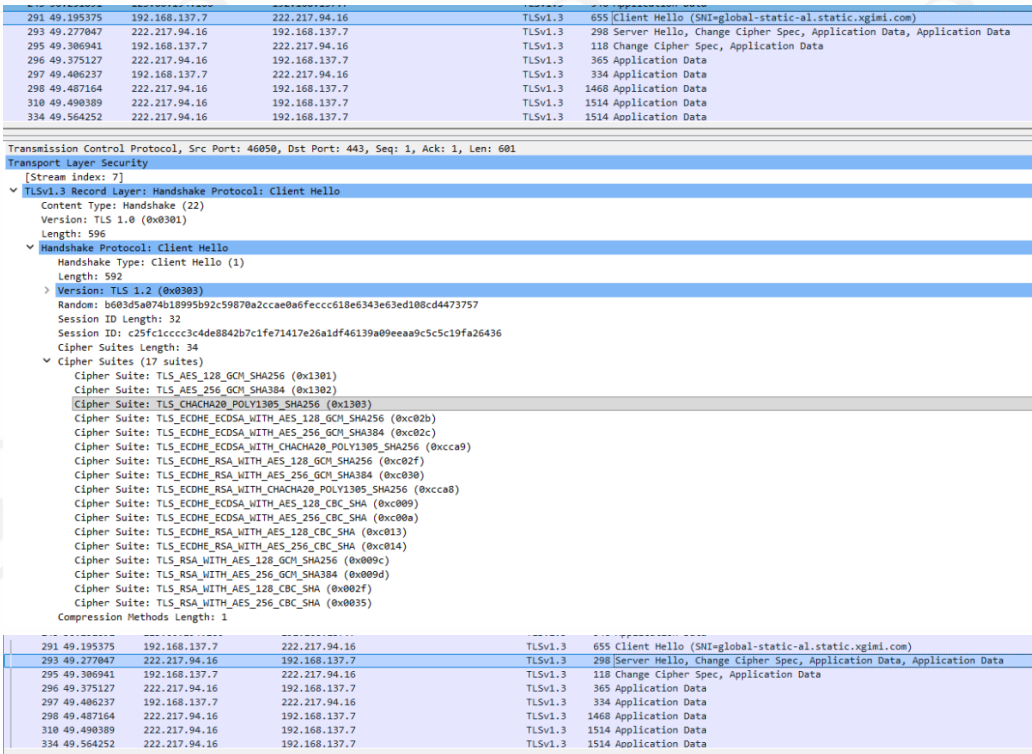
Identifier [AUM-2]-01	[E.Info.AUM-2-1.AuthenticationMechanism]: AUM-1-1: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.		
Decision node	Decision [E.Info.DT.AUM-2]		Justification [E.Just.DT.AUM-2]
DT.AUM-2.DN-1	Yes (✓)	No	[E.Info.AUM-2.AuthenticationMechanism.AuthFactor]: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.
Assignment of verdict:	Pass		

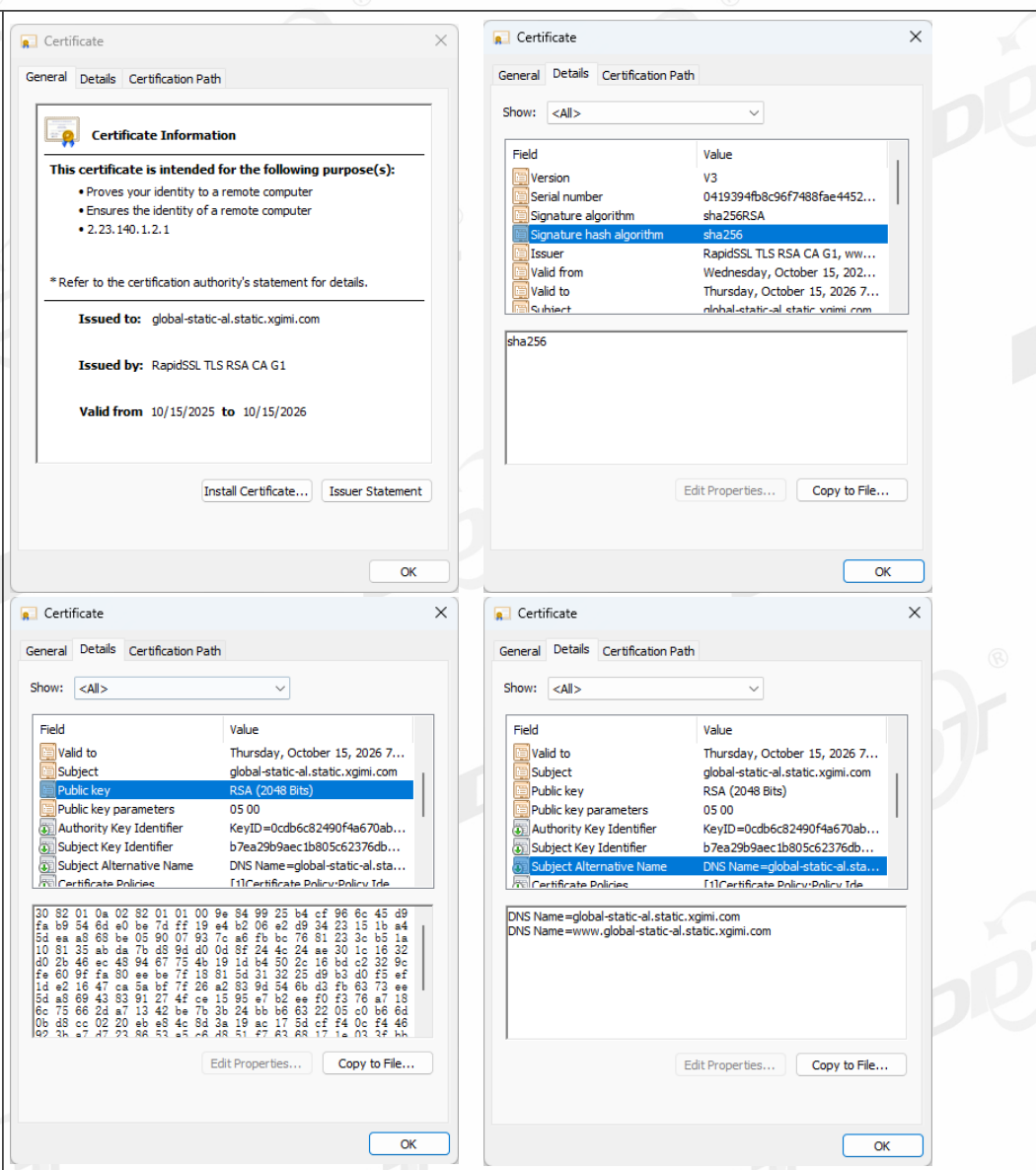
--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) are implemented as documented.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each authentication mechanism required by AUM-1-1 (network interface) or AUM-1-2 (user interface) recorded in [E.Info.AUM-2.AuthenticationMechanism], perform an authentication and evaluate whether the authentication mechanism is implemented as recorded.
Result:	Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.  Certificate

	
Assignment of verdict:	Pass

3.2.3 [AUM-3] Authenticator validation

--Conceptual assessment--

Identifier [AUM-3]-01	[E.Info.AUM-3.AUM]: AUM-1-1: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.		
Decision node	Decision [E.Info.DT.AUM-3]	Justification [E.Just.DT.AUM-3]	
DT.AUM-3.DN-1	Yes (√)	[E.Info.AUM-3.AUM.AuthVal]: The identity verification is carried out by means of the SSL certificate issued by the Certificate Authority RapidSSL TLS RSA CA G1. The certificate uses	

		the sha256WithRSAEncryption signature algorithm and a 2048-bit RSA key strength. By verifying the information such as the subject of issuance in the certificate, the issuer, and the validity period, the legitimacy of the device identity is confirmed, and the authenticity and integrity of the communication between the device and the server during the OTA process are guaranteed. [E.Info.AUM-3.AUM.AuthEnv]: For the device in the OTA scenario, its usage environment information covers the network environment when the device interacts with the OTA server through a secure HTTPS channel and relying on the OpenSSL 3.0.15 code library. [IC.AUM-3.CertificatePrivateKey]: The SSL certificate issued by the RapidSSL TLS RSA CA G1.
Assignment of verdict:	Pass	

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the authentication mechanism required per AUM-1-1 or AUM-1-2 validates all required properties.
Preconditions:	The equipment is in an operational state.
Operation steps:	[AU.AUM-3.CertificatePrivateKey]: If the authenticator belongs to [IC.AUM-3.CertificatePrivateKey], functionally confirm the validation of the relevant properties of the authenticator documented in [E.Info.AUM-3.AUM.AuthVal] by examining whether: — incorrect private keys to a trusted certificate can be used for successful authentication; and — (if the confidentiality of the messages exchanged during authentication via network interfaces is not protected) a replay of a recorded successful authentication attempt can be used for successful authentication; and — valid private keys to untrusted or invalid certificates can be used for successful authentication; and NOTE untrusted or invalid certificates can be certificates revoked by the certificate authority, expired certificates, certificates with an invalid chain of trust e.g., generated by an untrusted entity containing an expected “Common Name” (CN) entry. — (if different user accounts exist or can be created) private keys to a trusted certificate of other entities can be used for authentication.
Result:	Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.

356	49.581056	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
373	49.610833	192.168.137.7	222.217.94.17	TLSv1.3	618 Client Hello (SN=global-static-al.static.xgimi.com)
404	49.680563	222.217.94.17	192.168.137.7	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
408	49.767946	222.217.94.17	192.168.137.7	TLSv1.3	1514 Application Data
409	49.768046	222.217.94.17	192.168.137.7	TLSv1.3	251 Application Data, Application Data
412	49.808821	192.168.137.7	222.217.94.17	TLSv1.3	118 Change Cipher Spec, Application Data
413	49.887222	222.217.94.17	192.168.137.7	TLSv1.3	365 Application Data
414	49.888438	222.217.94.17	192.168.137.7	TLSv1.3	365 Application Data

> Ethernet II, Src: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1), Dst: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1)

> Internet Protocol Version 4, Src: 192.168.137.7, Dst: 222.217.94.17

> Transmission Control Protocol, Src Port: 36880, Dst Port: 443, Seq: 1, Ack: 1, Len: 564

> Transport Layer Security

[Stream index: 8]

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 559

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 555

> Version: TLS 1.2 (0x0303)

Random: c8673981c52b8fdac1d1399b6c9065a33f997b5d6b687d80d2d700020dc8a

Session ID Length: 32

Session ID: 90cefal5de2911bf76b1dba64f1fe2e411967ebeca510a94dda91a3ad8df9607

Cipher Suites Length: 30

> Cipher Suites (15 suites)

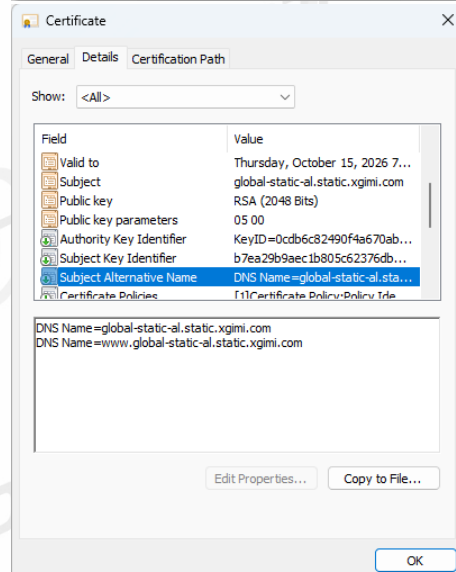
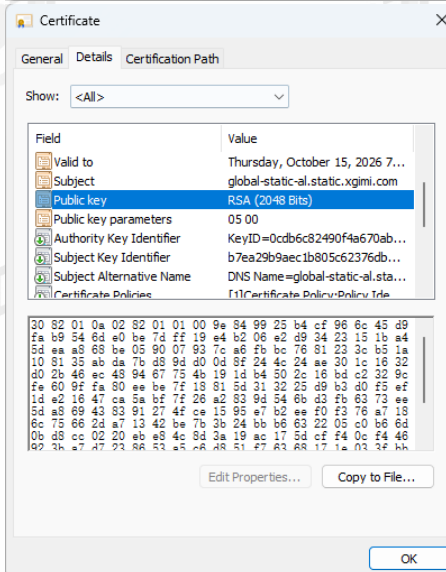
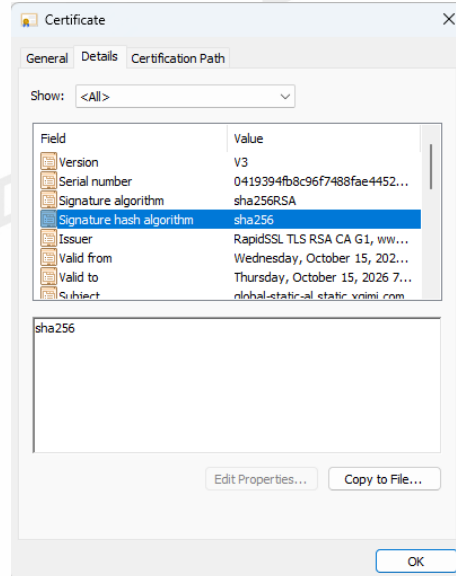
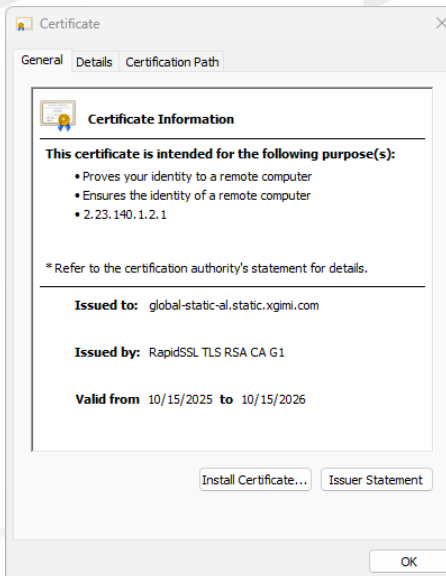
Compression Methods Length: 1

> Compression Methods (1 method)

Extensions Length: 452

> Extension: server_name (len=38) name=global-static-al.static.xgimi.com

Certificate



A DNS spoofing test was conducted using a forged certificate (*.xgimi.com), and a concurrent test was performed on the OTA upgrade function. The man-in-the-middle server indicated that the product returned a "handshake failure" prompt with the OTA server. This demonstrates that the

	product is capable of identifying forged certificates and rejecting the establishment of communication connections. <pre> [17:03:46.260][192.168.50.97:50094] client connect [17:03:46.230][192.168.50.97:50094] server connect 119.3.116.145:443 [17:03:46.286][192.168.50.97:50094] Client TLS handshake failed. The client does not trust the proxy's certificate for adapi.xgim i.com (OpenSSL Error([('SSL routines', '', 'ssl/tls alert certificate unknown')])) [17:03:46.287][192.168.50.97:50094] client disconnect [17:03:46.288][192.168.50.97:50094] server disconnect 119.3.116.145:443 [17:03:55.055][192.168.50.97:58322] client connect [17:04:02.107][192.168.50.97:56574] client connect [17:04:02.138][192.168.50.97:56574] server connect 123.60.127.54:443 [17:04:02.193][192.168.50.97:56574] Client TLS handshake failed. The client does not trust the proxy's certificate for api.goss.x gimi.com (OpenSSL Error([('SSL routines', '', 'ssl/tls alert certificate unknown')])) [17:04:02.194][192.168.50.97:56574] client disconnect [17:04:02.195][192.168.50.97:56574] server disconnect 123.60.127.54:443 [17:04:06.504][192.168.50.97:59054] client connect [17:04:06.533][192.168.50.97:59054] server connect 119.3.116.112:443 [17:04:06.586][192.168.50.97:59054] Client TLS handshake failed. The client does not trust the proxy's certificate for adapi.xgim i.com (OpenSSL Error([('SSL routines', '', 'ssl/tls alert certificate unknown')])) [17:04:06.587][192.168.50.97:59054] client disconnect [17:04:06.588][192.168.50.97:59054] server disconnect 119.3.116.112:443 [17:04:15.111][192.168.50.97:41276] client connect [17:04:19.425][192.168.50.97:46926] client connect [17:04:19.439][192.168.50.97:46926] server connect 124.225.195.12:443 [17:04:19.487][192.168.50.97:46926] Client TLS handshake failed. The client does not trust the proxy's certificate for global-sta tic-al.static.xgimi.com (OpenSSL Error([('SSL routines', '', 'ssl/tls alert certificate unknown')])) [17:04:19.488][192.168.50.97:46926] client disconnect [17:04:19.489][192.168.50.97:46926] server disconnect 124.225.195.12:443 [17:04:19.508][192.168.50.97:46938] client connect [17:04:19.523][192.168.50.97:46938] server connect 124.225.195.12:443 [17:04:20.460][192.168.50.97:36366] server disconnect 123.60.194.160:443 [17:04:22.437][192.168.50.97:35212] client connect [17:04:22.468][192.168.50.97:35212] server connect 119.3.116.160:443 [17:04:22.520][192.168.50.97:35212] Client TLS handshake failed. The client does not trust the proxy's certificate for api.goss.x gimi.com (OpenSSL Error([('SSL routines', '', 'ssl/tls alert certificate unknown')])) [17:04:22.521][192.168.50.97:35212] client disconnect [17:04:22.521][192.168.50.97:35212] server disconnect 119.3.116.160:443 [17:04:26.878][192.168.50.97:40132] client connect [17:04:26.908][192.168.50.97:40132] server connect 123.60.127.23:443 [17:04:26.960][192.168.50.97:40132] Client TLS handshake failed. The client does not trust the proxy's certificate for adapi.xgim i.com (OpenSSL Error([('SSL routines', '', 'ssl/tls alert certificate unknown')])) [17:04:26.961][192.168.50.97:40132] client disconnect [17:04:26.962][192.168.50.97:40132] server disconnect 123.60.127.23:443 [17:04:35.165][192.168.50.97:44092] client connect </pre>
Assignment of verdict:	Pass

3.2.4 [AUM-4] Changing authenticators

--Conceptual assessment--

Identifier [AUM-4]-01	[E.Info.AUM-4.AUM]: AUM-1-1: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.		
Decision node	Decision [E.Info.DT.AUM-4]		Justification [E.Just.DT.AUM-4]
DT.AUM-4.DN-2	Yes (√)	No	[E.Info.AUM-4.AUM.AuthChange]: The trigger sources for validator changes include the RapidSSL TLS RSA CA G1 - CA certificate updates, OTA server configuration changes, or security policy upgrades. On the server side, change instructions (containing new certificate metadata, URLs, and algorithm rules) are pushed through the JSON file associated with the preset URL. On the device side, secure pull - up via the HTTPS channel is implemented relying on OpenSSL 3.0.15; after parsing the JSON, the firmware interface is called to update the certificate storage, URL configuration, and encryption algorithm; then the authentication module is restarted, and the effective change is confirmed through bidirectional verification between the device and the server. Meanwhile, the validator on the server side synchronously updates verification rules such as CA root certificates, URL whitelists, and

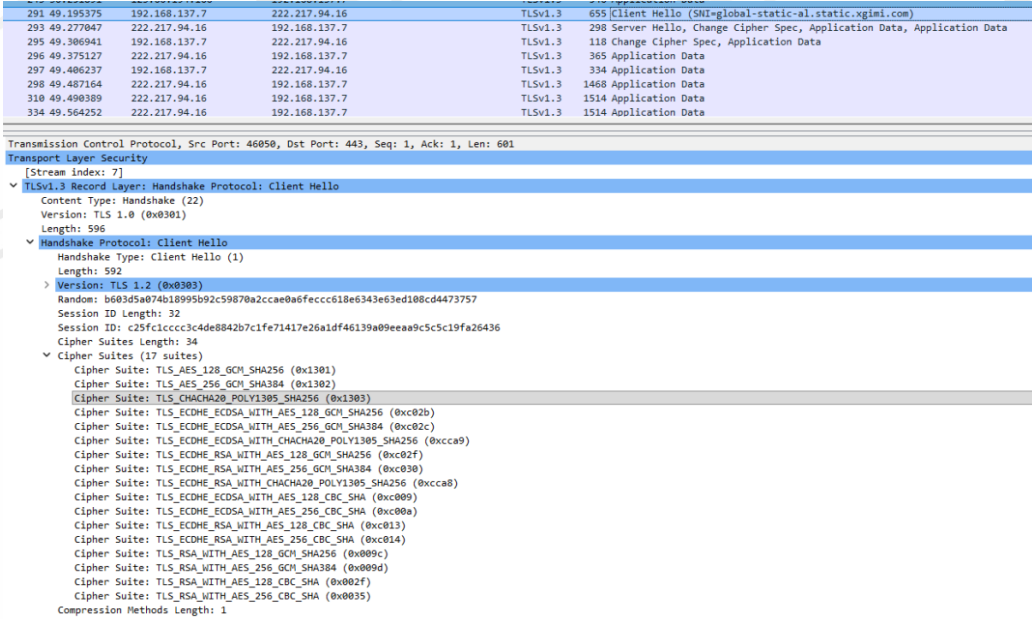
		algorithm support lists to ensure the closed - loop authentication logic after the change.
Assignment of verdict:	Pass	

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the documented authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) allow for changing the authenticator as documented in [E.Info.AUM-4.AUM.AuthChange].
Preconditions:	The equipment is in an operational state.
Operation steps:	For each authentication mechanism that is required per AUM-1-1 (network interface) or AUM-1-2 (user interface) documented in [E.Info.AUM-4.AUM], functionally confirm the ability to change authenticator as documented in [E.Info.AUM-4.AUM.AuthChange] by - checking whether the newly assigned authenticator grants access on each path to security assets and/or network assets; and - checking whether the previous authenticator does no longer grant access on any path to security assets and/or network assets after changing the authenticator.
Result:	Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication. 

291.49.199375	192.168.137.7	222.217.94.16	TLSv1.3	655 Client Hello (SN=global-static-al.static.xgmi.com)
291.49.277947	222.217.94.16	192.168.137.7	TLSv1.3	298 Server Hello, Change Cipher Spec, Application Data
295.49.306941	192.168.137.7	222.217.94.16	TLSv1.3	118 Change Cipher Spec, Application Data
296.49.375127	222.217.94.16	192.168.137.7	TLSv1.3	365 Application Data
297.49.406237	192.168.137.7	222.217.94.16	TLSv1.3	334 Application Data
298.49.487164	222.217.94.16	192.168.137.7	TLSv1.3	1468 Application Data
310.49.490389	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
334.49.564252	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data

> Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \Device\NPF_{A2089E98-90CA-4773-A2C0-5B8161605298}, id 0

> Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1)

> Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7

> Transmission Control Protocol, Src Port: 443, Dst Port: 46850, Seq: 1, Ack: 602, Len: 244

> Transport Layer Security

[Stream Index: 7]

> TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 128

> Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 124

> Version: TLS 1.2 (0x0303)

Random: 087f1ce4c9bd86732750948dea47576977c8f2e4e91b13a40fd74127b6ec35

Session ID Length: 32

Session ID: c25f1ccccc34de8842b7c1fe71417e26a1df46139a09eeaa9c5c5c19fa26436

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 52

> Extension: supported_versions (len=2) TLS 1.3

> Extension: key_share (len=36) x25519

> Extension: pre_shared_key (len=2)

[JA3S Fullstring: 771,4865,43-51-41]

[JA3S: fcb2d4d0991292272fcb1e464eedfd43]

Certificate

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.1

*Refer to the certification authority's statement for details.

Issued to: global-static-al.static.xgmi.com

Issued by: RapidSSL TLS RSA CA G1

Valid from: 10/15/2025 to 10/15/2026

Install Certificate... Issuer Statement

OK

Certificate

General Details Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	0419394fb8c96f7488fae4452...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	RapidSSL TLS RSA CA G1, ww...
Valid from	Wednesday, October 15, 202...
Valid to	Thursday, October 15, 2026 7...
Subject	global-static-al.static.xgmi.com

sha256

Edit Properties... Copy to File...

OK

Certificate

General Details Certification Path

Show: <All>

Field	Value
Valid to	Thursday, October 15, 2026 7...
Subject	global-static-al.static.xgmi.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=0cdbc82490f4a670ab...
Subject Key Identifier	b7ea29b9aec1b805c62376db...
Subject Alternative Name	DNS Name=global-static-al.sta...
Certificate Policies	[1]Certificate Policy: Policy Id...

30 82 01 0a 02 82 01 01 00 9e 84 99 25 b4 cf 98 6c 45 d9
fa b9 54 6d e0 be 7d ff 19 e4 b2 06 a2 d9 34 23 15 1b a4
5d ea a3 68 be 05 90 07 93 fc a6 f2 bc 76 81 23 3c b5 1a
10 81 35 ab da 7b d3 98 40 01 5f 24 4c 54 ae 30 1c 18 32
40 2b 46 e8 43 94 67 75 4b 19 1d b4 50 3c 16 bd c2 32 9c
fe 60 9f fa 80 ee be 7f 18 81 5d 31 32 25 d9 b3 40 f5 ef
1d e2 16 47 ca 3a bf 7f 26 a2 83 9d 54 6b d3 fb 63 73 ee
5d a8 69 43 93 91 27 4f ce 15 95 e7 b2 ee f0 13 76 a7 18
6c 75 68 2d a7 13 42 be 7b 3b 24 b6 b3 22 05 c0 b6 6d
0b d8 cc 02 20 eb e8 4c 9d 3a 19 ac 17 5d cf f4 0c f4 46
92 3b e7 a7 23 86 52 e5 a8 88 51 f7 a3 88 17 1a 03 2f b8

Edit Properties... Copy to File...

OK

Certificate

General Details Certification Path

Show: <All>

Field	Value
Valid to	Thursday, October 15, 2026 7...
Subject	global-static-al.static.xgmi.com
Public key	RSA (2048 Bits)
Public key parameters	05 00
Authority Key Identifier	KeyID=0cdbc82490f4a670ab...
Subject Key Identifier	b7ea29b9aec1b805c62376db...
Subject Alternative Name	DNS Name=global-static-al.sta...
Certificate Policies	[1]Certificate Policy: Policy Id...

DNS Name=global-static-al.static.xgmi.com
DNS Name=www.global-static-al.static.xgmi.com

Edit Properties... Copy to File...

OK

Assignment of
verdict:

Pass

3.2.5 [AUM-5] Password strength

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

--Conceptual assessment--

Identifier [AUM-5-1]-01	/		
Decision node	Decision [E.Info.DT.AUM-5-1]	Justification [E.Just.DT.AUM-5-1]	
/	/	/	/
Assignment of verdict:	N/A There is no password that is used for authentication.		

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 are implemented as required per AUM-5-1.		
Preconditions:	The equipment is in the factory default state and not commissioned. (If the method documented in [E.Info.AUM-5-1.AUM.PwdProperty] belongs to [IC.AUM-5-1.UniqueBestPractice]) The equipment's actual factory default password is available.		
Operation steps:	/		
Result:	/		
Assignment of verdict:	N/A There is no password that is used for authentication.		

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

--Conceptual assessment--

Identifier [AUM-5-2]-01	/		
Decision node	Decision [E.Info.DT.AUM-5-2]	Justification [E.Just.DT.AUM-5-2]	
/	/	/	/
Assignment of verdict:	N/A There is no password that is used for authentication.		

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 are implemented as required per AUM-5-2.
Preconditions:	The equipment is in the factory default state and not commissioned.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A There is no password that is used for authentication.

