EN 18031-2

Test_Report

For

MiTag

MODEL NUMBER: HD-P16

ISSUE DATE: 2025/06/30

Prepared by

Guangdong Global Testing Technology Co., Ltd.

Room 101-105, 203-210, Building 1, No.2, Keji 8 Road, Songshan Lake Park, Dongguan city, Guangdong, People's Republic of China, 523808

Revision History

Rev.	Issue Date	Revisions	Revised By
V0	June 30, 2025	Initial Issue	Angda

Summary of Test Results

Requirement		Results
ACM	Access control mechanism	PASS
ACM-1	Applicability of access control mechanisms	PASS
ACM-2	Appropriate access control mechanisms	PASS
ACM-3	Default access control for children in toys	N/A
ACM-4	Default access control to children's privacy assets for toys and childcare equipment	N/A
ACM-5	Parental/Guardian access controls for children in toys	N/A
ACM-6	Parental/Guardian access controls for other entities' access to managedchildren's privacy assets in toys	N/A
AUM	Authentication mechanism	PASS
AUM-1	Applicability of authentication mechanisms	PASS
AUM-2	Appropriate authentication mechanisms	PASS
AUM-3	Authenticator validation	PASS
AUM-4	Changing authenticator	PASS
AUM-5	password strength	N/A
AUM-6	Brute force protection	N/A
SUM	Secure update mechanism	N/A
SUM-1	Applicability of update mechanisms	N/A
SUM-2	Secure updates	N/A
SUM-3	Automated updates	N/A
SSM	Secure storage mechanism	N/A
SSM-1	Applicability of secure storage mechanisms	N/A

SSM-2	Appropriate integrity protection for secure storage mechanisms	N/A
SSM-3	Appropriate confidentiality protection for secure storage mechanisms	N/A
SCM	Secure communication mechanism	N/A
SCM-1	Applicability of secure communication mechanisms	N/A
SCM-2	Appropriate integrity and authenticity protection for secure communication mechanisms	N/A
SCM-3	Appropriate confidentiality protection for secure communication mechanisms	N/A
SCM-4	Appropriate replay protection for secure communication mechanisms	N/A
LGM	Logging mechanism	PASS
LGM-1	Applicability of logging mechanisms	PASS
LGM-2	Persistent storage of log data	N/A
LGM-3	Minimum number of persistently stored events	PASS
LGM-4	Time-related information of persistently stored log data	PASS
DLM	Deletion mechanism	PASS
DLM-1	Applicability of deletion mechanisms	PASS
UNM	User notification mechanism	PASS
UNM-1	Applicability of user notification mechanisms	PASS
UNM-2	Appropriate user notification content	PASS
CCK	Confidential cryptographic keys	PASS
CCK-1	Appropriate CCKs	PASS
CCK-2	CCK generation mechanisms	PASS
CCK-3	Preventing static default values for preinstalled CCKs	PASS
GEC	General equipment capabilities	PASS

GEC-1	Up-to-date software and hardware with NO publicly known exploitable	PASS
GEC-2	Limit exposure of services via related network interfaces	PASS
GEC-3	Configuration of optional services and the related exposed network interfaces	N/A
GEC-4	Documentation of exposed network interfaces and exposed services via network interfaces	PASS
GEC-5	NO unnecessary external interfaces	PASS
GEC-6	Input validation	N/A
GEC-7	Documentation of external sensing capabilities	N/A
CRY	Cryptography	PASS
CRY-1	Best practice cryptography	PASS

not e:

1. N/A: In this whole report not applicable.

Report directory structure

The name of the document	Description
C04A2506088200101 EN18031-2 Report	This document is the final report of EN18031-2
IXIT	This document is a stand-alone addendum document.This document is intended as evidence of a functional adequacy assessment and is primarily supplemented by a description of the device.

CONTENTS

1. ATTESTATION OF TEST RESULTS 9
2. TEST METHODOLOGY 11
3. TEST EQUIPMENT DESCRIPTION 11
3.1. Test Software 11
3.2. Test Hardware 11
4. TEST RESULTS 13
4.1. ACM 13
4.1.1. ACM-1 13
4.1.2. ACM-2 16
4.1.3. ACM-3 17
4.1.4. ACM-4 18
4.1.5. ACM-5 18
4.1.6. ACM-6 19
4.2. AUM 19
4.2.1. AUM-1 19
4.2.2. AUM-2 22
4.2.3. AUM-3 24
4.2.4. AUM-4 26
4.2.5. AUM-5 27
4.2.6. AUM-6 27
4.3. SUM 28
4.3.1. SUM-1 28
4.3.2. SUM-2 28
4.3.3. SUM-3 29
4.4. SSM 29
4.4.1. SSM-1 29

4.4.2. SSM-2 29
4.4.3. SSM-3 30
4.5. SCM 30
4.5.1. SCM-2 30
4.5.2. SCM-2 31
4.5.3. SCM-3 31
4.5.4. SCM-4 31
4.6. LGM 32
4.6.1. LGM-1 32
4.6.2. LGM-2 33
4.6.3. LGM-3 33
4.6.4. LGM-4 35
4.7. DLM 36
4.7.1. DLM-1 36
4.8. UNM 38
4.8.1. UNM-1 38
4.8.2. UNM-2 40
4.9. CCK 42
4.9.1. CCK-1 42
4.9.2. CCK-2 44
4.9.3. CCK-3 46
4.10. GEC 48
4.10.1. GEC-1 48
4.10.2. GEC-2 49
4.10.3. GEC-2 51
4.10.4. GEC-4 51
4.10.5. GEC-5 52

4.10.6. GEC-6 53
4.10.7. GEC-7 54
4.11. CRY 54
4.11.1. CRY-1 54
5. EQUIPMENT UNDER TEST 56
5.1. Product Photo 56
5.2. Photographs of The Eut 57

1. ATTESTATION OF TEST RESULTS

Applicant Information	
Company Name:	
Address:	
Manufacturer Information	
Company Name:	
Address:	
EUT Information	
Product Designation	MiLi MiTag
Product Description:	This is a Bluetooth anti-lost device that can be used with the Find My app on Apple phones and the Google Find Hub app on Android phones.
Model :	HD-P16
Brand:	MiLi
Sample Received Date:	2025/06/20
Sample Status :	Normal
Sample ID :	A25060882-1
Date of Tested:	2025/06/20-2025/06/30

APPLICABLE STANDARDS	
STANDARD	**TEST RESULTS**
EN 18031-2	**PASS**

Prepared By:

Angda Zou

Project Engineer

Check ed By:

Hardy Yuan

Laboratory Leader

Approved By:

Shawn Wen

Laboratory Manager

2. TEST METHODOLOGY

All tests were performed in accordance with the standard E N 18031-2

3. TEST EQUIPMENT DESCRIPTION

In compliance with EN18031 -2 requirements, all software and hardware used in this test have been validated and are within their operational validity periods.

