DEKRA Testing and Certification (Shanghai) Ltd. Guangzhou Branch.
Building 5, No. 3 Qiyun Road, Huangpu District, Guangzhou,
Guangdong Province, 510663, P.R. China

Test report No:
NIE: 4944367RCS.001

Security Evaluation Report
DEKRA Evaluation framework

(*) Identification of item tested	Portable power bank
(*) Trademark	ECOFLOW OR EF ECOFLOW
(*) Model and /or type reference tested	Dc013
(*) Other identification of the product	Software version: v5.17.87.12 FreeRTOS v10.5.1 NanoPB v0.4.5 Expressif IDF v4.4.2 Hardware version: 2.0.2.52
Ratings	Charge Mode: ALT IN Port Input: 12/24V⎓ (11-31V⎓), 75A Max, BATTERY Port Output: 24V⎓ /40-60V⎓ , 20A Max, 1000W Max Battery Maintenance Mode: BATTERY Port Input: 40-60V⎓ , 3A Max, ALT IN Port Output: 13.8/27.6V⎓ , 100W Max Reverse Charge Mode: BATTERY Port Input: 40-60V⎓ , 20A Max, ALT IN Port Output: 13.8/27.6V⎓ , 75A Max
Manufacturer	EcoFlow Inc. RM 401, Plant #1, Runheng Industrial Zone, Fuyuanyi Road, Zhancheng Community, Fuhai Street, Bao'an District, Shenzhen City, Guangdong Province, P.R.China
Summary	IN COMPLIANCE
Test method requested	EN 18031-1:2024
Approved by (name / position & signature)	John He, Project manager 
Date of issue	2025/11/17
Report template No	FDT08_24 **(*) "Data provided by the client"**

Table of Contents

Competences and guarantees

DEKRA Testing and Certification guarantees the reliability of the data presented in this report, which is the result of the measurements and the tests performed to the item under test on the date and under the conditions stated on the report and, it is based on the knowledge and technical facilities available at DEKRA Testing and Certification at the time of performance of the test.

DEKRA Testing and Certification is liable to the client for the maintenance of the confidentiality of all information related to the item under test and the results of the test.

The results presented in this Test Report apply only to the particular item under test established in this document.

IMPORTANT: No parts of this report may be reproduced or quoted out of context, in any form or by any means, except in full, without the previous written permission of DEKRA Testing and Certification.

General conditions

1. This report is only referred to the item that has undergone the test.
2. This report does not constitute or imply on its own an approval of the product by the Certification Bodies or competent Authorities.
3. This document is only valid if complete; no partial reproduction can be made without previous written permission of DEKRA Testing and Certification.
4. This test report cannot be used partially or in full for publicity and/or promotional purposes without previous written permission of DEKRA Testing and Certification and the Accreditation Bodies.

Uncertainty

Uncertainty does not apply to this valuation according to the RED.

Data provided by the client

The following data has been provided by the client:

1. Information relating to the description of the sample ("Identification of the item tested", "Trademark", "Model and/or type reference tested", “Firmware version of the DUT”).
2. Cloud services of the DUT have been also provided by the client. However, tests have been done only on the DUT.

DEKRA Testing and Certification (Shanghai) Ltd. GuangZhou Branch declines any responsibility with respect to the information provided by the client and that may affect the validity of results.

Usage of samples

The following samples have been provided by the costumer to be evaluated:

Control Nº	Description	Model	Serial Nº	Date of

				reception
4944367/001	Portable Power Station	Dc013	/	2025/10/20

Test sample description

Sample Components…… :	Hardware		
	EFR705 WIFI module 2.0.1.35		
Documents as provided by the applicant..... :	Description	File name	Issue date
	Product Evaluation Document	Product RED DA security design document CN.docx	2025/09/08
	Development documentation	固件安全设计方案(1).pdf	2025/09/08
		关键安全参数生命周期流程管理文档.pdf	2025/09/08
		蓝牙加密相关细节说明.pdf	2025/09/08
		设备存储和传输功能说明(1).pdf	2025/09/08

Identification of the client

COMPANY	EcoFlow Inc.
ADDRESS	RM 401, Plant #1, Runheng Industrial Zone, Fuyuanyi Road, Zhancheng Community, Fuhai Street, Bao'an District, Shenzhen City, Guangdong Province, P.R.China

Testing period and place

Test Location	DEKRA Testing and Certification (Shanghai) Ltd. Guangzhou Branch
Date (Start)	2025/09/08
Date (finish)	2025/11/17

Document history

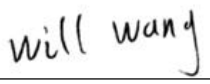
Report Number	Date	Description
4944367RCS.001	2025/11/17	Emitted Evaluation Report 001.

Environmental conditions

Environmental conditions do not apply to this valuation according to the RED.

Remarks and Comments

- Evaluation of the Portable power bank.
- The following table includes the name, position and signature of the person/s that participate in the evaluation (not including the reviewer).

Name	Position	Signature
Will Wang	Evaluator	

The following table shows the tools used in this evaluation:

Name	Type	Code	Version
Wireshark	Software		4.4.6
Nmap	Software		7.95
sslsplit	Software		0.5.5
tcpreplay	Software		4.5.1
GattTool	Software		5.0.0
Boofuzz	Software		0.4.2
Nmap	Software		7.94
binwalk	Software		2.3.4

Testing verdicts

PASS	P
FAIL	F
NA	NA
INCONCLUSIVE	INC

Summary

Access control Mechanism	**VERDICT**			
	P	F	NA	INC
ACM-1 Application of access control mechanisms	X			
ACM-2 Appropriate access controls mechanisms	X			

Authentication mechanism	VERDICT			
	P	F	NA	INC
AUM-1 Applicability of authentication mechanisms	X			
AUM-2 Appropriate authentication mechanisms	X			
AUM-3 Authenticator validation	X			
AUM-4 Changing authenticator	X			
AUM-5 Preventing static and default values	X			
AUM-6 Brute force protection	X			

Secure update mechanism	VERDICT			
	P	F	NA	INC
SUM-1 Application of update mechanism	X			
SUM-2 Secure updates	X			
SUM-3 Automated updates	X			

Secure storage mechanism	VERDICT			
	P	F	NA	INC
SSM-1 Application of secure storage mechanisms	X			
SSM-2 Appropriate integrity protection for secure storage mechanisms	X			
SSM-3 Appropriate confidentiality protection for secure storage mechanisms	X			

Secure communication mechanism	VERDICT			
	P	F	NA	INC
SCM-1 Application of secure communication mechanisms	X			
SCM-2 Appropriate integrity and authenticity protection for secure communication mechanisms	X			
SCM-3 Appropriate confidentiality protection for secure communication	X			

mechanisms				
SCM-4 Appropriate replay protection for secure communication mechanisms	X			

Resilience mechanism	VERDICT			
	P	F	NA	INC
RLM-1 Application of resilience mechanism	X			

Network monitoring mechanism	VERDICT			
	P	F	NA	INC
NMM-1 Application of network monitoring mechanisms			X	

Traffic control mechanism	VERDICT			
	P	F	NA	INC
TCM-1 Application of traffic control mechanism			X	

Confidential Security Parameters	VERDICT			
	P	F	NA	INC
CCK-1 Appropriate CCKs	X			
CCK-2 CCK generation mechanisms	X			
CCK-3 Preventing static default values for preinstalled CCKs			X	

General equipment capabilities	VERDICT			
	P	F	NA	INC
GEC-1 Up-to-date software and hardware with no publicly known exploitable vulnerabilities	X			
GEC-2 Limit exposure of services via related network interfaces	X			
GEC-3 Configuration of optional services and the related exposed network interfaces			X	
GEC-4 Documentation of exposed services via network interfaces.	X			
GEC-5 No unnecessary external interfaces	X			
GEC-6 Input validation	X			

Cryptography	VERDICT			
	P	F	NA	INC
CRY-1 Best practice Cryptography	X			

Appendix A: Evaluation Results

1. Categories, Security Features and Categories Summary

Security Evaluation of the DUT has been divided into different categories, Security Analysis of each category is structured in different security features. In the same way, each security feature can be composed of several tests.

The following table shows the security features defined per each category and the number of tests of each security feature.

Category	Security Features	Nº TESTS
1. Art. D	1.1 Access control Mechanism	2
	1.2 Authentication mechanism	6
	1.3 Secure update mechanism	3
	1.4 Secure storage mechanism	3
	1.5 Secure communication mechanism	4
	1.6 Resilience mechanism	1
	1.7 Network monitoring mechanism	1
	1.8 Traffic control mechanism	1
	1.9 Confidential Security Parameters	4
	1.10 General equipment capabilities	6
	1.11 Cryptography	2
2. Art. E	2.1 Access control Mechanism	6
	2.2 Authentication mechanism	5
	2.3 Secure update mechanism	3
	2.4 Secure storage mechanism	3
	2.5 Secure communication mechanism	4
	2.6 Logging mechanism	4
	2.7 Deletion mechanism	1
	2.8 User notification mechanism	2
	2.9 Confidential cryptographic keys	1
	2.10 General equipment capabilities	7
	2.11 Cryptography	1
3. Art. F	3.1 Access control Mechanism	2
	3.2 Authentication mechanism	6
	3.3 Secure update mechanism	3
	3.4 Secure storage mechanism	3
	3.5 Secure communication mechanism	4
	3.6 Logging mechanism	4
	3.7 Confidential cryptographic keys	4
	3.8 General equipment capabilities	6

	3.9 Cryptography	1

Appendix A.1: Radio Equipment Directive - Cybersecurity Requirements

Art. D Test Analysis

1. Applicable Evaluation Cases

Pentesting procedures for Radio Equipment Directive - Cybersecurity Requirements (Art. D,E & F) - August 2024 Evaluation Results cover 11 different evaluation areas with a total of 31 evaluation cases

For this particular evaluation and according with the technical criteria of the evaluator the following evaluation cases has been considered applicable to this specific DUT:

Evaluation Area	Identifier	Evaluation Case Title	Apply	Relevant results
Access control Mechanism Area	ACM-1	Application of access control mechanisms	Y	PASS
Access control Mechanism Area	ACM-2	Appropriate access controls mechanisms	Y	PASS
Authentication mechanism Area	AUM-1	Applicability of authentication mechanisms for external interfaces	Y	PASS
Authentication mechanism Area	AUM-2	Appropriate authentication mechanisms for external interfaces	Y	PASS
Authentication mechanism Area	AUM-3	Authenticator validation	Y	PASS
Authentication mechanism Area	AUM-4	Changing authenticators	Y	PASS
Authentication mechanism Area	AUM-5	Password strength	Y	PASS
Authentication mechanism Area	AUM-6	Brute force protection	Y	PASS
Secure update mechanism Area	SUM-1	Application of update mechanism	Y	PASS
Secure update mechanism Area	SUM-2	Secure updates	Y	PASS
Secure update mechanism Area	SUM-3	Automated updates	Y	PASS
Secure storage mechanism Area	SSM-1	Application of secure storage mechanisms	Y	PASS

Evaluation Area	Identifier	Evaluation Case Title	Apply	Relevant results
Secure storage mechanism Area	SSM-2	Appropriate integrity protection for secure storage mechanisms	Y	PASS
Secure storage mechanism Area	SSM-3	Appropriate confidentiality protection for secure storage mechanisms	Y	PASS
Secure communication mechanism Area	SCM-1	Application of secure communication mechanisms	Y	PASS
Secure communication mechanism Area	SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	Y	PASS
Secure communication mechanism Area	SCM-3	Appropriate confidentiality protection for secure communication mechanisms	Y	PASS
Secure communication mechanism Area	SCM-4	Appropriate replay protection for secure communication mechanisms	Y	PASS
Resilience mechanism Area	RLM-1	Appropriate integrity and authenticity protection for secure communication mechanisms	Y	PASS
Network monitoring mechanism area	NMM-1	Application of resilience mechanism	N	NA
Traffic control mechanism Area	TCM-1	Application of traffic control mechanism	N	NA
Confidential Security Parameters Area	CCK-1	Appropriate CCKs	Y	PASS
Confidential Security Parameters Area	CCK-2	CCK generation mechanisms	Y	PASS
Confidential Security Parameters Area	CCK-3	Preventing static default values for preinstalled CCKs	Y	PASS
General equipment capabilities Area	GEC-1	Up-to-date software and hardware with no publicly known exploitable vulnerabilities	Y	PASS

Evaluation Area	Identifier	Evaluation Case Title	Apply	Relevant results
General equipment capabilities Area	GEC-2	Limit exposure of services via related network interfaces	Y	PASS
General equipment capabilities Area	GEC-3	Configuration of optional services and the related exposed network interfaces	N	NA
General equipment capabilities Area	GEC-4	Documentation of exposed services via network interfaces.	Y	PASS
General equipment capabilities Area	GEC-5	No unnecessary external interfaces	Y	PASS
General equipment capabilities Area	GEC-6	Input validation	Y	PASS
Cryptography Area	CRY-1	Best practice Cryptography	Y	PASS

2. Results of Evaluation Procedure

The set of evaluation procedures have been split into 31 sub-categories or areas for a total of 76 evaluation cases.

Evaluation Areas:

1. Art. D

Following is detailed the results obtained for the 31 evaluation areas in each evaluation case:

3. Art. D

3.1 Access control mechanism

3.1.1 ACM-1: Applicability of access control mechanisms

Conceptional assessment results

Identifier	Asset-1 WI-FI SSID and Password Asset-2 Bluetooth Function Asset-3 Remote Control Function Asset-4 OTA Data		
Decision Node	Decision [E.Info.DT.ACM-1]		Justification [E.Just.DT.ACM-1]
DT.ACM-1.DN-1	Yes	No [x]	Equipment is not expected to be public assets.
DT.ACM-1.DN-2	Yes	No [x]	No physical or logical measures in the targeted operational environment can limit the accessibility to authorized entities.
DT.ACM-1.DN-3	Yes	No [x]	There are no applicable legal provisions required.
DT.ACM-1.DN-4	Yes [x]	No	These assets are protected by [ACM-1-APP], which implements the access control.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is PASS because at least one path in the decision tree **E.Info.DT.ACM-1** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional Completeness Assessment

After examining the equipment functions, all accessible assets are documented in [E.Info.ACM-1.NetworkAsset] and [E.Info.ACM-1.SecurityAsset].

The DUT establishes a connection with the mobile app via [Interface-1 Bluetooth] and transmits part of assets through [Interface-2 WLAN].

Functional sufficiency assessment

Regarding to the existence of the documented assets,

[Asset-1 Wi-Fi SSID and password], [Asset-3 Remote Control Function], [Asset-4 OTA data] and [Asset-2 Bluetooth function] are protected by [ACM-1-APP], which implements an access control mechanism.

Login to the app requires authentication via a password-based access control mechanism. Only entities that are successfully authenticated through this access control are authorized to issue control functions or perform OTA command operations.

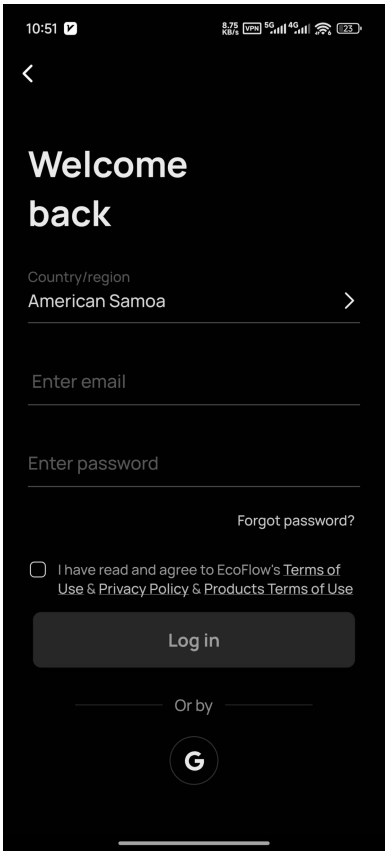


Figure 1: APP Login

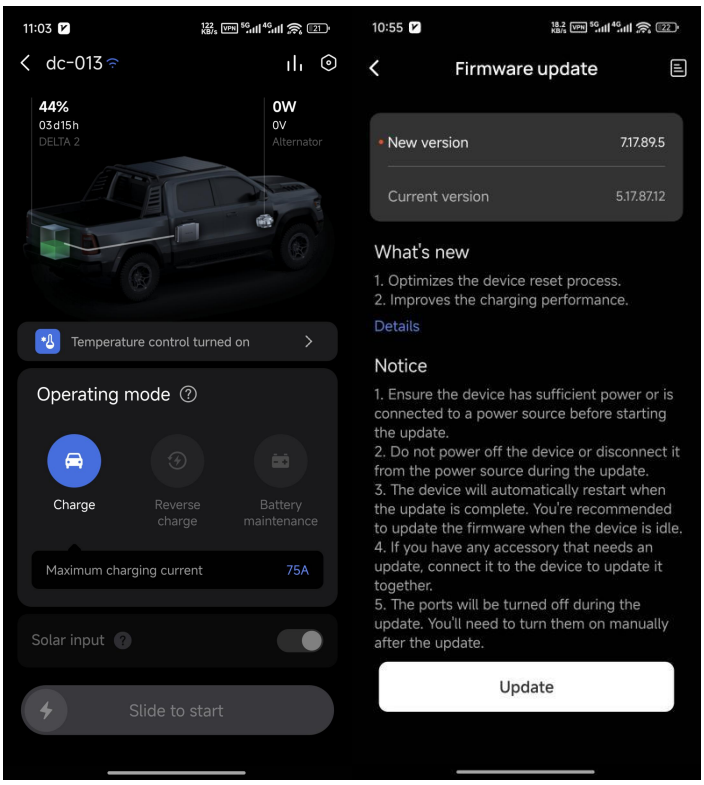


Figure 2: Assets protected by APP

The figure above shows that after connecting to the app, [Asset-2 Remote control function], [Asset-1 Wi-Fi SSID and Password], and [Asset-4 OTA data] can be accessed via [Interface-1 Bluetooth] or [Interface-2 WLAN].

Access to the security assets and network assets defined in [E.Info.ACM-1.SecurityAsset] and [E.Info.ACM-1.NetworkAsset] is restricted to end users by the access control mechanism specified in [ACM-1-APP].

Therefore, TL assigns **PASS** to this because the [ACM-1-APP] are implemented as documented for each security assets and network assets.

RESULT:	**PASS**

3.1.2 ACM-2: Appropriate access controls mechanisms

Conceptional assessment results

Identifier	ACM-1-APP		
Decision Node	Decision [E.Info.DT.ACM-2]		Justification [E.Just.DT.ACM-2]
DT.ACM-2.DN-1	Yes [x]	No	To log in the app, correct account and password are necessary to authorize users to access the security and network asset. The correct account and password can be seen as an authorization to make authorized entities to access security and network assets.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.ACM-1** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional sufficiency assessment

[ACM-1-APP] is categorized as RBAC. Only authorized users with the correct Password code could have access corresponding assets and functions.The wrong Password code will be rejected in the verification process.