3.2.6 [AUM-6] Brute force protection

--Conceptual assessment--

Identifier [AUM-6]-01	[E.Info.AUM-6.AUM]: AUM-1-1: Communication is implemented via a secure HTTPS channel based on the OpenSSL 3.0.15 library. The DUT and the server establish a secure connection using the TLS protocol (TLS 1.3 supported), negotiating cryptographic parameters during the handshake. Certificate-based identity verification and key exchange mechanisms are employed to establish an encrypted connection for authentication.		
Decision node	Decision [E.Info.DT.AUM-6]	Justification [E.Just.DT.AUM-6]	
DT.AUM-6.DN-1	Yes (√)	No	[E.Info.AUM-6.AUM.BFProtection]: [IC.AUM-6.AuthenticatorComplexity]: The RSA key length is 2048 bits. For a brute - force attack to crack the RSA key, it needs to enumerate all possible private key combinations. Given the extremely large number of combinations for a 2048 - bit key, with current computing power, the conventional method of brute - force enumeration of private keys can hardly be completed within a reasonable time. This fundamentally greatly increases the difficulty of brute - force cracking and builds a solid basic protection for the certificate and the encrypted communication that relies on it.
Assignment of verdict:	Pass		

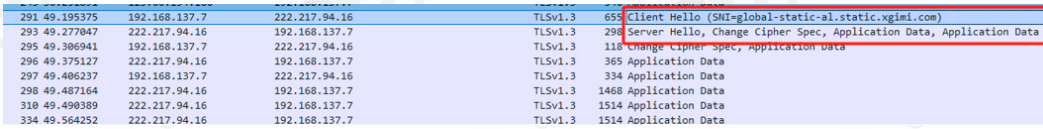
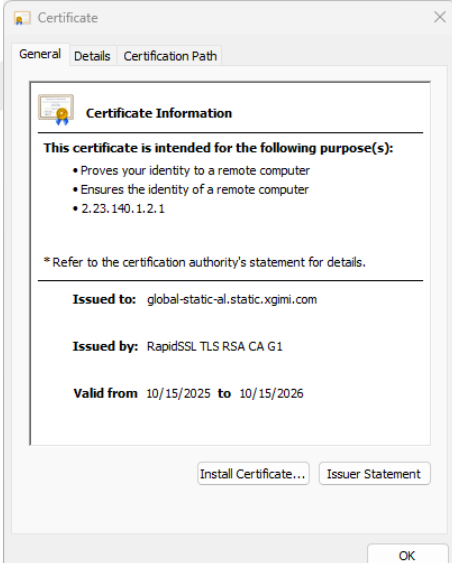
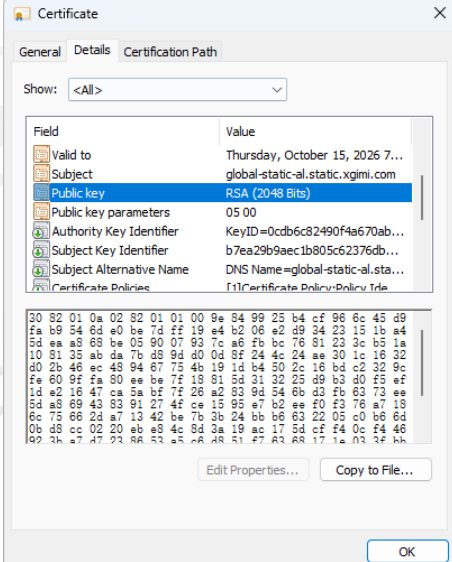
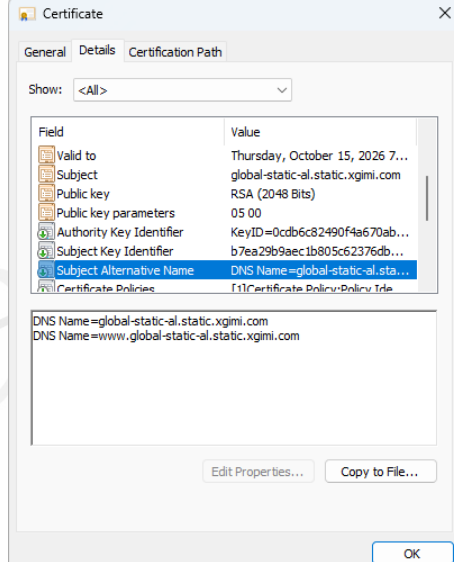
--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the authentication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the authentication mechanisms required by AUM-1-1 or AUM-1-2 comply with the requirement for AUM-6.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each authentication mechanism documented in [E.Info.AUM-6.AUM]:

	[AU.AUM-6.AuthenticatorComplexity]: If the method documented in [E.Info.AUM-6.AUM.BFProtection] belongs to [IC.AUM-6.AuthenticatorComplexity], functionally confirm the implementation of the methods documented in [E.Info.AUM-6.AUM.BFProtection] by: — trying to assign an authenticator that does not meet the complexity criteria documented in [E.Info.AUM-6.AUM.BFProtection]; and — performing a brute force attack on the authentication mechanism.
Result:	The RSA key length is 2048 bits.    
Assignment of verdict:	Pass

3.3 [SUM] Secure update mechanism

3.3.1 [SUM-1] Applicability of update mechanisms

--Conceptual assessment--

Identifier [SUM-1]-01	[E.Info.SUM-1.PartOfSoftw]: The device's entire software can be updated via the Internet.		
Decision node	Decision [E.Info.DT.SUM-1]	Justification [E.Just.DT.SUM-1]	
[DT.SUM-1.DN-5]	Yes (√)	No	[E.Info.SUM-1.PartOfSoftw.SUM]: The device connects to the OTA server via Wi-Fi or Ethernet, downloads the firmware, and completes the update.
Assignment of verdict:	Pass		

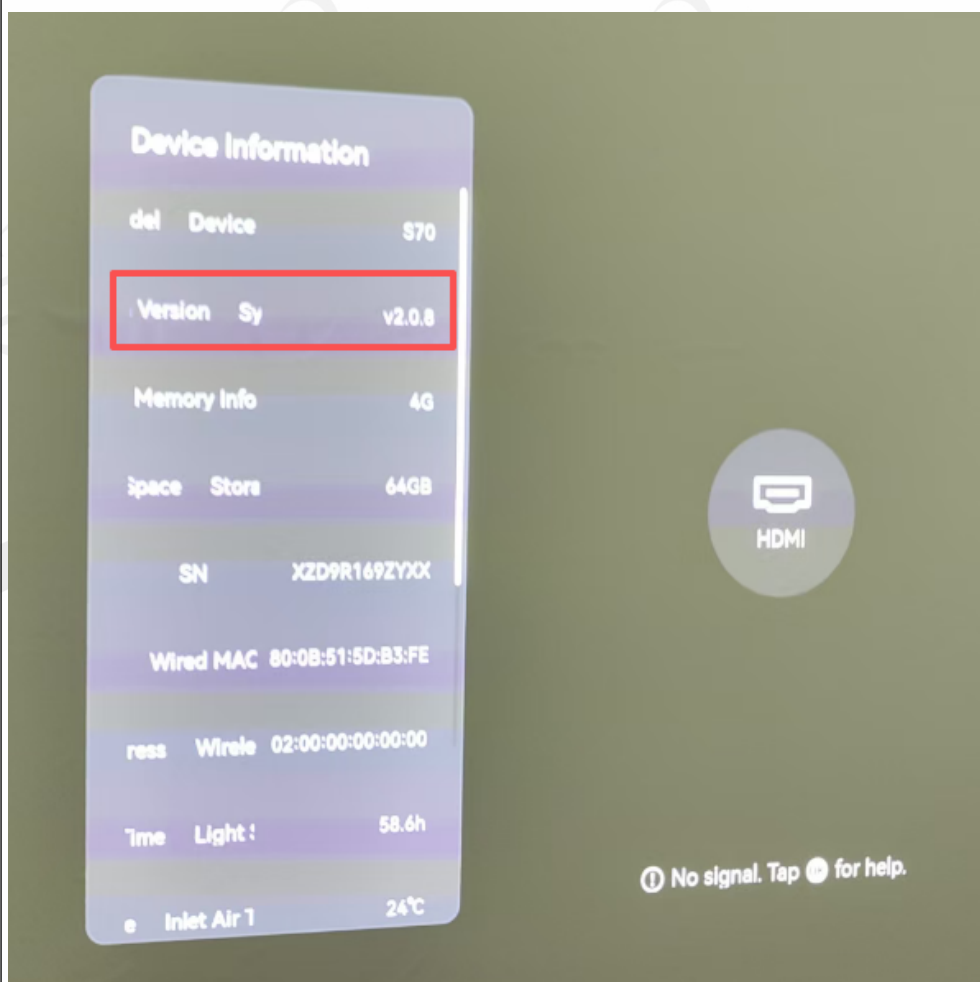
Identifier [SUM-1]-02	[E.Info.SUM-1.PartOfSoftw]: The device can be updated by reading the firmware file from a local USB flash drive.		
Decision node	Decision [E.Info.DT.SUM-1]	Justification [E.Just.DT.SUM-1]	
[DT.SUM-1.DN-5]	Yes (√)	No	[E.Info.SUM-1.PartOfSoftw.SUM]: The device can be updated by reading the firmware from a USB flash drive via the USB interface.
Assignment of verdict:	Pass		

--Completeness testing--

None.

--Sufficiency testing--

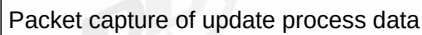
Assessment purpose:	The purpose of this assessment case is the functional assessment whether the equipment supports update mechanisms for parts of the software affecting security assets and/or network assets as documented in [E.Info.SUM-1.PartOfSoftw.SUM].
Preconditions:	The equipment is in an operational state. For each update mechanism described in [E.Info.SUM-1.PartOfSoftw.SUM], the manufacturer provides updated software (in the following: SW-a) which is integrity-protected and authenticity-protected using a mechanism that the equipment natively supports.
Operation steps:	For each update mechanism recorded in [E.Info.SUM-1.PartOfSoftw.SUM] that ends with "PASS" in the SUM-1 conceptual evaluation, install SW-a on the device.
Result:	1. The device connects to the OTA server via Wi-Fi and Ethernet, downloads the firmware, and completes the update. Version Before Update



Updating

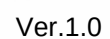


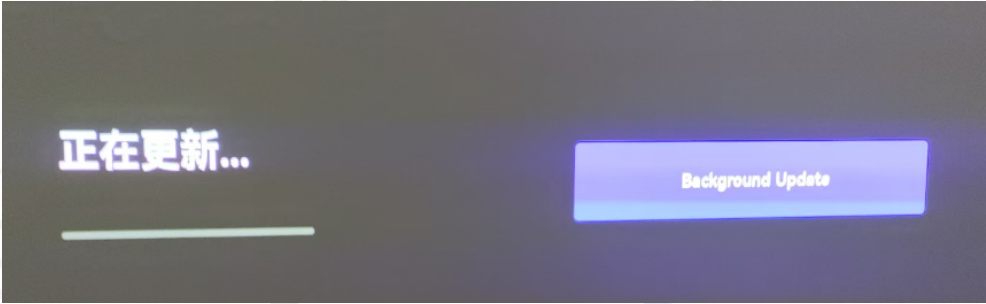
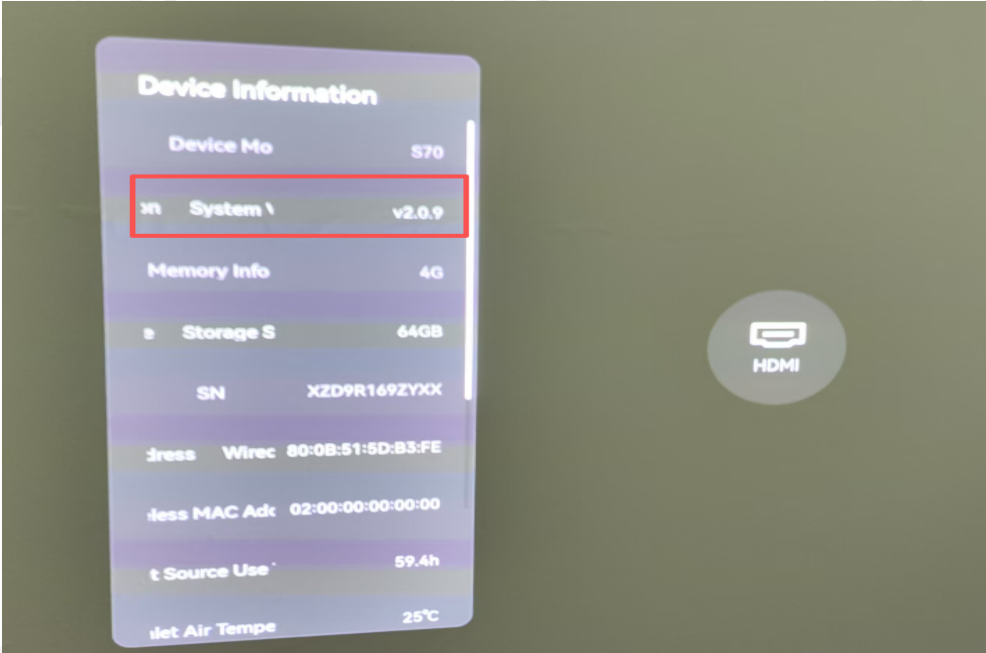
Version after update



373	49.	610833	222.217.94.16	192.168.137.7	222.217.94.17	TLVv1.3	618 Client Hello (SNI=global-static-al.static.xgimi.com)
404	49.	686563	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Server Hello, Change Cipher Spec, Application Data
408	49.	767946	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
409	49.	768046	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	251 Application Data, Application Data
412	49.	888821	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	118 Change Cipher Spec, Application Data
413	49.	887222	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	365 Application Data
414	49.	888438	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	365 Application Data
415	49.	909355	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	296 Application Data
417	49.	998560	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1807 Application Data
429	50.	005562	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
461	50.	075730	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
472	50.	075981	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
483	50.	093054	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
495	50.	095925	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
506	50.	099958	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
517	50.	104093	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
592	50.	194298	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
604	50.	197092	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data
615	50.	201476	222.217.94.17	192.168.137.7	222.217.94.17	TLVv1.3	1514 Application Data

- Version Before Update



	Updating  Version after update 
Assignment of verdict:	Pass

3.3.2 [SUM-2] Secure updates

--Conceptual assessment--

Identifier [SUM-2]-01	[E.Info.SUM-2.SUM]: The device connects to the OTA server, downloads the firmware, and completes the update.		
Decision node	Decision	Justification	
	[E.Info.DT.SUM-2]	[E.Just.DT.SUM-2]	
[DT.SUM-2.DN-1]	Yes (√)	No	[E.Info.SUM-2.SUM.SecChan]: [IC.SUM-2.AuthIntVal.SecChan]: During device updates, the firmware update package is downloaded from the update server via HTTPS (based on the TLS 1.3 protocol).
Assignment of verdict:	Pass		

Identifier	[E.Info.SUM-2.SUM]:
------------	---------------------

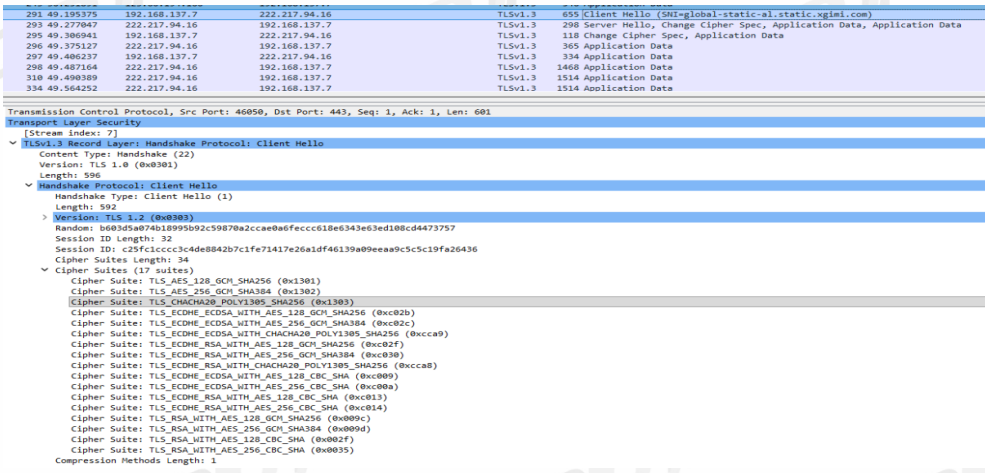
[SUM-2]-02	The device can be updated by reading the firmware file from a local USB flash drive.		
Decision node	Decision	Justification	
	[E.Info.DT.SUM-2]	[E.Just.DT.SUM-2]	
[DT.SUM-2.DN-1]	Yes (√)	No	[E.Info.SUM-2.SUM.Sign]: [IC.SUM-2.AuthIntVal.Sign]: The firmware package is digitally signed using a certificate-based SHA-256 with RSA2048 algorithm, ensuring integrity and authenticity.
Assignment of verdict:	Pass		

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the secure update mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

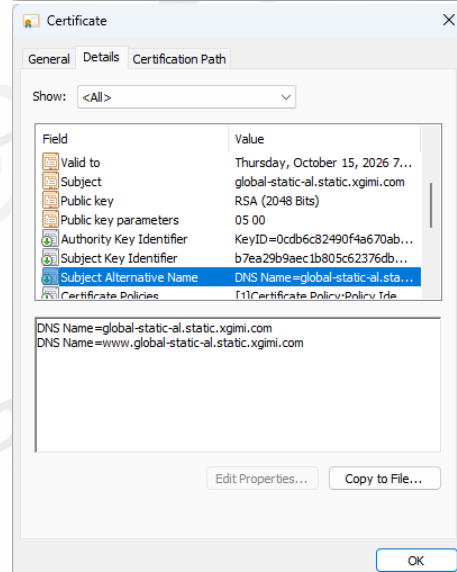
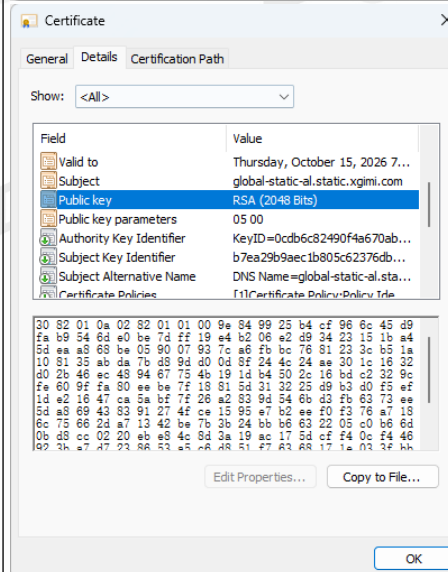
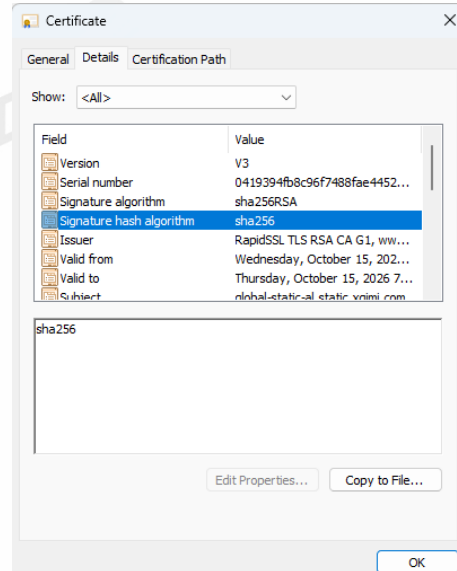
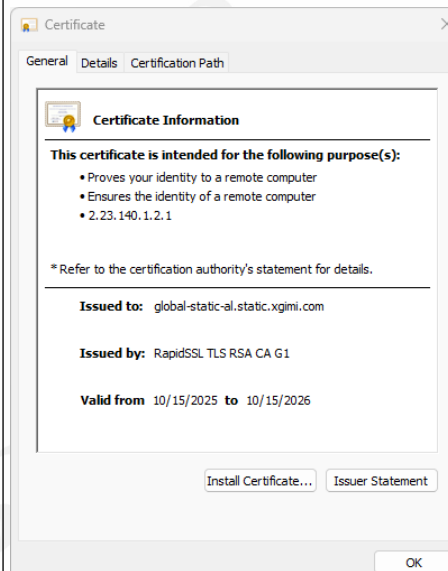
Assessment purpose:	The purpose of this assessment case is the functional assessment whether the update mechanisms for parts of the software affecting security assets and/or network assets only install software whose integrity and authenticity are valid at the time of the installation as documented in [E.Info.SUM-2.SUM.Generic].
Preconditions:	The equipment is in an operational state. For any update mechanism, the manufacturer provides updated software.
Operation steps:	For each update mechanism documented in [E.Info.SUM-2.SUM]: [AU.SUM-2.SecChan]: When the implementation is based on [IC.SUM-2.AuthIntVal.SecChan], functionally confirm that: — it is implemented using the secure communication mechanism according to SCM; and — a software update from an unauthorized source is not installed; and — the secure communication channel does not allow to impersonate the authorized software updates source via a man-in-the-middle attack; and — a software update that is modified during communication is not installed.
Result:	Online updates use the TLS 1.3 protocol for communication Client Hello 

Server Hello

291	49.195375	192.168.137.7	222.217.94.16	192.168.137.7	TLSv1.3	655 Client Hello (SN:global-static-al.static.xgimi.com)
293	49.277947	222.217.94.16	192.168.137.7	192.168.137.7	TLSv1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295	49.306941	192.168.137.7	222.217.94.16	192.168.137.7	TLSv1.3	118 Change Cipher Spec, Application Data
296	49.375127	222.217.94.16	192.168.137.7	192.168.137.7	TLSv1.3	365 Application Data
297	49.406237	192.168.137.7	222.217.94.16	192.168.137.7	TLSv1.3	334 Application Data
298	49.487164	222.217.94.16	192.168.137.7	192.168.137.7	TLSv1.3	1468 Application Data
310	49.490389	222.217.94.16	192.168.137.7	192.168.137.7	TLSv1.3	1514 Application Data
334	49.564252	222.217.94.16	192.168.137.7	192.168.137.7	TLSv1.3	1514 Application Data

> Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \Device\NPF_{A2009E98-90CA-4773-A2C0-588161605298}, id 0
> Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1)
> Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7
> Transmission Control Protocol, Src Port: 443, Dst Port: 46050, Seq: 1, Ack: 602, Len: 244
✓ Transport Layer Security
[Stream index: 7]
✓ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 128
✓ Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 124
Version: TLS 1.2 (0x0303)
Random: 007f1c4c9b0d6732750948dea4756977cbc8f2e4e91b13a40fd74127b6ec35
Session ID Length: 32
Session ID: c25f1cccc3c4de8842b7c1fe71417e26ald46139a09eeaa9c5c19fa26436
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Compression Method: null (0)
Extensions Length: 52
Extension: supported_versions (len=2) TLS 1.3
Extension: key_share (len=36) x25519
Extension: pre_shared_key (len=2)
[JA3S Fullstring: 771,4865,43-51-41]
[JA3S: fcb2d4d0991292272fcb1e464eedfd43]

Certificate



The firmware package is digitally signed using a certificate-based SHA-256 with RSA2048

```

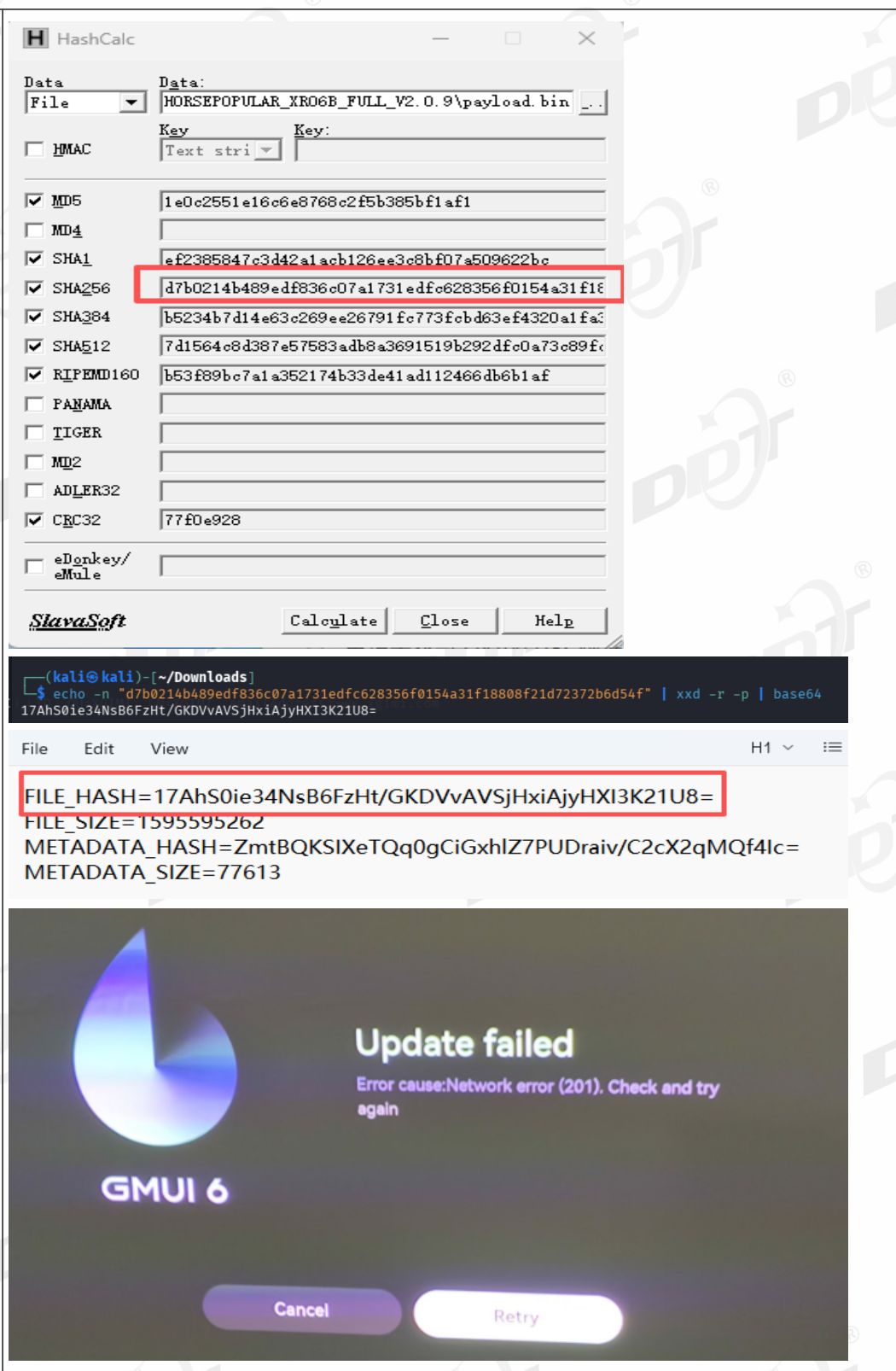
199104474 0xBE17DA AKM instructions, function prototype
199539884 0x8E4BCAC xz compressed data
200902048 0xBF985A0 xz compressed data
202353372 0xC0FAADC xz compressed data
203673116 0xC23CE1C xz compressed data
205157616 0xC3A74F0 xz compressed data
205953596 0xC469A3C Zip archive data, at least v2.0 to extract, name: META-INF/CERT
.RSA
205955650 0xC46A242 Zip archive data, at least v2.0 to extract, name: META-INF/MANIFEST.MF
205992260 0xC473144 Certificate in DER format (x509 v3), header length: 4, sequence
length: 1607
206102965 0xC48E1B5 Zip archive data, at least v1.0 to extract, compressed size: 67
109216, uncompressed size: 353435392, name:

```

```
ta/boot.config
1335191515 0x4F9567DB Zip archive data, at least v2.0 to extract, name: assets/bin/Da
ta/data.unity3d
1335599490 0x4F9BA182 JB00T STAG header, image id: 14, timestamp 0xCDA73ECD, image si
ze: 4219715997 bytes, image JB00T checksum: 0xD3BF, header JB00T checksum: 0xFA5E
1338678655 0x4FCA9D7F JB00T STAG header, image id: 0, timestamp 0x3B41A484, image siz
e: 388422537 bytes, image JB00T checksum: 0x8429, header JB00T checksum: 0x4B18
1346557887 0x5042D7BF xz compressed data
1346621463 0x5043D017 ARM instructions, function prologue
1348653547 0x5062D1EB xz compressed data
1349435204 0x506EBF44 Certificate in DER format (x509 v3), header length: 4, sequence
length: 998
1350234935 0x507AF337 xz compressed data
```

The device fails to upgrade after a locally modified firmware package is installed.