3.1. Test Software

NO .	Name	Version	Type	Function	Operation system	latest acceptance verification date
1	Wireshark	v4.2.5	Packet capturing tool	Packet capture test	Kali	2025/ 4 /11
2	Nmap	v7.94SVN	Port scanning tool	Port scanning test	Kali	2025/ 4 /11
3	vmware	VMware Workstation 17 Player	Virtual Machine Management Software	Manage virtual machines	windows11	2025/ 4 /11
4	Kali Linux	v2023.4	Hacker operating system	Penetration test	vmware	2025/ 4 /11
5	Burp Suite	Community Edition v202 5.1.1	Black box tool	Web attack suite	Kali	2025/ 4 /11
6	Dirbuster	v1.0-RC1	Black box tool	Web directory scanning	Kali	2025/ 4 /11
7	OWASP ZAP	v2.15.0	Black box tool	Penetration scanning	windows11	2025/ 4 /11
8	SSLscan	v2.1.4	Black box tool	TLS/SSL certificate scanning	Kali	2025/ 4 /11
9	SQLmap	1.8.6.3	Black box tool	SQL Injection attack	Kali	2025/ 4 /11

3.2. Test Hardware

NO .	Name	Manufacturer	Model
1	Stationary PC	Lenovo	M4000q 2024
2	Gigabit Switch	TP-LINK	TL-SG1005D
3	broadband network	CHINA TELECOM	Dial-up Networking

4	Soft Routing Device	FISUSEN	wifi6-n5000-ES 8G+128G
5	zigbee wireless card	wavgat	CC2531
6	Zigbee card debugger	wavgat	CC Debugger
7	WIFI Pineapple	Hak5	WIFI Pineapple Mark VII
8	USB Ethernet converter	acer	USB3.0*3+Type
9	Zigbee burning line	wavgat	CC2531 Sniffer USB dongle Btool
1 0	Antistatic wrist strap	BAIGE	——
1 1	Test laptop	DELL	Latitude 7480
1 2	Ethernet Signal Amplifier	YANEW	——
1 3	Testing Phone	HUAWEI	nova 12

4. TEST RESULTS

Case NO.: A25060882-1	**Applicant:**
Product Name: MiLi MiTag	**Trademark:** MiLi
Model Name: HD-P16	**Serial Model Name:** HD-P16,HD-P16-1,HD-P16-2,HD-P16-3,HD-P16-6,HD-P16-8,HD-P16-10,HD-P16-A,HD-P16-B,HD-P16-C,HD-P16-D,HD-P16-E,HD-P16-F,HD-P16-L,HD-P16-P,HD-P16-S,HD-P16-T,HD-P16-W,HD-P16-X,HD-P16-Y,HD-P16-Z.
Software Version: V1.0.5	**Tested by :** Angda
Technical Specification	2.4G Bluetooth Function☑
	2.4G WIFI Function☐
	5G/6G/7G WIFI Function☐
Operating temperature	26℃
Test location	Network Security Lab on the 2nd floor of Jianhuacan R&D Center, Keji 8th Road, Songshanhu Park, Dongguan, Guangdong

4.1. ACM

4.1.1. ACM-1

The following table - Required information for ACM-1 records the customer-provided asset materials

Types of Assessment	Evaluation Unit	describe
E.Info.ACM-1.Security Asset	Device pairing key	The authentication credentials used when the device is bound to the app
	Bluetooth broadcast signal	When the device is bound, it needs to scan via Bluetooth
E.Info.ACM-1.Privacy Asset	Device location data	The device's latitude and longitude geographic location information

Table - Required information for ACM-1

4.1.1.1. Conceptual assessment

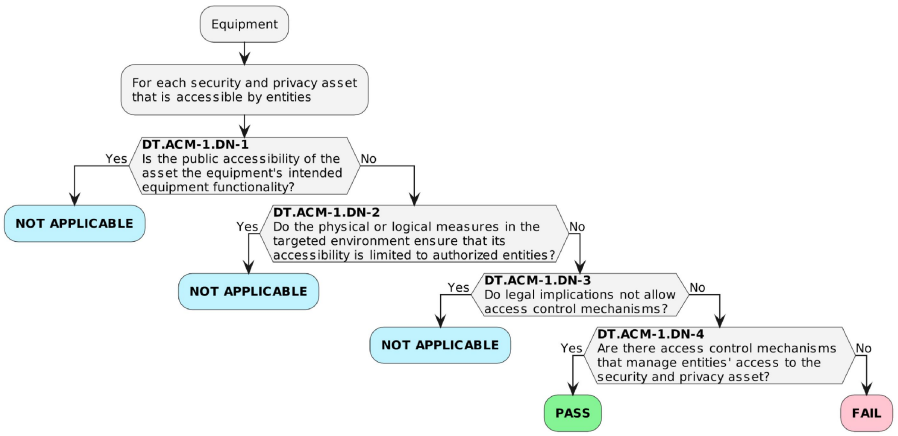

Figure - Decision tree for requirement ACM-1

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
ACM-1	1	DT.ACM-1.DN-1	Is the public accessibility of the asset the equipment's intended equipment functionality?	NO	Refer to 6.1.1.4.3 of EN18031-2 regulation. When public accessibility is the intended function of the test object, it is an exception and no access control is required. Otherwise, pass the next node.
	2	DT.ACM-1.DN-2	Do the physical or logical measures in the targeted environment ensure that its accessibility is limited to authorized entities?	NO	Refer to 6.1.1.4.3 of EN18031-2. When the environment or logical measures in the operating environment of the test object limit the accessibility of the authorized entity to it, it is an exception and no access control is required. Otherwise, the next node is passed.
	3	DT.ACM-1.DN - 3	Do legal implications not allow Access control mechanisms?	NO	Refer to 6.1.1.4.3 of EN18031-2. When the law does not allow the test object to implement an access control mechanism, it is an

					exception and no access control mechanism is required. Otherwise, go to the next node.
	4	DT.ACM-1.DN - 4	Are there access controls mechanisms that manage entities ' access to the security and privacy asset?	YES	Refer to 6.1.1.4.3 of EN18031-2 regulation. When the test object does not fall into the exception, the access control mechanism should be used to manage the entity's access to the test object. If so, the concept assessment is passed. Otherwise, it fails.