The figure 3 shows that the TL's attempt at the password-based access control.

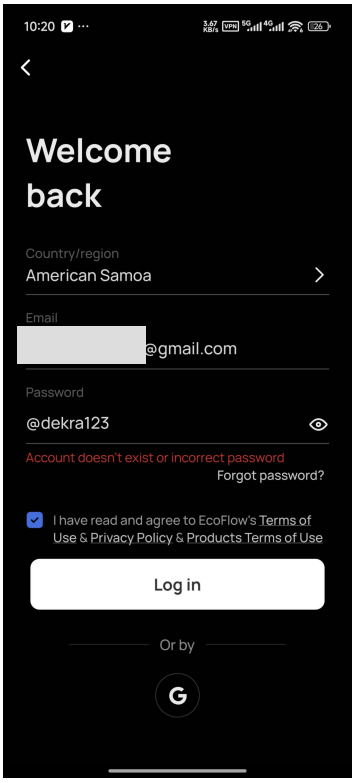


Figure 3: Password-based access control

TL attempted to login and test it, and the following was observed:

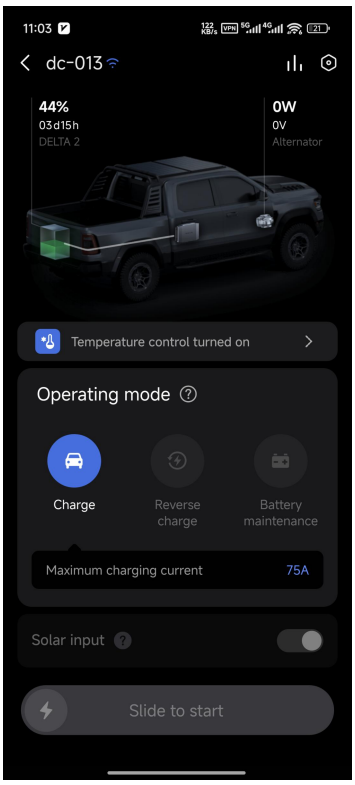


Figure 4: Basic function after logging in and pairing

The figure above shows TL's confirmation of the access control mechanism for the device's assets after unlocking the device. TL also confirmed that:

1. The roles assigned through [ACM-1-APP] will be granted the roles and permissions as the end users which can use most functions of devices.
2. The roles' permissions are associated with the principle of least privilege in this case.
3. The security and network assets can only be read,accessed or modified by users which entering correct Password code.
4. Roles cannot be changed by end users themselves.

The verdict is **PASS** because for each security asset documented in [E.Info.ACM-2.SecurityAsset] and each network asset documented in [E.Info.ACM-2.NetworkAsset], the confirmations in the implementation category dependent assessment unit have been successful.

RESULT:	PASS

3.2 Authentication mechanism

3.2.1 AUM-1: Applicability of authentication mechanisms

Conceptional assessment results

Identifier	ACM-1-APP	
Decision Node	Decision [E.Info.DT.AUM-1-2]	Justification [E.Just.DT.AUM-1-2]

DT.AUM-1-2.DN-1	Yes	No [x]	DUT cannot provide confidence in any physical or logical environment.
DT.AUM-1-2.DN-2	Yes	No [x]	DUT requires a Password code to read the network function or configuration.
DT.AUM-1-2.DN-3	Yes	No [x]	There is no law that restricts or prohibits the implementation of access mechanisms.
DT.AUM-1-2.DN-4	Yes [x]	No	Access is restricted through a password-based authentication mechanism.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is PASS because at least one path in the decision tree **E.Info.DT.AUM-1** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional Completeness Assessment

According to **E.Info.AUM** and **ACM-1**,

no other access control could be found to read confidential network function configuration or confidential security parameters or modify sensitive network function configuration or confidential security parameters or modify sensitive network function configuration or sensitive security parameters, use network functions or security functions that are not documented in the **E.Info.AUM**.

Functional sufficiency assessment

According to **E.Info.AUM**,

TL confirms that the [ACM-1-APP] implements a password-based authentication mechanism, with [AUM-1-APP] used to authenticate and manage access.

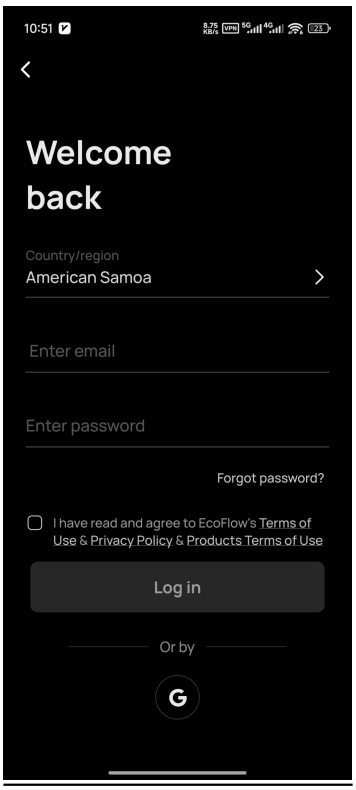


Figure 5: Password-based authentication mechanism

The verdict is **PASS** because there is no evidence of any authentication mechanism documented in [E.Info.AUM-1-2.ACM.AuthenticationMechanism] that is not implemented.

RESULT:	PASS

3.2.2 AUM-2: Appropriate authentication mechanisms

Conceptional assessment results

Identifier	AUM-1-APP		
Decision Node	Decision [E.Info.DT.AUM-2]		Justification [E.Just.DT.AUM-2]
DT.AUM-3.DN-1	Yes [x]	No	[AUM-1-APP] is required correct password to login the account, which use the "Knowledge" as the factor of the authentication.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is PASS because at least one path in the decision tree **E.Info.DT.AUM-2** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional sufficiency assessment

For [AUM-1-APP], only verified user can use functions of device. Device will reject all the suspicious requests.

The figure below shows the Password-based authentication mechanism. TL tried both the correct and incorrect PINs to test if this Password-based authentication mechanism is implemented.

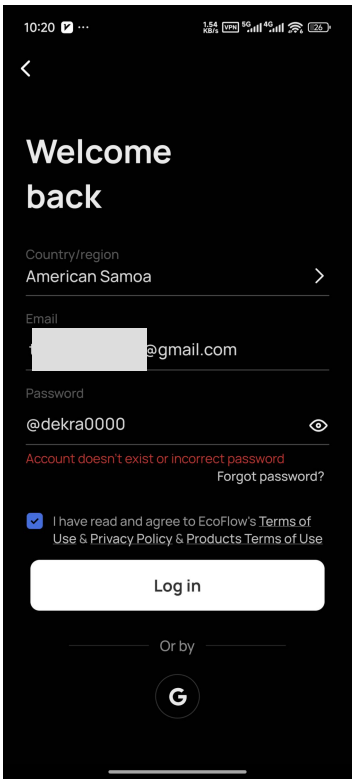


Figure 6: Password-based authentication

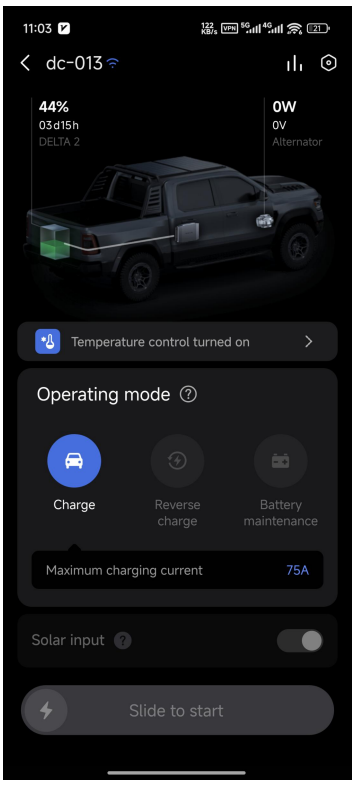


Figure 7: Login successfully

The TL attempted to log in using the correct and incorrect passwords to perform the authentication process. The correct password successfully granted access.

According to TL's test, the results show that this authentication mechanism can correctly identify the correct and incorrect PINs, with the correct PIN unlocking the device.

Therefore, the TL considers that the authentication mechanism is implemented as documented.

RESULT:	PASS

3.2.3 AUM-3: Authenticator validation

Conceptual assessment result

Identifier	AUM-1-APP		
Decision Node	Decision [E.Info.DT.AUM-3]		Justification [E.Just.DT.AUM-3]
DT.AUM-3.DN-1	Yes [x]	No	The authenticator is a password, which belongs to [IC.AUM-3.Password]. Wrong Password will be rejected.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is PASS because at least one path in the decision tree **E.Info.DT.AUM-3** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional sufficiency assessment

For [AUM-1-APP], as shown in AUM-1,AUM-2,it requires the correct Password code.

Because the authenticator belongs to [IC.AUM-3.Password], TL attempted to authenticate using an incorrect password, a partial correct password, and correct password of other account but none of these attempts were able to unlock. Only the correct Password was able to log in and successfully authenticate.

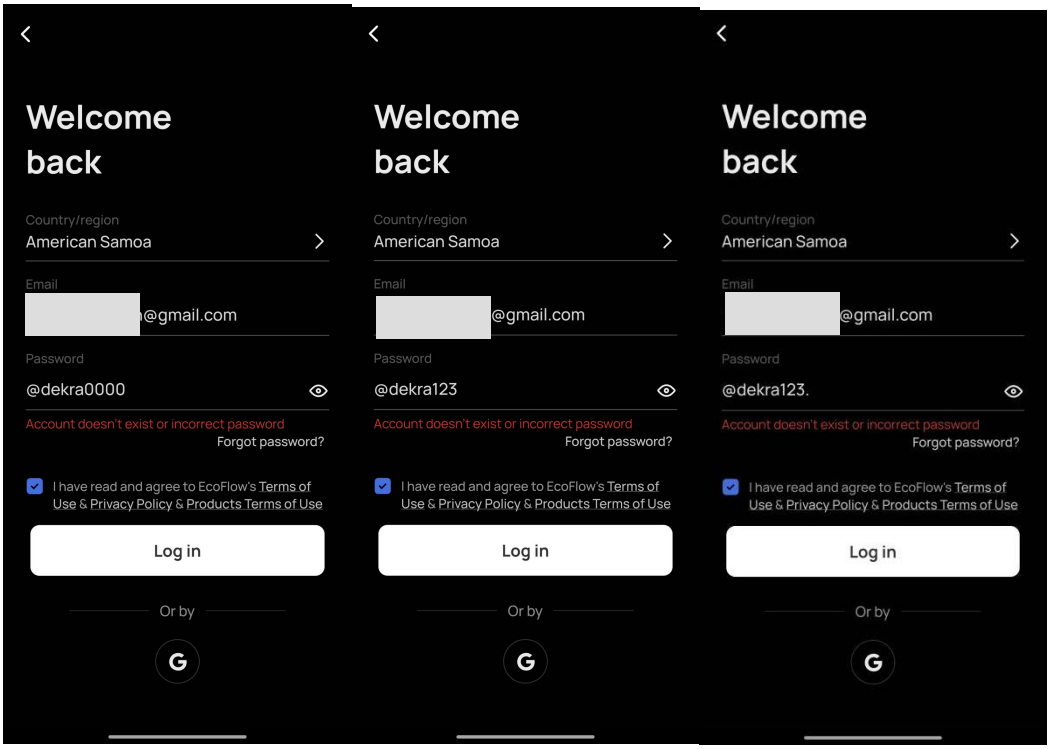


Figure 8: Incorrect password attempts, partial incorrect password attempts and correct password attempts for other accounts

As a result, TL determines the authentication mechanism is implemented successfully as only the correct password can login APP.

The verdict **PASS** for the assessment case is assigned because of for each authentication mechanism documented in [E.Info.AUM-3.AUM] the confirmations in the implementation category dependent assessment unit are successful.

RESULT:	PASS

3.2.4 AUM-4: Changing authenticators

Conceptual assessment result

Identifier	AUM-1-APP	
Decision Node	Decision [E.Info.DT.AUM-3]	Justification [E.Just.DT.AUM-3]

DT.AUM-4.DN-1	Yes	No [x]	Changing the authenticator does not conflict with the basic functions of the equipment.
DT.AUM-4.DN-2	Yes [x]	No	Authentication mechanism can be modified through the application.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is PASS because at least one path in the decision tree **E.Info.DT.AUM-4** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional assessment result

[AUM-1-APP] can be change through APP. Users need to login in first and reset password through using the function of “Forget Password”.

The figure below illustrates the password change process through the APP. To change the password, users can navigate to Account settings → Change password. TL attempted to modify the existing password and tested whether the new password successfully logged into the account, while also verifying that the previous password no longer allowed access.

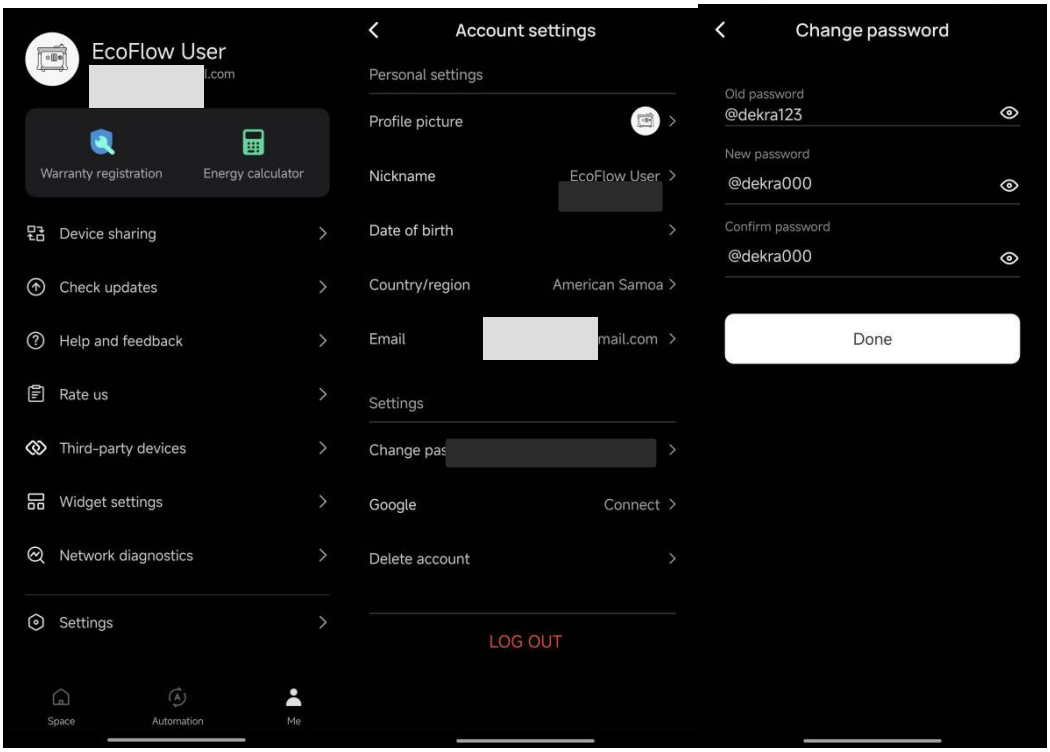


Figure 9: Changing the APP password

Account ’s password can also be changed via the “Forgot Password” . TL used this method to reset the account password and tested that the new password successfully logged in, while also confirming that the previous password no longer granted access.

TL observed that a verification code is send to the registered email address, account password can be changed only after correct verification code is applied. The verification code is invalid after 30 minutes.

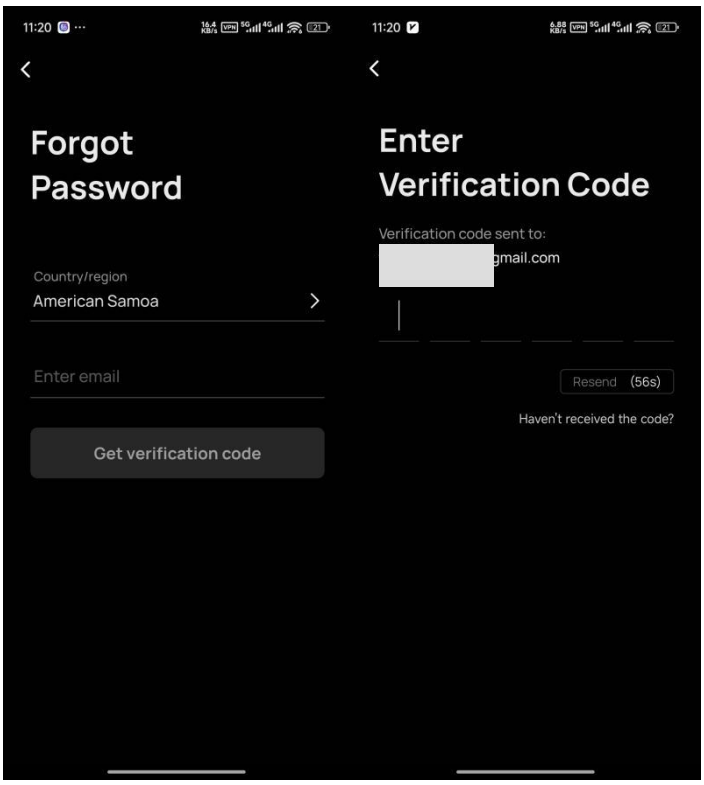


Figure 10: *Password changed need a verification code*

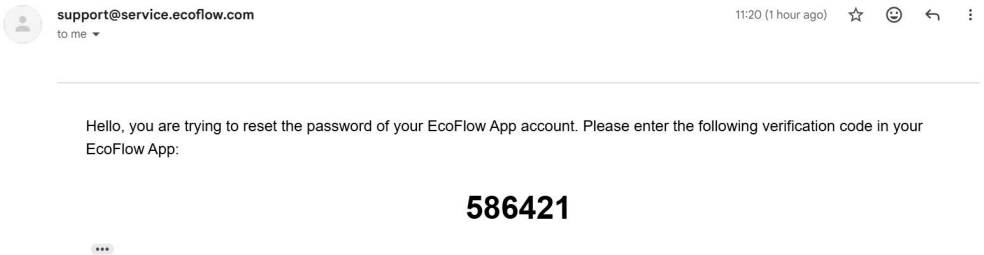


Figure 11: verification code

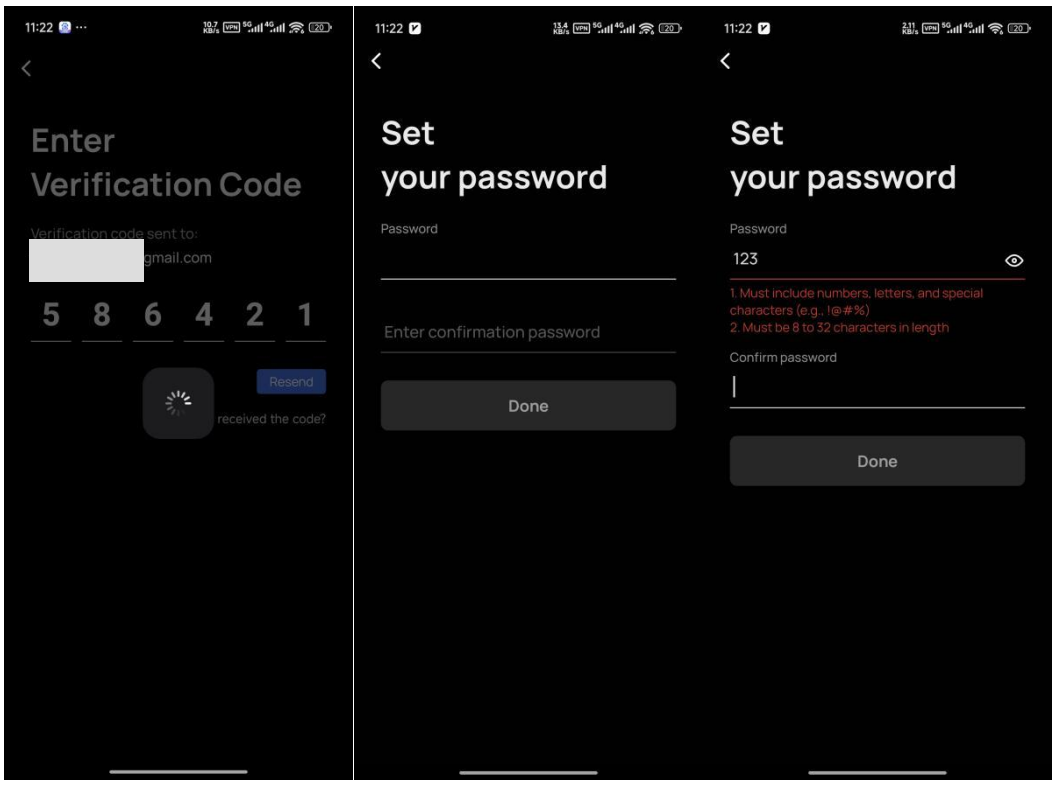


Figure 12: Password changed based on verification code

After changing the Password, TL was able to login the account using the new password and access both security assets and network assets. The previous password could no longer be used to login the account and could not be used to authenticate for access to the assets.