	
Assignment of verdict:	Pass

3.3.3 [SUM-3] Automated updates

--Conceptual assessment--

Identifier	[E.Info.SUM-3.SUM]:
------------	---------------------

[SUM-3]-01	The device connects to the manufacturer's OTA server, downloads the firmware, and completes the update.		
Decision node	Decision		Justification
	[E.Info.DT.SUM-3]		[E.Just.DT.SUM-3]
[DT.SUM-3.DN-3]	Yes (✓)	No	[E.Info.SUM-3.SUM.Automation]: After the device is connected to the Internet, it will automatically check the update server for the latest version. If a new version is available, the device will prompt the user that a new version exists. When the user clicks the Update button, the device will automatically download the software from the update server. Once the download is complete, the device will execute the software update. After the update is finished, the newly updated version number can be viewed.
Assignment of verdict:	Pass		

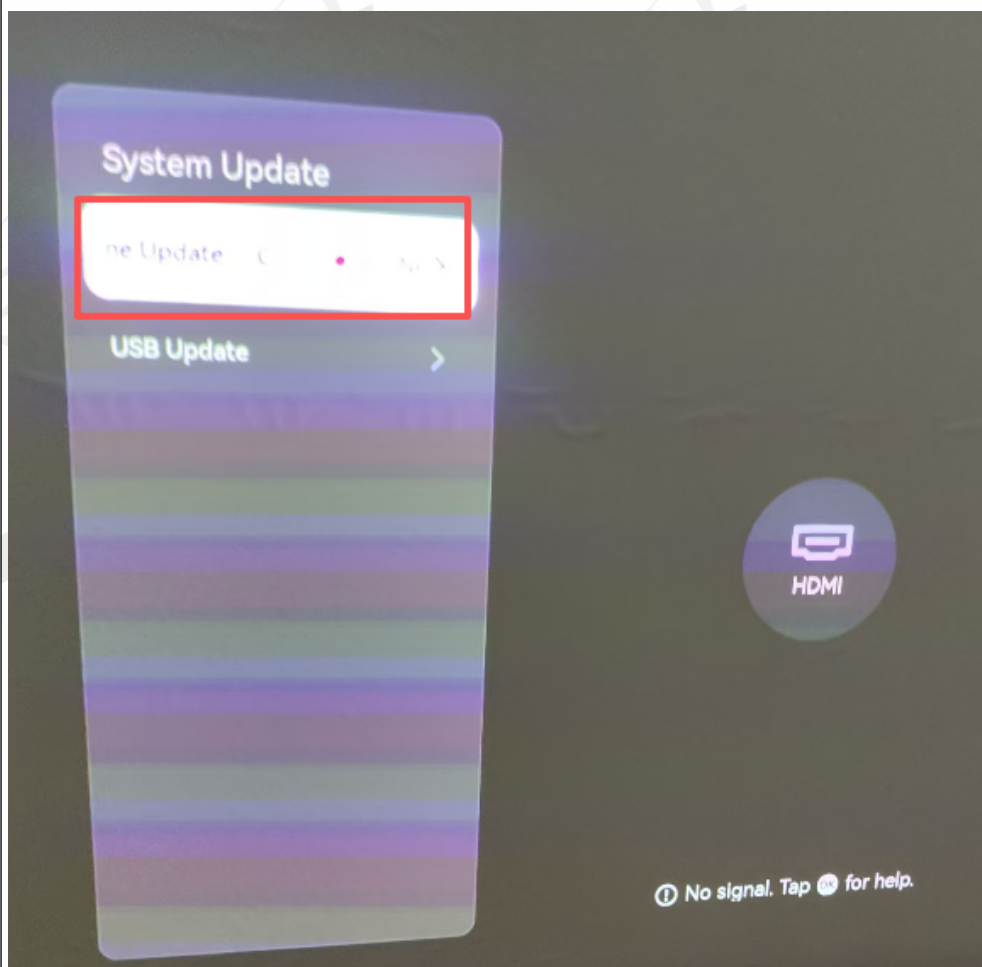
--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the secure update mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

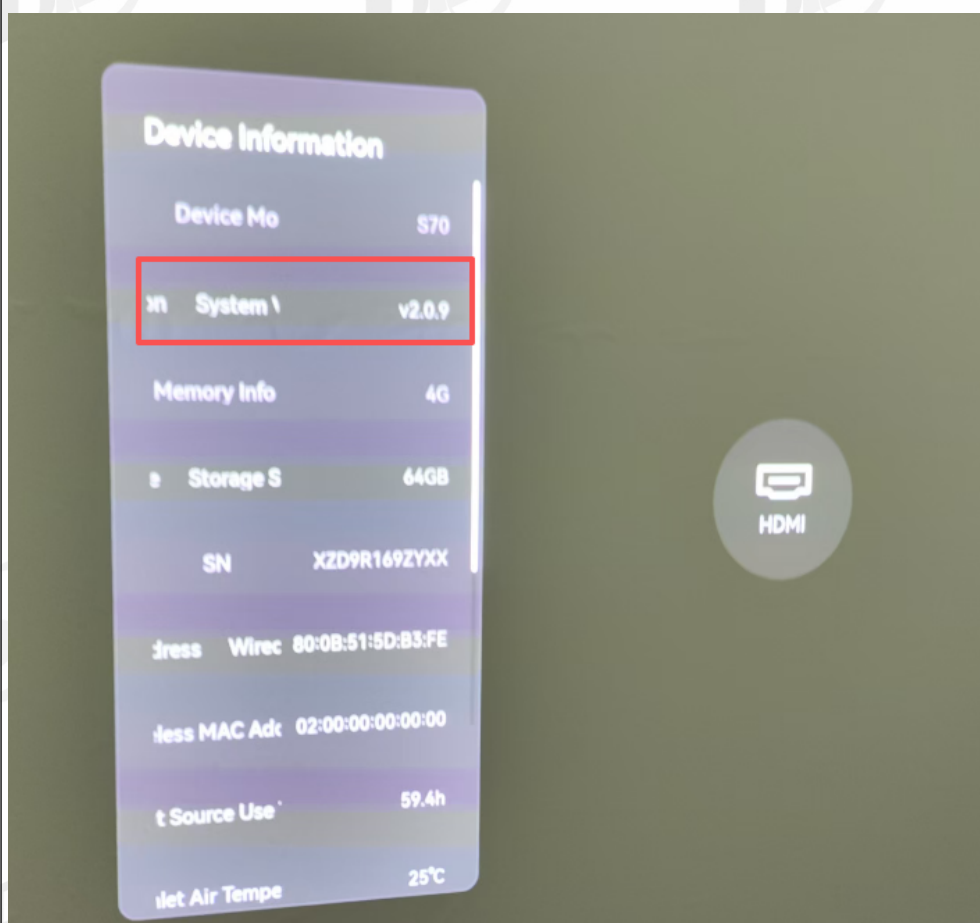
Assessment purpose:	The purpose of this assessment case is the functional assessment whether the update mechanisms for parts of the software affecting security assets and/or network assets are automated as documented in [E.Info.SUM-3.SUM.Automation].
Preconditions:	The equipment is in an operational state. The manufacturer provides the means to perform automated updates.
Operation steps:	For each update mechanism documented in [E.Info.SUM-3.SUM] functionally assess whether the automation implementation deviates from [E.Info.SUM-3.SUM.Automation] by: — checking the software version on the equipment; and — making a software update available at the source holding security updates; and — checking whether the equipment performs the software update: - o without human intervention at the equipment; or - o via scheduling the installation of an update under human approval; or - o via triggering the installation of an update under human approval; and — checking on the equipment that the software version has been updated to a new version number.
Result:	The device prompts that an update is available.



Packet capture of online firmware update.

356 49.581056	222.217.94.16	192.168.137.7	TLsv1.3	1514 Application Data
373 49.610833	192.168.137.7	222.217.94.17	TLsv1.3	618 Client Hello (SNI=global-static-al.static.xgimi.com)
404 49.686563	222.217.94.17	192.168.137.7	TLsv1.3	1514 Server Hello, Change Cipher Spec, Application Data
408 49.767946	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
409 49.768046	222.217.94.17	192.168.137.7	TLsv1.3	251 Application Data, Application Data
412 49.808821	192.168.137.7	222.217.94.17	TLsv1.3	118 Change Cipher Spec, Application Data
413 49.887222	222.217.94.17	192.168.137.7	TLsv1.3	365 Application Data
414 49.888438	222.217.94.17	192.168.137.7	TLsv1.3	365 Application Data
415 49.909355	192.168.137.7	222.217.94.17	TLsv1.3	296 Application Data
417 49.908560	222.217.94.17	192.168.137.7	TLsv1.3	1007 Application Data
429 50.005562	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
461 50.075730	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
472 50.075993	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
483 50.093054	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
495 50.095925	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
506 50.099958	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
517 50.104093	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
592 50.194298	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
604 50.197092	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
615 50.201476	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
626 50.204164	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
637 50.208165	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
711 50.208747	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
722 50.281259	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
733 50.282148	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
744 50.282833	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
756 50.283996	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
767 50.284625	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
778 50.285489	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data
789 50.298875	222.217.94.17	192.168.137.7	TLsv1.3	1514 Application Data

Version of the device after the update.



Assignment of
verdict:

Pass

3.4 [SSM] Secure storage mechanism

3.4.1 [SSM-1] Applicability of secure storage mechanisms

--Conceptual assessment--

Identifier	[E.Info.SSM-1.SecurityAsset]:
[SSM-1]-01	SecurityAsset-1.1: HTTPS certificate

	SecurityAsset-1.2: Wi-Fi password SecurityAsset-1.3: The AES-CCM-128 encryption key used in the Bluetooth 5.2 protocol is generated through negotiation during the first pairing process and then stored in the device's flash memory. SecurityAsset-1.4: Public Key for OTA Signature Verification		
Decision node	Decision		Justification
	[E.Info.DT.SSM-1]		[E.Just.DT.SSM-1]
[DT.SSM-1.DN-1]	Yes (✓)	No	[E.Info.SSM-1.SecurityAsset.SSM]: The asset is stored inside the device, protected by its outer casing, with no interface available for accessing the asset.
Assignment of verdict:	N/A		

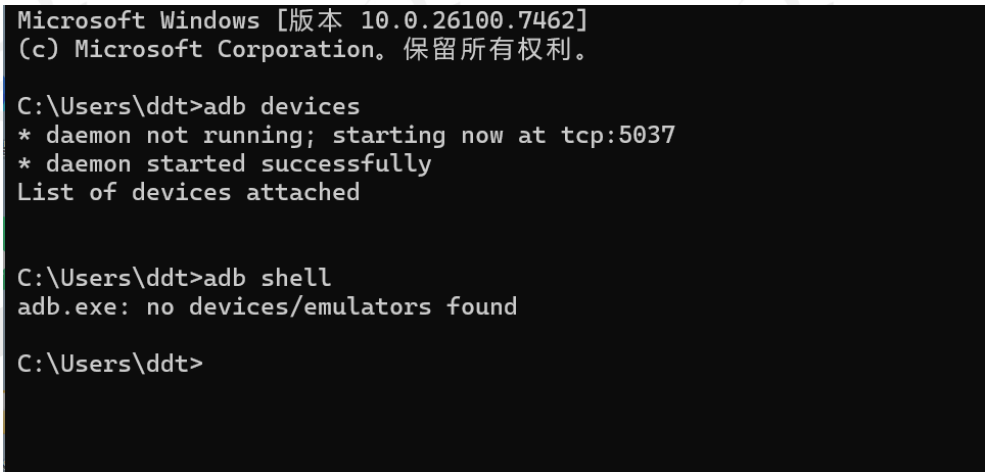
Identifier [SSM-1]-02	[E.Info.SSM-1.NetworkAsset]: NetworkAsset-5.1: Paired Devices Access Rights NetworkAsset-5.2: Saved Wi-Fi Networks NetworkAsset-5.3: Network configuration parameters		
Decision node	Decision		Justification
	[E.Info.DT.SSM-1]		[E.Just.DT.SSM-1]
[DT.SSM-1.DN-1]	Yes (✓)	No	[E.Info.SSM-1.NetworkAsset.SSM]: Physical contact with the device is required to access this asset.
Assignment of verdict:	N/A		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether security assets documented in [E.Info.SSM-1.SecurityAsset] and network assets documented in [E.Info.SSM-1.NetworkAsset] are complete.
Preconditions:	The equipment is in an operational state.
Operation steps:	Functionally assess whether there are security assets persistently stored on the equipment, which are not listed in [E.Info.SSM-1.SecurityAsset]. Functionally assess whether there are network assets persistently stored on the equipment, which are not listed in [E.Info.SSM-1.NetworkAsset].
Result:	/
Assignment of verdict:	N/A

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether secure storage mechanisms are implemented when required per SSM-1.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each security asset documented in [E.Info.SSM-1.SecurityAsset], functionally confirm it is persistently stored solely via secure storage mechanisms documented in [E.Info.SSM-

	1.SecurityAsset.SSM]. For each network asset documented in [E.Info.SSM-1.NetworkAsset], functionally confirm it is persistently stored solely via secure storage mechanisms documented in [E.Info.SSM-1.NetworkAsset.SSM].
Result:	The device does not support ADB access. 
Assignment of verdict:	N/A

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

--Conceptual assessment--

Identifier [SSM-2]-01	/		
Decision node	Decision [E.Info.DT.SSM-2]	Justification [E.Just.DT.SSM-2]	
/	/	/	/
Assignment of verdict:	N/A For the security assets and network assets stored persistently in SSM-1, physical or logical measures have been implemented in the target environment to ensure that only authorized entities can access such assets stored on the device, with no other secure storage mechanisms in place.		

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the secure storage mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the secure storage mechanisms required per SSM-1 provide the required integrity protection.
Preconditions:	The equipment is in an operational state.
Operation steps:	/

Result:	/
Assignment of verdict:	N/A

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

--Conceptual assessment--

Identifier [SSM-3]-01	/		
Decision node	Decision [E.Info.DT.SSM-3]	Justification [E.Just.DT.SSM-3]	
/	/	/	/
Assignment of verdict:	N/A For the security assets and network assets stored persistently in SSM-1, physical or logical measures have been implemented in the target environment to ensure that only authorized entities can access such assets stored on the device, with no other secure storage mechanisms in place.		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the assets documented in [E.Info.SSM-3.SSM.Asset] are complete.
Preconditions:	The equipment is in an operational state.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the secure storage mechanisms required per SSM-1 that persistently store confidential security parameters or confidential network function configuration provide the required confidentiality protection.
Preconditions:	The equipment is in an operational state.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A

3.5 [SCM] Secure communication mechanism

3.5.1 [SCM-1] Applicability of secure communication mechanisms

--Conceptual assessment--

Identifier	[E.Info.SCM-1.NetworkInterface]:
------------	----------------------------------

[SCM-1]-01	Bluetooth BR/EDR/LE		
Decision node	Decision		Justification
	[E.Info.DT.SCM-1]		[E.Just.DT.SCM-1]
[DT.SCM-1.DN-1]	Yes (✓)	No	[E.Info.SCM-1.NetworkInterface.Protocol]: Bluetooth protocol 5.2 [E.Info.SCM-1.NetworkInterface.Radio]: 2402~2480 MHz [E.Info.SCM-1.SecurityAsset]: Bluetooth pairing code [E.Info.SCM-1.SecurityAsset.Com]: When the device establishes a connection with other devices for the first time, it will be paired based on the Bluetooth pairing code. [E.Info.SCM-1.SecurityAsset.NetworkInterface]: Bluetooth interface [E.Info.SCM-1.SCM]: Common Bluetooth handshake process [E.Info.SCM-1.SCM.Protocol]: Bluetooth protocol 5.2 [E.Info.SCM-1.SCM.States]: When the device establishes a connection with other devices for the first time. [E.Info.SCM-1.SCM.SecObjectives]: It prevents man-in-the-middle attacks and protects the security of the device's assets during the communication process.
Assignment of verdict:	Pass		

Identifier [SCM-1]-02	[E.Info.SCM-1.NetworkInterface]: Wi-Fi		
Decision node	Decision		Justification
	[E.Info.DT.SCM-1]		[E.Just.DT.SCM-1]
[DT.SCM-1.DN-1]	Yes (✓)	No	[E.Info.SCM-1.NetworkInterface.Protocol]: IEEE 802.11, 802.11 a/b/g/n/ac/ax, WPA/WPA2-PSK(TKIP/AES), WPA3-SAE(AES), WPA2-PSK/WPA3-SAE(AES), TLS 1.3, Open SSL 3.0.15 [E.Info.SCM-1.NetworkInterface.Radio]: 2.412GHz~2.472GHz, 5.15GHz~5.35GHz, 5.47GHz~5.85GHz [E.Info.SCM-1.SecurityAsset]: SecurityAsset-2.1: The DUT connects to the server via Wi-Fi. SecurityAsset-2.3: Perform over-the-air (OTA) firmware updates for devices via the OTA server. [E.Info.SCM-1.SecurityAsset.Com]: The TLS 1.3 protocol is used for connecting the DUT to the server, with business instructions transmitted via this secure channel to perform business operations. [E.Info.SCM-1.SecurityAsset.NetworkInterface]: Wi-Fi interface [E.Info.SCM-1.SecurityAsset.Class]: SecurityAsset-1.1, SecurityAsset-1.2, SecurityAsset-2.1, SecurityAsset-2.3 [E.Info.SCM-1.NetworkAsset.Class]: NetworkAsset-1.2, NetworkAsset-1.3, NetworkAsset-2.1, NetworkAsset-3.1, NetworkAsset-5.2, NetworkAsset-5.3

		[E.Info.SCM-1.SCM]: Common Wi-Fi handshake process [E.Info.SCM-1.SCM.Protocol]: IEEE 802.11, 802.11 a/b/g/n/ac/ax, WPA/WPA2-PSK(TKIP/AES), WPA3-SAE(AES), WPA2-PSK/WPA3-SAE(AES), TLS 1.3, Open SSL 3.0.15 [E.Info.SCM-1.SCM.States]: When the device is connected to the router's Wi-Fi network. [E.Info.SCM-1.SCM.SecObjectives]: It prevents man-in-the-middle attacks and protects the security of the device's assets during the communication process.
Assignment verdict:	of	Pass

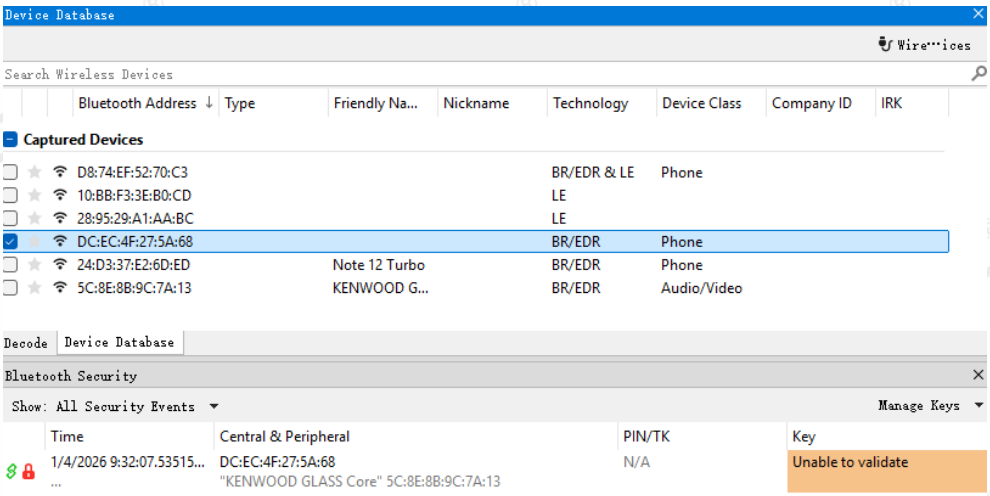
Identifier [SCM-1]-03	[E.Info.SCM-1.NetworkInterface]: Ethernet (LAN)	
Decision node	Decision [E.Info.DT.SCM-1]	Justification [E.Just.DT.SCM-1]
DT.SCM-1.DN-1	Yes (✓)	No [E.Info.SCM-1.NetworkInterface.Protocol]: IEEE 802.3, DHCP Server, Static IP, IPv4/IPv6, IGMP Snooping, HTTPS, TLS 1.3, Open SSL 3.0.15 [E.Info.SCM-1.NetworkInterface.Radio]: 10Mbps-1000Mbps [E.Info.SCM-1.SecurityAsset]: SecurityAsset-2.2: The DUT connects to the server via Ethernet. SecurityAsset-2.3: Perform over-the-air (OTA) firmware updates for devices via the OTA server. [E.Info.SCM-1.SecurityAsset.Com]: The TLS 1.3 protocol is used for connecting the DUT to the server, with business instructions transmitted via this secure channel to perform business operations. [E.Info.SCM-1.SecurityAsset.NetworkInterface]: Ethernet interface [E.Info.SCM-1.SecurityAsset.Class]: SecurityAsset-1.1, SecurityAsset-2.2, SecurityAsset-2.3 [E.Info.SCM-1.NetworkAsset.Class]: NetworkAsset-2.1, NetworkAsset-5.3 [E.Info.SCM-1.SCM.Protocol]: IEEE 802.3, DHCP Server, Static IP, IPv4/IPv6, IGMP Snooping, HTTPS, TLS 1.3, Open SSL 3.0.15 [E.Info.SCM-1.SCM.States]: When wired devices are connected via Ethernet cables. [E.Info.SCM-1.SCM.SecObjectives]: During communication, it can prevent man-in-the-middle attacks and protect the security of device assets.
Assignment of	Pass	

verdict:	
----------	--

--Completeness testing--

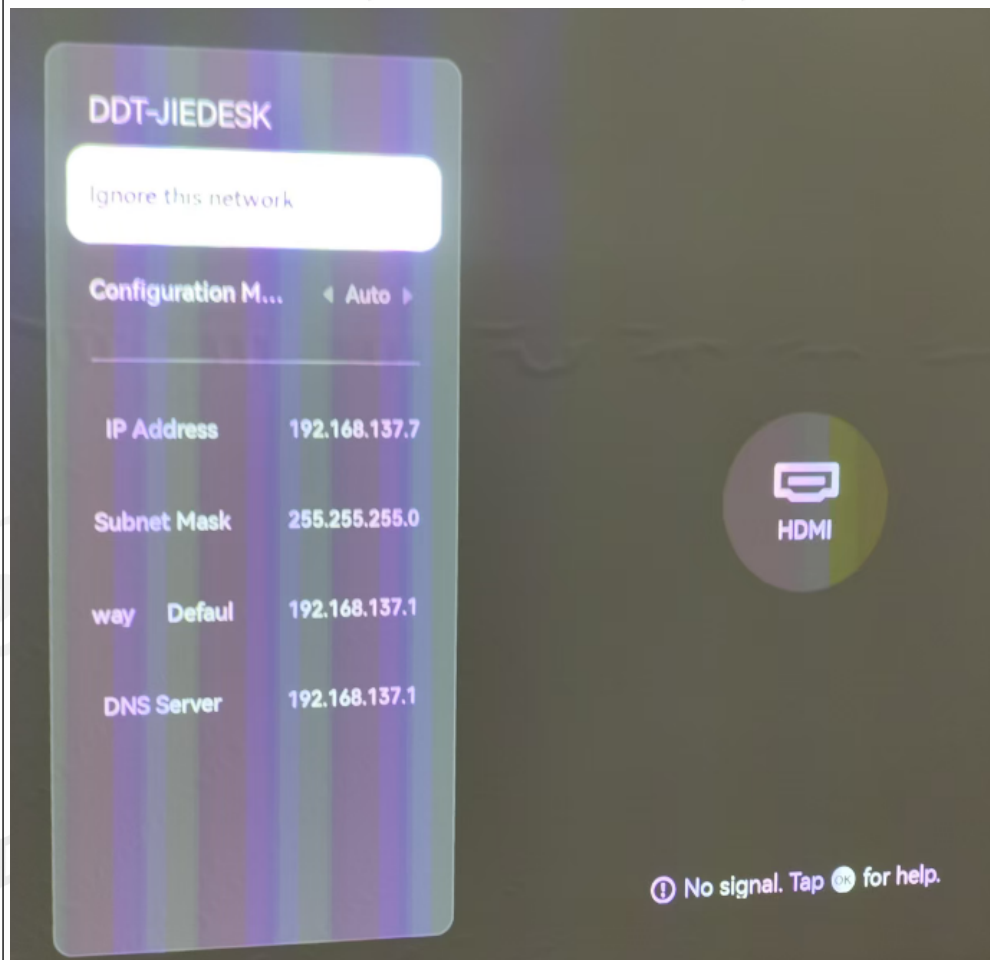
Assessment purpose:	The purpose of this assessment case is the functional assessment whether the documentation is complete.
Preconditions:	The equipment is in an operational state.
Operation steps:	Using the latest assessment methods, functionally assess whether there are stored security assets that have engaged in communication and are not recorded in [E.Info.SCM-1.SecurityAsset]. Using the latest assessment methods, functionally assess whether there are stored network assets that have engaged in communication and are not recorded in [E.Info.SCM-1.NetworkAsset].
Result:	All stored security assets identified as having communicated are recorded in [E.Info.SCM-1.SecurityAsset], and all identified network assets are recorded in [E.Info.SCM-1.NetworkAsset].
Assignment of verdict:	Pass

--Sufficiency testing--

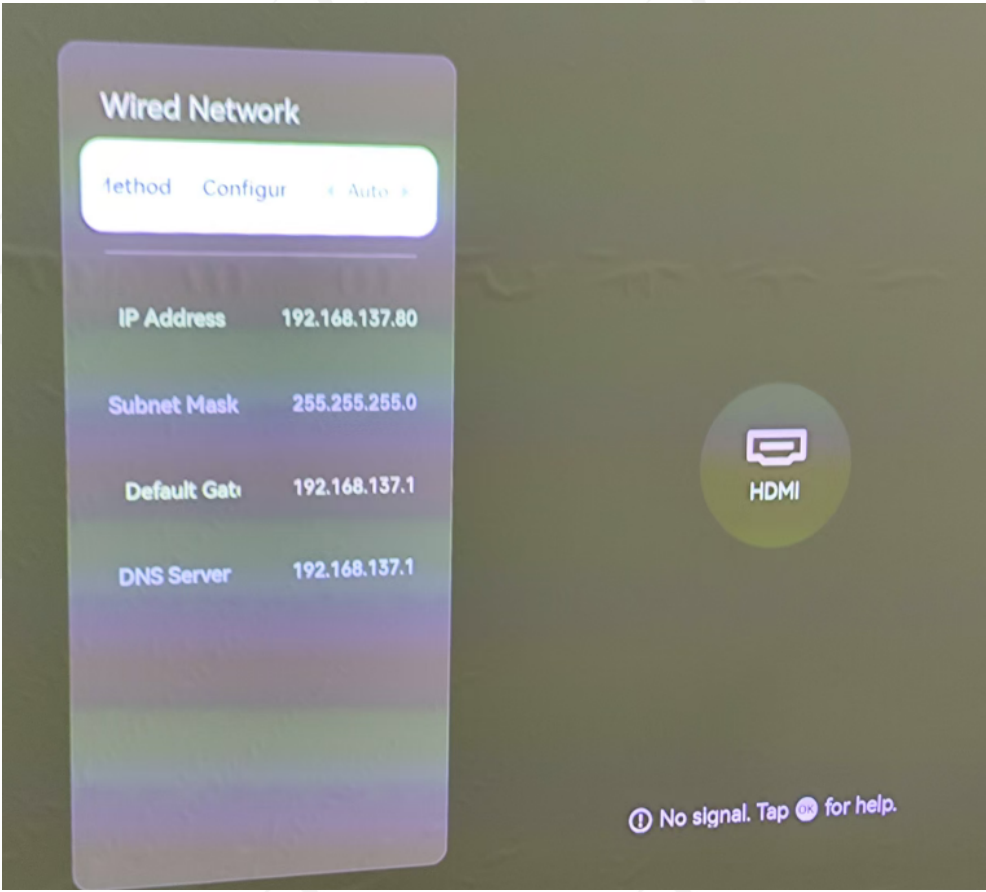
Assessment purpose:	The purpose of this assessment case is the functional assessment whether the secure communication mechanisms are implemented when they are required per SCM-1.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each security asset recorded in [E.Info.SCM-1.SecurityAsset] and each network asset recorded in [E.Info.SCM-1.NetworkAsset], using the latest assessment methods, functionally confirm the existence of secure communication mechanisms in accordance with [E.Info.SCM-1.SCM] and taking into account the recorded device status.
Result:	There is no evidence that the secure communication mechanisms recorded in [E.Info.SCM-1.SCM] have not been implemented. Bluetooth BR/EDR/LE broadcast: 

Device Database								
Search Wireless Devices								
	Bluetooth Address ↓	Type	Friendly Na...	Nickname	Technology	Device Class	Company ID	IRK
Captured Devices								
☐	F9:A5:F5:FB:C5:A2	Static			LE			
☐	F5:36:FE:F9:F0:1B	Static			LE			
☐	DE:3A:1E:57:04:D5	Static			LE			
☒	DC:EC:4F:27:5A:68				LE			
☐	7F:C5:BB:0E:58:C3	RPA			LE			
☐	7F:A0:8D:43:5C:22	RPA			LE			
☐	7D:9A:02:C8:BA:91	RPA			LE			
Decode Device Database								
Bluetooth Security								
Show: All Security Events					Manage Keys			
	Time	Central & Peripheral	PIN/TK	Key				
	1/6/2026 1:49:00.56642...	DC:EC:4F:27:5A:68 60:68:32:4D:9D:8E	Just Works	Enter Long Term Key				

Wi-Fi connection:



Ethernet (LAN):

	
Assignment of verdict:	Pass

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

--Conceptual assessment--

Identifier [SCM-2]-01	[E.Info.SCM-2.SCM]: Wi-Fi networking uses the TLS 1.3 protocol to establish a connection with the server, HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack.		
Decision node	Decision	[E.Info.DT.SCM-2]	Justification [E.Just.DT.SCM-2]
[DT.SCM-2.DN-2]	Yes (✓)	No	[E.Info.SCM-2.SecurityAsset]: Over-the-Air (OTA) Firmware Update [E.Info.SCM-2.SecurityAsset.Com]: Online Firmware Upgrade is enabled through secure HTTPS communication based on the OpenSSL 3.0.15 library. [E.Info.SCM-2.NetworkInterface]: Wi-Fi [E.Info.SCM-2.NetworkInterface.Protocol]:HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack. [E.Info.SCM-2.SCM]: HTTPS [E.Info.SCM-2.SCM.Capabilities]: HTTPS with TLS 1.3.

			Communication Encryption Suite: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA [E.Info.SCM-2.SCM.Generic]: [IC.SCM-2 Generic]: Signed certificate for communication with the companion application.
Assignment of verdict:	N/A		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 1. These cipher suites use encryption and hashing algorithms that are no longer recommended. While they provide basic encryption capabilities, they lack enhanced support for data integrity and authentication. 2. For the purpose of compatibility with communications of other products or services, the adopted encryption algorithm suite is not based on best practices (but rather prioritizes compatibility).

Identifier [SCM-2]-02	[E.Info.SCM-2.SCM]: The LAN uses the TLS 1.3 protocol to establish a connection with the server, HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack.		
Decision node	Decision [E.Info.DT.SCM-2]	Justification [E.Just.DT.SCM-2]	
DT.SCM-2.DN-2	Yes (✓)	No	[E.Info.SCM-2.SecurityAsset]: Over-the-Air (OTA) Firmware Update [E.Info.SCM-2.SecurityAsset.Com]: Online Firmware Upgrade is enabled through secure HTTPS communication based on the OpenSSL 3.0.15 library. [E.Info.SCM-2.NetworkInterface]: LAN [E.Info.SCM-2.NetworkInterface.Protocol]:HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack.

			[E.Info.SCM-2.SCM]: HTTPS [E.Info.SCM-2.SCM.Capabilities]: HTTPS with TLS 1.3. Communication Encryption Suite: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA [E.Info.SCM-2.SCM.Generic]: [IC.SCM-2 Generic]: Signed certificate for communication with the companion application.
Assignment of verdict:	N/A TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 1. These cipher suites use encryption and hashing algorithms that are no longer recommended. While they provide basic encryption capabilities, they lack enhanced support for data integrity and authentication. 2. For the purpose of compatibility with communications of other products or services, the adopted encryption algorithm suite is not based on best practices (but rather prioritizes compatibility).		