Table - Conceptual assessment for ACM-1

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Device pairing key	PASS
Bluetooth broadcast signal	NOT APPLICABLE
Device location data	PASS

4.1.1.2. Functional completeness assessment

Types of Assessment	Evaluation Unit	Is it recorded in Table - ACM-1.Asset middle	Compliance Conclusion
E.Info.ACM-1.Security Asset	Device pairing key	√	PASS
E.Info.ACM-1.Privacy Asset	Device location data	√	PASS

Table - Functional completeness assessment for ACM-1

4.1.1.3. Functional sufficiency assessment

Types of Assessment	Evaluation Unit	Expected Results
E.Info.ACM-1.Security Asset	Device pairing key	The user physically touches the device to start pairing mode, the app starts Bluetooth scanning, and the binding is successful after authorization. The private key is stored in the Secure

		Enclave, and the public key is uploaded to iCloud
E.Info.ACM-1.Privacy Asset	Device location data	Only authorized users can decrypt location data, and third parties cannot obtain user location

Continued from the table above

Actual Results	Compliance Conclusion	Supporting materials
Same as expected	PASS	Refer to IXIT1-ACM 1-1
Same as expected	PASS	Refer to IXIT1-ACM 1-2

Table - Functional sufficiency assessment for ACM-1

4.1.2. ACM-2

4.1.2.1. Conceptual assessment

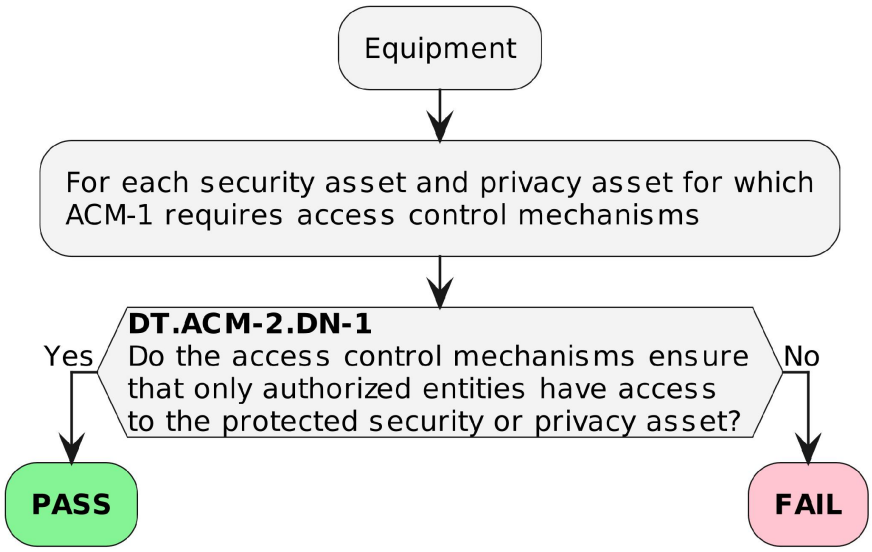

Figure - Decision tree for requirement ACM-2

Standard Terms	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
ACM-2	DT.ACM - 2.DN-1	Do the access control mechanisms ensure that only authorized entities	YES	Refer to 6.1.2.4.3 of EN18031-2 regulation . If the test object is only accessible to

		have access to the protected security asset?		authorized entities, it passes the concept assessment. Otherwise, it fails.

Table - Conceptual assessment for ACM-2

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Device pairing key	PASS
Device location data	PASS

4.1.2.2. Functional completeness assessment

According to EN18031-2 clause 6.1.2.4.5, please refer to Functional sufficiency assessment.

4.1.2.3. Functional sufficiency assessment

Types of Assessment	Evaluation Unit	Expected Results
E.Info.ACM-1.Security Asset	Device pairing key	Once the device owner has bound the device, when the device is unbound by an unauthorized user, other users cannot bind the device again. In addition, the pairing key is only available to the bound user and cannot be used by a third party.
E.Info.ACM - 1.Privacy Asset	Device location data	Access permissions are tied to the user's Apple ID, and the approximate location of the device can be shared with the primary user's authorization.

Continued from the table above

Actual Results	Compliance Conclusion	Supporting materials
Same as expected	PASS	Refer to IXIT1-ACM 1-3
Same as expected	PASS	Refer to IXIT1-ACM 1-4

Table - Functional sufficiency assessment for ACM-2

4.1.3. ACM-3

4.1.3.1. Conceptual assessment

According to requirement 6.1.3.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-3 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a concept assessment of the ACM-3 standard.

4.1.3.2. Functional completeness assessment

According to the 6.1.3.1 requirement of EN18031-2 regulation, when the device is a children's toy, it needs to comply with the ACM-3 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional integrity assessment of the ACM-3 standard.

4.1.3.3. Functional sufficiency assessment

According to requirement 6.1.3.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-3 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional adequacy assessment of the ACM-3 standard.

4.1.4. ACM-4

4.1.4.1. Conceptual assessment

According to requirement 6.1.4.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-4 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a concept assessment of the ACM-4 standard.

4.1.4.2. Functional completeness assessment

According to the 6.1.4.1 requirement of EN18031-2 regulation, when the device is a children's toy, it needs to comply with the ACM-4 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional integrity assessment of the ACM-4 standard.

4.1.4.3. Functional sufficiency assessment

According to requirement 6.1.4.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-4 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional adequacy assessment of the ACM-4 standard.

4.1.5. ACM-5

4.1.5.1. Conceptual assessment

According to requirement 6.1.5.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-5 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a concept assessment of the ACM-5 standard.

4.1.5.2. Functional completeness assessment

According to the 6.1.5.1 requirement of EN18031-2 regulation, when the device is a children's toy, it needs to comply with the ACM-5 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional integrity assessment of

the ACM-5 standard.

4.1.5.3. Functional sufficiency assessment

According to requirement 6.1.5.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-5 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional adequacy assessment of the ACM-5 standard.

4.1.6. ACM-6

4.1.6.1. Conceptual assessment

According to requirement 6.1.6.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-6 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a concept assessment of the ACM-6 standard.

4.1.6.2. Functional completeness assessment

According to requirement 6.1.6.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-6 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional integrity assessment of the ACM-6 standard.

4.1.6.3. Functional sufficiency assessment

According to requirement 6.1.6.1 of EN18031-2, when a device is a children's toy, it needs to comply with the ACM-6 standard. However, the current device is a consumer-grade Bluetooth anti-lost device, not a children's device, so there is no need to conduct a functional adequacy assessment of the ACM-6 standard.