The verdict **PASS** for the assessment case is assigned because of there is no evidence that an implementation of changing an authenticator deviates from [E.Info.AUM-4.AUM.AuthChange].

RESULT:	PASS

3.2.5 AUM-5: Password strength

Conceptual assessment result

Identifier	AUM-1- APP		
Decision Node	Decision [E.Info.DT.AUM-5-2]		Justification [E.Just.DT.AUM-5-2]
DT.AUM-5-2.DN-1	Yes [x]	No	The user needs to set up the password of 6-20 characters when first time register the account, categorized as [IC.AUM-5-2.SettingFirstUse].
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.AUM-5** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional assessment result

According to **E.Info.DT.AUM-5**,

The password is used in [AUM-1-APP] and belongs to the non-factory default passwords, which is categorized as [IC.AUM-5-2.SettingFirstUse]. The user needs to set up the password when first time register the account. The rule for the password is that it should use 6-20 characters with a mix of letters and numbers. When the account is created, the device could remotely control the device from the APP and then connect to the network.

Password needs to be set up by the user in the first use and the device could connect to the network after the initialization state. And the password needs to be 6-20 characters with a mix of letters and numbers. If the strength of password is not fulfilled the condition of password set, App is not allowed user to reset or register the account.

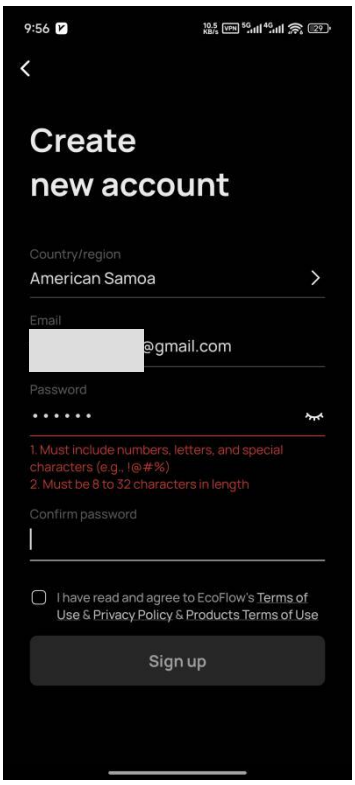


Figure 13: Strength of the password

The verdict **PASS** for the assessment case is assigned because there is no evidence that an implementation of an authentication mechanism's non-factory default password deviates from [E.Info.AUM-5-2.AUM.PwdProperty].

RESULT:	PASS

3.2.6 AUM-6: Brute force protection

Conceptual assessment result

Identifier	AUM-1-APP	
Decision Node	Decision [E.Info.DT.AUM-3]	Justification [E.Just.DT.AUM-3]

DT.AUM-3.DN-1	Yes [x]	No	After several unsuccessful attempts, the account will be temporarily locked. This defends against brute-force attacks through limited attempts and CAPTCHA verification, which is recognized as [IC.AUM-6.LimitAttempts].
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.AUM-6** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional assessment result

According to [AUM-1-APP], after 5 failed attempts, CAPTCHA will be triggered to prevent automated brute force attack scripts or tools. And after 15 failed attempts, the account will be locked for 15 minutes.

The figure below shows that incorrect Password attempts will be rejected by the authorization mechanism.

TL conducted the following tests:

1. repeatedly performing authentication attempts using erroneous authenticators
2. counting the number consecutive failed attempts before the equipment prevents further attempts

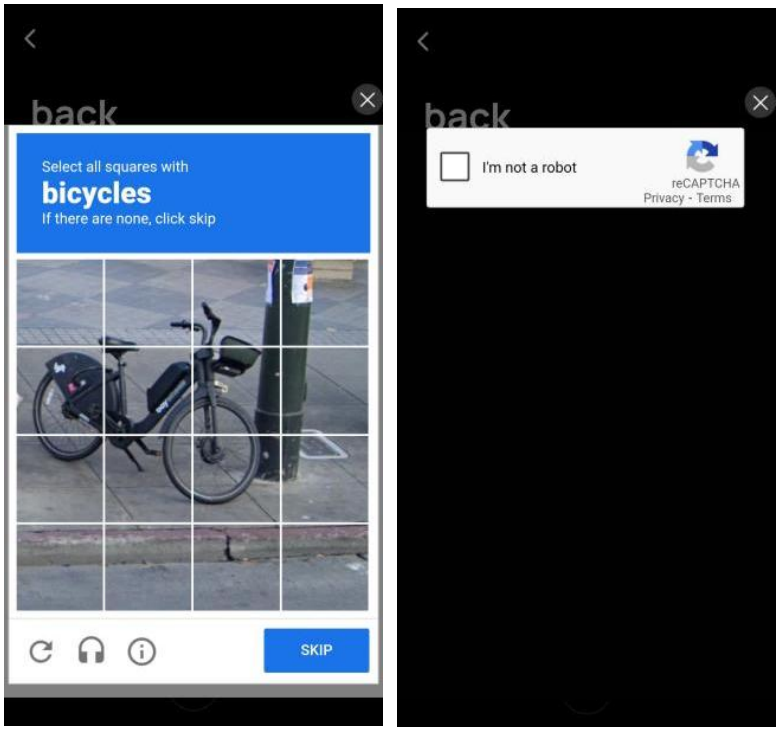


Figure 14: Graphic-based verification

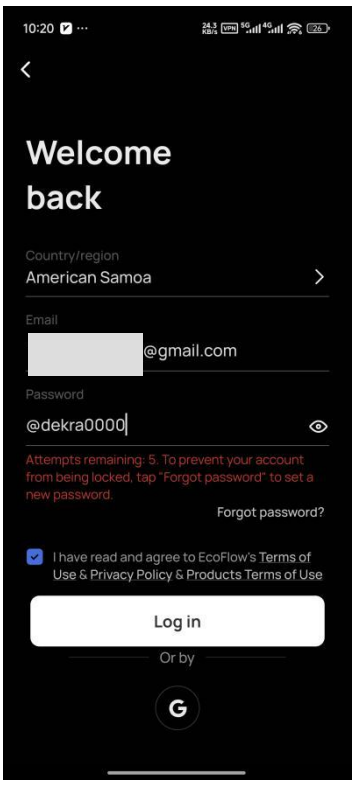


Figure 15: Account locked after consecutive failed attempts

In conclusion, the measures to prevent brute force attacks are based on the password implementation of [IC.AUM-3.Password] in AUM-1-APP. If more than 15 failed attempts are made, [AUM-1-APP] will temporarily lock the account, which falls under [AU.AUM-6.LimitedAttemps].

The verdict **PASS** for the assessment case is assigned because for each authentication mechanism documented in [E.Info.AUM-6.AUM] the confirmations in the implementation category dependent assessment unit are successful.

RESULT:	PASS

3.3 Secure update mechanism

3.3.1 SUM-1: Applicability of update mechanisms

Conceptional assessment results

Identifier	Software-1 Firmware		
Decision Node	Decision [E.Info.DT.SUM-1]		Justification [E.Just.DT.SUM-1]
DT.SUM-1.DN-1	Yes [x]	No	Wireless module firmware, which has FreeRTOS as its operating system updatable via SUM-1. It will affect the security asset and network asset.
DT.SUM-1.DN-2	Yes	No [x]	The equipment functionality allows for updatability.
DT.SUM-1.DN-3	Yes	No [x]	For security reasons, the equipment firmware needs to be

			updatable.
DT.SUM-1.DN-4	Yes	No [x]	There are no alternative measures to protect the equipment 's security assets and network assets throughout its lifecycle.
DT.SUM-1.DN-5	Yes [x]	No	The equipment upgrades the firmware by OTA update.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SUM-1** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional sufficiency assessment

According to **E.Info.PartOfSoftw** and **E.Info.SUM**,

The DUT updates the software component with the firmware upgrade function.

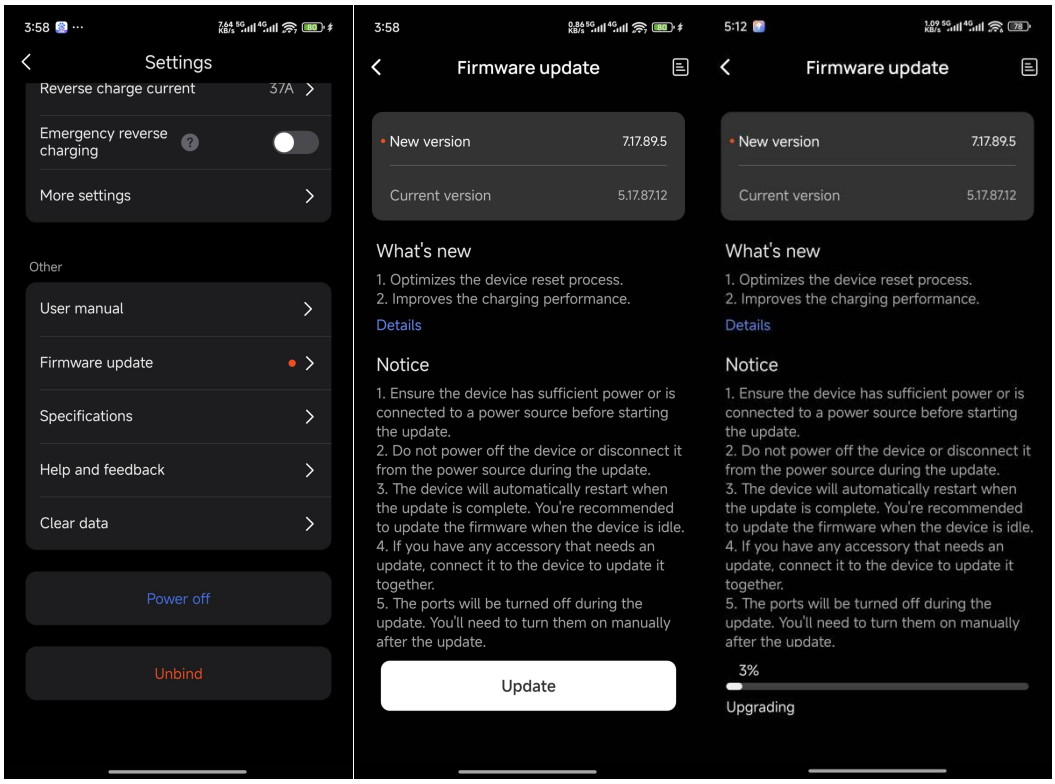


Figure 16: Device update function

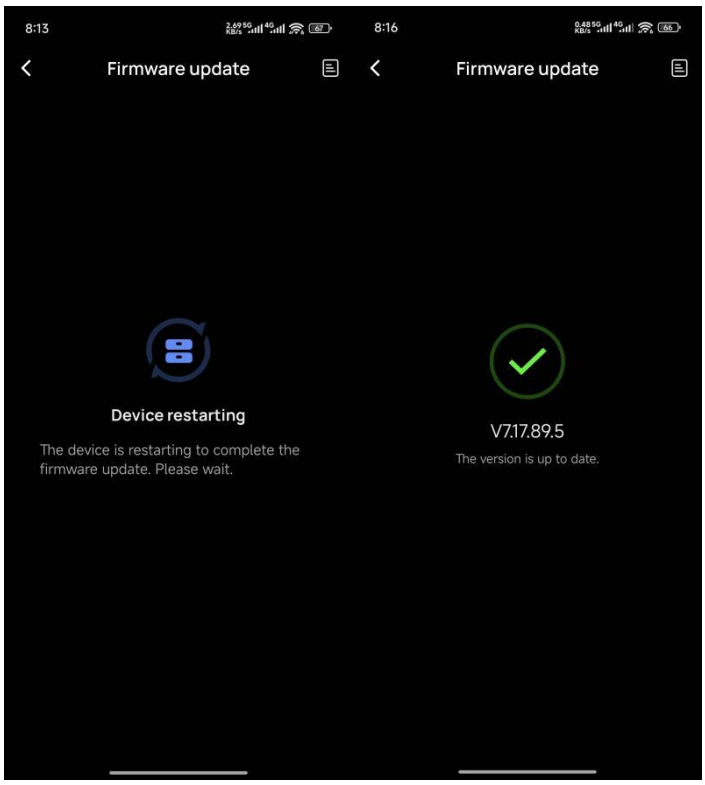


Figure 17: Successful update

TL used the update mechanism recorded in [E.Info.SUM-1.PartOfSoftw.SUM] and successfully installed the firmware onto the device.

The verdict is **PASS** because [Software-1 Firmware] has been successfully upgraded and installed by the update mechanism documented in [E.Info.SUM-1.PartOfSoftw.SUM].

RESULT:	PASS

3.3.2 SUM-2: Secure updates

Conceptional assessment results

Identifier	SUM-1-OTA update		
Decision Node	Decision [E.Info.DT.SUM-2]		Justification [E.Just.DT.SUM-2]
DT.SUM-2.DN-1	Yes [x]	No	The firmware package is first processed with SHA256 and then signed. The processed firmware package is transmitted to the device for signature verification, where it checks if the signature matches, and then the upgrade is performed. OTA update mechanism can make sure the integrity and authenticity are valid at the time of installation.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SUM-2** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional sufficiency assessment

The device uses firmware update packages that are encrypted and then transmitted over HTTP.

On the server side, the firmware undergoes SHA256 processing. The server first calculates the SHA256 value of the BIN file and then signs the SHA256 value using the ECC algorithm. The signed firmware package consists of the firmware image and the signature. When the firmware package is transmitted to the device, the device uses the public key to verify the signature and check whether it matches the signature. If they match, the upgrade proceeds; if they do not match, the upgrade is not performed.

TL attempted a man-in-the-middle attack on the entire update process. As the first step, TL configured traffic-forwarding rules for ports 443 and 8883 on the attacking machine. During testing, TL observed that port 443 enforces certificate verification; when an invalid certificate is presented, the app cannot retrieve any device information, causing the man-in-the-middle attack to fail.