Identifier [SCM-2]-03	[E.Info.SCM-2.SCM]: Bluetooth BR/EDR/LE adopts the Bluetooth 5.2 protocol. The device achieves communication via proprietary services, with the AES-CCM-128 algorithm employed for encryption.		
Decision node	Decision	Justification	
	[E.Info.DT.SCM-2]	[E.Just.DT.SCM-2]	
DT.SCM-2.DN-1	Yes (√)	No	[E.Info.SCM-2.SCM.CCK]: The AES-CCM-128 algorithm is implemented based on the hardware AES at the underlying level, and the random numbers are true random numbers generated by the hardware TRNG (True Random Number Generator). [E.Info.SCM-2.NetworkInterface]:

		Bluetooth interface [E.Info.SCM-2.NetworkInterface.Protocol]: Bluetooth 5.2 protocol [E.Info.SCM-2.SecurityAsset.Com]: During the network provisioning process, the user device pairs and connects with the device under test via a Bluetooth pairing code. [E.Info.SCM-2.SCM.ThreatProtection]: It prevents man-in-the-middle attacks and protects the security of the device's assets during the communication process. [E.Info.SCM-2.SCM.Capabilities]: It prevents man-in-the-middle attacks and protects the security of the device's assets during the communication process. [E.Info.SCM-2.SCM.SecChanExchange]: When the device pairs with other devices, an AES-128 key will be negotiated according to the Bluetooth protocol, and all subsequent communications will be encrypted with this key. [E.Info.SCM-2.SCM.ImplDetail]: When the device pairs with other devices, an AES-128 key will be negotiated according to the Bluetooth protocol, and all subsequent communications will be encrypted with this key.
Assignment of verdict:	Pass	

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the secure communication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the security assets and network assets communicated are protected against unnoticed tampering.
Preconditions:	The equipment is in an operational state.
Operation steps:	[AU.SCM-2.PKI-based]: For [IC.SCM-2.AU.SCM-2.PKI-based], in accordance with the records in [E.Info.SCM-2.SCM.AU.SCM-2.PKI-based], functionally confirm the following: — Forged certificates are not accepted; and — Tampered information is not regarded as having integrity; and — Unauthorized messages are not regarded as authentic messages; and — If channel-based communication is used, Man-in-the-Middle (MitM) attacks cannot succeed.
Result:	Wi-Fi: The device connects to the Internet via Wi-Fi, and WireShark is used for packet capture during the device's firmware upgrade.

属性

网络属性

编辑

名称: DDT-JIEDESK
密码: 123456789
频段: 2.4 GHz

扫描以连接:



已连接的设备: 1台(共 8台)

设备名称	IP 地址	物理地址(MAC)
未知	192.168.137.7	d6:22:0b:c1:e4:a1

Client Hello

291 49.195375	192.168.137.7	222.217.94.16	TLSv1.3	655 Client Hello (SNI=global-static-al.static.xgimi.com)
293 49.277047	222.217.94.16	192.168.137.7	TLSv1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295 49.306941	192.168.137.7	222.217.94.16	TLSv1.3	118 Change Cipher Spec, Application Data
296 49.375127	222.217.94.16	192.168.137.7	TLSv1.3	365 Application Data
297 49.406237	192.168.137.7	222.217.94.16	TLSv1.3	334 Application Data
298 49.487164	222.217.94.16	192.168.137.7	TLSv1.3	1468 Application Data
310 49.490389	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
334 49.564252	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data

Transmission Control Protocol, Src Port: 46050, Dst Port: 443, Seq: 1, Ack: 1, Len: 601

Transport Layer Security

(Stream Index: 7)

TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 596

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 592

> Version: TLS 1.2 (0x0303)

Random: b603d5a074b18995b92c59870a2ccae0a6feccc618e634e3ed108cd4473757

Session ID Length: 32

Session ID: c25fc1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c5c19fa26436

Cipher Suites Length: 34

> Cipher Suites (17 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc02d)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc013)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA256 (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

Server Hello

291 49.195375	192.168.137.7	222.217.94.16	TLSv1.3	655 Client Hello (SNI=global-static-al.static.xgimi.com)
293 49.277047	222.217.94.16	192.168.137.7	TLSv1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295 49.306941	192.168.137.7	222.217.94.16	TLSv1.3	118 Change Cipher Spec, Application Data
296 49.375127	222.217.94.16	192.168.137.7	TLSv1.3	365 Application Data
297 49.406237	192.168.137.7	222.217.94.16	TLSv1.3	334 Application Data
298 49.487164	222.217.94.16	192.168.137.7	TLSv1.3	1468 Application Data
310 49.490389	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
334 49.564252	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data

> Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \Device\NPF_{A2009E98-90CA-4773-A2C0-58B161605298}, id 0

> Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1)

> Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7

> Transmission Control Protocol, Src Port: 443, Dst Port: 46050, Seq: 1, Ack: 602, Len: 244

Transport Layer Security

(Stream Index: 7)

TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 128

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 124

> Version: TLS 1.2 (0x0303)

Random: 007f1cc4c9bd86732750948dea47576977cbc8f2e4e91b13a40fd74127b6ec35

Session ID Length: 32

Session ID: c25fc1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c5c19fa26436

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 52

> Extension: supported_versions (len=2) TLS 1.3

> Extension: key_share (len=36) x25519

> Extension: pre_shared_key (len=2)

[JA3S Fullstring: 771,4665,43-51-41]

[JA3S: fcb2d4d8991292272fcb1e464eedfd43]

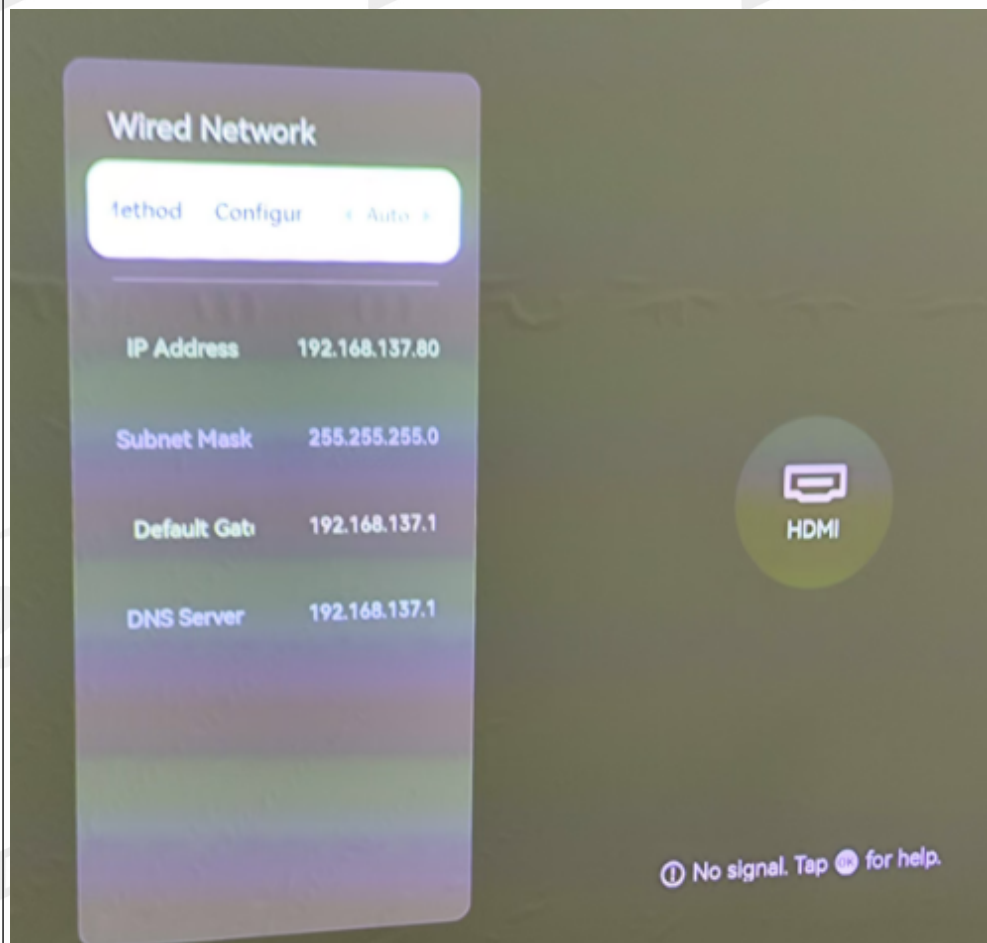
Secure Communication: WPA3

```
33 0.00014/ iPlinkTechno_ff:3c Intel_7b:5d:86 802.11 1b Request-to-send, Flags=.....
34 0.000151 TplinkTechno_ff:3c Intel_7b:5d:86 802.11 16 Request-to-send, Flags=.....
35 0.001420 da:ec:4f:27:5a:67 Broadcast 802.11 192 Beacon frame, SN=648, FN=0, Flags=....., BI=100, SSID="AndroidAP4505"
36 0.001458 TplinkTechno_ff:3c Intel_7b:5d:86 802.11 16 Request-to-send, Flags=.....
37 0.001464 TplinkTechno_ff:3c Intel_7b:5d:86 802.11 10 Clear-to-send, Flags=.....

> Bitmap control: 0x00
Partial Virtual Bitmap: 00
> Tag: RSN Information
Tag Number: RSN Information (48)
Tag Length: 24
RSN Version: 1
> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
Pairwise Cipher Suite Count: 1
> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
Auth Key Management (AKM) Suite Count: 2
> Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
> Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
Auth Key Management (AKM) type: PSK (2)
> Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
Auth Key Management (AKM) type: SAE (SHA256) (8)
> RSN Capabilities: 0x0000
> Tag: HT Capabilities
Tag Number: HT Capabilities (45)
```

Ethernet (LAN):

The device connects to the Internet via LAN, and WireShark is used for packet capture during the device's firmware upgrade.



Client Hello

233	20.739947	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
257	20.764267	192.168.137.80	222.217.94.18	TLSv1.3	571 Client Hello (SNI=global-static-al.static.xgimi.com)
266	20.923548	222.217.94.18	192.168.137.80	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
268	20.923608	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
269	20.923635	222.217.94.18	192.168.137.80	TLSv1.3	251 Application Data, Application Data

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 512

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 508

> Version: TLS 1.2 (0x0303)

Random: b69f0754f44a1c03d9229f533ed5ff29a007d2408f5dd539ff7794b3aab39730

Session ID Length: 32

Session ID: 2d5187a5d47f0a62895d3dbdde5cb2ff7f99180a90b29d65be9512c74a3c7908

Cipher Suites Length: 30

▼ Cipher Suites (15 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

Server Hello

233	20.739947	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
257	20.764267	192.168.137.80	222.217.94.18	TLSv1.3	571 Client Hello (SNI=global-static-al.static.xgimi.com)
266	20.923548	222.217.94.18	192.168.137.80	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
268	20.923608	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
269	20.923635	222.217.94.18	192.168.137.80	TLSv1.3	251 Application Data, Application Data

> Internet Protocol Version 4, Src: 222.217.94.18, Dst: 192.168.137.80

> Transmission Control Protocol, Src Port: 443, Dst Port: 54344, Seq: 1, Ack: 518, Len: 1460

▼ Transport Layer Security

[Stream Index: 3]

▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 122

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 118

> Version: TLS 1.2 (0x0303)

Random: c2b81f2435ab1755aa4039c29985a1703e2de7eea889f080b27f2a52e1810121

Session ID Length: 32

Session ID: 2d5187a5d47f0a62895d3dbdde5cb2ff7f99180a90b29d65be9512c74a3c7908

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 46

> Extension: supported_versions (len=2) TLS 1.3

Bluetooth BR/EDR/LE adopts the Bluetooth 5.2 protocol, supporting secure connections and protection against man-in-the-middle attacks.

Frame 614: (Central) Len=34

Baseband:

RSSI: -69.875 dBm (weak)

Initial Center Frequency Offset: -9.31 kHz

Link: 2

Role: Central (0xdc-ec-4f-27-5a-68)

Channel: 39 - 2441 MHz

Clock: 0x00222614

Packet Status: OK

FLOW: Go

TYPE: DM1

Payload Data Rate: 1 Mbps

LT_ADDR: 1

SEQN: 1

ARQN: 0

L2CAP Flow: N/A [1]

Logical Link ID: LMP

Decrypted by Bluetooth ComProbe: No

Payload Length: 6

LMP:

Link: 2

Role: Central

Address: 1

Opcode: LMP_version_req

Transaction ID: Initiated by central

Version: Bluetooth Core Specification 5.2

Company Identifier: MediaTek, Inc.

Subversion: 9225

Frame 1,431: (Central) Len=30

Baseband:

RSSI: -72.375 dBm (weak)

Initial Center Frequency Offset: -10.72 kHz

Link: 2

Role: Central (0xdc-ec-4f-27-5a-68)

Channel: 21 - 2423 MHz

Clock: 0x00225e10

Packet Status: OK

FLOW: Go

TYPE: DM1

Payload Data Rate: 1 Mbps

LT_ADDR: 1

SEQN: 1

ARQN: 0

L2CAP Flow: N/A [1]

Logical Link ID: LMP

Decrypted by Bluetooth ComProbe: No

Payload Length: 2

LMP:

Link: 2

Role: Central

Address: 1

Opcode: LMP_encryption_key_size_req

Transaction ID: Initiated by central

Key Size: 16 bytes

Decode | Device Database

Bluetooth Security

Show: All Security Events ▼

Time	Central & Peripheral
1/4/2026 9:32:07.53515...	DC:EC:4F:27:5A:68
...	"KENWOOD GLASS Core" 5C:8E:8B:9C:7A:13

	- Baseband: - RSSI: -71.125 dBm (weak) - Initial Center Frequency Offset: -10.09 kHz - Link: 2 - Role: Central (0xdc-ec-4f-27-5a-68) - Channel: 25 - 2427 MHz - Clock: 0x002227bc - Packet Status: OK - FLOW: Go - TYPE: DM1 - Payload Data Rate: 1 Mbps - LT_ADDR: 1 - SEQN: 0 - ARQN: 1 - L2CAP Flow: N/A [1] - Logical Link ID: LMP - Decrypted by Bluetooth ComProbe: No - Payload Length: 12 - LMP: - Link: 2 - Role: Central - Address: 1 - Escape opcode: 127 - Transaction ID: Initiated by central - Extended Opcode: LMP_features_req_ext - Feature's Page Number: 1 - Max Supported Feature's Pages: 2 - Extended Features - Secure Connections (Host Support): Supported - Previously used (Simultaneous LE and BR/EDR to Same Device Capable (Host)): Not Supported - LE Supported (Host): Supported - Secure Simple Pairing (Host Support): Supported - Frame 1,096: Len=52 - LE BB: - LE PKT: - Preamble: 0x55 - Access Address: 0xf626a837 - BD Address: dc:ec:4f:27:5a:68 - CRC: 0xa7601d - LE DATA: - L2CAP: - SMP: - Code: Pairing Request - IO Capabilities: KeyboardDisplay - OOB data flag: OOB Authentication data not present - AuthReq - Bonding_Flags: Bonding - MITM: MITM Protection: Yes - Secure Connection Pairing: Yes - Keypress Notifications: No - CT2: Supports h7 Function: Yes - Maximum Encryption Key Size: 16 Octets - Initiator Key Distribution - Responder Key Distribution
Assignment of verdict:	Pass

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

--Conceptual assessment--

Identifier [SCM-3]-01	[E.Info.SCM-3.SCM]: Wi-Fi networking uses the TLS 1.3 protocol to establish a connection with the server, HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack.		
Decision node	Decision [E.Info.DT.SCM-3]		Justification [E.Just.DT.SCM-3]
[DT.SCM-3.DN-2]	Yes (✓)	No	[E.Info.SCM-3.SecurityAsset]: Over-the-Air (OTA) Firmware Update [E.Info.SCM-3.SecurityAsset.Com]: Online Firmware Upgrade is enabled through secure HTTPS communication based on the OpenSSL 3.0.15 library. [E.Info.SCM-3.NetworkInterface]: Wi-Fi [E.Info.SCM-3.NetworkInterface.Protocol]: HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack. [E.Info.SCM-3.SCM]: HTTPS [E.Info.SCM-3.SCM.Capabilities]: HTTPS with TLS 1.3. Communication Encryption Suite: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

		TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA [E.Info.SCM-3.Generic]: [IC.SCM-3. Generic]: The device adopts the best practice implementation of HTTPS with TLS in OpenSSL.
Assignment of verdict:	N/A TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 1. These cipher suites use encryption and hashing algorithms that are no longer recommended. While they provide basic encryption capabilities, they lack enhanced support for data integrity and authentication. 2. For the purpose of compatibility with communications of other products or services, the adopted encryption algorithm suite is not based on best practices (but rather prioritizes compatibility).	

Identifier [SCM-3]-02	[E.Info.SCM-3.SCM]: The LAN uses the TLS 1.3 protocol to establish a connection with the server, HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack.		
Decision node	Decision [E.Info.DT.SCM-3]	Justification [E.Just.DT.SCM-3]	
[DT.SCM-3.DN-2]	Yes (✓)	No	[E.Info.SCM-3.SecurityAsset]: Over-the-Air (OTA) Firmware Update [E.Info.SCM-3.SecurityAsset.Com]: Online Firmware Upgrade is enabled through secure HTTPS communication based on the OpenSSL 3.0.15 library. [E.Info.SCM-3.NetworkInterface]: LAN [E.Info.SCM-3.NetworkInterface.Protocol]: HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack. [E.Info.SCM-3.SCM]: HTTPS [E.Info.SCM-3.SCM.Capabilities]: HTTPS with TLS 1.3. Communication Encryption Suite: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

			TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA [E.Info.SCM-3.Generic]: [IC.SCM-3. Generic]: The device adopts the best practice implementation of HTTPS with TLS in OpenSSL.
Assignment of verdict:	N/A TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 1. These cipher suites use encryption and hashing algorithms that are no longer recommended. While they provide basic encryption capabilities, they lack enhanced support for data integrity and authentication. 2. For the purpose of compatibility with communications of other products or services, the adopted encryption algorithm suite is not based on best practices (but rather prioritizes compatibility).		

Identifier [SCM-3]-03	[E.Info.SCM-3.SCM]: Bluetooth BR/EDR/LE adopts the Bluetooth 5.2 protocol. The device achieves communication via proprietary services, with the AES-CCM-128 algorithm employed for encryption.		
Decision node	Decision [E.Info.DT.SCM-2]	Justification [E.Just.DT.SCM-3]	
DT.SCM-3.DN-1	Yes (✓)	No	[E.Info.SCM-3.SCM.CCK]: The AES-CCM-128 algorithm is implemented based on the hardware AES at the underlying level, and the random numbers are true random numbers generated by the hardware TRNG (True Random Number Generator). [E.Info.SCM-3.NetworkInterface]: Bluetooth interface [E.Info.SCM-3.NetworkInterface.Protocol]: Bluetooth 5.2 protocol [E.Info.SCM-3.SecurityAsset.Com]: During the network provisioning process, the user device pairs and connects with the device under test via a Bluetooth pairing code. [E.Info.SCM-3.SCM.ThreatProtection]: It prevents man-in-the-middle attacks and protects the security of the device's assets during the communication process.

		[E.Info.SCM-3.SCM.Capabilities]: It prevents man-in-the-middle attacks and protects the security of the device's assets during the communication process. [E.Info.SCM-3.SCM.SecChanExchange]: When the device pairs with other devices, an AES-128 key will be negotiated according to the Bluetooth protocol, and all subsequent communications will be encrypted with this key. [E.Info.SCM-3.SCM.ImplDetail]: When the device pairs with other devices, an AES-128 key will be negotiated according to the Bluetooth protocol, and all subsequent communications will be encrypted with this key.
Assignment of verdict:	Pass	

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the secure communication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the security assets or network assets communicated are protected against eavesdropping.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each security asset recorded in [E.Info.SCM-3.SecurityAsset] and each network asset recorded in [E.Info.SCM-3.NetworkAsset], perform legitimate communication between the device and authorized communication endpoints. In accordance with [E.Info.SCM-3.SCM], taking into account the recorded device status, use the latest assessment methods to functionally confirm that the communication mechanisms ensure confidentiality protection and apply the recorded implementation categories: [AU.SCM-3.ChannelEnc]: For [IC.SCM-3.ChannelEnc], in accordance with the records in [E.Info.SCM-3.SCM.ChannelEnc], the following are functionally confirmed: — The key used to encrypt information in the communication channel cannot be intercepted; and — The security assets and network assets of the communication will not be eavesdropped on.
Result:	Wi-Fi: The device connects to the Internet via Wi-Fi, and WireShark is used for packet capture during the device's firmware upgrade.

属性

网络属性

编辑

名称: DDT-JIEDESK
密码: 123456789
频段: 2.4 GHz

扫描以连接:


已连接的设备: 1台(共 8 台)

设备名称	IP 地址	物理地址(MAC)
未知	192.168.137.7	d6:22:0b:c1:e4:a1

Client Hello

291	49.195375	192.168.137.7	222.217.94.16	TLSv1.3	655 Client Hello (SNI=global-static-al.static.xgimi.com)
293	49.277047	222.217.94.16	192.168.137.7	TLSv1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295	49.306941	192.168.137.7	222.217.94.16	TLSv1.3	118 Change Cipher Spec, Application Data
296	49.375127	222.217.94.16	192.168.137.7	TLSv1.3	365 Application Data
297	49.406237	192.168.137.7	222.217.94.16	TLSv1.3	334 Application Data
298	49.487164	222.217.94.16	192.168.137.7	TLSv1.3	1468 Application Data
310	49.490389	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
334	49.564252	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data

Transmission Control Protocol, Src Port: 46050, Dst Port: 443, Seq: 1, Ack: 1, Len: 601

Transport Layer Security

Stream Index: 71

TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 596

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 592

Version: TLS 1.2 (0x0303)

Random: b603d5a074b18995b92c59b70a2ccae8a6feccc618e634e63ed108cd4473757

Session ID Length: 32

Session ID: c25fc1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c5c19fa26436

Cipher Suites Length: 34

Cipher Suites (17 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc02d)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

Server Hello

291	49.195375	192.168.137.7	222.217.94.16	TLSv1.3	655 Client Hello (SNI=global-static-al.static.xgimi.com)
293	49.277047	222.217.94.16	192.168.137.7	TLSv1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295	49.306941	192.168.137.7	222.217.94.16	TLSv1.3	118 Change Cipher Spec, Application Data
296	49.375127	222.217.94.16	192.168.137.7	TLSv1.3	365 Application Data
297	49.406237	192.168.137.7	222.217.94.16	TLSv1.3	334 Application Data
298	49.487164	222.217.94.16	192.168.137.7	TLSv1.3	1468 Application Data
310	49.490389	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
334	49.564252	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data

> Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \Device\NPF_{A2009E98-90CA-4773-A2C0-58B161605298}, id 0

> Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1)

> Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7

> Transmission Control Protocol, Src Port: 443, Dst Port: 46050, Seq: 1, Ack: 682, Len: 244

Transport Layer Security

Stream Index: 71

TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 128

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 124

Version: TLS 1.2 (0x0303)

Random: 007f1ce4c9bd86732750948dea47576977cbc8f2e4e91b13a40fd74127b6ec35

Session ID Length: 32

Session ID: c25fc1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c5c19fa26436

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 52

> Extension: supported_versions (len=2) TLS 1.3

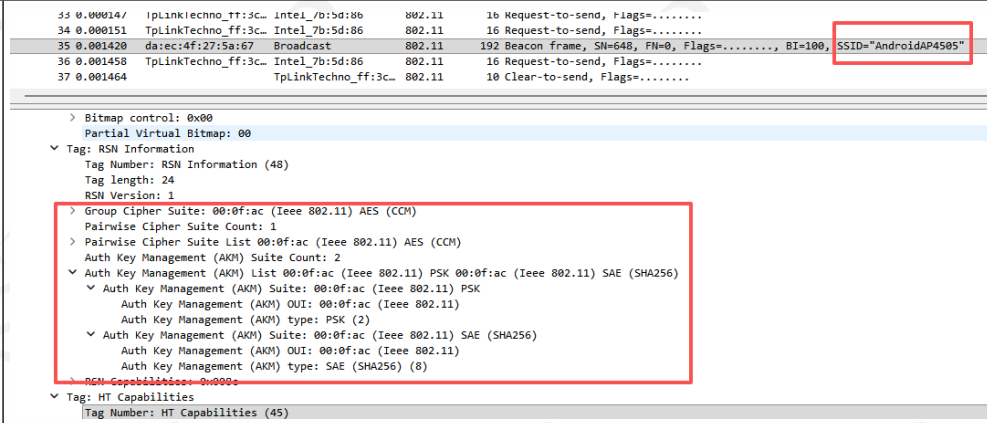
> Extension: key_share (len=36) x25519

> Extension: pre_shared_key (len=2)

[JA3S Fullstring: 771,4865,43-51-41]

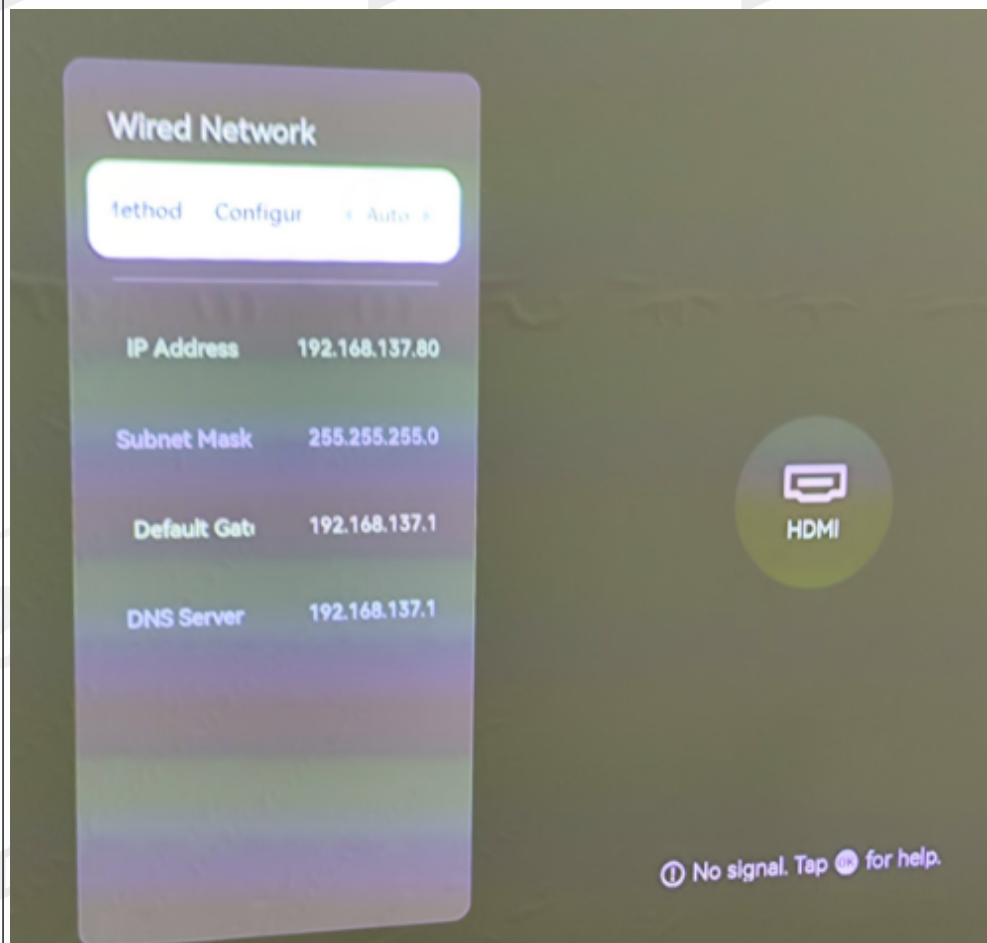
[JA3S: fcb2d4d0991292272fcb1e464eedfd43]

Secure Communication: WPA3



Ethernet (LAN):

The device connects to the Internet via LAN, and WireShark is used for packet capture during the device's firmware upgrade.



Client Hello

233	20.739947	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
257	20.764267	192.168.137.80	222.217.94.18	TLSv1.3	571 Client Hello (SNI=global-static-al.static.xgimi.com)
266	20.923548	222.217.94.18	192.168.137.80	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
268	20.923608	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
269	20.923635	222.217.94.18	192.168.137.80	TLSv1.3	251 Application Data, Application Data

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 512

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 508

► Version: TLS 1.2 (0x0303)

Random: b69f0754f44alc03d9229f533ed5ff29a007d2408f5dd539ff7794b3aab39730

Session ID Length: 32

Session ID: 2d5187a5d47f0a62895d3dbdde5cb2ff7f99180a90b29d65be9512c74a3c7908

Cipher Suites Length: 30

▼ Cipher Suites (15 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

Server Hello

233	20.739947	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
257	20.764267	192.168.137.80	222.217.94.18	TLSv1.3	571 Client Hello (SNI=global-static-al.static.xgimi.com)
266	20.923548	222.217.94.18	192.168.137.80	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
268	20.923608	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
269	20.923635	222.217.94.18	192.168.137.80	TLSv1.3	251 Application Data, Application Data

► Internet Protocol Version 4, Src: 222.217.94.18, Dst: 192.168.137.80

► Transmission Control Protocol, Src Port: 443, Dst Port: 54344, Seq: 1, Ack: 518, Len: 1460

▼ Transport Layer Security

[Stream index: 3]

▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 122

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 118

► Version: TLS 1.2 (0x0303)

Random: c2b81f2435ab1755aa4039c29985a1703e2de7eea889f080b27f2a52e1810121

Session ID Length: 32

Session ID: 2d5187a5d47f0a62895d3dbdde5cb2ff7f99180a90b29d65be9512c74a3c7908

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Compression Method: null (0)

Extensions Length: 46

► Extension: supported_versions (len=2) TLS 1.3

Bluetooth BR/EDR/LE adopts the Bluetooth 5.2 protocol, supporting secure connections and protection against man-in-the-middle attacks.