4.2. AUM

4.2.1. AUM-1

The following table shows the required information for AUM-1

Types of Assessment	Evaluation Unit	describe
E.Info.AUM-1-1.ACM	BLE broadcast signal	Enable Bluetooth scanning during device pairing
	Find My Network Communications	Get the precise location of the device through GPS, WiFi, and cellular networks, and finally display it in the user's APP

Table - Required information for AUM-1

4.2.1.1. Conceptual assessment

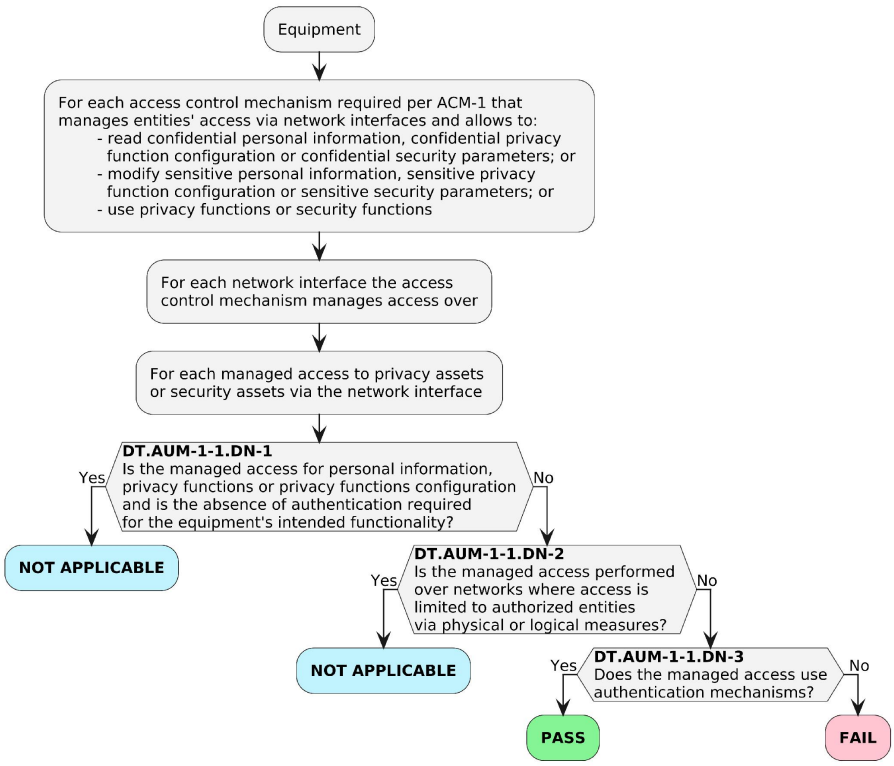

Figure - Decision tree for requirement AUM-1-1

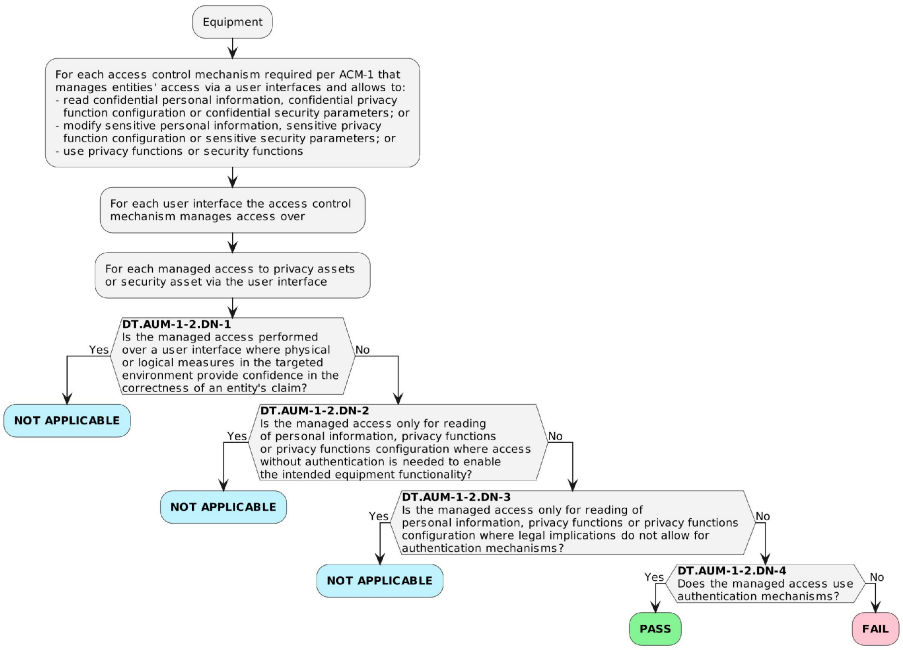

Figure - Decision tree for requirement AUM-1-2

Standard Terms	NO .	Decision Tree Node	Decision Tree Description	YES / No	Judgment description

		Name			
AUM-1-1	1	DT.AUM-1-1.DN-1	Is the managed access for personal information, privacy functions or privacy functions configuration and is the absence of authentication re q uired for the equipment's intended functionality?	NO	Refer to 6.2.1.5.3 of EN18031-2. When the test object belongs to a public function, it is an exception and no certification mechanism is required. When the test object does not belong to a public function, it passes the next node.
	2	DT.AUM-1-1.DN-2	Is the managed access performed over networks where access is limited to authorized entities via physical or logical measures?	NO	Refer to 6.2.1.5.3 of EN18031-2. When the test object is protected by the network environment, it is an exception and no authentication mechanism is required. When the test object is not protected by the network, it passes the next node.
	3	DT.AUM-1-1.DN-3	Does the managed access use authentication mechanisms?	YES	According to 6.2.1.5.3 of EN18031-2, if the test object has a certification mechanism, it passes the concept assessment, otherwise it fails
AUM-1-2	1	DT.AUM-1-2.DN-1	Is the managed access performed over a user interface where physical or logical measures in the targeted environment provide confidence in the correctness of an entity's claim?	NO	Refer to 6.2.1.6.3 of EN18031-2. When the test object has physical environmental protection, it is an exception and no certification mechanism is required. Otherwise, pass the next node
	2	DT.AUM-1-2.DN-2	Is the managed access only for reading of personal information, privacy functions or privacy functions configuration where access without authentication is needed to enable the intended functionality of the equipment?	NO	Refer to 6.2.1.6.3 of EN18031-2 regulation. When the test object only displays non-sensitive information and has read-only function, it is an exception and no authentication mechanism is required. Otherwise, pass the next node.
	3	DT.AUM-1-2.DN-3	Is the managed access only for reading of personal information, privacy functions or privacy functions configuration where legal implications do not allow for authentication mechanisms?	NO	Refer to 6.2.1.6.3 of EN18031-2 regulations. When the test object is prohibited by law, it is an exception and no certification mechanism is required. Otherwise, pass the next node
	4	DT.AUM-1-2.DN-4	Does the managed access use authentication mechanisms?	YES	Refer to 6.2.1.6.3 of EN18031-2. If the test object uses an identity authentication mechanism, it passes the concept assessment.

					Otherwise, it fails.