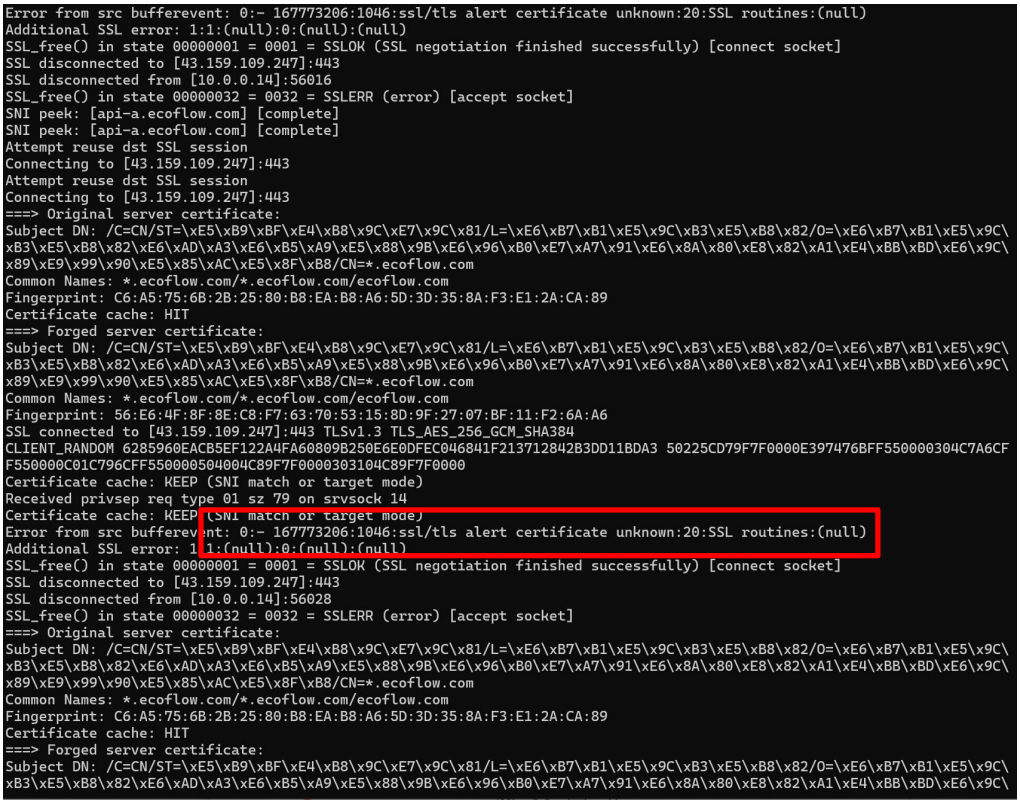


Figure 18: MITM test fail for 443 port

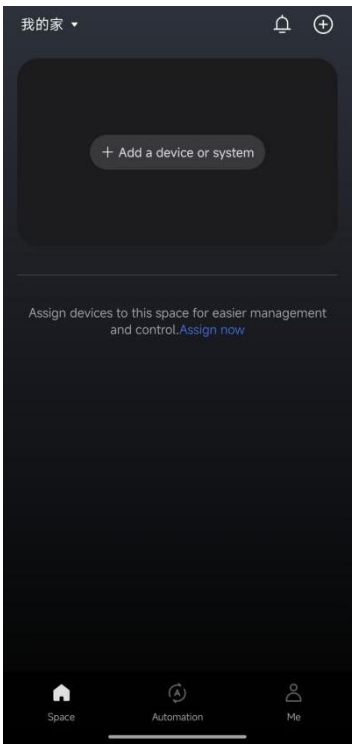


Figure 19: app cannot retrieve any device information

TL then attempted to allow traffic on port 443 and intercept only port 8883. In this configuration, the app was able to obtain basic device information. However, after entering the device page, it failed to establish a connection and could not initiate the OTA upgrade. On the attacking machine, TL also observed indications that port 8883 had detected and blocked the man-in-the-middle attack.

```
Common Names: *.ecoflow.com/*.ecoflow.com/ecoflow.com
Fingerprint: C6:A5:75:6B:2B:25:80:B8:EA:B8:A6:5D:3D:35:8A:F3:E1:2A:CA:89
Certificate cache: HIT
===> Forged server certificate:
Subject DN: /C=CN/ST=\xE5\xB9\xBF\xE4\xB8\x9C\xE7\x9C\x81/L=\xE6\xB7\xB1\xE5\x9C\xB3\xE5\xB8\x82/O=\xE6\xB7\xB1\xE5\x9C\
xB3\xE5\xB8\x82\xE6\xAD\xA3\xE6\xB5\xA9\xE5\x88\x9B\xE6\x96\xB0\xE7\xA7\x91\xE6\x8A\x80\xE8\x82\xA1\xE4\xBB\xBD\xE6\x9C\
x89\xE9\x99\x90\xE5\x85\xAC\xE5\x8F\xB8/CN=*.ecoflow.com
Common Names: *.ecoflow.com/*.ecoflow.com/ecoflow.com
Fingerprint: E0:53:EF:7D:A0:1F:3F:30:FF:11:62:54:C9:1A:39:ED:2E:AF:56:37
SSL connected to [4.236.82.215]:8883 TLSv1.3 TLS_AES_256_GCM_SHA384
CLIENT_RANDOM F8EC63A849F1110D9143DFB553381D1566ADA7054043761B0FB39035AF1C8199 506249514F7F0000E3779E62CE5500000047FB62C
E550000E046FB62CE55000090410 3404F7F0000B04103404F7F0000
Certificate cache: KEEP (SNI match or target mode)
Received privsep req type 01 sz 78 on srvsock 14
Certificate cache: KEEP (SNI match or target mode)
Error from src bufferevent: 0:- 167773206:1046:ssl/tls alert certificate unknown:20:SSL routines:(null)
Additional SSL error: 1:1:(null):0:(null):(null)
SSL_free() in state 00000001 = 0001 = SSLOK (SSL negotiation finished successfully) [connect socket]
SSL disconnected to [4.236.82.215]:8883
SSL disconnected from [10.0.0.14]:36312
SSL_free() in state 00000032 = 0032 = SSLERR (error) [accept socket]
SNI peek: [mqtt-a.ecoflow.com] [complete]
Attempt reuse dst SSL session
Connecting to [4.236.82.215]:8883
===> Original server certificate:
Subject DN: /C=CN/ST=\xE5\xB9\xBF\xE4\xB8\x9C\xE7\x9C\x81/L=\xE6\xB7\xB1\xE5\x9C\xB3\xE5\xB8\x82/O=\xE6\xB7\xB1\xE5\x9C\
xB3\xE5\xB8\x82\xE6\xAD\xA3\xE6\xB5\xA9\xE5\x88\x9B\xE6\x96\xB0\xE7\xA7\x91\xE6\x8A\x80\xE8\x82\xA1\xE4\xBB\xBD\xE6\x9C\
x89\xE9\x99\x90\xE5\x85\xAC\xE5\x8F\xB8/CN=*.ecoflow.com
Common Names: *.ecoflow.com/*.ecoflow.com/ecoflow.com
Fingerprint: C6:A5:75:6B:2B:25:80:B8:EA:B8:A6:5D:3D:35:8A:F3:E1:2A:CA:89
Certificate cache: HIT
===> Forged server certificate:
Subject DN: /C=CN/ST=\xE5\xB9\xBF\xE4\xB8\x9C\xE7\x9C\x81/L=\xE6\xB7\xB1\xE5\x9C\xB3\xE5\xB8\x82/O=\xE6\xB7\xB1\xE5\x9C\
xB3\xE5\xB8\x82\xE6\xAD\xA3\xE6\xB5\xA9\xE5\x88\x9B\xE6\x96\xB0\xE7\xA7\x91\xE6\x8A\x80\xE8\x82\xA1\xE4\xBB\xBD\xE6\x9C\
x89\xE9\x99\x90\xE5\x85\xAC\xE5\x8F\xB8/CN=*.ecoflow.com
Common Names: *.ecoflow.com/*.ecoflow.com/ecoflow.com
Fingerprint: E0:53:EF:7D:A0:1F:3F:30:FF:11:62:54:C9:1A:39:ED:2E:AF:56:37
SSL connected to [4.236.82.215]:8883 TLSv1.3 TLS_AES_256_GCM_SHA384
CLIENT_RANDOM 3EF462884 0832A6550934D15540C1C6F30F8F4A077494968619509F55CE23AD2 506249514F7F0000E3779E62CE5500002047FB62C
E550000E046FB62CE55000050 9702404F7F0000709702404F7F0000
Certificate cache: KEEP (SNI match or target mode)
Received privsep req type 01 sz 78 on srvsock 14
Certificate cache: KEEP (SNI match or target mode)
Error from src bufferevent: 0:- 167773206:1046:ssl/tls alert certificate unknown:20:SSL routines:(null)
```

Figure 20: MITM test fail for 8883 port

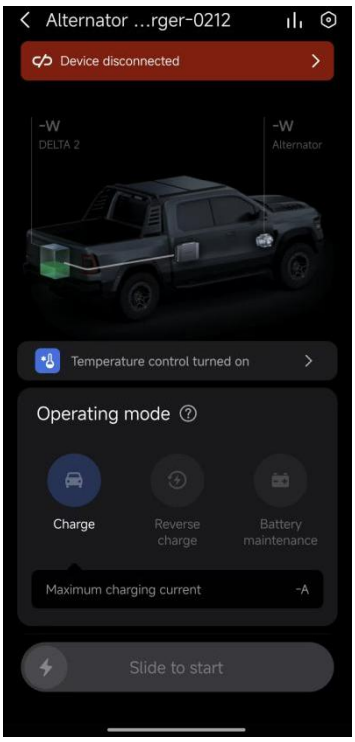


Figure 21: Can not initiate the OTA upgrade

The firmware signature verification mechanism ensures the security and reliability of the update process, eliminating the possibility of tampering and interception, thereby guaranteeing confidentiality and integrity.
The verdict is PASS because the installation process is protected by TLSv1.2 through [AU.SUM-2.SecChan] and the APP confirmation ensures the integrity and authenticity of the update.

RESULT:	PASS

3.3.3 SUM-3: Automated updates

Conceptional assessment results

Identifier	SUM-1-OTA update		
Decision Node	Decision [E.Info.DT.SUM-3]		Justification [E.Just.DT.SUM-3]
DT.SUM-3.DN-1	Yes	No [x]	The equipment does not support silent upgrades.
DT.SUM-3.DN-2	Yes	No [x]	The equipment cannot automatically upgrade during a scheduled time.
DT.SUM-3.DN-3	Yes [x]	No	Update mechanism is capable of updating the software via triggering the installation of an update under human approval.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SUM-3** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional sufficiency assessment

Firmware updates can be triggered manually in the APP. TL confirmed that clicking update function is required to enable the update, which follows the update mechanism of triggering the installation under human approval.

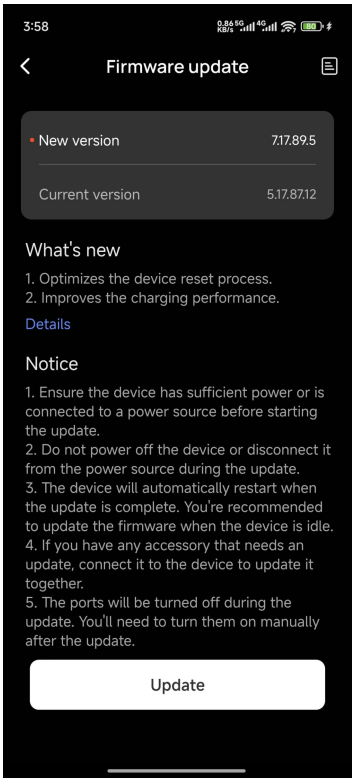


Figure 22: Firmware version before updating

As shown below, TL examined the device's update functionality. TL found that the device does not support silent upgrades or upgrades scheduled for a specific time. Triggering an upgrade requires human approval.

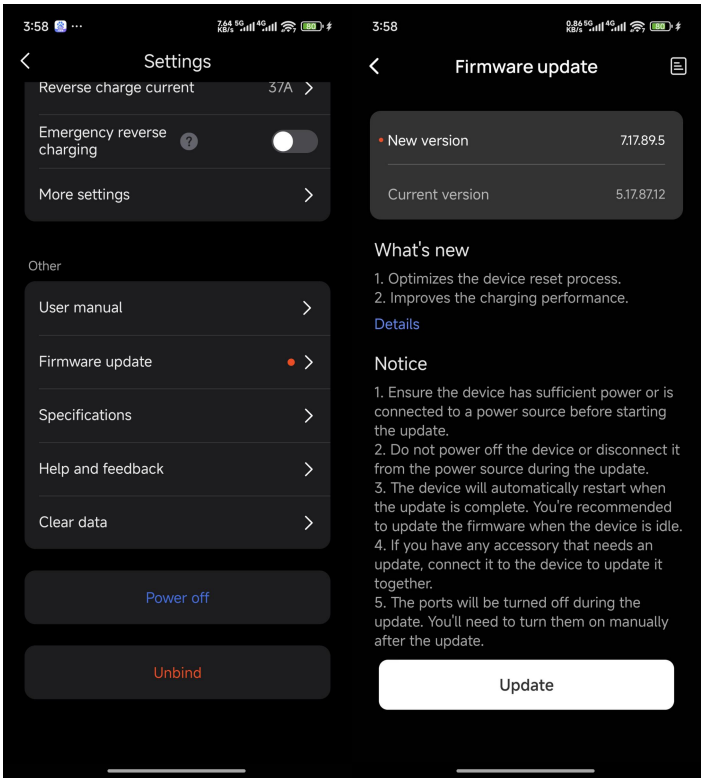


Figure 23: Update triggered by human approval

Therefore, TL assigns this as **PASS** because the update mechanism by human approval is needed.

RESULT:	PASS

3.4 Secure storage mechanism

3.4.1 SSM-1: Applicability of secure storage mechanisms

Conceptional assessment results

Identifier	Asset-1 Wi-Fi SSID and Password		
Decision Node	Decision [E.Info.DT.SSM-1]		Justification [E.Just.DT.SSM-1]
DT.SSM-1.DN-1	Yes	No [x]	The storage of the network assets or security assets can not be protected by physical or logical measures.
DT.SSM-1.DN-2	Yes [x]	No	This device ensures the integrity of stored security assets or network assets by employing an access control mechanism that denies unauthorized modifications.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SSM-1** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional assessment results

TL logs into the application using a username and password. TL discovers that only logged-in users can view the Wi-Fi SSID and password to which the device is connected. This can be regarded as an access control using authentication or authorization.

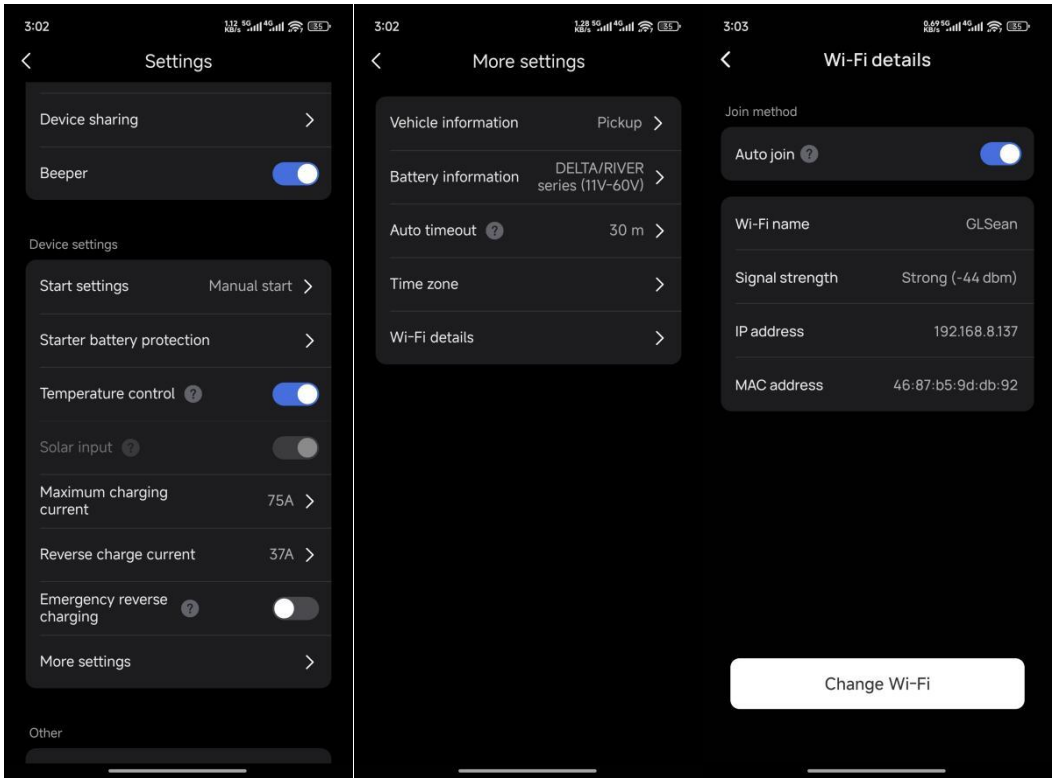


Figure 24: View path

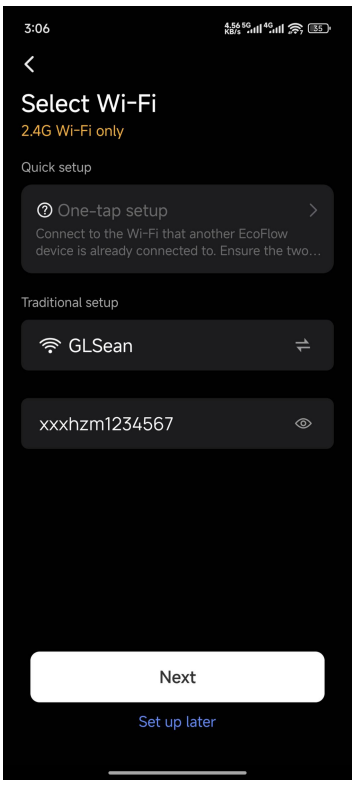


Figure 25: *Wi-Fi SSID and password*

TL concludes that, for [Asset-1 Wi-Fi SSID and Password], [SSM-1-Flash Encryption] is enabled and has been recorded in [E.Info.SSM-1.SecurityAsset.SSM].

The verdict is PASS because security asset is persistently stored via secure storage mechanisms documented in [E.Info.SSM-1.SecurityAsset.SSM].

RESULT:	PASS

3.4.2 SSM-2: Appropriate integrity protection for secure storage mechanisms

Conceptional assessment results

Identifier	SSM-1-Flash Encryption		
Decision Node	Decision [E.Info.DT.SSM-1]		Justification [E.Just.DT.SSM-1]
DT.SSM-1.DN-1	Yes [x]	No	The integrity of the asset is protected to ensure attacks on secure storage will not result in manipulation.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SSM-2** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional assessment results

The [Asset-1 Wi-Fi SSID and Password] are stored on the DUT. TL verifies that the DUT's secure storage mechanisms are protected by an access control system, which aligns with the requirements of [IC.SSM-2.AccessControl]. As specified in [E.Info.SSM-2.AccessControl], this system prevents unauthorized modification of these assets.

After logging in, TL can access the security asset.

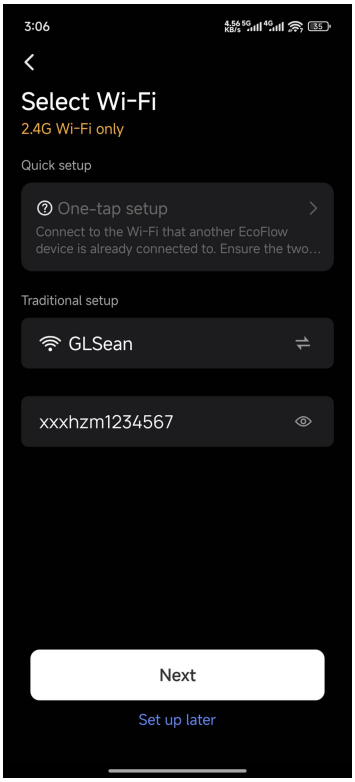


Figure 26: *Wi-Fi SSID and password*

The verdict is **PASS** because for each secure storage mechanism documented in [E.Info.SSM-2.SSM], the confirmations in the implementation-category–dependent assessment units are successful.

RESULT:	PASS

3.4.3 SSM-3: Appropriate confidentiality protection for secure storage mechanisms

Conceptional assessment results

Identifier	SSM-1-Flash Encryption		
Decision Node	Decision [E.Info.DT.SSM-1]		Justification [E.Just.DT.SSM-1]
DT.SSM-1.DN-1	Yes [x]	No	The confidentiality of the asset is protected to ensure attacks on

			secure storage will not result in manipulation.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SSM-3** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional assessment results

According to the **Test Case ACM-1** and **Test Case SSM-1**, the [Asset-1 Wi-Fi SSID and Password] are stored on the DUT. TL verifies that the DUT's secure storage mechanisms are protected by an access control system, which aligns with the requirements of [IC.SSM-3.AccessControl]. This is implemented according to **E.Info.SSM-3.AccessControl**, and unauthorized reading of stored confidential security parameters and confidential network function configurations is denied.