	Frame 614: (Central) Len=34 Baseband: - RSSI: -69.875 dBm (weak) - Initial Center Frequency Offset: -9.31 kHz - Link: 2 - Role: Central (0xdc-ec-4f-27-5a-68) - Channel: 39 - 2441 MHz - Clock: 0x00222614 - Packet Status: OK - FLOW: Go - TYPE: DM1 - Payload Data Rate: 1 Mbps - LT_ADDR: 1 - SEQN: 1 - ARQN: 0 - L2CAP Flow: N/A [1] - Logical Link ID: LMP - Decrypted by Bluetooth ComProbe: No - Payload Length: 6 LMP: - Link: 2 - Role: Central - Address: 1 - Opcode: LMP_version_req - Transaction ID: Initiated by central - Version: Bluetooth Core Specification 5.2 - Company Identifier: MediaTek, Inc. - Subversion: 9225 Baseband: - RSSI: -71.125 dBm (weak) - Initial Center Frequency Offset: -10.09 kHz - Link: 2 - Role: Central (0xdc-ec-4f-27-5a-68) - Channel: 25 - 2427 MHz - Clock: 0x002227bc - Packet Status: OK - FLOW: Go - TYPE: DM1 - Payload Data Rate: 1 Mbps - LT_ADDR: 1 - SEQN: 0 - ARQN: 1 - L2CAP Flow: N/A [1] - Logical Link ID: LMP - Decrypted by Bluetooth ComProbe: No - Payload Length: 12 LMP: - Link: 2 - Role: Central - Address: 1 - Escape opcode: 127 - Transaction ID: Initiated by central - Extended Opcode: LMP_features_req_ext - Feature's Page Number: 1 - Max Supported Feature's Pages: 2 Extended Features: - Secure Connections (Host Support): Supported - Previously used (Simultaneous LE and BR/EDR to Same Device Capable (Host)): Not Supported - LE Supported (Host): Supported - Secure Simple Pairing (Host Support): Supported Frame 1,431: (Central) Len=30 Baseband: - RSSI: -72.375 dBm (weak) - Initial Center Frequency Offset: -10.72 kHz - Link: 2 - Role: Central (0xdc-ec-4f-27-5a-68) - Channel: 21 - 2423 MHz - Clock: 0x00225e10 - Packet Status: OK - FLOW: Go - TYPE: DM1 - Payload Data Rate: 1 Mbps - LT_ADDR: 1 - SEQN: 1 - ARQN: 0 - L2CAP Flow: N/A [1] - Logical Link ID: LMP - Decrypted by Bluetooth ComProbe: No - Payload Length: 2 LMP: - Link: 2 - Role: Central - Address: 1 - Opcode: LMP_encryption_key_size_req - Transaction ID: Initiated by central - Key Size: 16 bytes Decode Device Database Bluetooth Security Show: All Security Events <table border="1"> <thead> <tr> <th>Time</th> <th>Central & Peripheral</th> </tr> </thead> <tbody> <tr> <td>1/4/2026 9:32:07.53515...</td> <td>DC:EC:4F:27:5A:68</td> </tr> <tr> <td>...</td> <td>"KENWOOD GLASS Core" 5C:8E:8B:9C:7A:13</td> </tr> </tbody> </table> Frame 1,096: Len=52 LE BB: LE PKT: - Preamble: 0x55 - Access Address: 0xf626a837 - BD Address: dc:ec:4f:27:5a:68 - CRC: 0xa7601d LE DATA: L2CAP: SMP: - Code: Pairing Request - IO Capabilities: KeyboardDisplay - OOB data flag: OOB Authentication data not present AuthReq - Bonding Flags: Bonding - MITM: MITM Protection: Yes - Secure Connection Pairing: Yes - Keypress Notifications: No - CT2: Supports h7 Function: Yes - Maximum Encryption Key Size: 16 Octets - Initiator Key Distribution - Responder Key Distribution	Time	Central & Peripheral	1/4/2026 9:32:07.53515...	DC:EC:4F:27:5A:68	...	"KENWOOD GLASS Core" 5C:8E:8B:9C:7A:13
Time	Central & Peripheral						
1/4/2026 9:32:07.53515...	DC:EC:4F:27:5A:68						
...	"KENWOOD GLASS Core" 5C:8E:8B:9C:7A:13						
Assignment of verdict:	Pass						

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

--Conceptual assessment--

Identifier [SCM-4]-01	[E.Info.SCM-4.SCM]: Each Wi-Fi data packet carries an increasing serial number. The receiver verifies the continuity of these numbers and rejects duplicate or expired packets.		
Decision node	Decision	Justification	
	[E.Info.DT.SCM-4]	[E.Just.DT.SCM-4]	
[DT.SCM-4.DN-1]	Yes (✓)	No	[E.Info.SCM-4.NetworkInterface]: Wi-Fi [E.Info.SCM-4.NetworkInterface.Protocol]:

		Wi-Fi, HTTPS (based on TLS 1.3) [E.Info.SCM-4.SecurityAsset.Com]: The Wi-Fi module establishes a secure connection with the server via the HTTPS protocol (TLS 1.3) (implemented by OpenSSL 3.0.15) and transmits service instructions based on this protocol to perform service operations. [E.Info.SCM-4.SCM.Capabilities]: It can prevent replay attacks and protect the security of device assets during communication. [E.Info.SCM-4.SCM.Repudiation]: The HTTPS connection (TLS 1.3, OpenSSL 3.0.15) adopts asymmetric + symmetric encryption mechanisms: Asymmetric encryption: TLS 1.3 uses asymmetric algorithms (e.g., RSA, ECDSA) during the handshake phase to negotiate and securely transmit symmetric session keys. Symmetric encryption: After the handshake, symmetric encryption (compliant with TLS 1.3 standards, e.g., AES series) is used for real-time encryption of service data, ensuring transmission efficiency. Verification & discard: The receiver (via OpenSSL 3.0.15) verifies the integrity and authenticity of data packets using TLS 1.3's built-in message authentication code (MAC) or digital signature; any packets that fail verification (e.g., tampered, invalid format) are discarded. [E.Info.SCM-4.SCM.SeqNum]: [IC.SCM-4.SeqNum]: The HTTPS protocol (TLS 1.3, OpenSSL 3.0.15) uses sequence numbers to protect against replay attacks: Each record sent in the TLS session is assigned a unique, incrementing sequence number (maintained independently for send and receive directions). The sequence number is included in the record's integrity check (e.g., HMAC calculation), ensuring that replayed or out-of-order packets cannot pass verification and will be discarded by the receiver. OpenSSL 3.0.15 implements this sequence number mechanism in compliance with TLS 1.3 specifications, ensuring the uniqueness and continuity of sequence numbers during the session.
Assignment of verdict:	Pass	

Identifier [SCM-4]-02	[E.Info.SCM-4.SCM]: The LAN uses the TLS 1.3 protocol to establish a connection with the server, HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack.		
Decision node	Decision [E.Info.DT.SCM-4]	Justification [E.Just.DT.SCM-4]	
DT.SCM-4.DN-1	Yes (✓)	No	[E.Info.SCM-4.NetworkInterface]: Ethernet [E.Info.SCM-4.NetworkInterface.Protocol]:

		Ethernet (IEEE 802.3), 10/100/1000 Mbps, Auto-Negotiation, Full/Half Duplex, Supports secure transport via TLS 1.3 and OpenSSL 3.0.15. [E.Info.SCM-4.SecurityAsset.Com]: The LAN establishes a secure connection between terminal devices and the local gateway via the TLS 1.3 protocol (implemented by OpenSSL 3.0.15) and transmits service instructions based on this protocol to perform local service operations. [E.Info.SCM-4.SCM.Capabilities]: It can prevent replay attacks and protect the security of device assets during communication. [E.Info.SCM-4.SCM.Repudiation]: The HTTPS connection (TLS 1.3, OpenSSL 3.0.15) adopts asymmetric + symmetric encryption mechanisms: Asymmetric encryption: TLS 1.3 uses asymmetric algorithms (e.g., RSA, ECDSA) during the handshake phase to negotiate and securely transmit symmetric session keys. Symmetric encryption: After the handshake, symmetric encryption (compliant with TLS 1.3 standards, e.g., AES series) is used for real-time encryption of service data, ensuring transmission efficiency. Verification & discard: The receiver (via OpenSSL 3.0.15) verifies the integrity and authenticity of data packets using TLS 1.3's built-in message authentication code (MAC) or digital signature; any packets that fail verification (e.g., tampered, invalid format) are discarded. [E.Info.SCM-4.SCM.SeqNum]: [IC.SCM-4.SeqNum]: The HTTPS protocol (TLS 1.3, OpenSSL 3.0.15) uses sequence numbers to protect against replay attacks: Each record sent in the TLS session is assigned a unique, incrementing sequence number (maintained independently for send and receive directions). The sequence number is included in the record's integrity check (e.g., HMAC calculation), ensuring that replayed or out-of-order packets cannot pass verification and will be discarded by the receiver. OpenSSL 3.0.15 implements this sequence number mechanism in compliance with TLS 1.3 specifications, ensuring the uniqueness and continuity of sequence numbers during the session.
Assignment of verdict:	Pass	

Identifier [SCM-4]-03	[E.Info.SCM-4.SCM]: Each Bluetooth packet will carry an increasing serial number, and the receiver will verify the continuity of the values and reject duplicate or expired packets.		
Decision node	Decision [E.Info.DT.SCM-4]	Justification [E.Just.DT.SCM-4]	
DT.SCM-4.DN-1	Yes (✓)	No	[E.Info.SCM-4.NetworkInterface]: Bluetooth interface

		[E.Info.SCM-4.NetworkInterface.Protocol]: Bluetooth 5.2 protocol [E.Info.SCM-4.SecurityAsset.Com]: During the network provisioning process, the user device pairs and connects with the device under test via a Bluetooth pairing code. [E.Info.SCM-4.SCM.Capabilities]: It can prevent replay attacks and protect the security of device assets during communication. [E.Info.SCM-4.SCM.Repudiation]: Each Bluetooth packet will carry an increasing serial number, and the receiver will verify the continuity of the values and reject duplicate or expired packets. [E.Info.SCM-4.SCM.SeqNumb]: [IC.SCM-4.SeqNumb]: Each Bluetooth packet will carry an increasing serial number, and the receiver will verify the continuity of the values and reject duplicate or expired packets.
Assignment of verdict:	Pass	

--Completeness testing--

The functional completeness assessment is covered by the functional sufficiency assessment of the secure communication mechanism's applicability.

Therefore, this functional completeness assessment is not necessary.

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the security assets and network assets communicated are protected against replay attacks.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each security asset recorded in [E.Info.SCM-4.SecurityAsset] and each network asset recorded in [E.Info.SCM-4.NetworkAsset], perform legitimate communication between the device and authorized communication endpoints. Record the communication sequence. In accordance with [E.Info.SCM-4.SCM], taking into account the recorded device status, use the latest assessment methods to functionally confirm that the communication mechanisms provide replay protection and apply the recorded implementation categories: [AU.SCM-4.SeqNumb]: For [IC.SCM-4.SeqNumb], in accordance with the records in [E.Info.SCM-4.SCM.SeqNumb], functionally confirm the following: — Incoming messages with duplicate sequence numbers (as part of the communication of security assets and network assets) are not accepted.
Result:	Wi-Fi: The device connects to the Internet via Wi-Fi, and WireShark is used for packet capture during the device's firmware upgrade.

属性

网络属性

编辑

名称: DDT-JIEDESK
密码: 123456789
频段: 2.4 GHz

扫描以连接:



已连接的设备: 1台(共 8台)

设备名称	IP 地址	物理地址(MAC)
未知	192.168.137.7	d6:22:0b:c1:e4:a1

Client Hello

291	49.195375	192.168.137.7	222.217.94.16	TLV1.3	655 Client Hello (SNI=global-static-al.static.xgimi.com)
293	49.277047	222.217.94.16	192.168.137.7	TLV1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295	49.306941	192.168.137.7	222.217.94.16	TLV1.3	118 Change Cipher Spec, Application Data
296	49.375127	222.217.94.16	192.168.137.7	TLV1.3	365 Application Data
297	49.406237	192.168.137.7	222.217.94.16	TLV1.3	334 Application Data
298	49.487164	222.217.94.16	192.168.137.7	TLV1.3	1468 Application Data
310	49.490389	222.217.94.16	192.168.137.7	TLV1.3	1514 Application Data
334	49.564252	222.217.94.16	192.168.137.7	TLV1.3	1514 Application Data

Transmission Control Protocol, Src Port: 46050, Dst Port: 443, Seq: 1, Ack: 1, Len: 601

Transport Layer Security

[Stream Index: 7]

TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 596

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 592

Random: b6b3d5a074b18995b92c59870a2ccae8a6feccc618e634e3ed108cd4473757

Session ID Length: 32

Session ID: c25f1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436

Cipher Suites Length: 34

Cipher Suites (17 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0xc1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0xc1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0xc1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc000)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x0002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

Server Hello

291	49.195375	192.168.137.7	222.217.94.16	TLV1.3	655 Client Hello (SNI=global-static-al.static.xgimi.com)
293	49.277047	222.217.94.16	192.168.137.7	TLV1.3	298 Server Hello, Change Cipher Spec, Application Data, Application Data
295	49.306941	192.168.137.7	222.217.94.16	TLV1.3	118 Change Cipher Spec, Application Data
296	49.375127	222.217.94.16	192.168.137.7	TLV1.3	365 Application Data
297	49.406237	192.168.137.7	222.217.94.16	TLV1.3	334 Application Data
298	49.487164	222.217.94.16	192.168.137.7	TLV1.3	1468 Application Data
310	49.490389	222.217.94.16	192.168.137.7	TLV1.3	1514 Application Data
334	49.564252	222.217.94.16	192.168.137.7	TLV1.3	1514 Application Data

> Frame 293: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits) on interface \Device\NPF{A2009E98-98CA-4773-A2C0-5B8161605298}, id 0

> Ethernet II, Src: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1), Dst: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1)

> Internet Protocol Version 4, Src: 222.217.94.16, Dst: 192.168.137.7

> Transmission Control Protocol, Src Port: 443, Dst Port: 46050, Seq: 1, Ack: 602, Len: 244

Transport Layer Security

[Stream Index: 7]

TLSv1.3 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 128

Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 124

> Version: TLS 1.2 (0x0303)

Random: 087f1c4c9bd86732750948dea47576977cb8f2e4e91b13a40fd74127b6ec35

Session ID Length: 32

Session ID: c25f1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436

Cipher Suite: TLS_AES_128_GCM_SHA256 (0xc1301)

Compression Method: null (0)

Extensions Length: 52

> Extension: supported_versions (len=2) TLS 1.3

> Extension: key_share (len=36) x25519

> Extension: pre_shared_key (len=2)

[JA35 Fullstring: 771,4865,43-51-41]

[JA35: fcb2d4d0991292272fcb1e464eeedf4d3]

Sequence Number

356	49.581056	222.217.94.16	192.168.137.7	TLSv1.3	1514 Application Data
373	49.610833	192.168.137.7	222.217.94.17	TLSv1.3	618 Client Hello (SNI=global-static-al.static.xgimi.com)
404	49.686563	222.217.94.17	192.168.137.7	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
408	49.767946	222.217.94.17	192.168.137.7	TLSv1.3	1514 Application Data


```
> Frame 373: Packet, 618 bytes on wire (4944 bits), 618 bytes captured (4944 bits) on interface \Device\NPF_{A2009E9B-90CA-4773-A2C0-588161609}
> Ethernet II, Src: d6:22:0b:c1:e4:a1 (d6:22:0b:c1:e4:a1), Dst: 22:bd:1d:50:68:f1 (22:bd:1d:50:68:f1)
> Internet Protocol Version 4, Src: 192.168.137.7, Dst: 222.217.94.17
> Transmission Control Protocol, Src Port: 36880, Dst Port: 443, Seq: 1, Ack: 1, Len: 564
  Source Port: 36880
  Destination Port: 443
  [Stream Index: 13]
  [Stream Packet Number: 4]
  [Conversation completeness: Complete, WITH DATA (47)]
  [TCP Segment Len: 564]
  Sequence Number: 1 (relative sequence number)
  Sequence Number (raw): 2801124717
  [Next Sequence Number: 565 (relative sequence number)]
  Acknowledgment Number: 1 (relative ack number)
  Acknowledgment number (raw): 1224374415
  0101 .... : Header Length: 20 bytes (5)
  > Flags: 0x018 /DCU, ACK
```

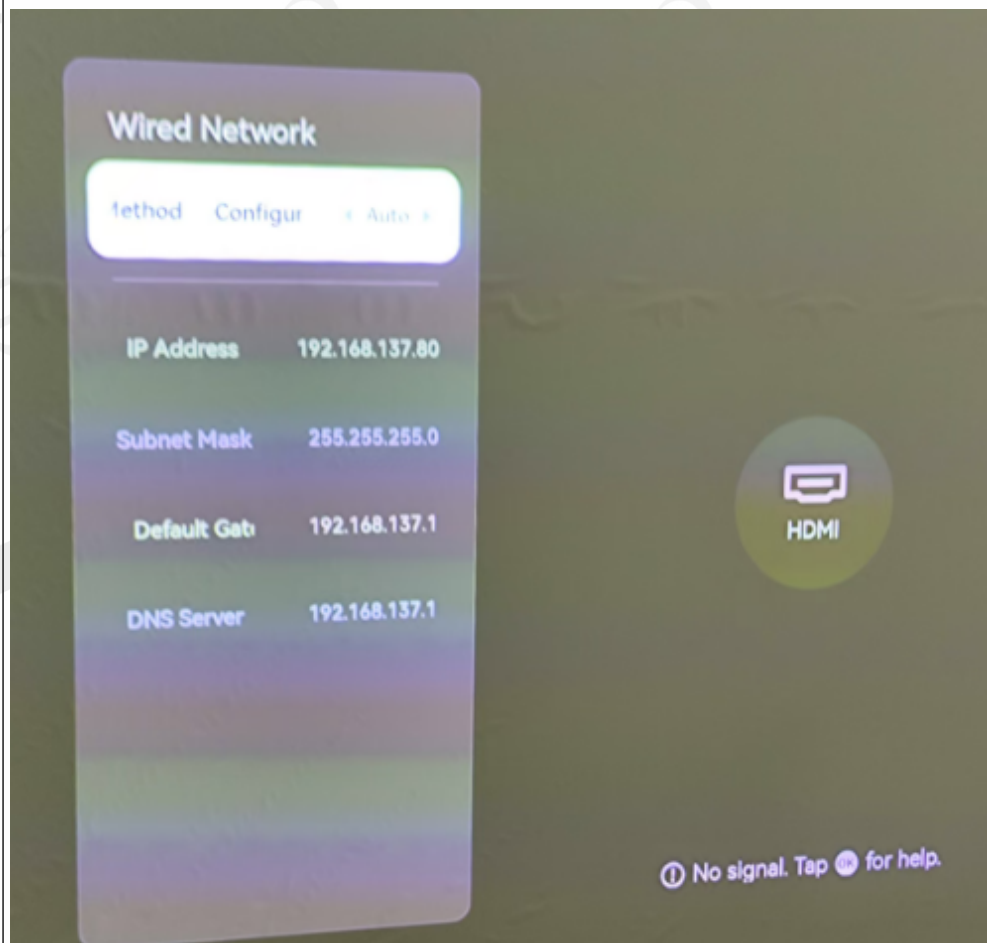
Secure Communication: WPA3

33	0.00014	TpLinkTechno_tr:3c	Intel_7b:5d:86	802.11	1b Request-to-send, Flags=.....
34	0.000151	TpLinkTechno_ff:3c	Intel_7b:5d:86	802.11	16 Request-to-send, Flags=.....
35	0.001420	da:ec:4f:27:5a:67	Broadcast	802.11	192 Beacon frame, SN=648, FN=0, Flags=....., BI=100, SSID="AndroidAP4505"
36	0.001458	TpLinkTechno_ff:3c	Intel_7b:5d:86	802.11	16 Request-to-send, Flags=.....
37	0.001464	TpLinkTechno_ff:3c	Intel_7b:5d:86	802.11	10 Clear-to-send, Flags=.....

```
> Bitmap control: 0x00
Partial Virtual Bitmap: 00
> Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 2
  > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
    > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: PSK (2)
    > Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: SAE (SHA256) (8)
  > RSN Capabilities: 0x0000
> Tag: HT Capabilities
  Tag Number: HT Capabilities (45)
```

Ethernet (LAN):

The device connects to the Internet via LAN, and WireShark is used for packet capture during the device's firmware upgrade.



Client Hello

233	20.739947	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
257	20.764267	192.168.137.80	222.217.94.18	TLSv1.3	571 Client Hello (SNI=global-static-al.static.xgimi.com)
266	20.923548	222.217.94.18	192.168.137.80	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
268	20.923608	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
269	20.923635	222.217.94.18	192.168.137.80	TLSv1.3	251 Application Data, Application Data

▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.0 (0x0301)

Length: 512

▼ Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 508

> Version: TLS 1.2 (0x0303)

Random: b69f0754f44a1c03d9229f533ed5ff29a007d2408f5dd539ff7794b3aab39730

Session ID Length: 32

Session ID: 2d5187a5d47f0a62895d3dbdde5cb2ff7f99180a90b29d65be9512c74a3c7908

Cipher Suites Length: 30

▼ Cipher Suites (15 suites)

Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)

Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)

Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Compression Methods Length: 1

Compression Methods (0x0000)

Server Hello

233	20.739947	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
257	20.764267	192.168.137.80	222.217.94.18	TLSv1.3	571 Client Hello (SNI=global-static-al.static.xgimi.com)
266	20.923548	222.217.94.18	192.168.137.80	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
268	20.923608	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data
269	20.923635	222.217.94.18	192.168.137.80	TLSv1.3	251 Application Data, Application Data

> Internet Protocol Version 4, Src: 222.217.94.18, Dst: 192.168.137.80
> Transmission Control Protocol, Src Port: 443, Dst Port: 54344, Seq: 1, Ack: 518, Len: 1460
✓ Transport Layer Security

[Stream index: 3]
▼ TLSv1.3 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 122
▼ Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 118
► Version: TLS 1.2 (0x0303)
Random: c2b81f2435ab1755aa4039c29985a1703e2de7eea889f080b27f2a52e1810121
Session ID Length: 32
Session ID: 2d5187a5d47f0a62895d3dbdde5cb2ff7f99180a90b29d65be9512c74a3c7908
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Compression Method: null (0)
Extensions Length: 46
► Extension: supported_versions (len=2) TLS 1.3

Sequence Number

257	20.764267	192.168.137.80	222.217.94.18	TLSv1.3	571 Client Hello (SNI=global-static-al.static.xgimi.com)
266	20.923548	222.217.94.18	192.168.137.80	TLSv1.3	1514 Server Hello, Change Cipher Spec, Application Data
268	20.923608	222.217.94.18	192.168.137.80	TLSv1.3	1514 Application Data

> Internet Protocol Version 4, Src: 192.168.137.80, Dst: 222.217.94.18
▼ Transmission Control Protocol, Src Port: 54344, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
Source Port: 54344
Destination Port: 443
[Stream index: 5]
[Stream Packet Number: 4]
> [Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 517]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 2705465793
[Next Sequence Number: 518 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1516814926
0101 = Header Length: 20 bytes (5)
► Flags: 0x018 (PSH, ACK)
Window: 1024

Bluetooth BR/EDR/LE adopts the Bluetooth 5.2 protocol, supporting secure connections and protection against man-in-the-middle attacks.

Frame 614: (Central) Len=34

Baseband:
RSSI: -69.875 dBm (weak)
Initial Center Frequency Offset: -9.31 kHz
Link: 2
Role: Central (0xdc-ec-4f-27-5a-68)
Channel: 39 - 2441 MHz
Clock: 0x00222614
Packet Status: OK
FLOW: Go
TYPE: DM1
Payload Data Rate: 1 Mbps
LT_ADDR: 1
SEQN: 1
ARQN: 0
L2CAP Flow: N/A [1]
Logical Link ID: LMP
Decrypted by Bluetooth ComProbe: No
Payload Length: 6
LMP:
Link: 2
Role: Central
Address: 1
Opcode: LMP_version_req
Transaction ID: Initiated by central
Version: Bluetooth Core Specification 5.2
Company Identifier: MediaTek, Inc.
Subversion: 9225

Frame 1,431: (Central) Len=30

Baseband:
RSSI: -72.375 dBm (weak)
Initial Center Frequency Offset: -10.72 kHz
Link: 2
Role: Central (0xdc-ec-4f-27-5a-68)
Channel: 21 - 2423 MHz
Clock: 0x00225e10
Packet Status: OK
FLOW: Go
TYPE: DM1
Payload Data Rate: 1 Mbps
LT_ADDR: 1
SEQN: 1
ARQN: 0
L2CAP Flow: N/A [1]
Logical Link ID: LMP
Decrypted by Bluetooth ComProbe: No
Payload Length: 2
LMP:
Link: 2
Role: Central
Address: 1
Opcode: LMP_encryption_key_size_req
Transaction ID: Initiated by central
Key Size: 16 bytes

Decode Device Database

Bluetooth Security

Show: All Security Events ▼

Time	Central & Peripheral
1/4/2026 9:32:07.53515...	DC:EC:4F:27:5A:68
...	"KENWOOD GLASS Core" 5C:8E:8B:9C:7A:13

	Baseband: - RSSI: -71.125 dBm (weak) - Initial Center Frequency Offset: -10.09 kHz - Link 2 - Role: Central (0xdc-ec-4f-27-5a-68) - Channel: 25 - 2427 MHz - Clock: 0x002227bc - Packet Status: OK - Flow: Go - Type: DM1 - Payload Data Rate: 1 Mbps - LT_ADDR: 1 - SEQN: 0 - ARQN: 1 - L2CAP Flow: N/A [1] - Logical Link ID: LMP - Decrypted by Bluetooth ComProbe: No - Payload Length: 12 LMP: - Link 2 - Role: Central - Address: 1 - Escape opcode: 127 - Transaction ID: Initiated by central - Extended Opcode: LMP_features_req_ext - Feature's Page Number: 1 - Max Supported Feature's Pages: 2 Extended Features - Secure Connections (Host Support): Supported - Previously used (Simultaneous LE and BR/EDR to Same Device Capable (Host)): Not Supported - LE Supported (Host): Supported - Secure Simple Pairing (Host Support): Supported Frame 1,096: Len=52 - LE BB: - LE PKT: - Preamble: 0x55 - Access Address: 0xf626a837 - BD Address: dc:ec:4f:27:5a:68 - CRC: 0xa7601d - LE DATA: - L2CAP: - SMP: - Code: Pairing Request - IO Capabilities: KeyboardDisplay - OOB data flag: OOB Authentication data not present - AuthReq - Bonding_Flags: Bonding - MITM: MITM Protection: Yes - Secure Connection Pairing: Yes - Keypress Notifications: No - CT2: Supports h7 Function: Yes - Maximum Encryption Key Size: 16 Octets - Initiator Key Distribution - Responder Key Distribution
Assignment of verdict:	Pass

3.6 [RLM] Resilience mechanism

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

--Conceptual assessment--

Identifier [RLM-1]-01	[E.Info.RLM-1.NetworkInterface]: Bluetooth BR/EDR/LE		
Decision node	Decision [E.Info.DT.RLM-1]		Justification [E.Just.DT.RLM-1]
DT.RLM-1.DN-1	Yes (√)	No	[E.Info.RLM-1.RLM]: Bluetooth BR/EDR/LE uses the Bluetooth V5.2 protocol. It supports connection initiation from any device, but only allows one device to establish a connection simultaneously. These measures can mitigate the impact of DoS attacks on network interfaces and restore the device to a specified state after an attack, including: strict authentication and key exchange to restrict malicious access, encryption verification during transmission to filter invalid data, sequence number and timestamp mechanisms to prevent replay attacks, resource limitation management to avoid resource exhaustion, and error handling and recovery mechanisms to promptly address anomalies.
Assignment of verdict:	Pass		

Identifier [RLM-1]-02	[E.Info.RLM-1.NetworkInterface]: Wi-Fi		
Decision node	Decision [E.Info.DT.RLM-1]		Justification [E.Just.DT.RLM-1]
DT.RLM-1.DN-1	Yes (√)	No	[E.Info.RLM-1.RLM]: Wi-Fi networking uses the TLS 1.3 protocol to establish a connection with the server, HTTPS with TLS 1.3, implemented based on the OpenSSL

			3.0.15 stack. These measures can mitigate the impact of DoS attacks on network interfaces and restore the device to a specified state after an attack, including: strict authentication and key exchange to restrict malicious access, encryption verification during transmission to filter invalid data, sequence number and timestamp mechanisms to prevent replay attacks, resource limitation management to avoid resource exhaustion, and error handling and recovery mechanisms to promptly address anomalies.
Assignment of verdict:	Pass		

Identifier [RLM-1]-03	[E.Info.RLM-1.NetworkInterface]: Ethernet (LAN)		
Decision node	Decision [E.Info.DT.RLM-1]	Justification [E.Just.DT.RLM-1]	
DT.RLM-1.DN-1	Yes (√)	No	[E.Info.RLM-1.RLM]: Ethernet networking uses the TLS 1.3 protocol to establish a connection with the server, HTTPS with TLS 1.3, implemented based on the OpenSSL 3.0.15 stack. These measures can mitigate the impact of DoS attacks on network interfaces and restore the device to a specified state after an attack, including: strict authentication and key exchange to restrict malicious access, encryption verification during transmission to filter invalid data, sequence number and timestamp mechanisms to prevent replay attacks, resource limitation management to avoid resource exhaustion, and error handling and recovery mechanisms to promptly address anomalies.
Assignment of verdict:	Pass		