Table - Conceptual assessment for AUM-1

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
BLE broadcast signal	NOT APPLICABLE
Find My Network Communications	PASS

4.2.1.2. Functional Conceptual assessment

Types of Assessment	Evaluation Unit	Is it recorded in Table - Required information for AUM-1?	Compliance Conclusion
E.Info.AUM-1-1.ACM	Find My Network Communications	√	PASS

Table - Functional completeness assessment for AUM-1

4.2.1.3. Functional sufficiency assessment

Types of Assessment	Evaluation Unit	Expected Results
E.Info.AUM-1-1.ACM	Find My Network Communications	Only when the device is bound to a unique user, and the bound user can achieve remote positioning through the APP, the binding operation can be considered as an authentication mechanism.

Continued from the table above

Actual Results	Compliance Conclusion	Supporting materials
Same as expected	PASS	Refer to 2-1 of IXIT2-AUM

Table - Functional sufficiency assessment for AUM-1

4.2.2. AUM-2

4.2.2.1. Conceptual assessment

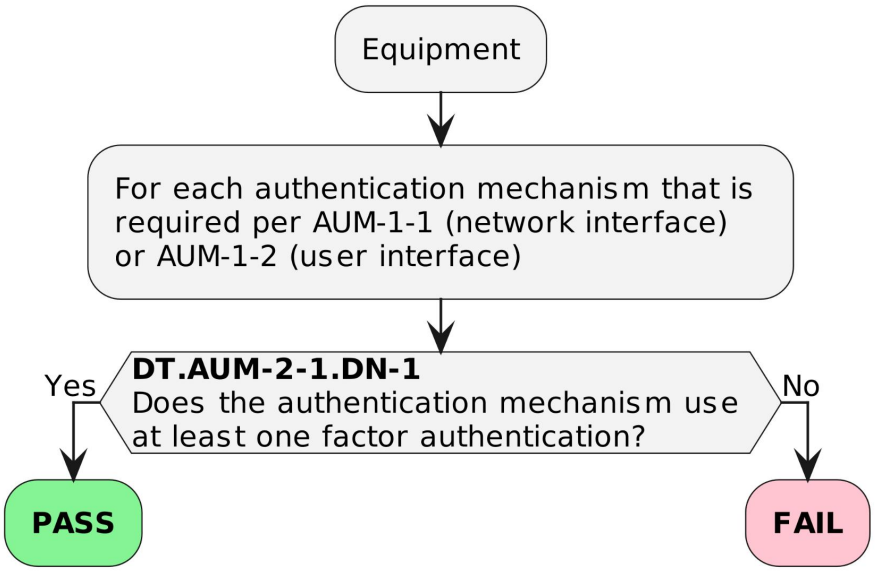

Figure - Decision tree for requirement AUM-2-1

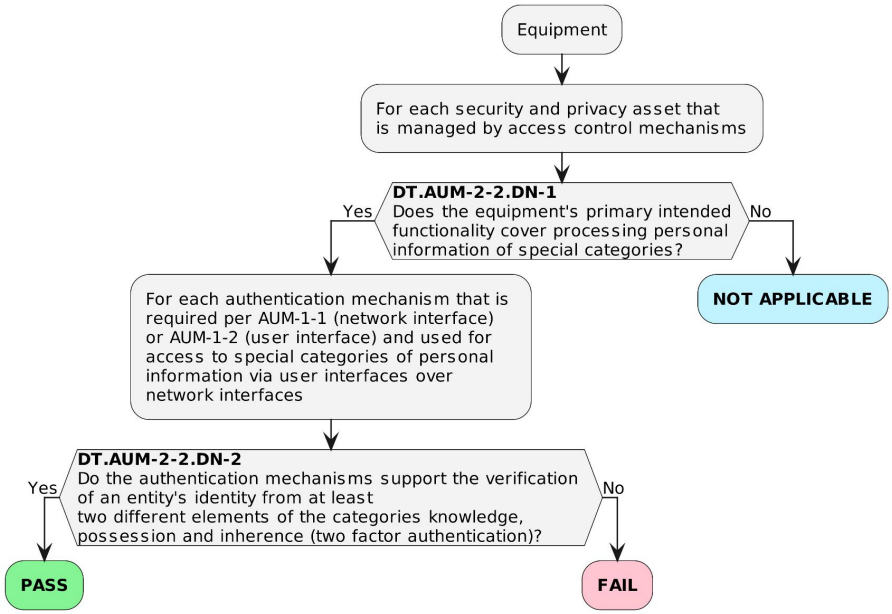

Figure - Decision tree for requirement AUM-2-2

Standard frame	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
AUM-2-1	1	DT.AUM-2.DN-1	Does the authentication mechanism use at least one factor authentication?	YES	Refer to 6.2.2.5.3 of EN18031-2 regulation. If the verification mechanism of the test object is based on checking at least one element of the knowledge,

					possession and inherent categories, it passes the concept assessment, otherwise it fails.
AUM-2-2	1	DT.AUM-2-2.DN-1	Does the equipment's primary intended functionality cover processing personal information of special categories?	YES	Refer to 6.2.2.6.3 of EN18031-2. If the test object covers personal information, it passes the concept assessment, otherwise it fails.
		DT.AUM-2-2.DN-2	Do the authentication mechanisms support the verification of an entity's identity from at least two different elements of the categories knowledge possession and inherence (two factor authentication)?	YES	Refer to 6.2.2.6.3 of EN18031-2 regulation. If the verification mechanism of the test object is based on checking at least two elements of the knowledge, possession and inherent categories, it passes the concept assessment, otherwise it fails.

Table - Conceptual assessment for AUM-2

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
BLE pairing process	PASS
Find My Network Communications	PASS

4.2.2.2. Functional completeness assessment

According to EN18031-2 clause 6.2.2.6.5, please refer to Functional sufficiency assessment.