The verdict is **PASS** because for each secure storage mechanism documented in [E.Info.SSM-3.SSM], the confirmations in the implementation-category–dependent assessment units are successful.

RESULT:	**PASS**

3.5 Secure communication mechanism

3.5.1 SCM-1: Applicability of secure communication mechanisms

Conceptional assessment results

Identifier	Asset-3 Remote Control Function Asset-4 OTA data		
Decision Node	Decision [E.Info.DT.SCM-1]		Justification [E.Just.DT.SCM-1]
DT.SCM-1.DN-1	Yes [x]	No	The DUT receives the [Asset-3 Remote control function] from the cloud server via the mobile app. It is protected by [SCM-1-TLSv1.2]. [Asset-4 OTA data] uses [SCM-3-HTTP with encrypted data]. The firmware package is first processed and signed on the cloud, then transmitted securely via HTTP, and finally verified and installed on the device.
Verdict	**Pass**		

Identifier	Asset-1 Wi-Fi SSID and Password	
Decision Node	Decision [E.Info.DT.SCM-1]	Justification [E.Just.DT.SCM-1]

DT.SCM-1.DN-1	Yes	No [x]	The device establishes initial contact with the app by transmitting [Asset-1 Wi-Fi SSID and Password] via [interface-1 Bluetooth].
DT.SCM-1.DN-2	Yes [x]	No	This is a temporary exposure of Wi-Fi transmission information to ensure the DUT can establish a connection to the network. It occurs during the initial Bluetooth pairing data transmission.
Verdict	**Not Applicable**		

Identifier	Asset-2 Bluetooth function		
Decision Node	Decision [E.Info.DT.SCM-1]		Justification [E.Just.DT.SCM-1]
DT.SCM-1.DN-1	Yes	No [x]	The device establishes initial contact with the app by transmitting [Asset-1 Wi-Fi SSID and Password] and [Asset-3 Remote Control Function] via [Interface-1Bluetooth].
DT.SCM-1.DN-2	Yes	No [x]	Assets are not temporary exposure for connection to establish the connection.
DT.SCM-1.DN-2	Yes [x]	No	Targeted environment can ensure that network assets and security assets will be only exposed to authorized entities.
Verdict	**Not Applicable**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SCM-1** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional Completeness Assessment

[Asset-3 Remote Control Function] is encrypted and transmitted via [SCM-1-TLSv1.2].

[Asset-4 OTA data] are encrypted and transmitted via [SCM-3-HTTP with encrypted data].

As a result, no assets beyond those listed in **E.Info.SCM.Asset** are present.

Functional sufficiency assessment

By capturing the communication of devices and app, it is confirmed that the equipment uses the TLS protocol to establish a connection and transmit information.

Figure below shows [Asset-3 Remote Control Function] is encrypted when transmitting by [SCM-1-TLSv1.2].

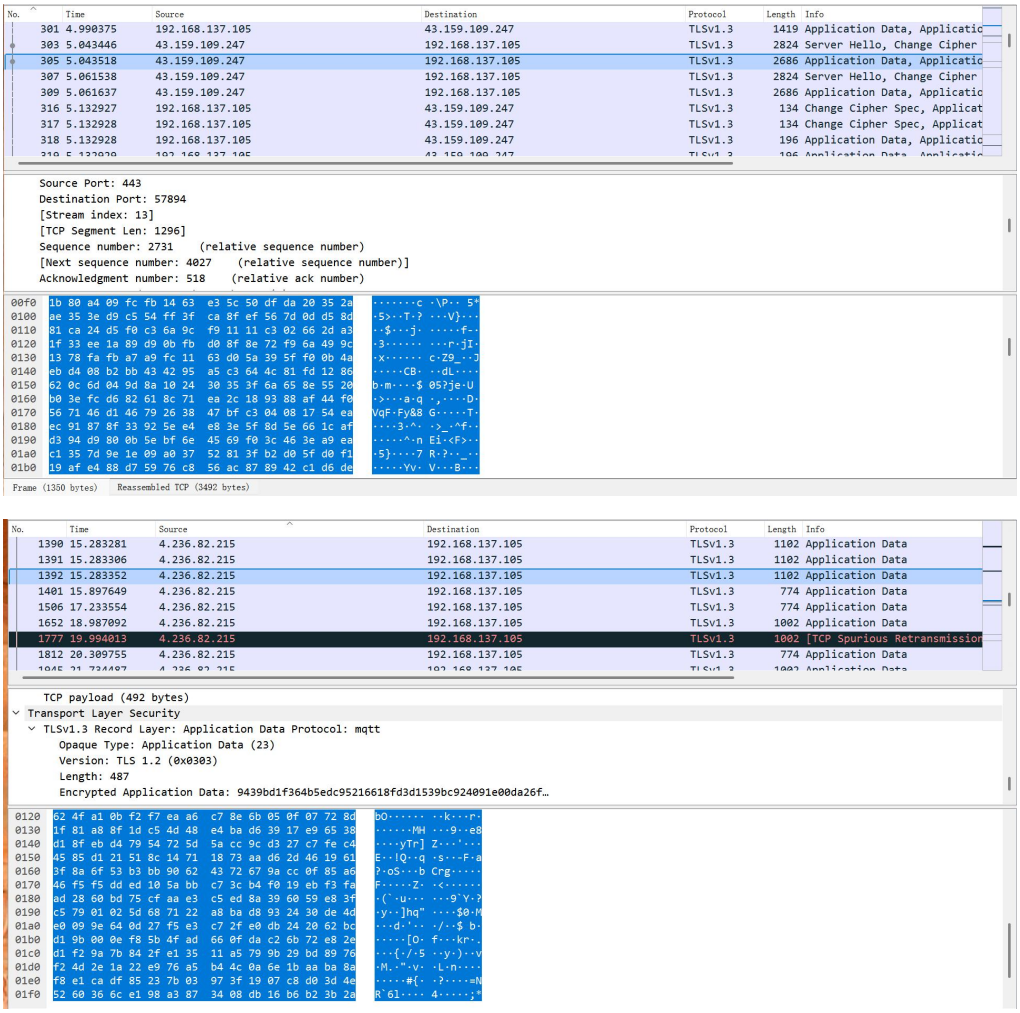


Figure 27: *Encrypted data on TLS traffic*

[Asset-3 Remote Control Function] is sent over [Interface-2 WLAN] and are protected by [SCM-1-TLSv1.2].

Figure below shows that TL monitored the network traffic during asset transmission by the device. TL discovered that during the transmission of [Asset-3 Remote control command] and [Asset-4 OTA data] between the cloud and the device, the TLSv1.2 cipher suite TLS_AES_256_GCM_SHA384 was used for encrypted communication.

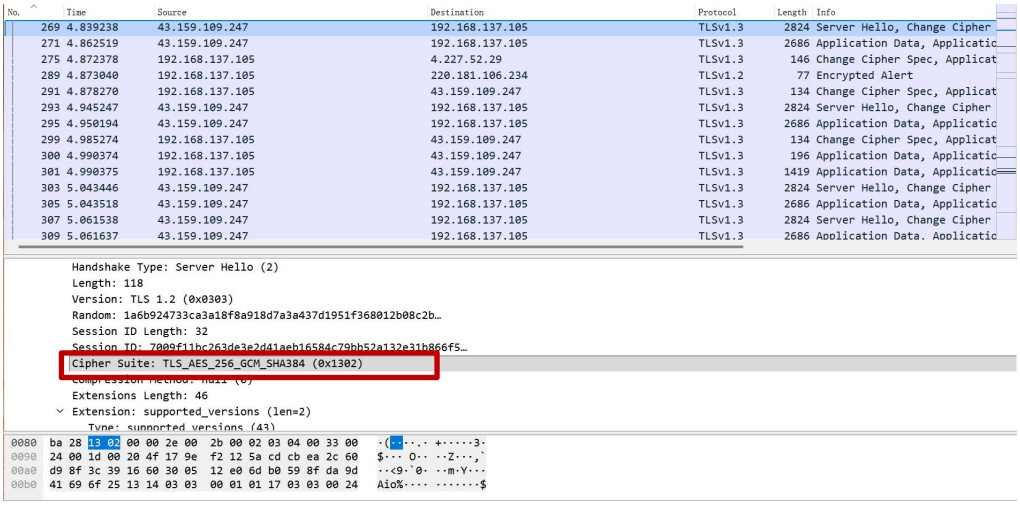


Figure 28: TLS communication mechanism

TL determines that for each security asset documented in [E.Info.SCM-1.SecurityAsset] and for each network asset documented in [E.Info.SCM-1.NetworkAsset], a secure communication mechanism has been enabled to ensure encrypted transmission or other forms of validation to guarantee security.

For [Asset-4 OTA data], the transmitted data is encrypted and signed in the cloud, and then transmitted via HTTP, using TLS_AES_256_GCM_SHA384 encryption. Upon arrival at the device, its authenticity and integrity are verified through secure boot.

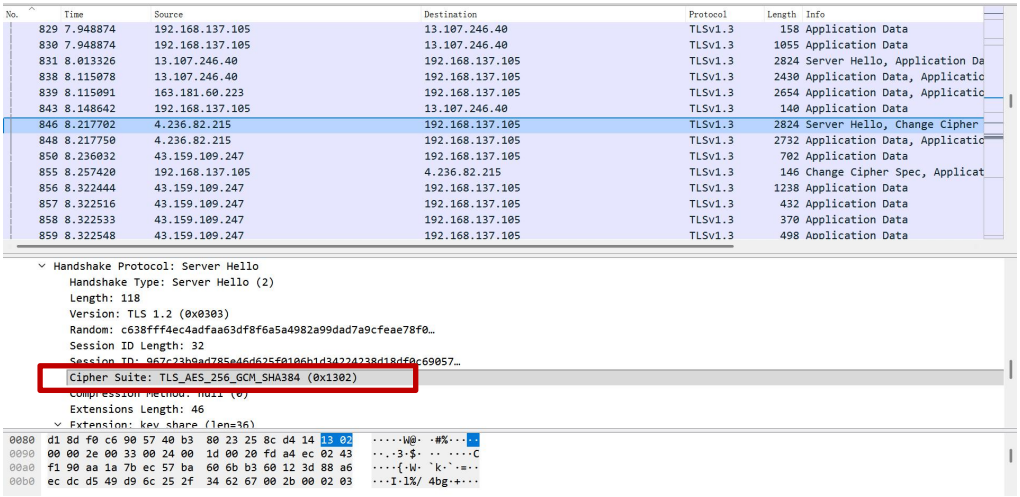


Figure 29: Encrypted data during OTA update

Therefore, the verdict is **PASS** because the secure communication mechanisms are implemented as documented in **E.Info.SCM**.

RESULT:	PASS

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

Conceptional assessment results

Identifier	SCM-1-TLSv1.2		
Decision Node	Decision [E.Info.DT.SCM-2]		Justification [E.Just.DT.SCM-2]
DT.SCM-2.DN-1	Yes [x]	No	The device uses TLSv1.2 for communication and the cipher suite TLS_AES_256_GCM_SHA384 to protect network and security assets. It is categorized as [IC.SCM-2. PKI-based].
Verdict	**Pass**		

Identifier	SCM-2-HTTP with encrypted data	
Decision Node	Decision [E.Info.DT.SCM-2]	Justification [E.Just.DT.SCM-2]

DT.SCM-2.DN-1	Yes [x]	No	The transmitted data is encrypted and signed in the cloud, then transferred via HTTP. TLS_AES_256_GCM_SHA384 ensuring its authenticity and integrity.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SCM-2** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

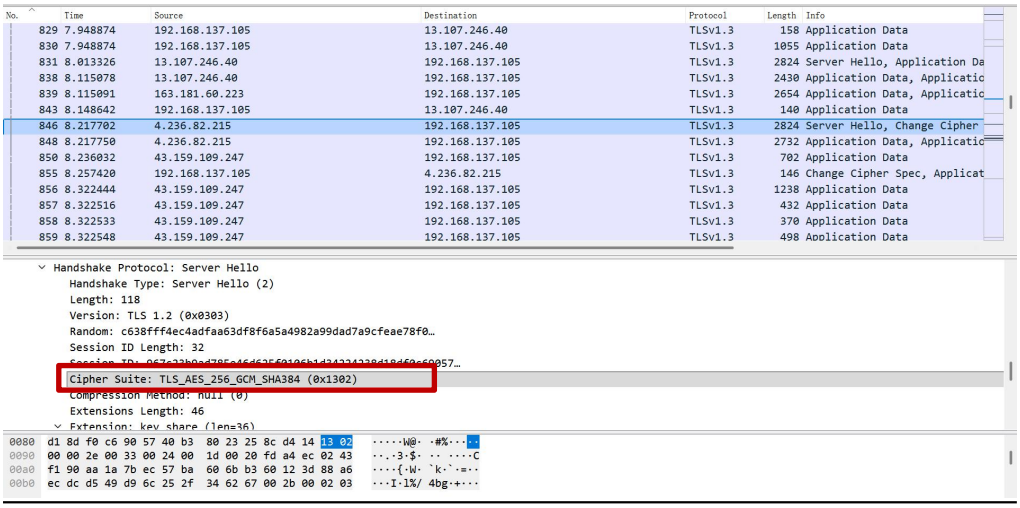
RESULT:	**PASS**

Functional assessment result

According to the **E.Info.SCM**,

For [SCM-1-TLSv1.2],

[SCM-1-TLSv1.2] is the communication encrypted by TLSv1.2. The communication between device and cloud use TLS_AES_256_GCM_SHA384 as cipher suite to protect the communication, which is categorized as [IC.SCM-2.PKI-based]. It is the best practice applied to protect the integrity and authenticity.



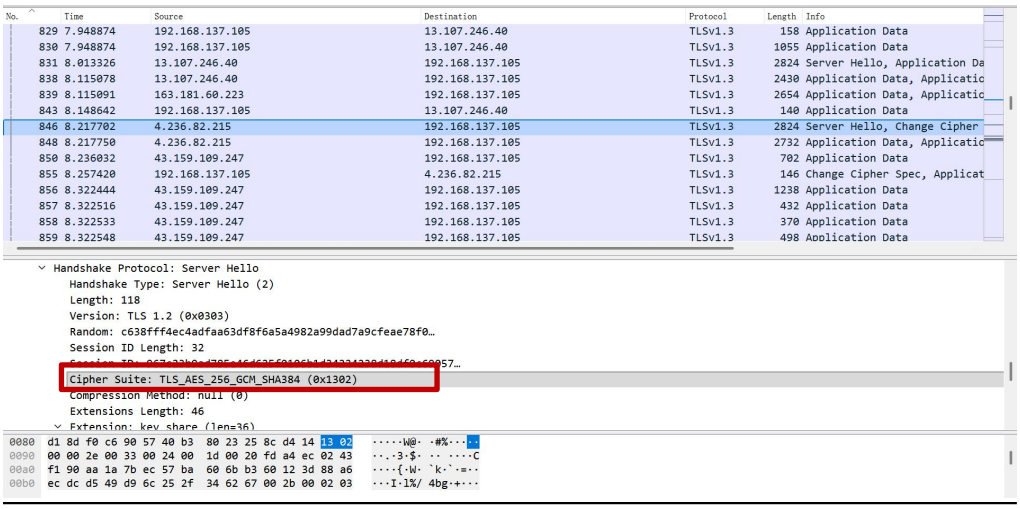


Figure 30: TLS communication mechanism

The figure below shows the device's behavior in a MITM attack. TL connected the device to a hotspot forged by TL and conducted a MITM attack by redirecting traffic and replacing certificates.

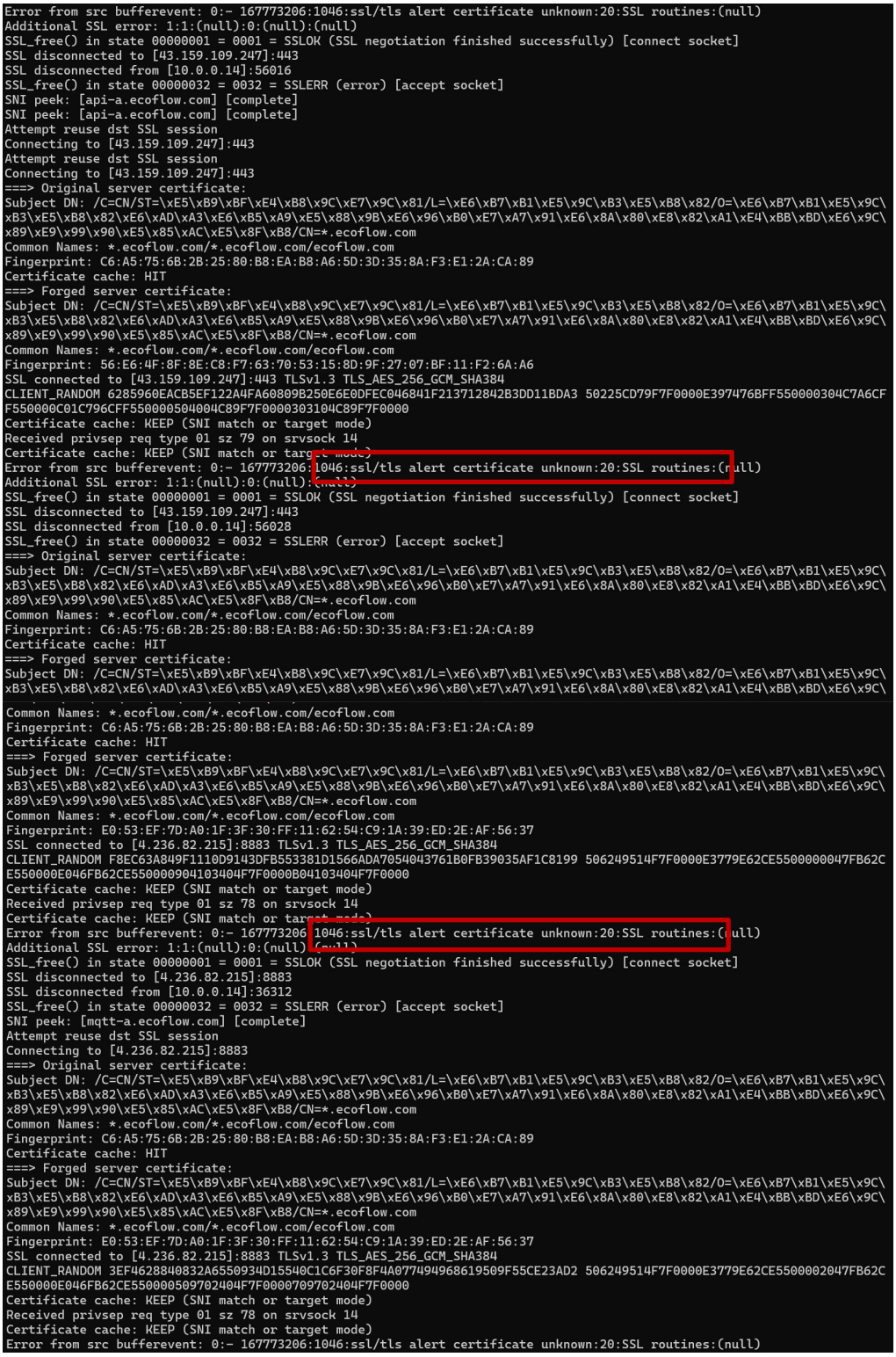


Figure 31: *Unknown* CA recored by script during MITM

During TL's testing, it was found that during certificate replacement, the device was unable to establish a connection with the cloud when connected to a hotspot performing a MITM attack. The device will only establish secure communication with the target if the certificate is successfully validated and shows no signs of tampering; otherwise, the connection will be terminated.