---Completeness testing---

Assessment purpose:	The purpose of this assessment case is the functional validation whether the resilience mechanisms implemented mitigate the effects of DoS Attacks on the network interfaces and that the equipment returns to a defined state after an attack with regard to completeness of documentation of network interfaces and the correctness of implementation.
Preconditions:	The equipment is in an operational state and each network interface documented in [E.Info.RLM-1.NetworkInterface] needs to either be enabled or configured so that each network interface can be tested. Where [E.Info.RLM-1.RLM] are used, documentation is provided that specifies information on what to configure/ the required configuration of the RLM to be able to test the implemented mechanisms.
Operation steps:	Functionally assess whether there are network interfaces not listed in [E.Info.RLM-1.NetworkInterface]. Functionally assess whether there are resilience mechanisms implemented that are not recorded in [E.Info.RLM-1.RLM].
Result:	There are no network interfaces not listed in [E.Info.RLM-1.NetworkInterface]. No resilience mechanisms that are not recorded in [E.Info.RLM-1.RLM] have been implemented.
Assignment of	Pass

verdict:							
--Sufficiency testing--							
Assessment purpose:	The purpose of this assessment case is the functional assessment whether the resilience mechanisms are implemented when required per RLM-1.						
Preconditions:	The equipment is in an operational state and each [E.Info.RLM-1.NetworkInterface] is either enabled or configured. Where [E.Info.RLM-1.RLM] are used the information on what to configure to be able to test the implemented mechanisms is provided.						
Operation steps:	Functionally confirm the usage of resilience mechanisms documented in [E.Info.RLM-1.RLM] and used in the justification [E.Just.DT.RLM-1]. Functionally assess whether the resilience mechanisms mitigate the effects of DoS attacks on the network interfaces and that the equipment returns to a defined state following an attack, considering the intended equipment functionality and its intended operational environment of use. Commercial tools may be used in testing. The purpose of the test tools is to identify if the equipment when subjected to simulated DoS attacks on the network interfaces is capable of returning to a defined state following the simulated attack scenarios.						
Result:	Bluetooth BR/EDR/LE: Secure Simple Pairing: Supported Baseband: - RSSI: -71.125 dBm (weak) - Initial Center Frequency Offset: -10.09 kHz - Link 2 - Role: Central (0xdc-ec-4f-27-5a-68) - Channel: 25 - 2427 MHz - Clock: 0x002227bc - Packet Status: OK - FLOW: Go - TYPE: DM1 - Payload Data Rate: 1 Mbps - LT_ADDR: 1 - SEQN: 0 - ARQN: 1 - L2CAP Flow: N/A [1] - Logical Link ID: LMP - Decrypted by Bluetooth ComProbe: No - Payload Length: 12 LMP: - Link 2 - Role: Central - Address: 1 - Escape opcode: 127 - Transaction ID: Initiated by central - Extended Opcode: LMP_features_req_ext - Feature's Page Number: 1 - Max Supported Feature's Pages: 2 Extended Features - Secure Connections (Host Support): Supported - Previously used (Simultaneous LE and BR/EDR to Same Device Capable (Host)): Not Supported - LE Supported (Host): Supported - Secure Simple Pairing (Host Support): Supported Frame 1,096: Len=52 LE BB: LE PKT: - Preamble: 0x55 - Access Address: 0xf626a837 - BD Address: dc:ec:4f:27:5a:68 - CRC: 0xa7601d LE DATA: L2CAP: SMP: - Code: Pairing Request - IO Capabilities: KeyboardDisplay - OOB data flag: OOB Authentication data not present AuthReq - Bonding_Flags: Bonding - MITM: MITM Protection: Yes - Secure Connection Pairing: Yes - Keypress Notifications: No - CT2: Supports h7 Function: Yes - Maximum Encryption Key Size: 16 Octets Initiator Key Distribution Responder Key Distribution Wi-Fi: Network properties Name: DDT-JIE Password: 12345678 Band: 2.4 GHz Scan to connect:  Devices connected: 1 of 8 <table><thead><tr><th>Device name</th><th>IP address</th><th>Physical address (MAC)</th></tr></thead><tbody><tr><td>未知</td><td>192.168.137.228</td><td>3e:06:75:42:30:40</td></tr></tbody></table> Launch a TCP attack using the Hping3 tool.	Device name	IP address	Physical address (MAC)	未知	192.168.137.228	3e:06:75:42:30:40
Device name	IP address	Physical address (MAC)					
未知	192.168.137.228	3e:06:75:42:30:40					

```
(kali@192)-[~]
$ ping 192.168.137.228
PING 192.168.137.228 (192.168.137.228) 56(84) bytes of data.
64 bytes from 192.168.137.228: icmp_seq=1 ttl=128 time=94.1 ms
64 bytes from 192.168.137.228: icmp_seq=2 ttl=128 time=113 ms
^C
--- 192.168.137.228 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 94.133/103.365/112.597/9.232 ms

(kali@192)-[~]
$ sudo hping3 -C 10000 -d 120 -S -A -p 8080 --flood 192.168.137.228
[sudo] kali 的密码:
HPING 192.168.137.228 (eth0 192.168.137.228): SA set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown

Reply from 192.168.137.228: bytes=32 time=135ms TTL=64
Reply from 192.168.137.228: bytes=32 time=107ms TTL=64
Reply from 192.168.137.228: bytes=32 time=115ms TTL=64
Reply from 192.168.137.228: bytes=32 time=22ms TTL=64
Reply from 192.168.137.228: bytes=32 time=15ms TTL=64
Reply from 192.168.137.228: bytes=32 time=61ms TTL=64
Reply from 192.168.137.228: bytes=32 time=66ms TTL=64
Reply from 192.168.137.228: bytes=32 time=88ms TTL=64
Reply from 192.168.137.228: bytes=32 time=2ms TTL=64
Reply from 192.168.137.228: bytes=32 time=49ms TTL=64
Reply from 192.168.137.228: bytes=32 time=215ms TTL=64
Reply from 192.168.137.228: bytes=32 time=235ms TTL=64
Reply from 192.168.137.228: bytes=32 time=35ms TTL=64
Reply from 192.168.137.228: bytes=32 time=44ms TTL=64
Reply from 192.168.137.228: bytes=32 time=95ms TTL=64
Reply from 192.168.137.228: bytes=32 time=79ms TTL=64
Reply from 192.168.137.228: bytes=32 time=207ms TTL=64
Reply from 192.168.137.228: bytes=32 time=98ms TTL=64
Reply from 192.168.137.228: bytes=32 time=23ms TTL=64
Reply from 192.168.137.228: bytes=32 time=117ms TTL=64
Reply from 192.168.137.228: bytes=32 time=275ms TTL=64
Reply from 192.168.137.228: bytes=32 time=140ms TTL=64
Reply from 192.168.137.228: bytes=32 time=52ms TTL=64
Reply from 192.168.137.228: bytes=32 time=180ms TTL=64
Reply from 192.168.137.228: bytes=32 time=181ms TTL=64
Reply from 192.168.137.228: bytes=32 time=108ms TTL=64
Reply from 192.168.137.228: bytes=32 time=98ms TTL=64
Reply from 192.168.137.228: bytes=32 time=110ms TTL=64
Request timed out.
Reply from 192.168.137.228: bytes=32 time=2ms TTL=64
Reply from 192.168.137.228: bytes=32 time=103ms TTL=64
Reply from 192.168.137.228: bytes=32 time=30ms TTL=64
Reply from 192.168.137.228: bytes=32 time=16ms TTL=64
Reply from 192.168.137.228: bytes=32 time=2ms TTL=64
Reply from 192.168.137.228: bytes=32 time=12ms TTL=64
```

Launch a ICMP attack using the Hping3 tool.

```
(kali@192)-[~]
$ ping 192.168.137.228
PING 192.168.137.228 (192.168.137.228) 56(84) bytes of data.
64 bytes from 192.168.137.228: icmp_seq=1 ttl=128 time=304 ms
64 bytes from 192.168.137.228: icmp_seq=2 ttl=128 time=36.1 ms
64 bytes from 192.168.137.228: icmp_seq=3 ttl=128 time=53.7 ms
^C
--- 192.168.137.228 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 36.108/131.215/303.833/122.270 ms

(kali@192)-[~]
$ sudo hping3 --icmp -C 10000 -d 120 -p 8080 --flood 192.168.137.228
HPING 192.168.137.228 (eth0 192.168.137.228): icmp mode set, 28 headers + 120 data
bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.137.228 hping statistic ---
1177498 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@192)-[~]
$

C:\Users>ping 192.168.137.228 -t
Pinging 192.168.137.228 with 32 bytes of data:
Reply from 192.168.137.228: bytes=32 time=7ms TTL=64
Reply from 192.168.137.228: bytes=32 time=370ms TTL=64
Reply from 192.168.137.228: bytes=32 time=1292ms TTL=64
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.137.228: bytes=32 time=3039ms TTL=64
Reply from 192.168.137.228: bytes=32 time=28ms TTL=64
Reply from 192.168.137.228: bytes=32 time=58ms TTL=64
Reply from 192.168.137.228: bytes=32 time=3ms TTL=64
Reply from 192.168.137.228: bytes=32 time=61ms TTL=64
Reply from 192.168.137.228: bytes=32 time=285ms TTL=64
Reply from 192.168.137.228: bytes=32 time=53ms TTL=64
Request timed out.
Reply from 192.168.137.228: bytes=32 time=4ms TTL=64
Reply from 192.168.137.228: bytes=32 time=53ms TTL=64
Reply from 192.168.137.228: bytes=32 time=5ms TTL=64
Reply from 192.168.137.228: bytes=32 time=2ms TTL=64
Reply from 192.168.137.228: bytes=32 time=27ms TTL=64
Reply from 192.168.137.228: bytes=32 time=170ms TTL=64
Reply from 192.168.137.228: bytes=32 time=308ms TTL=64
Reply from 192.168.137.228: bytes=32 time=76ms TTL=64
Reply from 192.168.137.228: bytes=32 time=20ms TTL=64
Reply from 192.168.137.228: bytes=32 time=11ms TTL=64
Reply from 192.168.137.228: bytes=32 time=3ms TTL=64
Reply from 192.168.137.228: bytes=32 time=16ms TTL=64
Reply from 192.168.137.228: bytes=32 time=12ms TTL=64
Reply from 192.168.137.228: bytes=32 time=2ms TTL=64
Reply from 192.168.137.228: bytes=32 time=88ms TTL=64
```

Launch a UDP attack using the Hping3 tool.

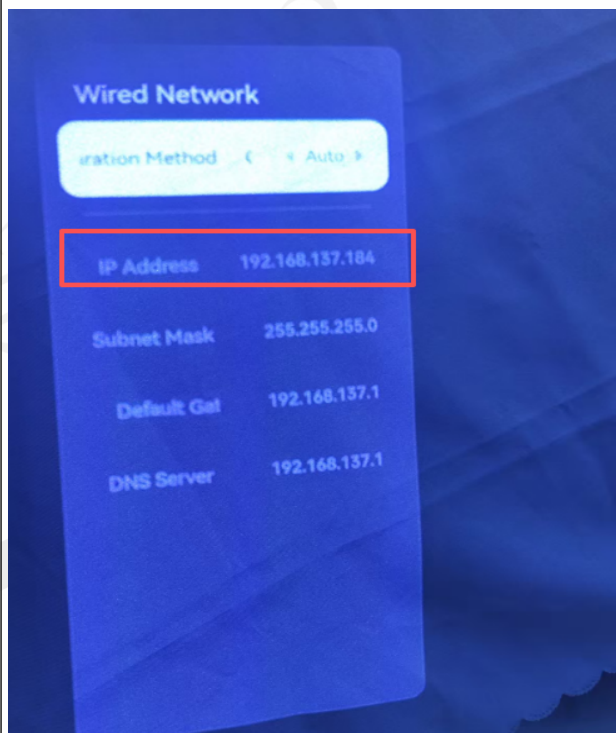
```
(kali@192)-[~]
$ ping 192.168.137.228
PING 192.168.137.228 (192.168.137.228) 56(84) bytes of data.
64 bytes from 192.168.137.228: icmp_seq=1 ttl=64 time=16.2 ms
64 bytes from 192.168.137.228: icmp_seq=2 ttl=64 time=20.2 ms
64 bytes from 192.168.137.228: icmp_seq=3 ttl=64 time=38.1 ms
64 bytes from 192.168.137.228: icmp_seq=4 ttl=64 time=58.0 ms
64 bytes from 192.168.137.228: icmp_seq=5 ttl=64 time=3.92 ms
^C
--- 192.168.137.228 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 3.921/27.254/57.954/18.850 ms

(kali@192)-[~]
$ sudo hping3 -2 --flood 192.168.137.228
HPING 192.168.137.228 (eth0 192.168.137.228): udp mode set, 28 headers + 0
data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.137.228 hping statistic ---
955630 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@192)-[~]
$

正在 Ping 192.168.137.228 具有 32 字节的数据:
来自 192.168.137.228 的回复: 字节=32 时间=219ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=26ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=34ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=276ms TTL=64
请求超时。
来自 192.168.137.228 的回复: 字节=32 时间=297ms TTL=64
请求超时。
请求超时。
来自 192.168.137.228 的回复: 字节=32 时间=66ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=43ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=77ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=93ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=104ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=22ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=47ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=136ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=69ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=135ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=104ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=110ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=24ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=31ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=38ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=155ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=64ms TTL=64
来自 192.168.137.228 的回复: 字节=32 时间=72ms TTL=64
```

LAN:



Launch a TCP attack using the Hping3 tool.

```
(kali@192)-[~]
$ ping 192.168.137.184
PING 192.168.137.184 (192.168.137.184) 56(84) bytes of data:
64 bytes from 192.168.137.184: icmp_seq=1 ttl=64 time=2.69 ms
64 bytes from 192.168.137.184: icmp_seq=2 ttl=64 time=4.80 ms
^C
--- 192.168.137.184 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 2.686/3.744/4.803/1.058 ms

(kali@192)-[~]
$ sudo hping3 -C 10000 -d 120 -S -A -p 8080 --frag 192.168.137.184 --flood
[sudo] kali 的密码:
HPING 192.168.137.184 (eth0 192.168.137.184): SA set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.137.184 hping statistic ---
131007 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali@192)-[~]
```

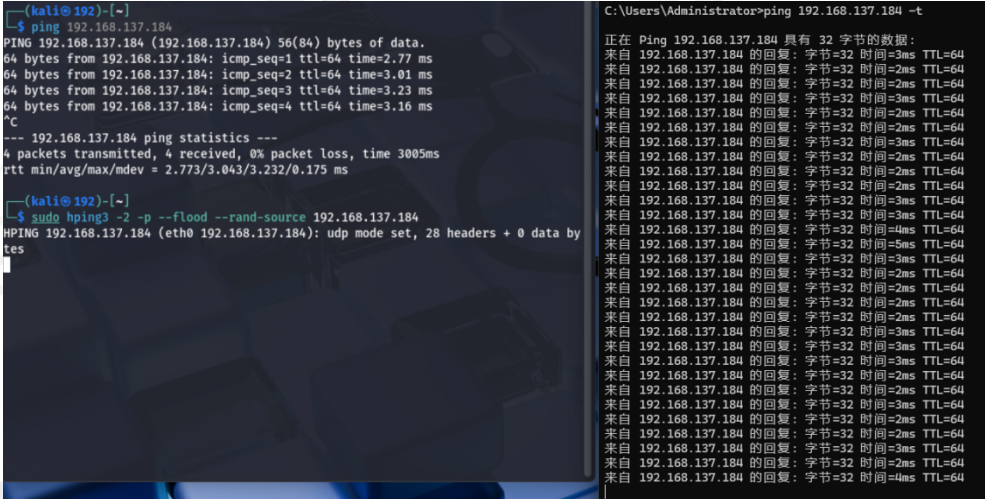
```
C:\Users\Administrator>ping 192.168.137.184 -t
正在 Ping 192.168.137.184 具有 32 字节的数据:
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=3ms TTL=64
请求超时。
请求超时。
请求超时。
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=3ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
```

Launch a ICMP attack using the Hping3 tool.

```
(kali@192)-[~]
$ ping 192.168.137.184
PING 192.168.137.184 (192.168.137.184) 56(84) bytes of data:
64 bytes from 192.168.137.184: icmp_seq=1 ttl=64 time=1.37 ms
64 bytes from 192.168.137.184: icmp_seq=2 ttl=64 time=1.57 ms
64 bytes from 192.168.137.184: icmp_seq=3 ttl=64 time=3.40 ms
64 bytes from 192.168.137.184: icmp_seq=4 ttl=64 time=2.70 ms
^C
--- 192.168.137.184 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.373/2.259/3.398/0.828 ms

(kali@192)-[~]
$ sudo hping3 --icmp -C 10000 -d 130 -p 8080 --flood 192.168.137.184
HPING 192.168.137.184 (eth0 192.168.137.184): icmp mode set, 28 headers + 130 data bytes
hping in flood mode, no replies will be shown
^C
```

```
C:\Users\Administrator>ping 192.168.137.184 -t
正在 Ping 192.168.137.184 具有 32 字节的数据:
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=7ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=8ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=8ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=8ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=4ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=5ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=9ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=2ms TTL=64
来自 192.168.137.184 的回复: 字节=32 时间=1ms TTL=64
```

	Launch a UDP attack using the Hping3 tool. 
Assignment of verdict:	Pass

3.7 [NMM] Network monitoring mechanism

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

--Conceptual assessment--

Identifier [NMM-1]-01	/		
Decision node	Decision [E.Info.DT.NMM-1]		Justification [E.Just.DT.NMM-1]
DT.NMM-1.DN-1	Yes	No (√)	[E.Info.NMM-1.NMM.NetworkEquipment]: The equipment is not a network equipment.
Assignment of verdict:	N/A		

--Completeness testing--

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

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional validation of the appropriateness of the Network Monitoring Mechanisms described in [E.Info.NMM-1.NMM]. The assessment verifies whether the traffic between networks (which is controlled or processed by the network equipment) is monitored and analysed to mitigate the risk related to security assets and network assets in the networks documented in [E.Info.NMM-1.NMM.NetworkEquipment].
Preconditions:	The equipment is operational and if available setup or configuration which is related to the traffic between networks did take place. Physical network connection to communicate between networks is established.

Operation steps:	/
Result:	/
Assignment of verdict:	N/A

3.8 [TCM] Traffic control mechanism

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

--Conceptual assessment--

Identifier [TCM-1]-01	/		
Decision node	Decision [E.Info.DT.TCM-1]		Justification [E.Just.DT.TCM-1]
DT.TCM-1.DN-1	Yes	No (√)	[E.Info.NMM-1.NMM.NetworkEquipment]: The equipment is not a network equipment.
Assignment of verdict:	N/A		

--Completeness testing--

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

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional validation of the appropriateness of the Traffic Control Mechanisms described in [E.Info.TCM-1.TCM]. The assessment verifies whether the traffic forwarded by the network equipment to a network is controlled to avoid compromising or harm the network assets and security assets in the networks which are controlled or served by the network equipment.
Preconditions:	The equipment is in an operational state and if available setup or configuration did take place which is related to the traffic between networks.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A

3.9 [CCK] Confidential cryptographic keys

3.9.1 [CCK-1] Appropriate CCKs

--Conceptual assessment--

Identifier [CCK-1]-01	[E.Info.CCK-1.CCK]: CCK-01: Communication Encryption Algorithm: TLS_AES_128_GCM_SHA256
--------------------------	--

	TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA CCK-02: Bluetooth Encryption Algorithm: AES-CCM-128 CCK-03: The firmware package is digitally signed using a certificate-based SHA-256 with RSA2048 algorithm.		
Decision node	Decision		Justification
	[E.Info.DT.CCK-1]		[E.Just.DT.CCK-1]
[DT.CCK-1.DN-2]	Yes (✓)	No	[E.Info.CCK-1.CCK.SecurityStrength]: All these CCKs meet the minimum security strength requirement of 112 bits.
Assignment of verdict:	Pass		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the documentation of CCKs is complete.
Preconditions:	The equipment is in an operational state.
Operation steps:	Functionally assess whether the device has preinstalled or generated CCKs that are not recorded in [E.Info.CCK-1.CCK].
Result:	The device has not preinstalled or generated any CCKs that are not recorded in [E.Info.CCK-1.CCK].
Assignment of verdict:	Pass

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the confidential cryptographic keys documented [E.Info.CCK-1.CCK] are implemented as documented. NOTE The assessment of the bit length is only a necessary condition and does not constitute a complete functional sufficiency assessment for security strength.
Preconditions:	The equipment is in an operational state.
Operation steps:	For each confidential cryptographic key documented in [E.Info.CCK-1.CCK] functionally assess whether the CCK's length as documented in [E.Info.CCK-1.CCK] is implemented in accordance

	with [E.Info.CCK-1.CCK.SecurityStrength].
Result:	The core security strength of all listed encryption algorithms is greater than 112 bits. CCK-01: Communication Encryption Algorithm: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA <pre> 291 49.195375 192.168.137.7 222.217.94.16 TLSv1.3 655 Client Hello (SHA256-static-el.static.xgimi.com) 293 49.277047 222.217.94.16 192.168.137.7 TLSv1.3 298 Server Hello, Change Cipher Spec, Application Data, Application Data 295 49.306941 192.168.137.7 222.217.94.16 TLSv1.3 118 Change Cipher Spec, Application Data 296 49.375127 222.217.94.16 192.168.137.7 TLSv1.3 365 Application Data 297 49.406237 192.168.137.7 222.217.94.16 TLSv1.3 334 Application Data 298 49.487164 222.217.94.16 192.168.137.7 TLSv1.3 1468 Application Data 310 49.490389 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data 334 49.564252 222.217.94.16 192.168.137.7 TLSv1.3 1514 Application Data </pre> Transmission Control Protocol, Src Port: 46050, Dst Port: 443, Seq: 1, Ack: 1, Len: 601 Transport Layer Security [Stream Index: 7] ▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello Content Type: Handshake (22) Version: TLS 1.0 (0x0301) Length: 596 ▼ Handshake Protocol: Client Hello Handshake Type: Client Hello (1) Length: 592 > Version: TLS 1.2 (0x0303) Random: b683d5e074818995b92c59870a2ccae0a6feccc618e6343e3ed108cd4473757 Session ID Length: 32 Session ID: c25f1cccc3c4de8842b7c1fe71417e26a1df46139a09eeaa9c5c19fa26436 Cipher Suites Length: 34 ▼ Cipher Suites (17 suites) Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301) Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302) Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc02d) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc031) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c) Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d) Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f) Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035) Connection Methods Length: 1 CCK-02: Bluetooth Encryption Algorithm: AES-CCM-128

Frame 1,431: (Central) Len=30

- Baseband:
 - RSSI: -72.375 dBm (weak)
 - Initial Center Frequency Offset: -10.72 kHz
 - Link: 2
 - Role: Central (0xdc-ec-4f-27-5a-68)
 - Channel: 21 - 2423 MHz
 - Clock: 0x00225e10
 - Packet Status: OK
 - FLOW: Go
 - TYPE: DM1
 - Payload Data Rate: 1 Mbps
 - LT_ADDR: 1
 - SEQN: 1
 - ARQN: 0
 - L2CAP Flow: N/A [1]
 - Logical Link ID: LMP
 - Decrypted by Bluetooth ComProbe: No
 - Payload Length: 2
- LMP:
 - Link: 2
 - Role: Central
 - Address: 1
 - Opcode: LMP_encryption_key_size_req
 - Transaction ID: Initiated by central
 - Key Size: 16 bytes

Decode Device Database

Bluetooth Security

Show: All Security Events ▼

Time	Central & Peripheral
1/4/2026 9:32:07.53515...	DC:EC:4F:27:5A:68
...	"KENWOOD GLASS Core" 5C:8E:8B:9C:7A:13

Baseband:

- RSSI: -71.125 dBm (weak)
- Initial Center Frequency Offset: -10.09 kHz
- Link: 2
- Role: Central (0xdc-ec-4f-27-5a-68)
- Channel: 25 - 2427 MHz
- Clock: 0x002227bc
- Packet Status: OK
- FLOW: Go
- TYPE: DM1
- Payload Data Rate: 1 Mbps
- LT_ADDR: 1
- SEQN: 0
- ARQN: 1
- L2CAP Flow: N/A [1]
- Logical Link ID: LMP
- Decrypted by Bluetooth ComProbe: No
- Payload Length: 12

LMP:

- Link: 2
- Role: Central
- Address: 1
- Escape opcode: 127
- Transaction ID: Initiated by central
- Extended Opcode: LMP_features_req_ext
- Feature's Page Number: 1
- Max Supported Feature's Pages: 2

Extended Features

- Secure Connections (Host Support): Supported
- Previously used (Simultaneous LE and BR/EDR to Same Device Capable (Host)): Not Supported
- LE Supported (Host): Supported
- Secure Simple Pairing (Host Support): Supported

CCK-03: The firmware package is digitally signed using a certificate-based SHA-256 with RSA2048 algorithm.

	<pre> \$ openssl x509 -in otacert.cer -text -noout Certificate: Data: Version: 3 (0x2) Serial Number: d0:19:71:b3:8a:35:de:b8 Signature Algorithm: sha256WithRSAEncryption Issuer: C=CN, ST=SHICHUAN, L=CHENGDU, O=XGIMI_CO_LTD, OU=XGIMI, CN=XGIMI, emailAddress=www.xgimi.com Validity Not Before: Sep 28 07:43:04 2018 GMT Not After : Feb 13 07:43:04 2046 GMT Subject: C=CN, ST=SHICHUAN, L=CHENGDU, O=XGIMI_CO_LTD, OU=XGIMI, CN=XGIMI, emailAddress=www.xgimi.com Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: 00:ba:11:71:12:02:7d:19:a7:56:cd:5b:b9:14:67: 60:82:da:36:1b:c1:b2:95:e1:88:00:0f:0a:35:09: 84:63:b1:9e:c4:1c:1e:d7:eb:da:2d:e0:9d:81:3c: 0c:c3:46:07:d7:16:7a:0c:ab:4a:b2:ae:ba:9d:90: 92:11:e8:4d:a8:8b:cb:4c:42:c1:b7:c4:73:fe:41: df:1d:b9:62:8d:c4:b0:ba:a9:56:57:be:2c:ed:b5: c5:47:9e:e3:4d:f6:ba:53:79:81:02:0e:e8:60:54: fd:21:5a:78:71:5e:ad:d3:a8:b5:b2:ec:d6:2a:a7: a4:e1:f1:48:ba:6e:af:db:b8:6c:15:2e:96:f2:ad: 8b:3b:3c:54:7a:2d:b1:df:0f:cd:d6:d9:8e:68:83: 6c:f2:2c:b6:09:42:ea:29:0b:7d:e1:f2:ba:8d:97: 5d:66:8e:34:57:26:78:c2:e9:18:91:f3:9f:87:e8: 12:9d:4f:dd:4b:e2:6d:81:3a:a3:a2:65:3f:9d:04: ad:19:b6:ee:02:ba:71:65:af:4a:2a:ed:6f:8e:81: e7:96:7b:ae:69:60:a2:fb:fb:94:d0:ae:7d:97:ba: aa:00:7a:4b:dd:66:0d:f7:ac:72:bc:28:45:2e:a6: b8:93:26:5f:99:64:1e:eb:e8:93:1c:da:07:d1:f9: da:b9 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Subject Key Identifier: 15:35:18:20:72:26:8D:84:03:C0:B2:E3:71:56:9C:E1:07:D0:E5:4D X509v3 Authority Key Identifier: 15:35:18:20:72:26:8D:84:03:C0:B2:E3:71:56:9C:E1:07:D0:E5:4D X509v3 Basic Constraints: critical CA:TRUE Signature Algorithm: sha256WithRSAEncryption Signature Value: 9c:0d:b4:ad:3d:12:bc:79:45:32:72:d1:d8:38:3e:a0:aa:f9: f8:3f:84:9a:55:9a:05:ae:e8:87:d2:b2:e8:b1:c1:03:9b:a8: 91:2a:e7:ae:fb:49:36:38:12:5a:e3:17:12:52:a4:79:e4:ac: 3b:e6:ab:a3:2b:fd:66:3d:72:d7:4c:1b:7e:0d:de:87:a6:b6: 8d:00:34:48:a4:95:ec:f3:a6:76:7a:66:6d:7c:4b:ad:f6:84: 04:91:cd:93:ad:23:28:f7:1c:49:d8:82:da:0d:01:de:ac:44: </pre>
Assignment of verdict:	Pass

3.9.2 [CCK-2] CCK generation mechanisms

--Conceptual assessment--

Identifier [CCK-2]-01	[E.Info.CCK-2.Generation]: CCK-01: Communication Encryption Algorithm: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA		
Decision node	<table> <tr> <td data-bbox="371 2047 632 2047">Decision</td><td data-bbox="632 2047 1457 2047">Justification</td></tr> </table>	Decision	Justification
Decision	Justification		

	[E.Info.DT.CCK-2]		[E.Just.DT.CCK-2]
[DT.CCK-2.DN-2]	Yes (✓)	No	[E.Info.CCK-2.Generation.CCK]: These communication encryption algorithms are negotiated and determined during the TLS handshake process. The symmetric encryption components (AES-128, AES-256, ChaCha20) are implemented based on the underlying cryptographic module, and the random numbers involved in key exchange and generation are true random numbers generated by the hardware TRNG (True Random Number Generator). [E.Info.CCK-2.Generation.RNSource]: The random numbers are true random numbers generated by the hardware TRNG (True Random Number Generator).
Assignment of verdict:	Pass		

Identifier [CCK-2]-02	[E.Info.CCK-2.Generation]: CCK-02: Bluetooth Encryption Algorithm: AES-CCM-128		
Decision node	Decision [E.Info.DT.CCK-2]		Justification [E.Just.DT.CCK-2]
[DT.CCK-2.DN-2]	Yes (✓)	No	[E.Info.CCK-2.Generation.CCK]: This key is negotiated and generated during the first Bluetooth pairing. AES-CCM-128 is implemented based on hardware AES at the underlying level, and the random numbers are true random numbers generated by the hardware TRNG (True Random Number Generator). [E.Info.CCK-2.Generation.RNSource]: The random numbers are true random numbers generated by the hardware TRNG (True Random Number Generator).
Assignment of verdict:	Pass		

Identifier [CCK-2]-03	[E.Info.CCK-2.Generation]: CCK-03: The firmware package is digitally signed using a certificate-based SHA-256 with RSA2048 algorithm.		
Decision node	Decision [E.Info.DT.CCK-2]		Justification [E.Just.DT.CCK-2]
[DT.CCK-2.DN-2]	Yes (✓)	No	[E.Info.CCK-2.Generation.CCK]: The firmware package is protected using a digital signature mechanism based on a certificate-based SHA-256 with RSA2048 algorithm. During firmware generation, a cryptographic hash of the firmware image is computed using the SHA-256 hash algorithm. The resulting hash value is then digitally signed using an RSA private key with a key length of 2048 bits. The corresponding public key is contained within a trusted digital certificate used for signature verification. During firmware verification, the system validates the digital signature using the public key extracted from the trusted certificate to ensure the authenticity and integrity of the firmware package. Only firmware images with a valid signature are accepted and allowed to be installed or executed.