4.2.2.3. Functional sufficiency assessment

Evaluation Unit	Expected Results
BLE pairing process	Verification requires physical device contact, meeting single-factor authentication requirements
Find My Network Communications	Output transmission requires Apple ID authentication to meet single-factor authentication

Continued from the table above

Actual Results	Compliance Conclusion	Supporting materials
Same as expected	PASS	Refer to IXIT2-AUM 2-2
Same as expected	PASS	Refer to IXIT2-AUM 2-3

Table - Functional sufficiency assessment for AUM-2

4.2.3. AUM-3

4.2.3.1. Conceptual assessment

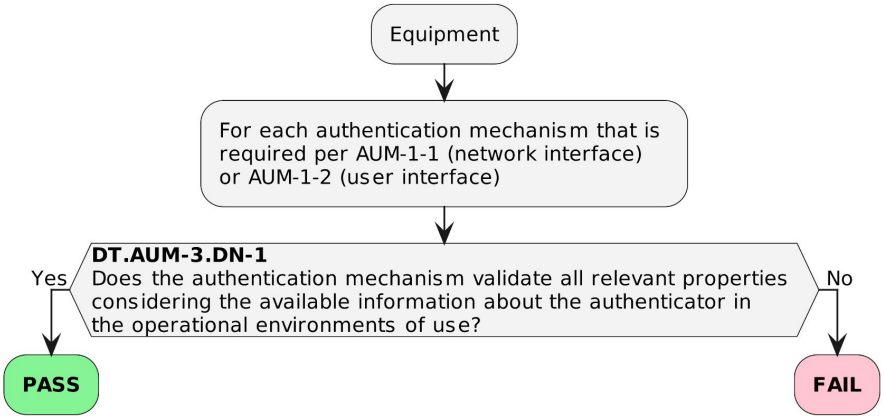

Figure - Decision tree for requirement AUM-3

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
AUM-3	1	DT.AUM-3.DN-1	Does the authentication mechanism validate all relevant properties considering the available information about the authenticator in the operational environments of use?	YES	Refer to 6.2.3.4.3 of EN18031-2 regulation. The test object verifies all relevant attributes of the authenticator and passes the concept assessment. Otherwise, it fails.

Table - Conceptual assessment for AUM-3

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
BLE pairing process	PASS

4.2.3.2. Functional completeness assessment

According to EN18031-2 clause 6.2.3.4.5, please refer to Functional sufficiency assessment.

4.2.3.3. Functional sufficiency assessment

Evaluation object	Expected Results
BLE pairing process	Pairing requires physical contact, user authorization, and Apple ID identity binding

Continued from the table above

Actual Results	Compliance	Supporting materials

	Conclusion	
Same as expected	PASS	Refer to IXIT2-AUM 2-4

Table - Functional sufficiency assessment for AUM-3

4.2.4. AUM-4

4.2.4.1. Conceptual assessment

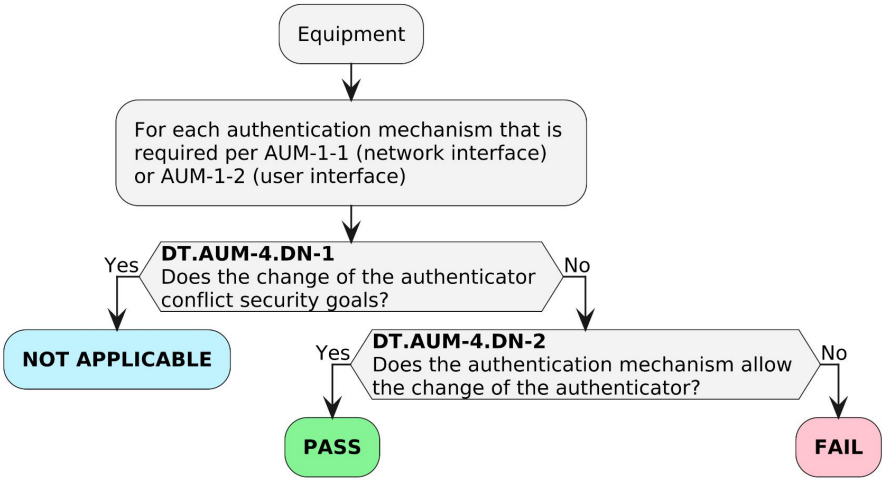

Figure - Decision tree for requirement AUM-4

Standard Terms	NO.	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
AUM-4	1	DT.AUM-4.DN-1	Does the change of the authenticator Conflict security goals?	NO	Refer to 6.2.4.4.3 of EN18031-2. When the test object has a conflict of security goals, it is an exception and no change of the authenticator is required. Otherwise, the next node is passed.
	2	DT.AUM-4.DN-2	Does the authentication mechanism allow the change of the authenticator?	YES	Refer to 6.2.4.4.3 of EN18031-2 regulation. If the test object allows the authenticator to be changed, the concept assessment is passed, otherwise it fails.

Table - Conceptual assessment for AUM-4

The following are the results of the concept evaluation of all test subjects

Evaluation Unit	Decision Tree Results

Device unbinding operation	PASS

4.2.4.2. Functional completeness assessment

According to EN18031-2 clause 6.2.4.4.5, please refer to Functional sufficiency assessment.

4.2.4.3. Functional sufficiency assessment

Evaluation Unit	Expected Results
Device unbinding operation	The user actively unbinds the device through the Find My app on the iPhone. After unbinding, the device can be re-binded to change the authentication credentials.

Continued from the table above

Actual Results	Compliance Conclusion	Supporting materials
Same as expected	PASS	Refer to IXIT2-AUM 2-5

Table - Functional sufficiency assessment for AUM-4

4.2.5. AUM-5

4.2.5.1. Conceptual assessment

The device does not have a conventional password, and all authentication functions are achieved through physical button pairing, so this provision is not applicable.

4.2.5.2. Functional completeness assessment

The device does not have a conventional password, and all authentication functions are achieved through physical button pairing, so this provision is not applicable.

4.2.5.3. Functional sufficiency assessment

The device does not have a conventional password, and all authentication functions are achieved through physical button pairing, so this provision is not applicable.

4.2.6. AUM-6

4.2.6.1. Conceptual assessment

According to the AUM-6 standard requirements of the EN18031-2 regulation, the authentication mechanism needs to have anti-brute force cracking capabilities. However, the binding mechanism between the test device and the Find My software of the Apple phone is different from the traditional authentication mechanism and does not involve brute force cracking scenarios. In addition, the responsibility for anti-brute force cracking is borne by the Apple ID, not the test device itself. Therefore, after evaluation, it was determined that the test device does not apply to the AUM-6 standard, so there is

no need for concept evaluation.

4.2.6.2. Functional completeness assessment

Because the test equipment is not subject to the AUM-6 standard, no functional integrity assessment is required.

4.2.6.3. Functional sufficiency assessment

Because the test equipment is not subject to the AUM-6 standard, no functional adequacy assessment is required.

4.3. SUM

4.3.1. SUM-1

4.3.1.1. Conceptual assessment

According to the SUM-1 standard of the EN18031-2 regulation, the device must provide a software and firmware update mechanism. However, the test device itself cannot be updated, and the Apple Find My network provides full life cycle security protection. The device itself has no update requirements, so the SUM-1 standard does not apply.

4.3.1.2. Functional completeness assessment

None

4.3.1.3. Functional sufficiency assessment

Because the test equipment is not subject to SUM-1 standards, no functional adequacy assessment is required

4.3.2. SUM-2

4.3.2.1. Conceptual assessment

According to the SUM-2 standard of the EN18031-2 regulation, each update mechanism based on the SUM-1 standard is required to require that the update mechanism should only install software with valid integrity and authenticity. Since the test equipment itself cannot be updated, SUM-1 is not applicable, so the SUM-2 standard is not applicable, and no concept evaluation is required.