At the same time, the device uses AES_256_GCM as the encryption method,

Integrity is ensured by the GCM mode. During encryption, the device generates an authentication tag (Authentication Tag / MAC). The receiver uses the same key and algorithm to recompute the tag and compares it with the received one. If the data is tampered with during transmission, the tag will not match.

Authenticity is ensured by certificates signed by a trusted CA. Only by presenting the corresponding certificate and participating in the handshake can the parties know the negotiated session key and generate the correct tag.

TL can get the following conclusion:

1. Device can successfully identify forged certificates, and the forged certificates will not be accepted.
2. Manipulated message is not accepted as being of integrity.
3. Unauthorized message is not accepted as authentic.
4. Successful MITM attack is not possible in case that channel-based communication is used.

The verdict **PASS** for the assessment case is assigned because of for each secure communication mechanism documented in [E.Info.SCM-2.SCM] the confirmations in the implementation category dependent assessment unit are successful.

RESULT:	PASS

3.5.3 SCM-3: Appropriate confidentiality protection for secure communication mechanisms

Conceptual assessment results

Identifier	SCM-1-TLSv1.2 SCM-2-HTTP with encrypted data		
Decision Node	Decision [E.Info.DT.SCM-1]		Justification [E.Just.DT.SCM-1]
DT.SCM-3.DN-1	Yes [x]	No	The device uses TLSv1.2 for communication to ensure the security of network assets or security assets. Before transmitting OTA data, the device will first perform encryption processing.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.SCM-3** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional assessment results

According to the questionnaire **E.Info.SCM**, **E.Info.Asset.SCM** and **E.Info.DT.SCM-3,**

[SCM-1-TLSv1.2] is a TLSv1.2 communication mechanism. It is categorized as [IC.SCM-2.PKI-based]. The traffic data during the communication of the device and the cloud is encrypted with the cipher suite: TLS_AES_256_GCM_SHA384 . It is the best practice to protect the confidentiality of security and network assets.

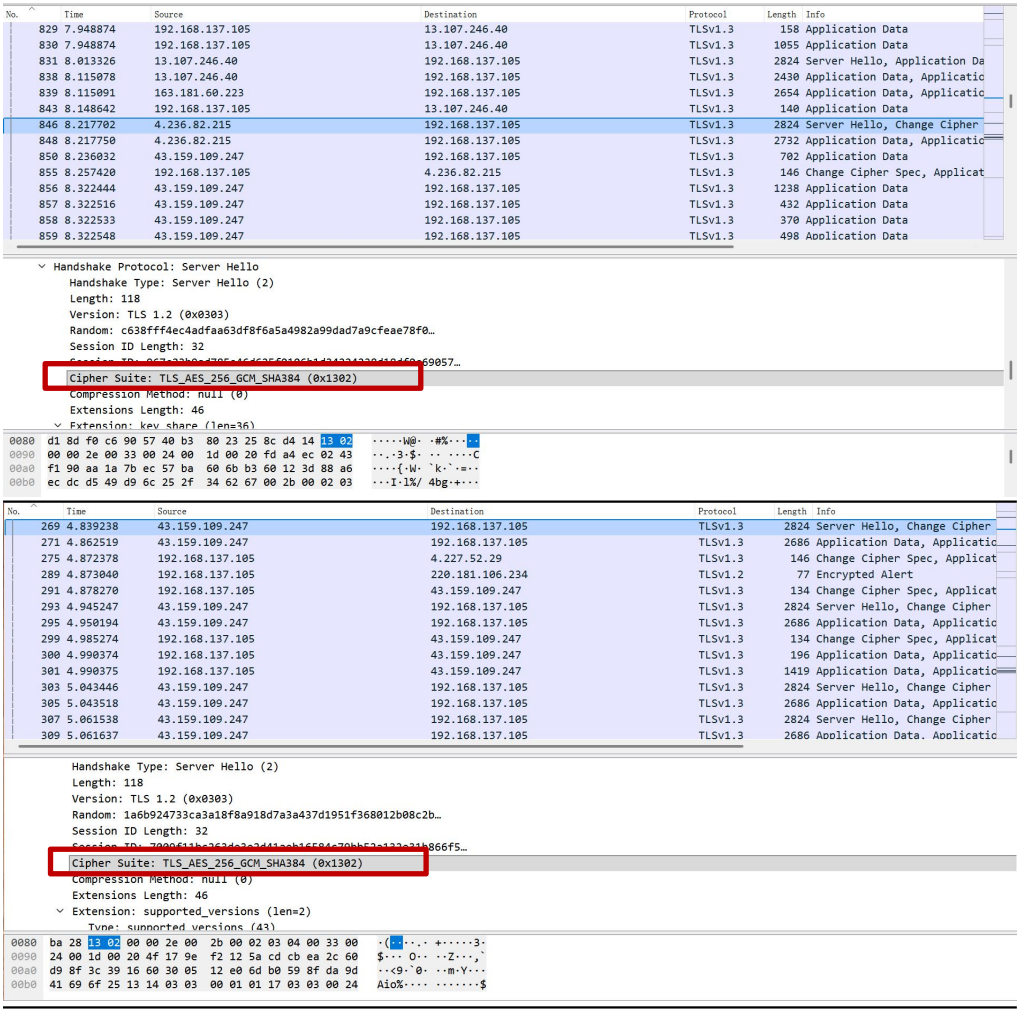


Figure 32: *TLS communication mechanism*

The cipher suite TLS_AES_256_GCM_SHA384 uses ECDHE for ephemeral key exchange with forward secrecy, RSA for authentication, AES-128-GCM for confidentiality, and SHA-256 for key derivation and message authentication.

It ensures:

- The key used to encrypt messages within the communication channel cannot be intercepted
- Only the parties involved in the key exchange can encrypt and decrypt the data.

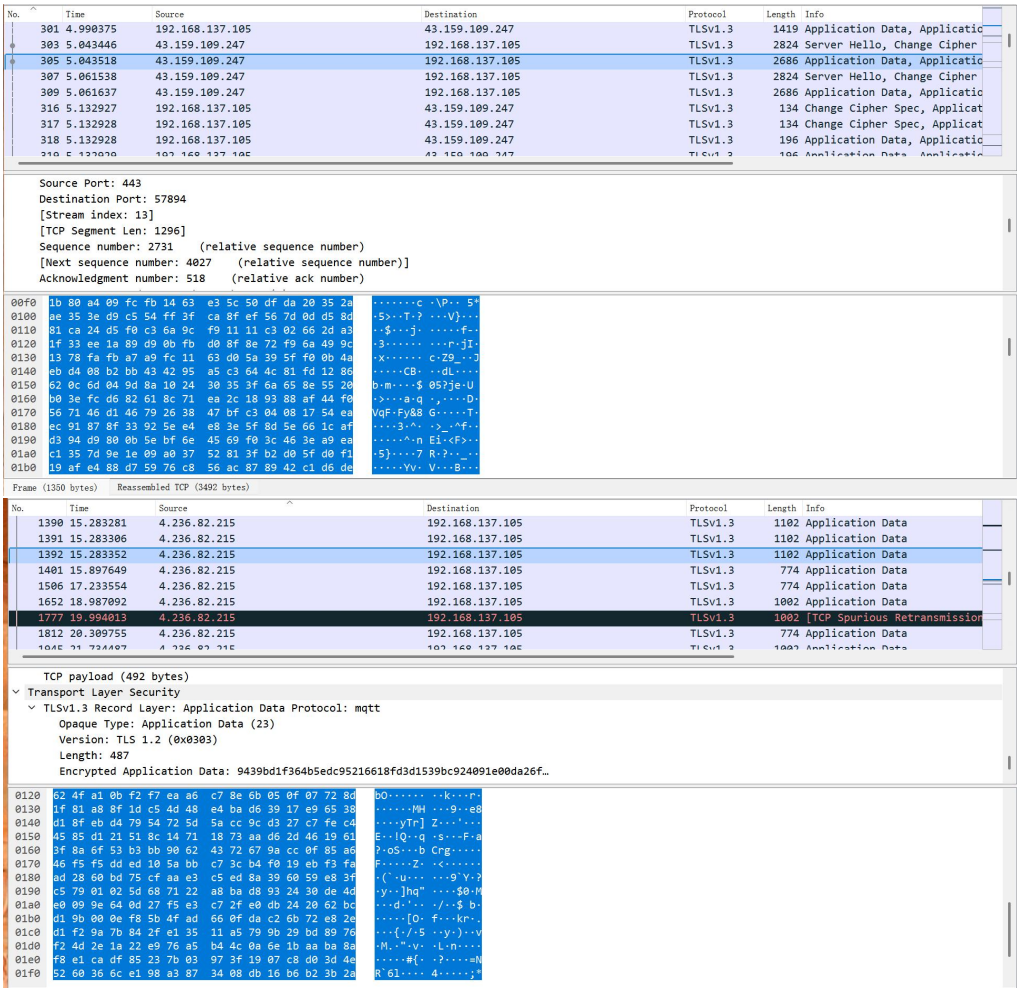


Figure 33: Security assets and network assets encrypt data

TL found that the data has been encrypted and transfer by TLS based on figure above.

In conclusion, TL analyzed the communication commands and data packets transmitted between the cloud and the device under [SCM-1-TLSv1.2] and [SCM-2-HTTP with encrypted data]. The results show that the data is encrypted, and both [SCM-1-TLSv1.2] and [SCM-2-HTTP with encrypted data] can ensure the confidentiality of the assets.

The verdict is **PASS** because [SCM-1-TLSv1.2] and [SCM-2-HTTP with encrypted data] are confirmed to provide appropriate confidentiality protection for secure communication mechanism.

RESULT:	PASS

3.5.4 SCM-4: Appropriate replay protection for secure communication mechanisms

Conceptual assessment results

Identifier	SCM-1-TLSv1.2		
Decision Node	Decision [E.Info.DT.SCM-4]		Justification [E.Just.DT.SCM-4]
DT.SCM-4.DN-1	Yes [x]	No	TLSv1.2 uses incrementing sequence numbers at the record layer

			protocol to prevent replay attack, which is belong to [IC.SCM-4.SeqNumb].
Verdict	**Pass**		

Identifier	SCM-2-HTTP with encrypted data		
Decision Node	Decision [E.Info.DT.SCM-4]		Justification [E.Just.DT.SCM-4]
DT.SCM-4.DN-1	Yes [x]	No	
Verdict	**Pass**		

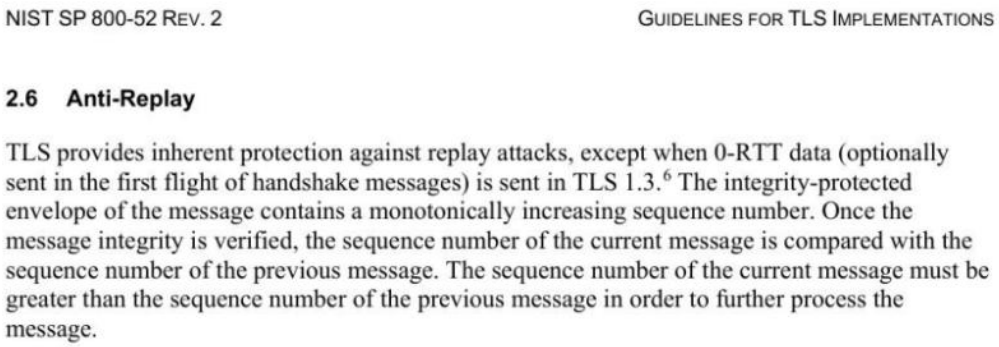
Therefore, the verdict of this conceptional test is PASS because at least one path in the decision tree **E.Info.DT.SCM-4** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional assessment results

[SCM-1-TLS] utilized a TLSv1.2 communication mechanism, the TLSv1.2 uses incrementing sequence numbers at the record layer protocol, which is belong to [IC.SCM-4.SeqNumb].

And according to NIST SP 8000-53 REV.2, TLS protects the asset during transmission against reply attack.



NIST SP 800-52 REV. 2 GUIDELINES FOR TLS IMPLEMENTATIONS

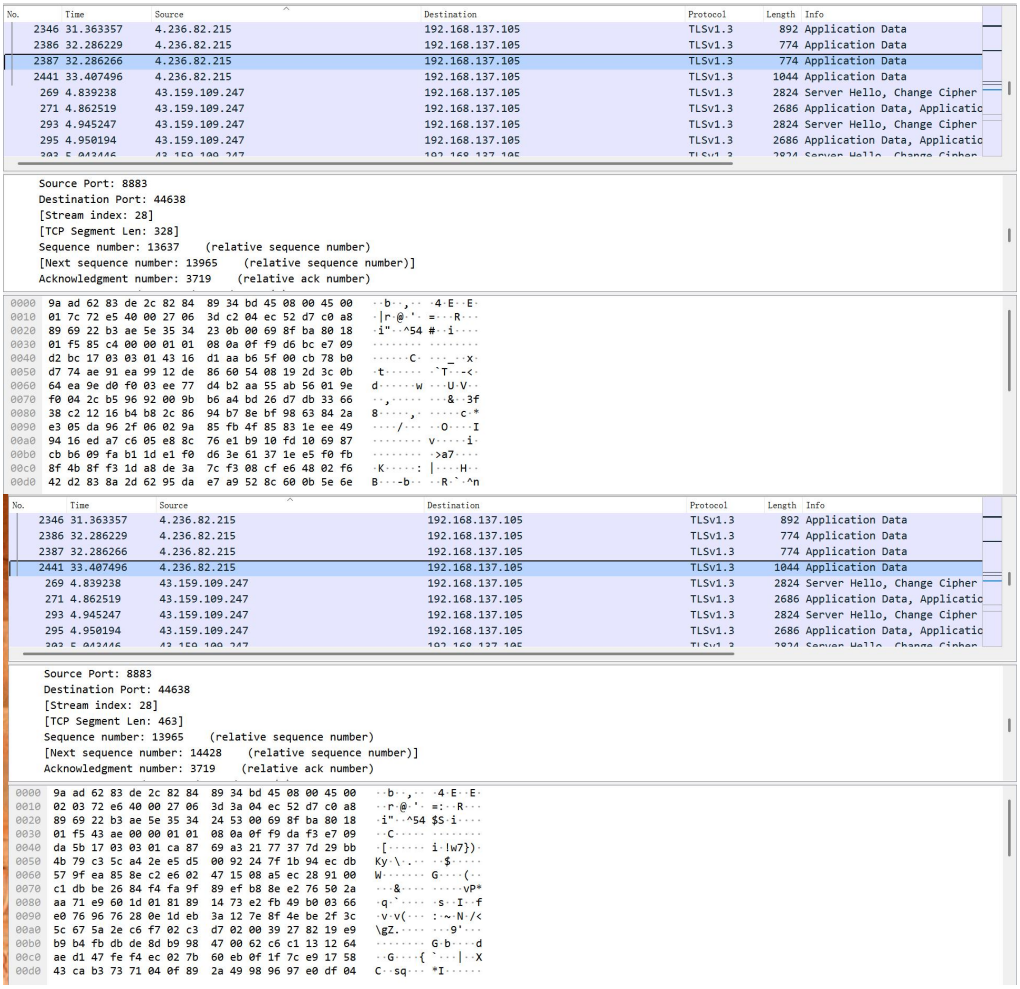
2.6 Anti-Replay

TLS provides inherent protection against replay attacks, except when 0-RTT data (optionally sent in the first flight of handshake messages) is sent in TLS 1.3.[6] The integrity-protected envelope of the message contains a monotonically increasing sequence number. Once the message integrity is verified, the sequence number of the current message is compared with the sequence number of the previous message. The sequence number of the current message must be greater than the sequence number of the previous message in order to further process the message.

Figure 34: Anti-replay mechanism for TLS

TLS use [AU.SCM-4.SeqNumb] to protect against replay attacks. Each packet in a TLS session contains a unique sequence number. Each message (including handshake messages, application data, etc.) has an incrementing sequence number, ensuring that the order of messages is unique. This mechanism ensures that even if an attacker intercepts and re-transmits a previously sent message, they cannot forge a valid session, thereby ensuring the integrity of the messages and preventing replay attacks.

As shown in the diagram below, the sequence number of the two consecutive data packets in a TLS communication increases irregularly.