			[E.Info.CCK-2.Generation.RNSource]: The random numbers are true random numbers generated by the hardware TRNG (True Random Number Generator).
Assignment of verdict:	Pass		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is to conceptually assess whether all generation mechanisms for confidential cryptographic keys on the equipment are documented in [E.Info.CCK-2.Generation].
Preconditions:	None.
Operation steps:	Through consistency assessment with [E.Info.CCK-1.CCK], assess whether there are confidential cryptographic key generation mechanisms on the device that are not recorded in [E.Info.CCK-2.Generation].
Result:	There is no evidence of the existence of confidential cryptographic key generation mechanisms that are not recorded in [E.Info.CCK-2.Generation].
Assignment of verdict:	Pass

--Sufficiency testing--

There is significant complexity surrounding the validation of cryptographic key generation mechanisms and typically they will be implemented by a third party with significant cryptographic expertise, who is unlikely to share details of such key generation processes. Given these considerations, no functional sufficiency assessment is provided for this requirement.

3.9.3 [CCK-3] Preventing static default values for preinstalled CCKs**--Conceptual assessment--**

Identifier [CCK-3]-01	/		
Decision node	Decision [E.Info.DT.CCK-3]	Justification [E.Just.DT.CCK-3]	
/	/	/	/
Assignment of verdict:	N/A This device contains no pre-stored confidential cryptographic keys.		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether all preinstalled CCKs are documented.
Preconditions:	The equipment is in the factory default state.
Operation steps: ®	/ ®
Result:	/
Assignment of	N/A

verdict:	This device contains no pre-stored confidential cryptographic keys.
-----------------	---

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether preinstalled CCKs that are claimed to be practically unique per equipment are sufficiently independent from each other.
Preconditions:	Two instances of the equipment are in a factory default state.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A This device contains no pre-stored confidential cryptographic keys.

3.10 [GEC] General equipment capabilities**3.10.1 [GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities****--Conceptual assessment--**

Identifier [GEC-1]-01	[E.Info.GEC-1.SoftwareDocumentation]: All the software of the device, and the software version is V2.0.8 [E.Info.GEC-1.HardwareDocumentation]: All the hardware of the device, and the hardware version is 11-000109-001		
Decision node	Decision		Justification
	[E.Info.DT.GEC-1]		[E.Just.DT.GEC-1]
[DT.GEC-1.DN-1]	Yes	No (✓)	[E.Info.GEC-1.SoftwareDocumentation]: All the software of the device, with the software version being: V2.0.8 [E.Info.GEC-1.ListOfVulnerabilities]: All the vulnerabilities contained in the device software can be found in the attachment. [E.Info.GEC-1.HardwareDocumentation]: All the hardware of the device, with the hardware version being: 11-000109-001 [E.Info.GEC-1.ListOfVulnerabilities]: All the vulnerabilities contained in the device hardware can be found in the attachment.
Assignment of verdict:	Pass		

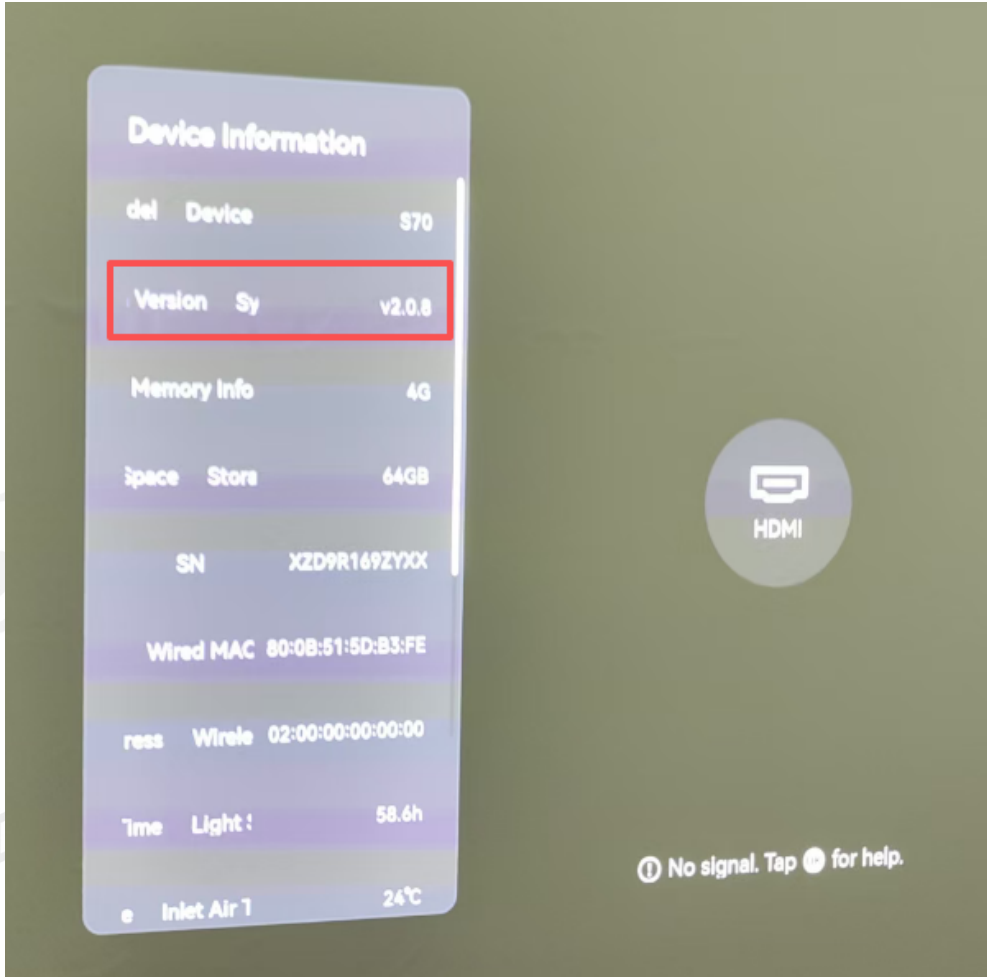
--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment of the equipment under test to verify the completeness of the documentation: that the vulnerabilities present in the equipment which affect privacy assets or security assets are only those listed in [E.Info.GEC-1.ListOfVulnerabilities].
Preconditions:	The equipment is in an operational state. The date for the source of the vulnerabilities to be used in the assessment of the list of publicly

	known exploitable vulnerabilities is recent.																														
Operation steps:	Use the Nessus vulnerability scanning tool to perform a vulnerability scan on the tested device and review the vulnerability report.																														
Result:	No medium-risk or high-risk vulnerabilities were detected during the scan. 192.168.137.228 <table><tr><td>0</td><td>0</td><td>0</td><td>1</td><td>9</td></tr><tr><td>CRITICAL</td><td>HIGH</td><td>MEDIUM</td><td>LOW</td><td>INFO</td></tr></table> Scan Information Start time: Sun Jan 4 11:16:12 2026 End time: Sun Jan 4 11:22:26 2026 Host Information IP: 192.168.137.228 MAC Address: 3E:06:75:42:30:40 OS: Linux Kernel 2.6 Vulnerabilities 10114 - ICMP Timestamp Request Remote Date Disclosure Statement Test item description: Projector Model/Type reference: XR06B Software Version(s): V2.0.8 Hardware Version(s): 11-000109-001 Manufacturer: XGIMI Technology Co., Ltd. <table><thead><tr><th>Risk</th><th>CVE</th><th>Name</th><th>Description</th></tr></thead><tbody><tr><td>Low</td><td>None</td><td>No applicable vulnerability</td><td>No vulnerabilities detected in this risk level.</td></tr><tr><td>Medium</td><td>None</td><td>No applicable vulnerability</td><td>No vulnerabilities detected in this risk level.</td></tr><tr><td>High</td><td>None</td><td>No applicable vulnerability</td><td>No vulnerabilities detected in this risk level.</td></tr><tr><td>Critical</td><td>None</td><td>No applicable vulnerability</td><td>No vulnerabilities detected in this risk level.</td></tr></tbody></table> Signature: Jan 15, 2026	0	0	0	1	9	CRITICAL	HIGH	MEDIUM	LOW	INFO	Risk	CVE	Name	Description	Low	None	No applicable vulnerability	No vulnerabilities detected in this risk level.	Medium	None	No applicable vulnerability	No vulnerabilities detected in this risk level.	High	None	No applicable vulnerability	No vulnerabilities detected in this risk level.	Critical	None	No applicable vulnerability	No vulnerabilities detected in this risk level.
0	0	0	1	9																											
CRITICAL	HIGH	MEDIUM	LOW	INFO																											
Risk	CVE	Name	Description																												
Low	None	No applicable vulnerability	No vulnerabilities detected in this risk level.																												
Medium	None	No applicable vulnerability	No vulnerabilities detected in this risk level.																												
High	None	No applicable vulnerability	No vulnerabilities detected in this risk level.																												
Critical	None	No applicable vulnerability	No vulnerabilities detected in this risk level.																												

Assignment of verdict:	Pass
------------------------	------

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment if the vulnerabilities present in the equipment which are listed in [E.Info.GEC-1.ListOfVulnerabilities] are not able to affect security assets or privacy assets, if exploited.
Preconditions:	The equipment is in an operational state. The date for the source of the vulnerabilities to be used in the assessment of the list of publicly known exploitable vulnerabilities is recent.
Operation steps:	Use the Nessus vulnerability scanning tool to perform a vulnerability scan on the tested device and review the vulnerability report.
Result:	No medium-risk or high-risk vulnerabilities were detected during the scan.  The screenshot shows a 'Device Information' screen with the following details: Device S70, Version Sy v2.0.8 (highlighted with a red box), Memory Info 4G, Space Store 64GB, SN XZD9R169ZY0X, Wired MAC 80:0B:51:5D:B3:FE, Wireless 02:00:00:00:00:00, Time Light 58.6h, and Inlet Air 24°C. There is also an HDMI icon and a message 'No signal. Tap for help.'

192.168.137.228

0

0

0

1

9

CRITICAL

HIGH

MEDIUM

LOW

INFO

Scan Information

Start time:

Sun Jan 4 11:16:12 2026

End time:

Sun Jan 4 11:22:26 2026

Host Information

IP:

192.168.137.228

MAC Address:

3E:06:75:42:30:40

OS:

Linux Kernel 2.6

Vulnerabilities

10114 - ICMP Timestamp Request Remote Date Disclosure

Statement

Test item description: Projector

Model/Type reference: XR06B

Software Version(s): V2.0.8

Hardware Version(s): 11-000109-001

Manufacturer: XGIMI Technology Co., Ltd.

Risk	CVE	Name	Description
Low	None	No applicable vulnerability	No vulnerabilities detected in this risk level.
Medium	None	No applicable vulnerability	No vulnerabilities detected in this risk level.
High	None	No applicable vulnerability	No vulnerabilities detected in this risk level.
Critical	None	No applicable vulnerability	No vulnerabilities detected in this risk level.

Signature:

Jan 15, 2026

Assignment of verdict:

Pass

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

--Conceptual assessment--

Identifier [GEC-2]-01	IF-01: Bluetooth BR/EDR/LE		
Decision node	Decision [E.Info.DT.GEC-2]		Justification [E.Just.DT.GEC-2]
[DT.GEC-2.DN-3]	Yes (√)	No	[E.Info.GEC-2.NetworkInterface.Exposure]: The Bluetooth function is enabled by default at the factory and is used to connect Bluetooth peripheral devices (such as speakers), as well as to support connections with Bluetooth remote controllers.
Assignment of verdict:	Pass		

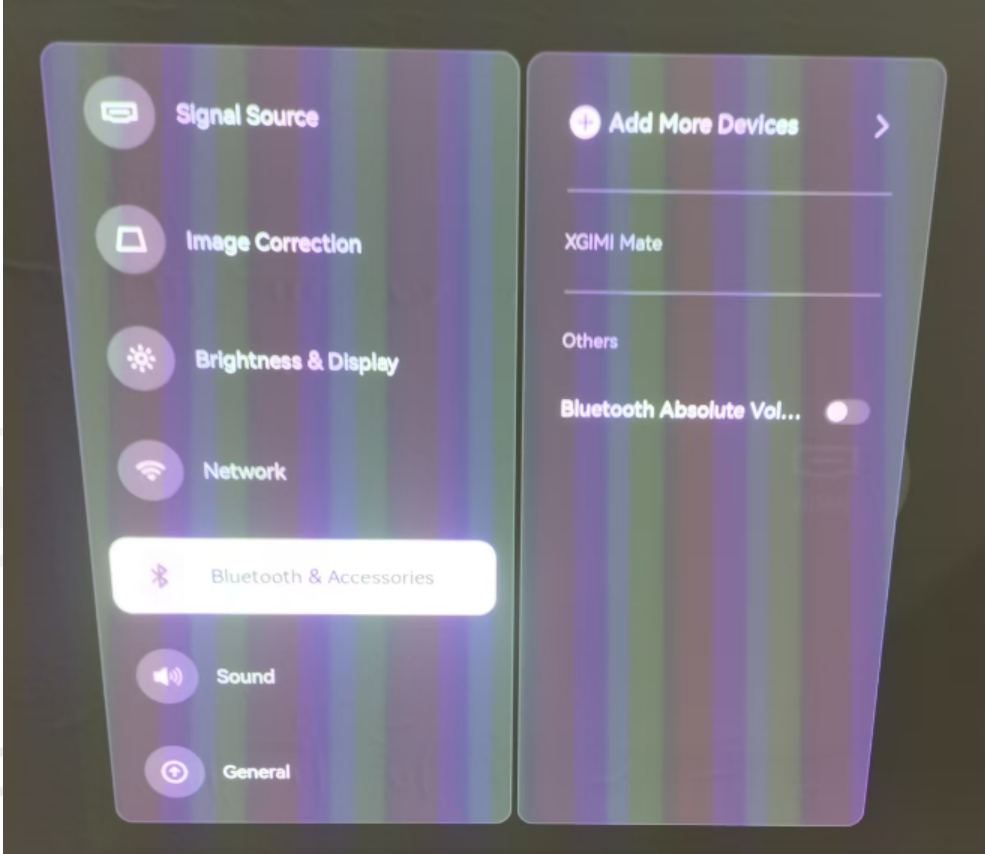
Identifier [GEC-2]-02	IF-02: Wi-Fi		
Decision node	Decision [E.Info.DT.GEC-2]		Justification [E.Just.DT.GEC-2]
[DT.GEC-2.DN-3]	Yes (√)	No	[E.Info.GEC-2.NetworkInterface.Exposure]: The TLS 1.3 protocol is used for connecting the DUT to the server, with business instructions transmitted via this secure channel to perform business operations.
Assignment of verdict:	Pass		

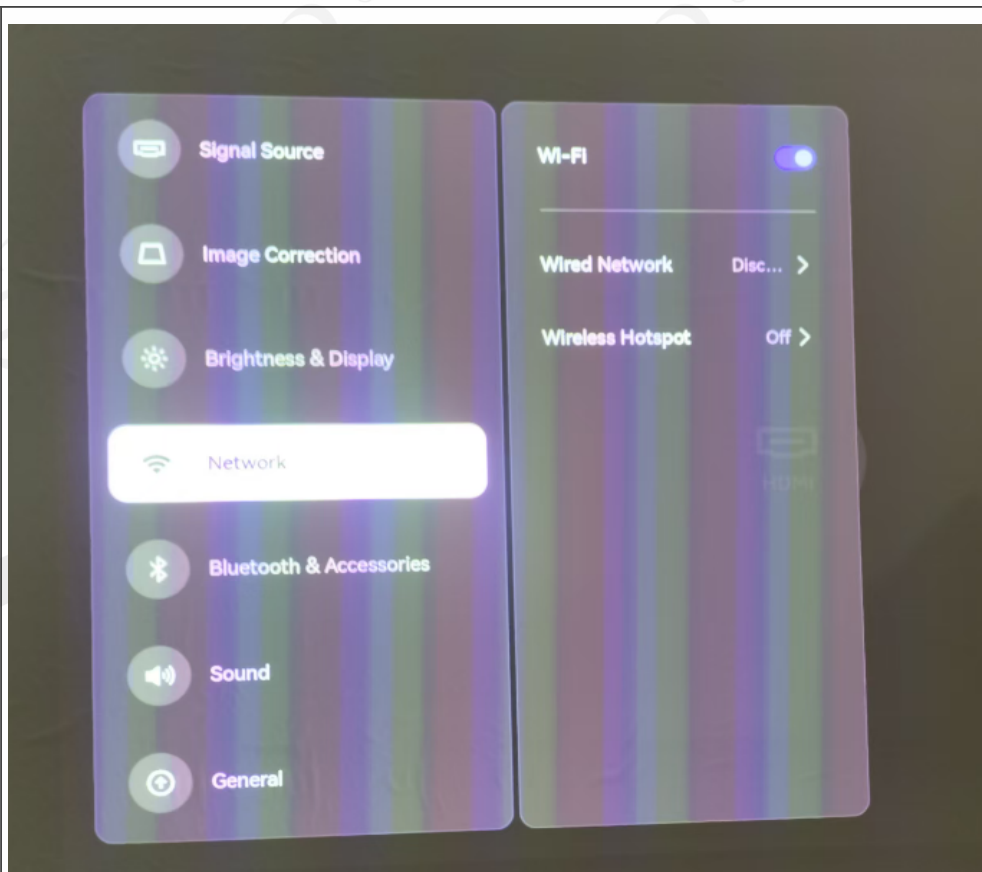
Identifier [GEC-2]-03	IF-03: LAN		
Decision node	Decision [E.Info.DT.GEC-2]		Justification [E.Just.DT.GEC-2]
[DT.GEC-2.DN-3]	Yes (√)	No	[E.Info.GEC-2.NetworkInterface.Exposure]: The TLS 1.3 protocol is used for connecting the DUT to the server, with business instructions transmitted via this secure channel to perform business operations.
Assignment of verdict:	Pass		

Identifier [GEC-2]-04	/		
Decision node	Decision [E.Info.DT.GEC-2]		Justification [E.Just.DT.GEC-2]
[DT.GEC-2.DN-2]	Yes (√)	No	[E.Info.GEC-2.NetworkInterface.Exposure]: 1. Open TCP service ports: 8080 Descriptions of the functions of each port: Port 8080 is the port for the setting to receive resources from the mobile terminal.
Assignment of	N/A		

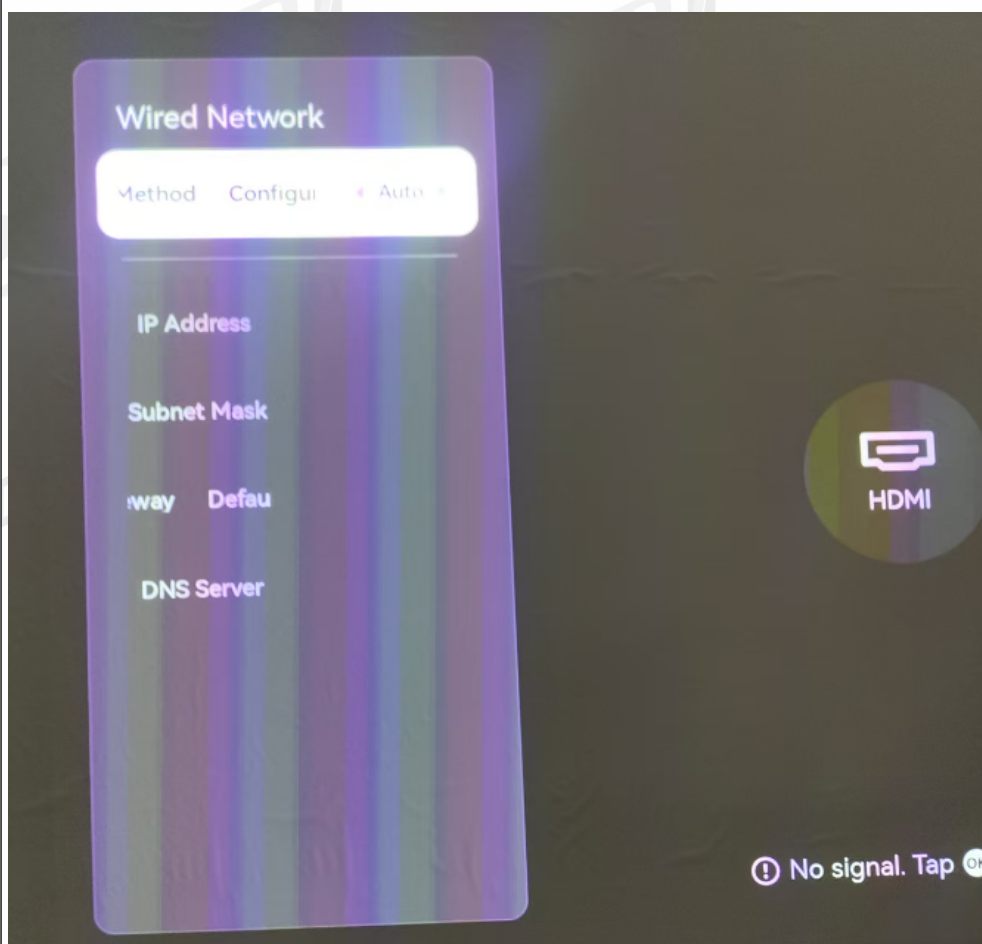
verdict:	
----------	--

--Completeness testing--

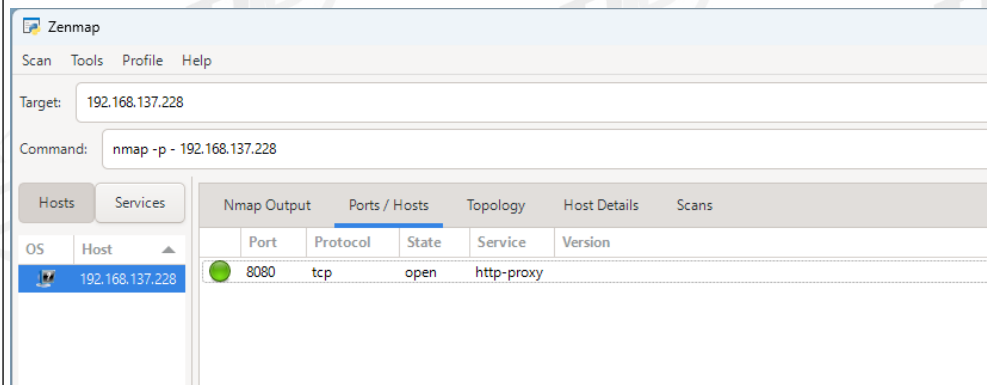
Assessment purpose:	The purpose of this assessment case is the functional assessment whether in the factory default state only network interfaces or exposed services (via network interfaces) which are required for setup or for the basic operation of the equipment are exposed.
Preconditions:	The equipment is in the factory default state and if available setup or another configuration did not take place until now. Physical network connections to check the exposure of services (via network interfaces) are established.
Operation steps:	Functionally assess whether, in the factory default state, there are other network interfaces or services (via network interfaces) exposed that are not listed in [E.Info.GEC-2.NetworkInterface.Exposure], or that are not required when setting up according to [E.Info.GEC-2.Setup] or when operating the device during basic operations.
Result:	Bluetooth Connection Function  Wi-Fi Connection Function



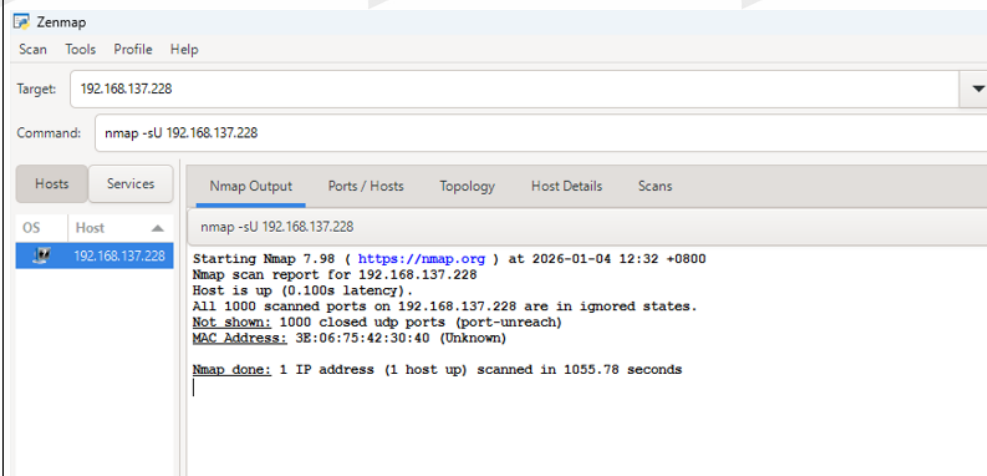
LAN Connection Function



TCP Port Scan



UDP Port Scan

Assignment of
verdict:

Pass

--Sufficiency testing--

N/A

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

--Conceptual assessment--

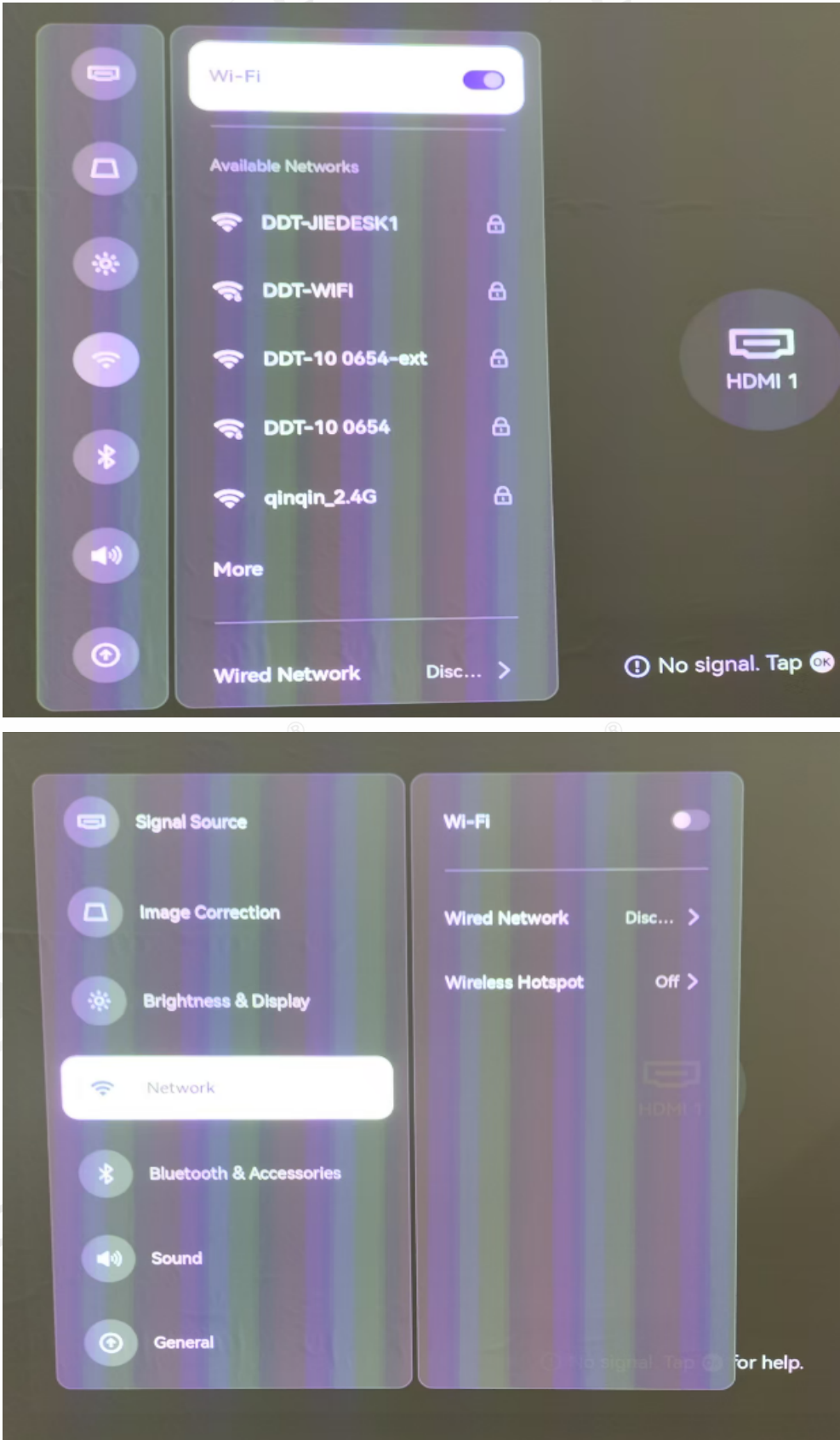
Identifier [GEC-3]-01	IF-01: Wi-Fi		
Decision node	Decision [E.Info.DT.GEC-3]		Justification [E.Just.DT.GEC-3]
[DT.GEC-3.DN-2]	Yes (✓)	No	[E.Info.GEC-3.NetworkInterface.Exposure]: The Wi-Fi function of the device is enabled by default at the factory, and users can disable this network interface on the DUT.
Assignment of verdict:	Pass		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether all optional network interfaces and exposed optional services (via network interfaces) which are part of the factory default state are configurable, at least with the option to enable and disable the service. Therefore, the completeness of documentation needs to be examined.
Preconditions:	The equipment is in an operational state and if available the setup is done. The necessary privileges are available for the configuration of the settings of the optional network interfaces or optional services (exposed via network interfaces).
Operation steps:	Functionally assess whether there are optional network interfaces or exposed optional services (via network interfaces), which are not listed in [E.Info.GEC-3.NetworkInterface.Exposure].
Result:	There are no optional network interfaces or exposed optional services (via network interfaces) that are not listed in [E.Info.GEC-3.NetworkInterface.Exposure].
Assignment of verdict:	Pass

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether all optional network interfaces and optional services (via network interfaces) exposed which are part of the factory default state are configurable, at least with the option to enable and disable the service.
Preconditions:	The equipment is in an operational state and if available the setup is done. The necessary privileges are available for the configuration of the settings of the optional network interfaces or optional services (via network interfaces).
Operation steps:	For each optional network interface and optional service (via network interface) exposed that is part of the factory default state: — Functionally assess whether the optional network interfaces and exposed optional services (via network interfaces) which are part of the factory default state and documented in [E.Info.GEC-3.NetworkInterface.Exposure] are configurable; and — functionally assess if it is possible to at least change the status of the optional network interfaces and exposed optional services (via network interfaces) to enabled and disabled; and — functionally assess whether the configuration of the settings of the optional network interfaces and exposed optional services (via network interfaces) which are part of the factory default state and listed in [E.Info.GEC-3.NetworkInterface.Exposure] is only possible by authorized users.
Result:	Enabling and Disabling Wi-Fi Service



Assignment of verdict:
Pass

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

--Conceptual assessment--

Identifier [GEC-4]-01	/		
Decision node	Decision [E.Info.DT.GEC-4]	Justification [E.Just.DT.GEC-4]	
/	/	/	/
Assignment of verdict:	N/A According to regulations EN18031-1, EN18031-2, and EN18031-3 Annex-ZA, GEC-4 is not classified as a mandatory test item under RED 3.3 (d), (e), (f), and is therefore determined as N/A.		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the user documentation describes every network interface and exposed service (via network interfaces) which are delivered as part of the factory default state.						
Preconditions:	The equipment is in a factory default state. Network connections to check the exposure of network interfaces and services (via network interfaces) are established.						
Operation steps:	/						
Result:	Annex ZA (informative) Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered This European Standard has been prepared under a Commission’s standardization request C(2022) 5637 and its amendment C(2023) 5624 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3). In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail. Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations. Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153] <table><tr><th>Essential Requirements of Directive 2014/53/EU</th><th>Clause(s)/sub-clause(s) of this EN</th><th>Remarks/Notes</th></tr><tr><td>3.3.(d)</td><td>Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11</td><td></td></tr></table> WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union. WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.	Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes	3.3.(d)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11	
Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes					
3.3.(d)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11						
Assignment of verdict:	N/A According to regulations EN18031-1, EN18031-2, and EN18031-3 Annex-ZA, GEC-4 is not classified as a mandatory test item under RED 3.3 (d), (e), (f), and is therefore determined as N/A.						