4.3.2.2. Functional completeness assessment

Because the test equipment is not applicable to SUM-2 standards, no functional integrity assessment is required

4.3.2.3. Functional sufficiency assessment

Because the test equipment is not subject to the SUM-2 standard, no functional adequacy assessment is

required.

4.3.3. SUM-3

4.3.3.1. Conceptual assessment

The test equipment is not applicable to the SUM-1 standard. Since SUM-3 is based on the required update mechanism required by the SUM-1 standard, the test equipment is not applicable to the SUM-3 standard either. No concept evaluation is required.

4.3.3.2. Functional completeness assessment

The test equipment is not applicable to SUM-3 standard, so no functional integrity assessment is required

4.3.3.3. Functional sufficiency assessment

The test equipment is not applicable to SUM-3 standards, so no functional adequacy assessment is required

4.4. SSM

4.4.1. SSM-1

4.4.1.1. Conceptual assessment

According to the SSM-1 requirements of the EN18031-2 regulation, the device must implement a secure storage mechanism for persistently stored security assets and privacy assets, unless the physical or logical measures of the target environment can ensure access only by authorized entities. Because the Bluetooth anti-loss device completely relies on the Find My software of the Apple phone to transmit location data through end-to-end encryption, and only the user himself has the authority to decrypt and view it, the test device does not persistently store any sensitive data, so the evaluation test equipment is not subject to the SSM-1 standard and no concept evaluation is required.

4.4.1.2. Functional completeness assessment

Test equipment is not subject to SSM-1 standards and does not need to be evaluated for functional integrity.

4.4.1.3. Functional sufficiency assessment

Test equipment is not subject to SSM-1 standards and does not need to be evaluated for functional adequacy.

4.4.2. SSM-2

4.4.2.1. Conceptual assessment

The test equipment itself is not applicable to the SSM-1 standard because it does not permanently store confidential personal information, confidential privacy configurations, and confidential security parameters.

The SSM-2 standard is implemented based on the SSM-1 standard, so the test equipment is also not applicable to the SSM-2 standard and no concept evaluation is required.

4.4.2.2. Functional completeness assessment

The test equipment is not subject to SSM-2 standards, so no functional integrity assessment is required.

4.4.2.3. Functional sufficiency assessment

The test equipment is not subject to SSM-2 standards and therefore does not need to be evaluated for functional adequacy.

4.4.3. SSM-3

4.4.3.1. Conceptual assessment

Since the test equipment is not applicable to the SSM-1 standard, and since the SSM-3 standard is implemented based on the SSM-1 standard, the test equipment is also not applicable to the SSM-3 standard, so there is no need for concept evaluation.

4.4.3.2. Functional completeness assessment

The test equipment does not need to be evaluated for functional integrity because it is not subject to the SSM-3 standard.

4.4.3.3. Functional sufficiency assessment

The test equipment does not need to be evaluated for functional adequacy because it is not subject to the SSM-3 standard.

4.5. SCM

4.5.1. SCM-2

4.5.1.1. Conceptual assessment

Because the test equipment is completely dependent on Find My for Apple phones or Google Find Hub for Android phones, its security is globally guaranteed by Apple or Google, which is a logical measure under the SCM-1 exception. Therefore, the SCM-1 standard is not applicable to the evaluation of the test equipment, so no concept evaluation is required.

4.5.1.2. Functional completeness assessment

Because the test equipment is not subject to SCM-1 standards, no functional integrity assessment is required.

4.5.1.3. Functional sufficiency assessment

Because the test equipment is not subject to SCM-1 standards, no functional adequacy assessment is required.

4.5.2. SCM-2

4.5.2.1. Conceptual assessment

Because the test equipment is not applicable to the SCM-1 standard and the SCM-2 standard is implemented based on the SCM-1 standard, the SCM-2 standard is also not applicable and no concept assessment is required.

4.5.2.2. Functional completeness assessment

Because the test equipment is not subject to SCM-2 standards, no functional integrity assessment is required.

4.5.2.3. Functional sufficiency assessment

Because the test equipment is not subject to SCM-2 standards, no functional integrity assessment is required.

4.5.3. SCM-3

4.5.3.1. Conceptual assessment

Because the test equipment is not subject to the SCM-1 standard and the SCM-3 standard is implemented based on the SCM-1 standard, the SCM-3 standard is also not applicable and no concept assessment is required.

4.5.3.2. Functional completeness assessment

Because the test equipment is not subject to the SCM-3 standard, no functional integrity assessment is required.

4.5.3.3. Functional sufficiency assessment

Because the test equipment is not subject to the SCM-3 standard, no functional integrity assessment is required.

4.5.4. SCM-4

4.5.4.1. Conceptual assessment

Because the test equipment is not applicable to the SCM-1 standard and the SCM-4 standard is implemented based on the SCM-1 standard, the SCM-4 standard is also not applicable and no concept assessment is required.

4.5.4.2. Functional completeness assessment

Because the test equipment is not subject to SCM-4 standards, no functional integrity assessment is required.

4.5.4.3. Functional sufficiency assessment

Because the test equipment is not subject to SCM-4 standards, no functional integrity assessment is required.

4.6. LGM

4.6.1. LGM-1

4.6.1.1. Conceptual assessment

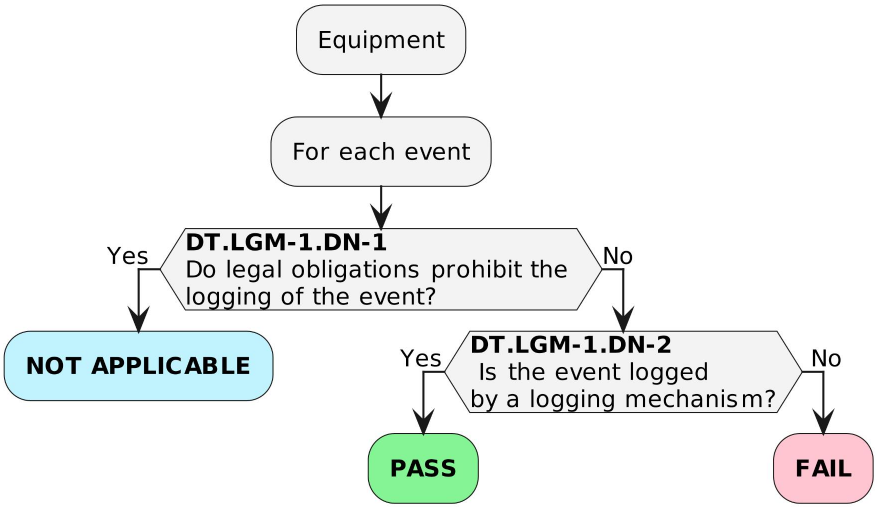

Figure - Decision tree for requirement LGM-1

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
LG M-1	1	DT.LGM-1.DN-1	Do legal obligations prohibit the logging of the event?	NO	Refer to 6.6.1.4.3 of EN18031-2. If there is no legal prohibition, pass the concept assessment, otherwise go to the next node.
	2	DT.LGM-1.DN-2	Is the event logged by a logging mechanism?	YES	Refer to 6.6.1.4.3 of EN18031-2. If a log mechanism is used for recording, the concept assessment passes. Otherwise, it fails.