No.	Time	Source	Destination	Protocol	Length	Info
2346	31.363357	4.236.82.215	192.168.137.105	TLSv1.3	892	Application Data
2386	32.286229	4.236.82.215	192.168.137.105	TLSv1.3	774	Application Data
2387	32.286266	4.236.82.215	192.168.137.105	TLSv1.3	774	Application Data
2441	33.407496	4.236.82.215	192.168.137.105	TLSv1.3	1044	Application Data
269	4.839238	43.159.109.247	192.168.137.105	TLSv1.3	2824	Server Hello, Change Cipher
271	4.862519	43.159.109.247	192.168.137.105	TLSv1.3	2686	Application Data, Applicatic
293	4.945247	43.159.109.247	192.168.137.105	TLSv1.3	2824	Server Hello, Change Cipher
295	4.950194	43.159.109.247	192.168.137.105	TLSv1.3	2686	Application Data, Applicatic

```
Source Port: 8883
Destination Port: 44638
[Stream index: 28]
[TCP Segment Len: 328]
Sequence number: 13637    (relative sequence number)
[Next sequence number: 13965    (relative sequence number)]
Acknowledgment number: 3719    (relative ack number)
```

```
0000  9a ad 62 83 de 2c 82 84  89 34 bd 45 08 00 45 00   ··b··,·· ·4·E··E·
0010  01 7c 72 e5 40 00 27 06  3d c2 04 ec 52 d7 c0 a8   ·|r·@·'· =···R···
0020  89 69 22 b3 ae 5e 35 34  23 0b 00 69 8f ba 80 18   ·i"··^54 #··i····
0030  01 f5 85 c4 00 00 01 01  08 0a 0f f9 d6 bc e7 09   ········ ········
0040  d2 bc 17 03 03 01 43 16  d1 aa b6 5f 00 cb 78 b0   ·····C· ···_··x·
0050  d7 74 ae 91 ea 99 12 de  86 60 54 08 19 2d 3c 0b   ·t····· ·`T··-<·
0060  64 ea 9e d0 f0 03 ee 77  d4 b2 aa 55 ab 56 01 9e   d·····w ···U·V··
0070  f0 04 2c b5 96 92 00 9b  b6 a4 bd 26 d7 db 33 66   ··,····· ···&··3f
0080  38 c2 12 16 b4 b8 2c 86  94 b7 8e bf 98 63 84 2a   8·····,· ·····c·*
0090  e3 05 da 96 2f 06 02 9a  85 fb 4f 85 83 1e ee 49   ····/··· ··O····I
00a0  94 16 ed a7 c6 05 e8 8c  76 e1 b9 10 fd 10 69 87   ········ v·····i·
00b0  cb b6 09 fa b1 1d e1 f0  d6 3e 61 37 1e e5 f0 fb   ········ ·>a7····
00c0  8f 4b 8f f3 1d a8 de 3a  7c f3 08 cf e6 48 02 f6   ·K·····: |····H··
00d0  42 d2 83 8a 2d 62 95 da  e7 a9 52 8c 60 0b 5e 6e   B···-b·· ··R·`·^n
```


No.	Time	Source	Destination	Protocol	Length	Info
2346	31.363357	4.236.82.215	192.168.137.105	TLSv1.3	892	Application Data
2386	32.286229	4.236.82.215	192.168.137.105	TLSv1.3	774	Application Data
2387	32.286266	4.236.82.215	192.168.137.105	TLSv1.3	774	Application Data
2441	33.407496	4.236.82.215	192.168.137.105	TLSv1.3	1044	Application Data
269	4.839238	43.159.109.247	192.168.137.105	TLSv1.3	2824	Server Hello, Change Cipher
271	4.862519	43.159.109.247	192.168.137.105	TLSv1.3	2686	Application Data, Applicatic
293	4.945247	43.159.109.247	192.168.137.105	TLSv1.3	2824	Server Hello, Change Cipher
295	4.950194	43.159.109.247	192.168.137.105	TLSv1.3	2686	Application Data, Applicatic

```
Source Port: 8883
Destination Port: 44638
[Stream index: 28]
[TCP Segment Len: 463]
Sequence number: 13965    (relative sequence number)
[Next sequence number: 14428    (relative sequence number)]
Acknowledgment number: 3719    (relative ack number)
```

```
0000  9a ad 62 83 de 2c 82 84  89 34 bd 45 08 00 45 00   ··b··,·· ·4·E··E·
0010  02 03 72 e6 40 00 27 06  3d 3a 04 ec 52 d7 c0 a8   ··r·@·'· =:··R···
0020  89 69 22 b3 ae 5e 35 34  24 53 00 69 8f ba 80 18   ·i"··^54 $S·i····
0030  01 f5 43 ae 00 00 01 01  08 0a 0f f9 da f3 e7 09   ··C····· ········
0040  da 5b 17 03 03 01 ca 87  69 a3 21 77 37 7d 29 bb   ·[····· i·!w7})·
0050  4b 79 c3 5c a4 2e e5 d5  00 92 24 7f 1b 94 ec db   Ky·\···· ··$·····
0060  57 9f ea 85 8e c2 e6 02  47 15 08 a5 ec 28 91 00   W····· G····(··
0070  c1 db be 26 84 f4 fa 9f  89 ef b8 8e e2 76 50 2a   ···&···· ·····vP*
0080  aa 71 e9 60 1d 01 81 89  14 73 e2 fb 49 b0 03 66   ·q·`···· ·s··I··f
0090  e0 76 96 76 28 0e 1d eb  3a 12 7e 8f 4e be 2f 3c   ·v·v(··· :·~·N·/<
00a0  5c 67 5a 2e c6 f7 02 c3  d7 02 00 39 27 82 19 e9   \gZ.···· ···9'···
00b0  b9 b4 fb db de 8d b9 98  47 00 62 c6 c1 13 12 64   ········ G·b····d
00c0  ae d1 47 fe f4 ec 02 7b  60 eb 0f 1f 7c e9 17 58   ··G····{ `···|··X
00d0  43 ca b3 73 71 04 0f 89  2a 49 98 96 97 e0 df 04   C··sq··· *I·····
```

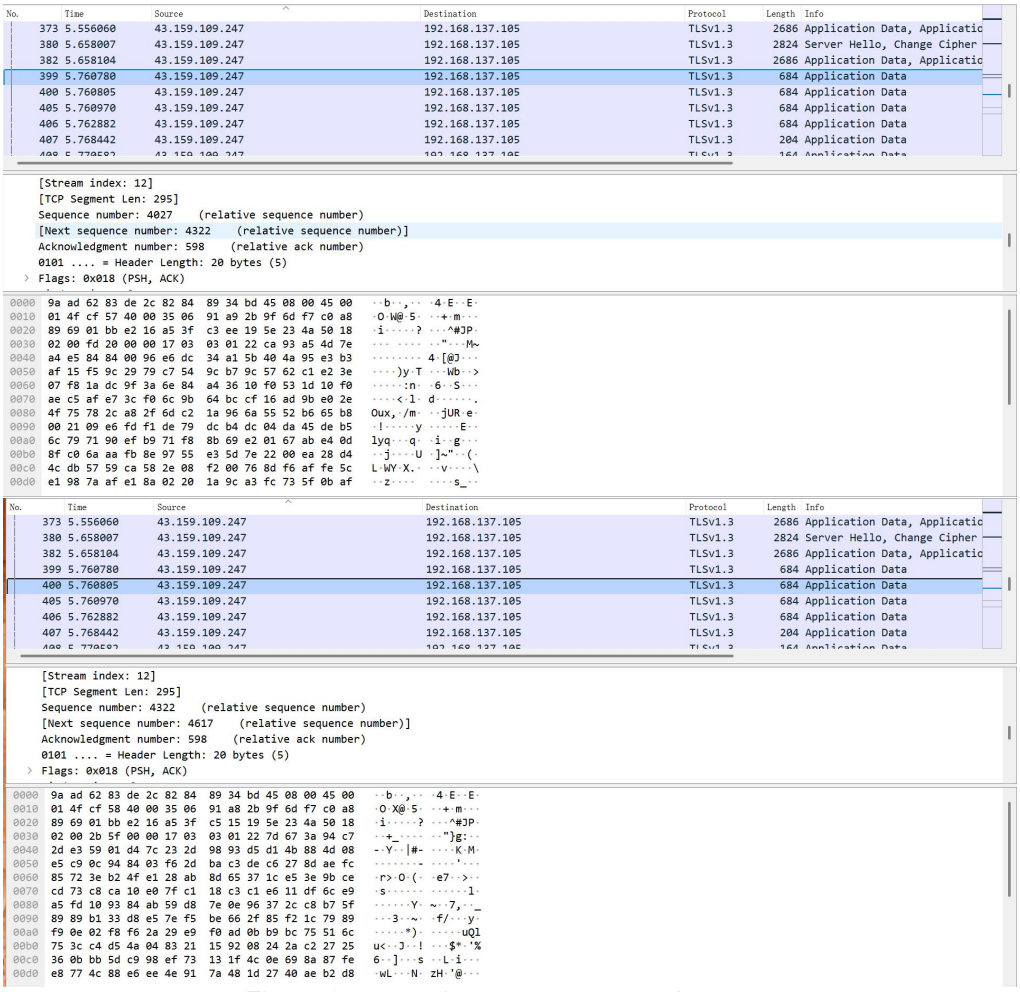


Figure 35: unique sequence number

TLS anti-replay mechanism belongs to [AU.SCM-4.SeqNumb], which uses a sequence number to prevent replay attacks, thereby ensuring that incoming messages with a repeating sequence number are not accepted.

Therefore, TL identified this as **PASS** because [SCM-1-TLSv1.2] and [SCM-2-HTTP with encrypted data]can effectively prevent replay attacks.

RESULT:	PASS

3.6 Resilience mechanism

3.6.1 RLM-1: Applicability and appropriateness of resilience mechanisms

Results

According to E.Info.RLM and E.Info.DT.RLM-1,

DUT is a terminal and is generally used in a local area network, protected by other network devices such as routers based on network interfaces where other devices in the network provide sufficient protection against DoS attacks and loss of essential functions for network operations.

The figure below illustrates the DoS attack on [Interface-1 Bluetooth]. TL attempted to launch a DoS attack on the device and observed whether the DUT could recover normal functionality after the attack ended.

```
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
[+] Packet sent to FC:01:2C:FB:71:46 -- Packet size: 600 -- Attack type: 1
```

Figure 36: BLE DoS attack

For [Interface-1 Bluetooth], TL attempted a DoS attack. During TL's testing, it was found that the device's remote control became temporarily unavailable under the attack. However, once the DoS attack ended, the device returned to its normal state.

Therefore, the verdict of this conceptional test is **PASS** since the resilience mechanism is implemented as documented in **E.Info.RLM**.

RESULT:	**PASS**

3.7 Network monitoring mechanism

3.7.1 NMM-1: Applicability and appropriateness of network monitoring mechanisms

Conceptual assessment results

The device is not a network equipment.

RESULT:	**NA**

Functional completeness assessment result

The device is not a network equipment.

RESULT:	**NA**

Functional sufficiency assessment result

The device is not a network equipment.

RESULT:	NA

3.8 Traffic control mechanism

3.8.1 TCM-1: Applicability of and appropriate traffic control mechanisms

Conceptual assessment results

The device is not a network equipment.

RESULT:	NA

Functional completeness assessment result

The device is not a network equipment.

RESULT:	NA

Functional sufficiency assessment result

The device is not a network equipment.

RESULT:	NA

3.9 Confidential cryptographic keys

3.9.1 CCK-1: Appropriate CCKs

Conceptual assessment results

Identifier	CCK-1 TLS_AES_256_GCM_SHA384		
Decision Node	Decision [E.Doc.DT.CCK-1]		Justification [E.Doc.DT.CCK-1]
DT. CCK -1.DN-1	Yes	No [x]	It doesn't have deviation under the terms of ACM or AUM or SCM or SUM or SSM.
DT. CCK -1.DN-2	Yes [x]	No	TLS_AES_256_GCM_SHA384 is used during the TLS handshake, the session key is generated with the key length of 128 bit, and the strength is more than 112 bits.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.CCK-1** ends with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional completeness assessment

According to [**E.Doc.CCK**] and [**E.Info.DT.CCK-1**],

For each confidential cryptographic key (preinstalled or generated during usage):

- [CCK-1]: Confidential cryptographic key used for secure communication mechanism [Secure communication-1], The communication is encrypted with a dynamically generated AES_256_GCM key by the equipment and the security strength is 128-bits which is more than minimum strength 112-bits.

The verdict **PASS** for the assessment case is assigned because of all CCKs found are documented in [E.Info.CCK-1.CCK].

RESULT:	PASS

Functional sufficiency assessment

According to **E.Doc.CCK**,

The cryptographic algorithm AES_256_GCM, it is admitted in sogis.eu and the security strength referring in “NIST SP 800-57” is larger than 112 bits.

Figure below shows AES_256_GCM is agreed by sogis.eu and its security strength is 128 bits, which is larger than 112 bits.

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	
Triple-DES FIPS46-3 ISO18033-3	k = 168 bits	L[2027]	2-SmallBlocksize
	k = 112 bits	L [2024]	2-SmallBlocksize 3-TripleDES2key

Figure 37: Agreed AES

Table 2: Comparable strengths

Bits of security	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA[18]	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

Figure 38: Security Strength

The device uses the TLS_AES_256_GCM_SHA384 cipher suite, with a key of AES_256_GCM. According to sogis comparable strengths, the security strength of AES-256 is 128 bits, which is larger than 112 bits.

Therefore, TL has assigned this verdict PASS because the strength of AES-256 is larger than 112 bits.

RESULT:	PASS

3.9.2 CCK-2: CCK generation mechanisms

Conceptual assessment results

According to the questionnaire **E.Doc.CCK** and **E.Info.DT.CCK-2**,

[CCK-1 TLS_AES_256_GCM_SHA384] is generated by ECDHE.

ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) is an elliptic curve-based ephemeral key exchange protocol used to securely generate a shared key between a client and a server. During this process, both the client and the server generate a pair of elliptic curve public and private keys and exchange their public keys. Using the Diffie-Hellman algorithm, both parties calculate the same shared secret using the other party's public key and their own private key. This shared secret, combined with the client and server random numbers in the TLS protocol, generates the pre-master secret. The pre-master secret is then converted into symmetric encryption keys using a key derivation function (KDF) to encrypt the communication data.

Besides, according to **SCM-2** under Art. D, TL has captured the key exchange package, verified that DUT and server will share the public keys to generate the secret key.

Therefore, the verdict of this conceptual test is **PASS** because at least one path in the decision tree [E.Doc.DT.CCK-2]ends with PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

3.9.3 CCK-3: Preventing static default values for preinstalled CCKs

Conceptual assessment results

According to [**E.Doc.CCK**] and [**E.Info.DT.CCK-3**],

There is no preinstalled CCK on equipment.

The verdict **NOT APPLICABLE** for the assessment case is assigned.

RESULT:	NA

Functional completeness assessment result

According to [**E.Doc.CCK**] and [**E.Info.DT.CCK-3**],

There is no preinstalled CCK on equipment.

The verdict **NOT APPLICABLE** for the assessment case is assigned.

RESULT:	NA

Functional sufficiency assessment result

According to [**E.Doc.CCK**] and [**E.Info.DT.CCK-3**],

There is no preinstalled CCK on equipment.

The verdict **NOT APPLICABLE** for the assessment case is assigned.

RESULT:	NA

3.10 General equipment capabilities

3.10.1 GEC-1: Up-to-date software and hardware with no publicly known exploitable vulnerabilities

Conceptual assessment results

Identifier	Software-1 Firmware		
Decision Node	Decision [E.Doc.DT.GEC-1]		Justification [E.Doc.DT.GEC-1]
DT.GEC-1.DN-1	Yes	No [x]	[Software-1 Firmware] does not contain any publicly known exploitable vulnerabilities.
Verdict	**Pass**		

Functional assessment result

According to E.Doc.DT.GEC-1, TL uses Blackduck to scan the publicly known exploitable vulnerabilities for software and no publicly known exploitation vulnerabilities exist.

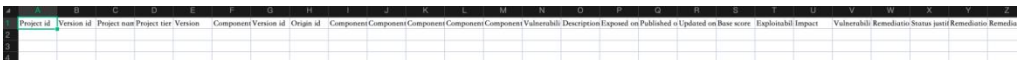


Figure 39: Result of Blackduck Scanning result

The verdict is **PASS** because no publicly known exploitable vulnerabilities exist.

RESULT:	PASS

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

Conceptual assessment results

Identifier	Interface-1 Bluetooth Interface-2 WLAN		
Decision Node	Decision [E.Doc.DT.GEC-2]		Justification [E.Doc.DT.GEC-2]
DT.GEC-2.DN-1	Yes [x]	No	The interface is available in the factory default state.
DT.GEC-2.DN-2	Yes [x]	No	It will affect the security assets and network assets.
DT.GEC-2.DN-3	Yes [x]	No	WLAN is used for network connection. Bluetooth is used for broadcasting devices to connect to APP. They are necessary for equipment setup and basic operation.
Verdict	**PASS**		

Functional completeness assessment

The figure below shows the scanning result of nmap. It can be seen that no opened ports are detected. Filtered ports are not considered as open ports.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo nmap -sT -p- -T5 --max-retries 0 --min-rate 2000 192.168.8.137
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-17 16:50 CST
Warning: 192.168.8.137 giving up on port because retransmission cap hit (0).
Nmap scan report for ecoflow.lan (192.168.8.137)
Host is up (0.15s latency).
All 65535 scanned ports on ecoflow.lan (192.168.8.137) are in ignored states.
Not shown: 65489 filtered tcp ports (no-response), 46 closed tcp ports (conn-refused)
MAC Address: FC:01:2C:FB:71:44 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 33.12 seconds
```

Figure 40: *TCP port scan results*

TL scanned the UDP ports and It can be seen that no opened ports are detected. Filtered ports are not considered as open ports.