--Sufficiency testing--

None.

3.10.5 [GEC-5] No unnecessary external interfaces

--Conceptual assessment--

Identifier [GEC-5]-01	[E.Info.GEC-5.PhysicalExternalInterface]: Power Button / Status LED		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Used to turn the device on or off, and simultaneously indicate the device's operating status (such as power-on, standby, etc.). [E.Info.SCM-1.PhysicalExternalInterface.Type]: Mechanical button + LED status indicator light. [E.Info.GEC-5.IntFunc]: Used to turn the device on or off, and simultaneously indicate the device's operating status (such as power-on, standby, etc.).
Assignment of verdict:	Pass		

Identifier [GEC-5]-02	[E.Info.GEC-5.PhysicalExternalInterface]: Power Port		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Connect to an external power adapter to supply stable power to the device. [E.Info.SCM-1.PhysicalExternalInterface.Type]: Dedicated DC power input port (DC-IN). [E.Info.GEC-5.IntFunc]: Connect to an external power adapter to supply stable power to the device.
Assignment of verdict:	Pass		

Identifier [GEC-5]-03	[E.Info.GEC-5.PhysicalExternalInterface]: Set Button		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Used for functional configuration of the device. [E.Info.SCM-1.PhysicalExternalInterface.Type]: Mechanical button. [E.Info.GEC-5.IntFunc]:

		Used for functional configuration of the device.
Assignment of verdict:	Pass	

Identifier [GEC-5]-04	[E.Info.GEC-5.PhysicalExternalInterface]: USB Port		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Provides ultra-high-speed data transfer, peripheral connection, and device charging functionality (e.g., supports USB-PD). It can be used to connect docking stations, storage devices, high-bandwidth peripherals, etc. [E.Info.SCM-1.PhysicalExternalInterface.Type]: USB2.0, USB3.0 interface [E.Info.GEC-5.IntFunc]: Provides ultra-high-speed data transfer, peripheral connection, and device charging functionality (e.g., supports USB-PD). It can be used to connect docking stations, storage devices, high-bandwidth peripherals, etc.
Assignment of verdict:	Pass		

Identifier [GEC-5]-05	[E.Info.GEC-5.PhysicalExternalInterface]: HDMI Port		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Provides connection to external displays, outputting high-quality video and audio signals. [E.Info.SCM-1.PhysicalExternalInterface.Type]: HDMI 1, HDMI 2 interface [E.Info.GEC-5.IntFunc]: Provides connection to external displays, outputting high-quality video and audio signals.
Assignment of verdict:	Pass		

Identifier [GEC-5]-06	[E.Info.GEC-5.PhysicalExternalInterface]: RS232 Port		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Supports point-to-point serial data transmission, device configuration and debugging, as well as short-distance communication between peripheral devices. It can be used to connect serial port debugging tools, industrial

			control equipment, data acquisition terminals, etc. [E.Info.SCM-1.PhysicalExternalInterface.Type]: RS232 interface [E.Info.GEC-5.IntFunc]: Supports point-to-point serial data transmission, device configuration and debugging, as well as short-distance communication between peripheral devices. It can be used to connect serial port debugging tools, industrial control equipment, data acquisition terminals, etc.
Assignment of verdict:	Pass		

Identifier [GEC-5]-07	[E.Info.GEC-5.PhysicalExternalInterface]: AUDIO		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Supports analog audio input/output for connecting headphones, speakers, microphones and other audio peripherals. [E.Info.SCM-1.PhysicalExternalInterface.Type]: 3.5mm interface [E.Info.GEC-5.IntFunc]: Supports analog audio input/output for connecting headphones, speakers, microphones and other audio peripherals.
Assignment of verdict:	Pass		

Identifier [GEC-5]-08	[E.Info.GEC-5.PhysicalExternalInterface]: REMOTE		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Supports remote control signal transmission and reception for device operation control via remote controllers or external control systems. [E.Info.SCM-1.PhysicalExternalInterface.Type]: 3.5mm interface [E.Info.GEC-5.IntFunc]: Supports remote control signal transmission and reception for device operation control via remote controllers or external control systems.
Assignment of verdict:	Pass		

Identifier [GEC-5]-09	[E.Info.GEC-5.PhysicalExternalInterface]: SERVICE		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]:

	(√)		Reserved for device maintenance, debugging and firmware upgrading, and only used by professional technicians. [E.Info.SCM-1.PhysicalExternalInterface.Type]: Type-C interface [E.Info.GEC-5.IntFunc]: Reserved for device maintenance, debugging and firmware upgrading, and only used by professional technicians.
Assignment of verdict:	Pass		

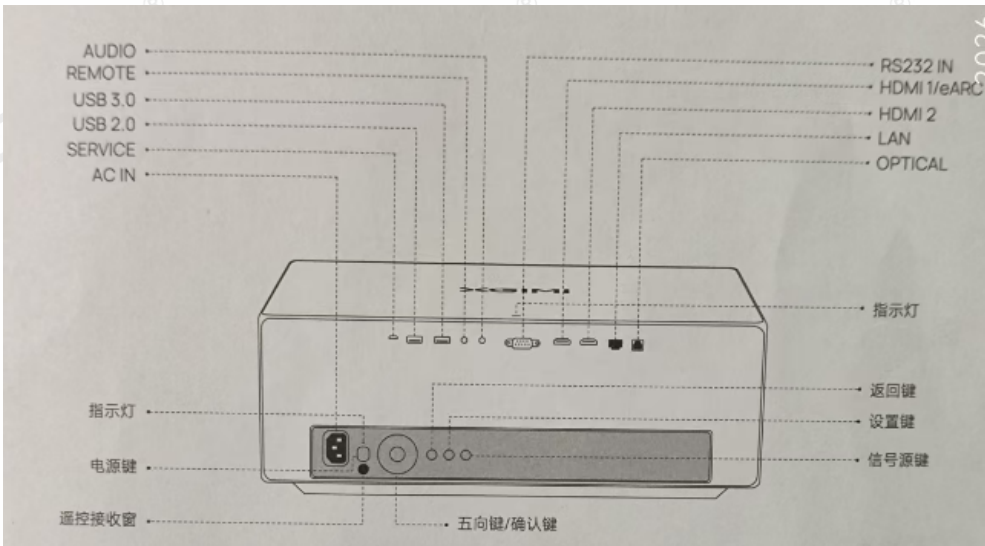
Identifier [GEC-5]-10	[E.Info.GEC-5.PhysicalExternalInterface]: OPTICAL		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Supports lossless digital audio signal output for connecting amplifiers, soundbars and other audio devices. [E.Info.SCM-1.PhysicalExternalInterface.Type]: Type-C interface [E.Info.GEC-5.IntFunc]: Supports lossless digital audio signal output for connecting amplifiers, soundbars and other audio devices.
Assignment of verdict:	Pass		

Identifier [GEC-5]-11	[E.Info.GEC-5.PhysicalExternalInterface]: Remote Control Receiver Window		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Used for receiving remote control signals. [E.Info.SCM-1.PhysicalExternalInterface.Type]: Windows [E.Info.GEC-5.IntFunc]: Used for receiving remote control signals.
Assignment of verdict:	Pass		

Identifier [GEC-5]-12	[E.Info.GEC-5.PhysicalExternalInterface]: LAN		
Decision node	Decision [E.Info.DT.GEC-5]		Justification [E.Just.DT.GEC-5]
[DT.GEC-5.DN-1]	Yes (√)	No	[E.Info.GEC-5.PhysicalExternalInterface.Purpose]: Supports wired local area network high-speed data transmission, device network parameter configuration and remote maintenance management, as well as stable data interaction between the device and various

		networked terminal devices. It can be used to connect network switches, routers, networked control hosts, remote debugging terminals and other network equipment. [E.Info.SCM-1.PhysicalExternalInterface.Type]: RJ45 interface [E.Info.GEC-5.IntFunc]: Supports wired local area network high-speed data transmission, device network parameter configuration and remote maintenance management, as well as stable data interaction between the device and various networked terminal devices. It can be used to connect network switches, routers, networked control hosts, remote debugging terminals and other network equipment.
Assignment of verdict:	Pass	

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether only physical external interfaces are exposed, which are required for the intended functionality as documented in [E.Info.GEC-5.PhysicalExternalInterface].
Preconditions:	The equipment is in an operational state.
Operation steps:	Attempt to reveal any via the equipment exposed physical external interfaces even if the related function is not enabled or documented in [E.Info.GEC-5.PhysicalExternalInterface]: — Examine equipment documentation such as design documentation, use case documentation and user manual; and — examine which physical external interfaces are present on the equipment such as microphones, screens, buttons or slots for extension cards. For each revealed physical external interface during the examination of documentation and also the examination of the equipment assess the documentation in [E.Info.GEC-5.PhysicalExternalInterface].
Result:	All identified physical external interfaces are recorded in [E.Info.GEC-5.PhysicalExternalInterface]. 

串口配置			
•波特率: 115200			
功能	内容	命令	
信号源切换 指定主机信号源	切换到HDMI1	2A 2A 02 01 01 04	
	切换到HDMI2	2A 2A 02 01 02 05	
信息显示	显示机器当前相关信息	2A 2A 02 02 00 04	
	标准模式	2A 2A 02 03 01 06	
图像模式切换	用户自定义模式	2A 2A 02 03 03 08	
	性能模式	2A 2A 02 03 05 0A	
	影院模式	2A 2A 02 03 07 0C	
	DICOM	2A 2A 02 03 24 29	
	明亮模式	2A 2A 02 03 25 2A	
	亮度1	2A 2A 02 05 01 08	
亮度设置 设置亮度等级1-10	亮度2	2A 2A 02 05 02 09	
	亮度3	2A 2A 02 05 03 0A	
	亮度4	2A 2A 02 05 04 0B	
	亮度5	2A 2A 02 05 05 0C	
	亮度6	2A 2A 02 05 06 0D	
	亮度7	2A 2A 02 05 07 0E	
	亮度8	2A 2A 02 05 08 0F	
	亮度9	2A 2A 02 05 09 10	
	亮度10	2A 2A 02 05 0A 11	
	恢复出厂设置	2A 2A 02 06 00 08	
模拟按键	关机	2A 2A 02 07 00 09	
	开机	2A 2A 07 09 77 61 68 65 75 70 9D	
	投屏	2A 2A 02 07 01 0A	
	工程测试	2A 2A 02 07 06 0F	
	镜头设置	2A 2A 02 07 07 10	
	信号源/自定义	2A 2A 02 07 08 11	
	方向上	2A 2A 02 07 09 12	
	方向下	2A 2A 02 07 0A 13	
	方向右	2A 2A 02 07 0B 14	
	方向左	2A 2A 02 07 0C 15	
	确认	2A 2A 02 07 0D 16	
	返回	2A 2A 02 07 0E 17	
	设置	2A 2A 02 07 0F 18	
	主页	2A 2A 02 07 10 19	
	音量加	2A 2A 02 07 11 1A	
	音量减	2A 2A 02 07 12 1B	

RS232端子
线序如下

RS232 输入端

DB9(母头)外视图

(5) (1)

(9) (6)

插针号码	信号名称	控制内容
(1)	-	NC
(2)	TXD	发送数据
(3)	RXD	接收数据
(4)	-	NC
(5)	GND	地
(6)	-	NC
(7)	-	NC
(8)	-	NC
(9)	-	NC

Inspect the device's appearance.



Assignment of verdict: Pass

--Sufficiency testing--

N/A

3.10.6 [GEC-6] Input validation

--Conceptual assessment--

Identifier [GEC-6]-01	[E.Info.GEC-6.ExternalInterface]: RS232 Port		
Decision node	Decision [E.Info.DT.GEC-6]		Justification [E.Just.DT.GEC-6]
[DT.GEC-6.DN-2]	Yes (✓)	No	[E.Info.GEC - 6.ExternalInterface.Validation]: Data received through the RS232 port is validated by ensuring successful serial link establishment, baud rate and parameter handshakes, and verification of frame format correctness based on RS232 communication frame descriptors. The system processes only data that conforms to required serial frame structural and protocol specifications, ensuring data integrity and semantic validity before further handling. [E.Info.GEC - 6.ExternalInterface.Capabilities]: The RS232 port operates using the standard RS232 serial communication protocol and supports point-to-point data interaction with external serial peripherals through standard serial communication APIs. It accepts serial data frames in compliance with RS232 electrical and framing specifications, following the universal asynchronous serial communication (UART) standards for data transmission and reception.
Assignment of verdict:	Pass		

Identifier [GEC-6]-02	[E.Info.GEC-6.ExternalInterface]: USB Port		
Decision node	Decision [E.Info.DT.GEC-6]		Justification [E.Just.DT.GEC-6]
[DT.GEC-6.DN-2]	Yes (✓)	No	[E.Info.GEC - 6.ExternalInterface.Validation]: Validates the legitimacy of USB devices and checks the integrity of input data and the consistency of the file system. [E.Info.GEC - 6.ExternalInterface.Capabilities]: Supports standard USB protocols, accepts input of files, audio and data streams, and is compatible with a variety of data types and file formats (e.g., the FAT32 file system).
Assignment of verdict:	Pass		

Identifier [GEC-6]-03	[E.Info.GEC-6.ExternalInterface]: Bluetooth BR/EDR/LE 5.2		
Decision node	Decision [E.Info.DT.GEC-6]		Justification [E.Just.DT.GEC-6]
[DT.GEC-6.DN-2]	Yes (✓)	No	[E.Info.GEC - 6.ExternalInterface.Validation]: Validates the legitimacy of Bluetooth pairing requests and verifies the correctness of data packet formats and commands. [E.Info.GEC - 6.ExternalInterface.Capabilities]: Supports Bluetooth protocols (e.g., A2DP, AVRCP, HFP), with input data types including audio data and control commands.
Assignment of	Pass		

verdict:			
Identifier [GEC-6]-04	[E.Info.GEC-6.ExternalInterface]: Wi-Fi		
Decision node	Decision [E.Info.DT.GEC-6]		Justification [E.Just.DT.GEC-6]
[DT.GEC-6.DN-2]	Yes (√)	No	[E.Info.GEC-6.ExternalInterface.Validation]: Wi-Fi is a wireless local area network protocol that focuses on "wireless data transmission interactions between devices (clients and access points)". The protocol itself provides built-in security mechanisms like WPA2/WPA3 for transmission encryption and identity authentication, but data content verification and illegal input filtering need to be implemented by upper-layer protocols (such as HTTPS, TCP) or applications on their own. [E.Info.GEC-6.ExternalInterface.Capabilities]: Wi-Fi is a wireless local area network protocol that focuses on "wireless data transmission interactions between devices (clients and access points)". It provides security capabilities through mechanisms like WPA2/WPA3 for transmission encryption and identity authentication. For data content verification and illegal input filtering, it relies entirely on upper-layer protocols (such as HTTPS, TCP) or applications, with no additional extensions within the Wi-Fi protocol itself.
Assignment of verdict:	Pass		

Identifier [GEC-6]-05	[E.Info.GEC-6.ExternalInterface]: Ethernet		
Decision node	Decision [E.Info.DT.GEC-6]		Justification [E.Just.DT.GEC-6]
[DT.GEC-6.DN-2]	Yes (√)	No	[E.Info.GEC-6.ExternalInterface.Validation]: Ethernet frames shall comply with the IEEE 802.3 standard and contain valid destination/source MAC addresses, length and checksum fields. IPv4/IPv6 packets shall include valid header fields (e.g., version, checksum, TTL). The port numbers in TCP/UDP datagrams shall fall within the range of 0 to 65535. [E.Info.GEC-6.ExternalInterface.Capabilities]: Supports Cat5/Cat6 network cables, adopts protocols including Ethernet, IP, TCP/UDP and HTTP, and transmits data such as MAC addresses, IP packets and TCP datagrams.
Assignment of verdict:	Pass		

Identifier [GEC-6]-06	[E.Info.GEC-6.ExternalInterface]: HDMI		
Decision node	Decision [E.Info.DT.GEC-6]		Justification [E.Just.DT.GEC-6]

[DT.GEC-6.DN-2]	Yes (✓)	No	[E.Info.GEC-6.ExternalInterface.Validation]: Checks the correctness of audio stream formats and prevents system exceptions caused by format errors. [E.Info.GEC-6.ExternalInterface.Capabilities]: Supports standard HDMI protocols, primarily accepts audio data input, and adopts specific data stream formats (e.g., PCM, Dolby).
Assignment of verdict:	Pass		

Identifier [GEC-6]-07	[E.Info.GEC-6.ExternalInterface]: AUDIO		
Decision node	Decision [E.Info.DT.GEC-6]	Justification [E.Just.DT.GEC-6]	
[DT.GEC-6.DN-2]	Yes (✓)	No	[E.Info.GEC-6.ExternalInterface.Validation]: Verifies that the physical electrical characteristics (impedance, level) are within the normal range. [E.Info.GEC-6.ExternalInterface.Capabilities]: Receives analog audio signals with no complex data protocols.
Assignment of verdict:	Pass		

Identifier [GEC-6]-08	[E.Info.GEC-6.ExternalInterface]: Power Port		
Decision node	Decision [E.Info.DT.GEC-6]	Justification [E.Just.DT.GEC-6]	
[DT.GEC-6.DN-2]	Yes (✓)	No	[E.Info.GEC-6.ExternalInterface.Validation]: Checks whether the voltage and current are within the safe range to prevent device damage caused by abnormal input. [E.Info.GEC-6.ExternalInterface.Capabilities]: Receives power input, with the protocol standard generally complying with fixed voltage/current specifications and no complex data transmission involved.
Assignment of verdict:	Pass		

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment of the external interfaces of the equipment and the related input mechanisms regarding the completeness of the documentation.
Preconditions:	The equipment is in an operational state and all external interfaces, which are part of the intended functionality, are either enabled or configurable to be enabled, so that each external interface can be tested. Where authentication is necessary to access an external interface, a means is provided to be able to test the interface.
Operation steps:	Functionally assess whether there are input methods that are not documented in [E.Info.GEC-6.ExternalInterface] by:

	— functionally assessing traffic of network interfaces to reveal input methods, e.g. via network analysing tools; use the information in [E.Info.GEC-6.ExternalInterface] as a guidance; and — functionally assessing equipment to reveal input methods of external interfaces which are no network interfaces via visual inspection, user manual and design-documentation; and — following the description in [E.Info.GEC-6.ExternalInterface.Capabilities] to trigger the related input methods, e.g. via generating the described messages (e.g., via a web interface or generic message generating tools, or fuzzing tools).
Result:	All identified external interfaces are recorded in [E.Info.GEC-6.ExternalInterface].
Assignment of verdict:	Pass

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment of the techniques to verify the implementation of the documented techniques.
Preconditions:	The equipment is in an operational state and all external interfaces, which are part of the intended functionality, are either enabled or configurable to be enabled, so that each external interface can be tested. Where authentication is necessary to access an external interface, a means is provided to be able to test the interface.
Operation steps:	Functionally assess whether each external interface is resilient against common input attacks considering their functionality and the intended functionality of the equipment by: — following the description in [E.Info.GEC-6.ExternalInterface] as guidance to test the related input methods e.g., via generating malformed or invalid messages (e.g., via a web interface or generic message generating tools, or fuzzing tools): Attempt to corrupt, extract or misuse the security assets described in [E.Info.GEC-6.SecurityAsset] and network assets described in [E.Info.GEC-6.NetworkAsset] by executing specific attacks related to the input mechanisms like SQL injection, Ajax injection, OS command injection or path traversal as well; and — functionally assessing if the behaviour or output described in [E.Info.GEC-6.ExternalInterface] is generated as documented, use equipment manual or design documentation as guidance.
Result:	The device does not support ADB access.  <pre> Microsoft Windows [版本 10.0.26100.7462] (c) Microsoft Corporation。保留所有权利。 C:\Users\ddt>adb devices * daemon not running; starting now at tcp:5037 * daemon started successfully List of devices attached C:\Users\ddt>adb shell adb.exe: no devices/emulators found C:\Users\ddt> </pre> SQL injection

	<table><tr><th>序号</th><th>任务名称</th><th>网站</th><th>站点信息</th><th>高风险</th><th>中风险</th><th>低风险</th><th>信息风险</th><th>开始时间</th><th>结束时间</th></tr><tr><td>1</td><td>投影机 (SQL注入) -20260127</td><td>http://192.168.16.73:8080</td><td></td><td>0</td><td>0</td><td>0</td><td>0</td><td>2026-01-27 17:40:44</td><td>2026-01-27 17:41:51</td></tr><tr><td colspan="10">任务参数</td></tr><tr><td>任务类型</td><td colspan="3">SQL注入</td><td colspan="2">探测次数</td><td colspan="4">103</td></tr><tr><td>扫描速度</td><td colspan="3">缓慢</td><td colspan="2">已扫描链接数</td><td colspan="4">10</td></tr><tr><td>耗时</td><td colspan="3">1分7秒</td><td colspan="2">引擎版本</td><td colspan="4">2.0.335.01261541</td></tr></table>	序号	任务名称	网站	站点信息	高风险	中风险	低风险	信息风险	开始时间	结束时间	1	投影机 (SQL注入) -20260127	http://192.168.16.73:8080		0	0	0	0	2026-01-27 17:40:44	2026-01-27 17:41:51	任务参数										任务类型	SQL注入			探测次数		103				扫描速度	缓慢			已扫描链接数		10				耗时	1分7秒			引擎版本		2.0.335.01261541			
序号	任务名称	网站	站点信息	高风险	中风险	低风险	信息风险	开始时间	结束时间																																																				
1	投影机 (SQL注入) -20260127	http://192.168.16.73:8080		0	0	0	0	2026-01-27 17:40:44	2026-01-27 17:41:51																																																				
任务参数																																																													
任务类型	SQL注入			探测次数		103																																																							
扫描速度	缓慢			已扫描链接数		10																																																							
耗时	1分7秒			引擎版本		2.0.335.01261541																																																							
Assignment of verdict:	Pass																																																												

3.11 [CRY] Cryptography

3.11.1 [CRY-1] Best practice cryptography

--Conceptual assessment--

Identifier [CRY-1]-01	[E.Info.CRY-1.Assets]: 1. Communication Encryption Algorithm: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA 2. Bluetooth Encryption Algorithm: AES-CCM-128 3. The firmware package is digitally signed using a certificate-based SHA-256 with RSA2048 algorithm.		
Decision node	Decision [E.Info.DT.CRY-1]		Justification [E.Just.DT.CRY-1]
[DT.CRY-1.DN-1]	Yes (√)	No	[E.Info.CRY-1.Assets.Cryptography]: We can check the best practices for cipher suites through this website: https://ciphersuite.info/ The supported TLS cipher suites include: TLS 1.3: TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256

		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 All the above cipher suites use ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) key exchange and provide forward secrecy. Even if the long-term private key is compromised, previously captured communication data cannot be decrypted. These cipher suites comply with modern TLS security standards and are currently recommended encryption configurations for secure communications. Bluetooth Encryption Algorithm: Bluetooth 4.2 and above mandate the use of AES-128-based encryption, which aligns with Bluetooth SIG-defined security requirements and current industry best practices. [E.Info.CRY-1.Assets.Deviation]: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA Firmware Package Encryption Algorithm: RSA-2048, RSA-2048 is no longer considered a best practice in 2026. For the purpose of compatibility with communications of other products or services, the adopted encryption algorithm suite is not based on best practices (but rather prioritizes compatibility).
Assignment of verdict:	N/A	

--Completeness testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the documentation in [E.Info.CRY-1.Assets.Cryptography] is complete.
Preconditions:	The equipment is in an operational state.
Operation steps:	/
Result:	/
Assignment of verdict:	N/A

--Sufficiency testing--

Assessment purpose:	The purpose of this assessment case is the functional assessment whether the cryptography documentation in [E.Info.CRY-1.Assets.Cryptography] is implemented as it is documented.
Preconditions:	The equipment is in an operational state.
Operation steps:	/
Result:	Communication Encryption Algorithm: TLS_AES_128_GCM_SHA256 Recommended TLS_AES_128_GCM_SHA256 TLS_AES_256_GCM_SHA384 Recommended TLS_AES_256_GCM_SHA384 TLS_CHACHA20_POLY1305_SHA256 Recommended TLS_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 Recommended TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 Recommended TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 Recommended TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 Secure TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 Secure TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 Secure TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA Weak TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA Weak TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_GCM_SHA256

Weak TLS_RSA_WITH_AES_128_GCM_SHA256

TLS_RSA_WITH_AES_256_GCM_SHA384

Weak TLS_RSA_WITH_AES_256_GCM_SHA384

TLS_RSA_WITH_AES_128_CBC_SHA

Weak TLS_RSA_WITH_AES_128_CBC_SHA

TLS_RSA_WITH_AES_256_CBC_SHA

Weak TLS_RSA_WITH_AES_256_CBC_SHA

Bluetooth Encryption Algorithm:

Bluetooth 4.2 and above mandate the use of AES-128-based encryption, which aligns with Bluetooth SIG-defined security requirements and current industry best practices.

Agreed Block Ciphers.

Primitive	Parameters' sizes	R/L	Notes
AES FIPS197 ISO18033-3	k = 128 bits	R	
	k = 192 bits	R	
	k = 256 bits	R	

Firmware Package Encryption Algorithm: RSA-2048, RSA-2048 is no longer considered a best practice in 2026.

Agreed RSA primitive sizes.

Primitive	Parameters' sizes	R/L	Notes
RSA	$n \geq 3000, \log_2(e) > 16$	R	
	$n \geq 1900, \log_2(e) > 16$	L [2025]	27-LegacyRSA

Agreed FF-DLOG Parameters.

Family	Group	R/L	Notes
MODP RFC3526	3072-bit MODP Group	R	
	4096-bit MODP Group	R	
	6144-bit MODP Group	R	
	8192-bit MODP Group	R	
	2048-bit MODP Group	L[2025]	29-Precomputation, 30-LegacyFF-DLOG
FFDHE RFC7919	3072-bit FFDHE Group	R	
	4096-bit FFDHE Group	R	
	6144-bit FFDHE Group	R	
	8192-bit FFDHE Group	R	
	2048-bit FFDHE Group	L[2025]	29-Precomputation, 30-LegacyFF-DLOG

For all agreed subgroups, we have $r = q = (p - 1)/2$.

Assignment of verdict:

N/A

- - END OF TEST REPORT - -