```
Nmap scan report for ecoflow.lan (192.168.8.137)
Host is up (0.36s latency).
All 65535 scanned ports on ecoflow.lan (192.168.8.137) are in ignored states.
Not shown: 65418 open|filtered udp ports (no-response), 117 closed udp ports (port-unreach)
MAC Address: FC:01:2C:FB:71:44 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 33.34 seconds
```

Figure 41: *UDP port scan results*

The figure below shows the service of Bluetooth exposed in the DUT. The equipment supports only BLE during the initialization and pairing phase. After pairing is complete, it is used to transmit control functions.

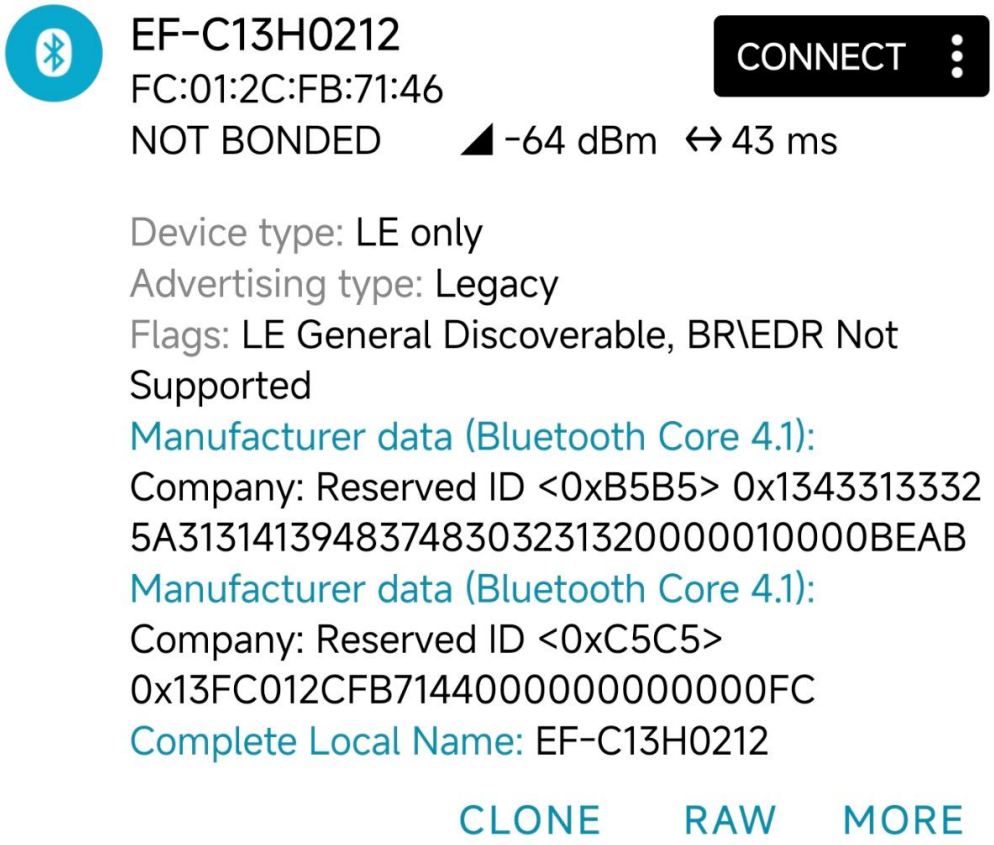


Figure 42: Bluetooth services exposed in the DUT

In the factory default state, all additional network interfaces or services are listed in [E.Info.GEC-2.NetworkInterface.Exposure] and are necessary for the device's setup or basic operation.

No other network interfaces or exposed services required for setup or basic operation are exposed.

The verdict is **PASS** because all discovered network interfaces or services in the factory default state are listed in [E.Info.GEC-2.NetworkInterface.Exposure] and are used for the device's setup or basic operations.

RESULT:	PASS

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

Conceptual assessment results

According to the **E.Doc.GEC** and **E.Info.DT.GEC-3**, there is no optional network interfaces is configurable.

Therefore, the verdict of this conceptional test is **NA** because there is no one path in the decision tree **E.Info.DT.GEC-3** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	NA

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

Conceptual assessment results

According to the questionnaire E.Doc.GEC and E.Info.DT.GEC-4,

For the network interface and exposed service:

- Bluetooth: It is documented in the APP.
- Wi-Fi: It is documented in the APP Operation Steps section in the user manual.

These network interfaces and exposed service are documented in the User Manual and related user documentation.

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.GEC-4** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional assessment results

According to the questionnaire **E.Doc.GEC** and **E.Info.DT.GEC-4**,

All of the network interfaces and services are documented in the specification section in the user manual or related documentation.

The figure below shows the reminder in the app regarding Bluetooth exposed in factory default state, indicating that Bluetooth needs to be enabled during the operation process.

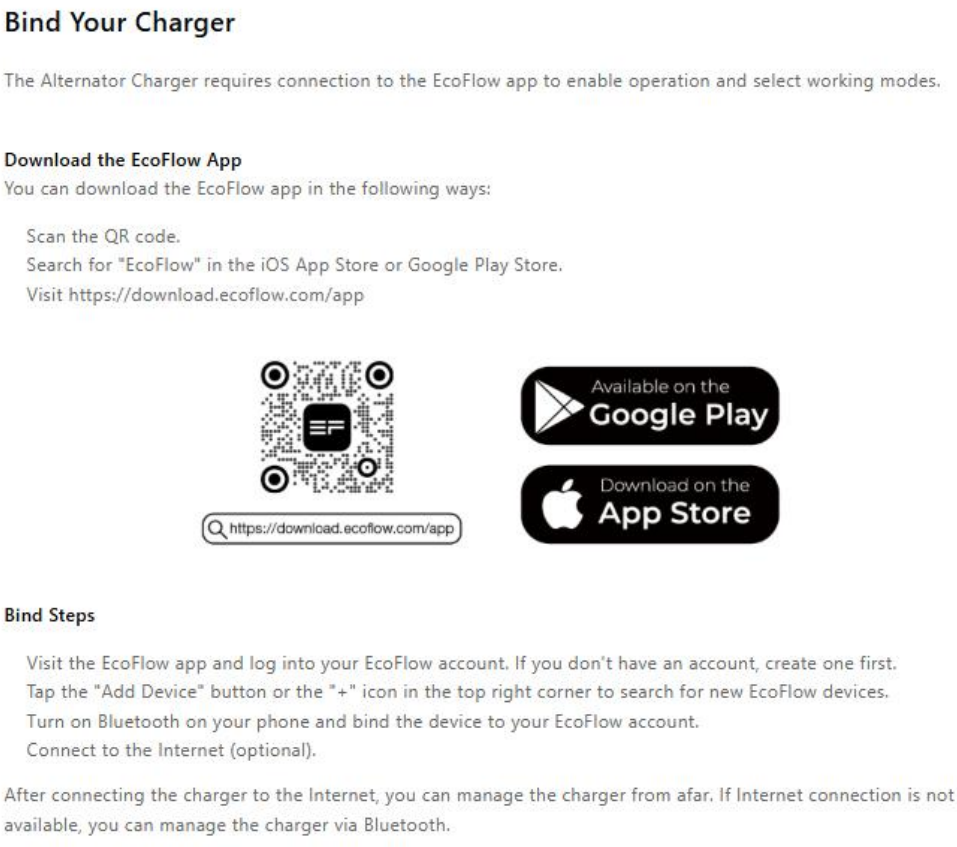


Figure 43: Documentation of Bluetooth

The figure below is the description of Wi-Fi in the user manual. The user manual states that [Interface-2 WLAN], as the interface for connecting to 2.4GHz Wi-Fi, is exposed in the factory default setting.

Specifications

Model	EF-AC-001
Net Weight	Approximately 1.7 kg
Dimensions (W × D × H)	276×187×38 mm
Wi-Fi	Supported
Bluetooth	Supported
Charge Mode	ALT IN Port Input: 12/24V⎓(11-31V⎓), 75A Max BATTERY Port Output: 24V⎓/40-60V⎓, 20A Max, 1000W Max
Battery Maintenance Mode	BATTERY Port Input: 40-60V⎓, 3A Max ALT IN Port Output: 13.8/27.6V⎓, 100W Max
Reverse Charge Mode	BATTERY Port Input: 40-60V⎓, 20A Max ALT IN Port Output: 13.8/27.6V⎓, 75A Max
Rated Current of Fuse	125A
Protection Type	Reverse polarity protection/Overcurrent protection/Short circuit protection/Overvoltage and undervoltage protection (Provided with integral protection against overloads)
Operating Temperature	–10°C to 45°C (14°F to 113°F)
Storage Temperature	–30°C to 70°C (–22°F to 158°F)
Operating Humidity	≤95%
Storage Humidity	≤95%
SOLAR Port Input	48V⎓(11-60V⎓), 15A Max, 300W Max

Figure 44: Documentation of Wi-Fi

In conclusion, all network interfaces and services exposed via network interfaces have been confirmed by TL and are documented in the user documentation.

The verdict is **PASS** for the assessment case because all network interfaces or exposed services (via network interfaces) in factory default state found are documented in [E.Info.GEC 4.NetworkInterface.Exposure].

RESULT:	PASS

3.10.5 GEC-5: No unnecessary external interfaces

Conceptual assessment results

Identifier	Interface-4 UART port		
Decision Node	Decision [E.Doc.DT.GEC-5]		Justification [E.Doc.DT.GEC-5]
DT.GEC-5.DN-1	Yes [x]	No	The physical external interface is necessary, and it is closed in the production line.
Verdict	**Pass**		

Identifier	Interface-3-Physical Button Interface-5-Charging ports		
Decision Node	Decision [E.Doc.DT.GEC-5]		Justification [E.Doc.DT.GEC-5]
DT.GEC-5.DN-1	Yes [x]	No	Physical Button is used to reset the device or enter the device into the set-up mode. It is necessary for the intended functionality. Charging ports is used to charging for DUT and does not used for receiving data.
Verdict	**Pass**		

Therefore, the verdict of this conceptional test is **PASS** because at least one path in the decision tree **E.Info.DT.GEC-3** end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Functional assessment results

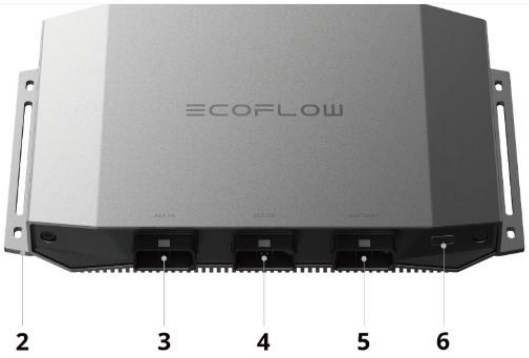
Figure below shows [Interface-3 Physical button], which is used for basic operations such as opening, closing, resetting.

Figure 45: Physical button and Charging port

The USB interfaces are not used for data transfer. Two USB-A ports and the USB-C port serve solely as power outputs.

1	**LED Indicators**	Displays the product's operating status.
2	**Mounting Holes**	Used to securely mount the product.
3	**ALT IN Port**	Connects to the car battery via the input cable.
4	**SOLAR Port**	Photovoltaic input port; connects to solar panels via the solar cable.
5	**BATTERY Port**	Connects to an EcoFlow portable power station via the output cable.
6	**Main Power Control Button**	**Power On/Off**: Press the button once to turn on the power station. Long press the button for 2 seconds to turn it off. **Reset IoT** : When powered off, press and hold for 5 seconds to reset Bluetooth and Wi-Fi connections.

Figure 46: *Appearance of charging port in user manual*



1	**LED Indicators**	Displays the product's operating status.
2	**Mounting Holes**	Used to securely mount the product.
3	**ALT IN Port**	Connects to the car battery via the input cable.
4	**SOLAR Port**	Photovoltaic input port; connects to solar panels via the solar cable.
5	**BATTERY Port**	Connects to an EcoFlow portable power station via the output cable.
6	**Main Power Control Button**	**Power On/Off**: Press the button once to turn on the power station. Long press the button for 2 seconds to turn it off. **Reset IoT** : When powered off, press and hold for 5 seconds to reset Bluetooth and Wi-Fi connections.

Figure 47: Appearance of charging port in user manual

TL reviewed all external interfaces of the device and checked the relevant documentation, and found that all external interfaces have been recorded in the user manual.

The verdict is **PASS** because all of the physical external interfaces have been documented in [E.Info.GEC-5.PhysicalExternalInterface].

RESULT:	PASS

3.10.6 GEC-6: Input validation

Conceptual assessment results

Identifier	Interface-1 Bluetooth Interface-2 WLAN		
Decision Node	Decision [E.Doc.DT.GEC-6]		Justification [E.Doc.DT.GEC-6]
DT.GEC-6.DN-1	Yes [x]	No	Interfaces above are used for communication.
DT.GEC-6.DN-2	Yes [x]	No	The DUT uses input validation functionality for inputs that may potentially affect security assets and/or network assets.
Verdict	**Pass**		

Therefore, the verdict of this test is PASS because at least one path in the decision tree E.Info.DT.AUM-3 end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	PASS

Functional assessment results

TL performed input validation test on the DUT's [Interface-2 WLAN], as shown in the diagram below. According to TL's observations, the test had no impact on the DUT. It was found that the DUT effectively resists and defends against fuzzing attacks, with no impact observed on the DUT.

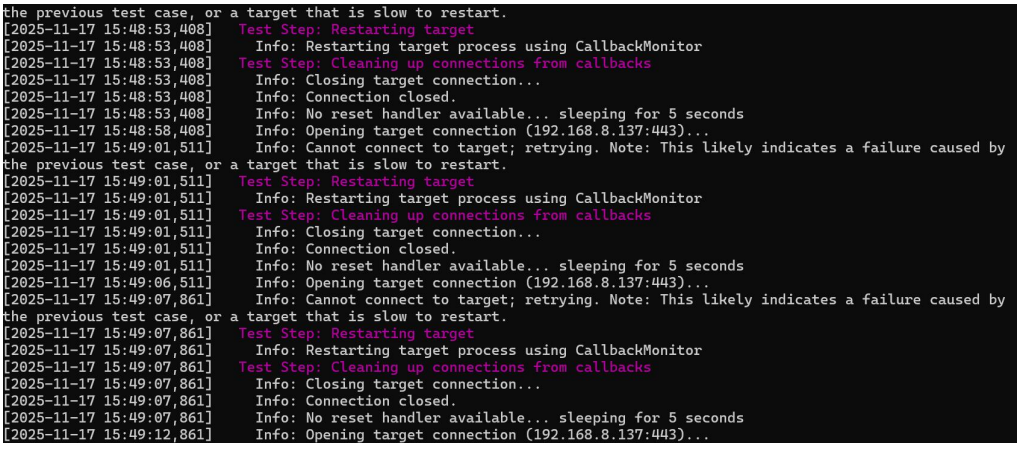


Figure 48: *Tcp Fuzzing test*

Test results shows that the fuzzing attacks had no impact on the DUT. The device can effectively withstand fuzzing attacks targeting [Interface-2 WLAN].

Figure below shows TL performed Bluetooth fuzzing on [Interface-1 Bluetooth] using a fuzzing script. This tool targets the Bluetooth protocol stack, specifically fuzzing the connection establishment process by generating malformed control packets, invalid link setup sequences, and unexpected protocol messages.

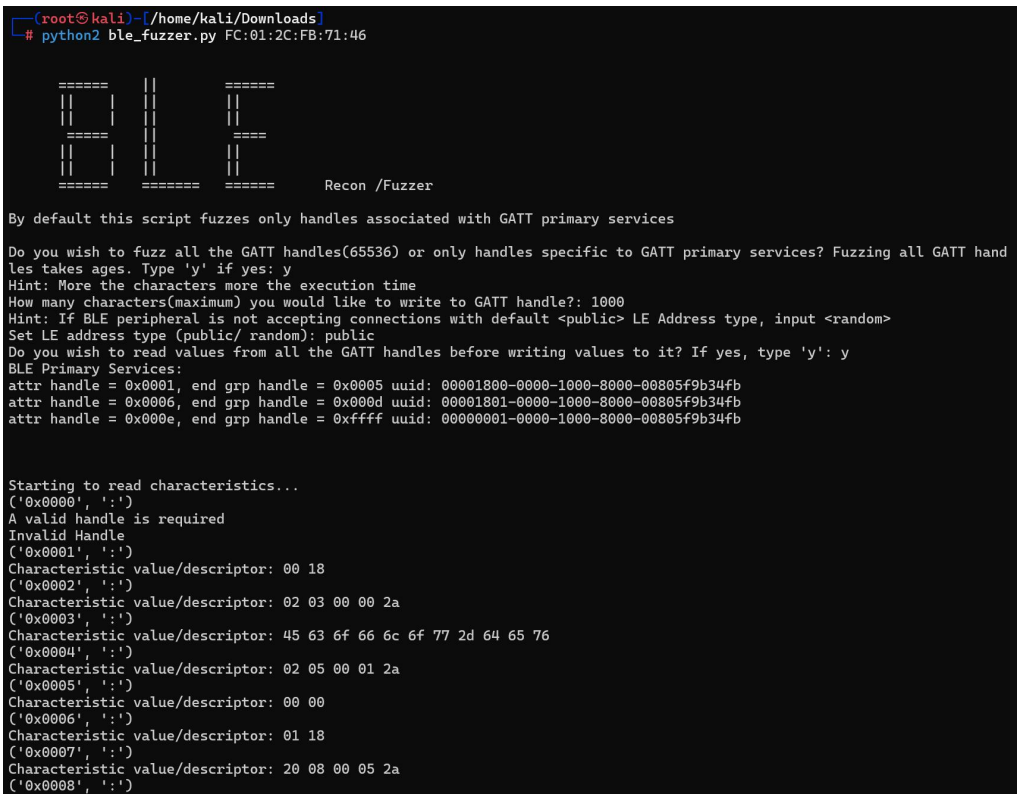


Figure 49: Fuzzing package toward BLE

The test results demonstrated that the fuzzing attacks had no impact on the DUT. The DUT implements input validation mechanisms for inputs that may potentially affect security assets and/or network assets, effectively mitigating risks associated with malformed or unexpected inputs.

The verdict is **PASS** because the input validation testing was not corrupt,extract or misuse the security assets and network assets.

RESULT:	**PASS**

3.11 Cryptography

3.11.1 CRY-1: Best practice Cryptography

Results

Identifier	CRY-1 TLS_AES_256_GCM_SHA384		
Decision Node	Decision [E.Doc.DT.GEC-5]		Justification [E.Doc.DT.GEC-5]
DT.CRY-1.DN-1	Yes	No [x]	It doesn't have deviation under the terms of ACM or AUM or SCM or SUM or SSM.
DT.CRY-1.DN-2	Yes [x]	No	TLS_AES_256_GCM_SHA384 is used during the TLS handshake. It is the best practise concerning the protection of the security assets and network assets.
Verdict	**Pass**		

TLS code	Cipher Suite	R/L	Notes
TLS v1.3 Cipher Suite			
0x1302	TLS_AES_256_GCM_SHA384	R	
0x1301	TLS_AES_128_GCM_SHA256	R	
0x1304	TLS_AES_128_CCM_SHA256	R	
TLS v1.2 Cipher Suite			
0xC02C	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	R	
0xC02B	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	R	
0xC0AD	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	R	
0xC0AC	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	R	
0xC024	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	L[2025]	46-TLSEncryptThenMAC
0xC023	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	L[2025]	46-TLSEncryptThenMAC
0xC028	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	L[2025]	46-TLSEncryptThenMAC
0xC027	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	L[2025]	46-TLSEncryptThenMAC
0xC030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	L	
0xC02F	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	L	
0x009F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	L	47-TLSDHE
0x009E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	L	47-TLSDHE
0xC09F	TLS_DHE_RSA_WITH_AES_256_CCM	L	47-TLSDHE
0xC09E	TLS_DHE_RSA_WITH_AES_128_CCM	L	47-TLSDHE
0x006B	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	L[2025]	47-TLSDHE,46-TLSEncryptThenMAC
0x0067	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	L[2025]	47-TLSDHE,46-TLSEncryptThenMAC
0x009D	TLS_RSA_WITH_AES_256_GCM_SHA384	L	48-TLSRSA
0x009C	TLS_RSA_WITH_AES_128_GCM_SHA256	L	48-TLSRSA
0xC09D	TLS_RSA_WITH_AES_256_CCM	L	48-TLSRSA
0xC09C	TLS_RSA_WITH_AES_128_CCM	L	48-TLSRSA
0x003D	TLS_RSA_WITH_AES_256_CBC_SHA256	L[2025]	48-TLSRSA,46-TLSEncryptThenMAC
0x003C	TLS_RSA_WITH_AES_128_CBC_SHA256	L[2025]	48-TLSRSA,46-TLSEncryptThenMAC

Figure 50: TLS_AES_256_GCM_SHA384 agreed by SOGIS

It can be seen that TLS_AES_256_GCM_SHA384 is evaluated by SOGIS as a legacy cipher suite. Nevertheless, its implementation is still regarded as consistent with recognized best practices in the current security context.

Therefore, the verdict of this test is **PASS** because at least one path in the decision tree E.Info.DT.CRY-1 end with one PASS leave; and no path ends with FAIL leave, also the justifications in the decision tree is rational and valid.

RESULT:	**PASS**

Appendix B: Photographs

Figure 1: Front view

Figure 2: Back view

Figure 3: Top view

Figure 4: Bottom view

---end of report---