Table - Conceptual assessment for LGM-1

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Logging mechanism	PASS

4.6.1.2. Functional completeness assessment

None

4.6.1.3. Functional sufficiency assessment

Evaluation Unit	Whether to implement a logging mechanism	Proof
Logging mechanism	yes	to IXIT 3 - LGM 3 - 1

Table - Functional sufficiency assessment for LGM-1

4.6.2. LGM-2

4.6.2.1. Conceptual assessment

According to the EN18031-2 regulation LGM-2 standard, the logging mechanism is required to store the log data of relevant events in the persistent storage of the device. However, if the relevant log data is outside the device, it is an exception because the test device itself does not store relevant logs and only records logs through the software itself. Therefore, the assessment believes that the test device is not applicable to the LGM-2 standard.

4.6.2.2. Functional completeness assessment

Because the test equipment falls under the exception to LGM-2, no functional integrity assessment is required

4.6.2.3. Functional sufficiency assessment

Because the test equipment falls within the exception to LGM-2, no functional adequacy assessment is required

4.6.3. LGM-3

4.6.3.1. Conceptual assessment

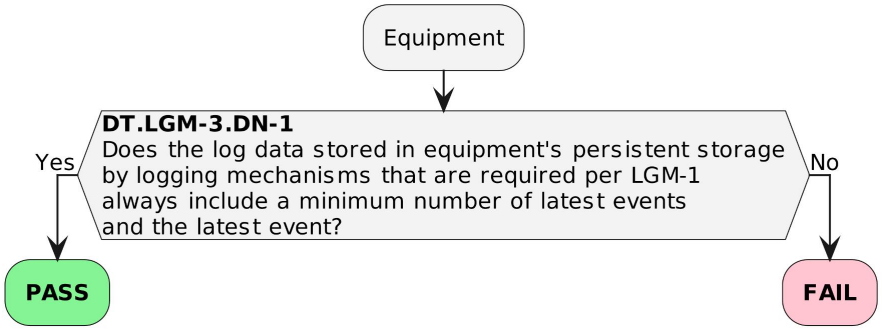

Figure - Decision tree for requirement LGM-3

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
LG M-3	1	DT.LGM-3.DN-2	Is the log data stored in the equipment's persistent storage?	YES	Refer to 6.6.3.4.3 of EN18031-2 regulation. If the log mechanism always contains the minimum number of the latest events and the latest events, it passes the concept assessment, otherwise it fails.

Table - Conceptual assessment for LGM-3

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Logging Events	PASS

4.6.3.2. Functional completeness assessment

According to EN18031-2 clause 6.6.3.4.5, please refer to Functional sufficiency assessment.

4.6.3.3. Functional sufficiency assessment

Evaluation Unit	Expected Results	Actual Results
Logging Events	The test device records at least 5 events	Consistent with expected results

Continued from the table above

Compliance Conclusion	Supporting materials
PASS	to IXIT 3 - LGM 3 - 2

Table - Functional sufficiency assessment for LGM-3

4.6.4. LGM-4

4.6.4.1. Conceptual assessment

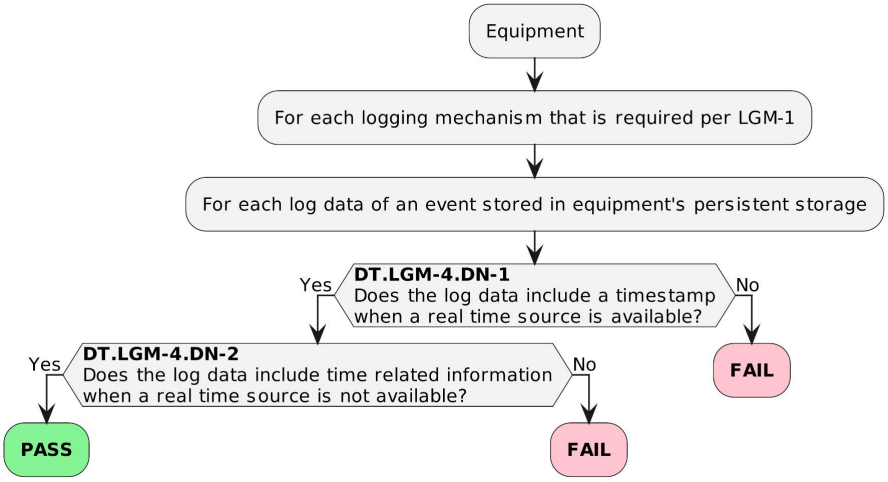

Figure - Decision tree for requirement LGM-4

Standard Terms	NO.	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
LGM-4	1	DT.LGM-4.DN-1	Does the log data include a timestamp when a real time source is available?	YES	Refer to 6.6.4.4.3 of EN18031-2 regulations. If the relevant log data has a timestamp, it passes the concept evaluation, otherwise it goes to the next node.
	2	DT.LGM-4.DN-2	Does the log data include time related information when a real time source is not available?	YES	Refer to 6.6.4.4.3 of EN18031-2 regulation. When there is no real-time source, the relevant data has a timestamp and the concept assessment passes. Otherwise, it fails.

Table - Conceptual assessment for LGM-4

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results

Logging information	PASS

4.6.4.2. Functional completeness assessment

According to EN18031-2 clause 6.6.4.4.5, please refer to Functional sufficiency assessment.

4.6.4.3. Functional sufficiency assessment

Evaluation Unit	Expected Results	Actual Results
Logging information	Contains log information such as timestamp	Same as expected

Continued from the table above

Compliance Conclusion	Supporting materials
PASS	Reference IXIT 3 - LGM 3 - 3

Table - Functional sufficiency assessment for LGM-4

4.7. DLM

4.7.1. DLM-1

The following table describes the sensitive information on the device:

Sensitive Information	describe
Location information stored on your device	Record the location information of the device at this time and the bound mobile phone location

Table 1- Sensitive information

Table 2 below describes the device deletion mechanism.

Deletion mechanism	describe
Remove device mechanism	Delete relevant information through the app

Table 2- Delete mechanism

4.7.1.1. Conceptual assessment

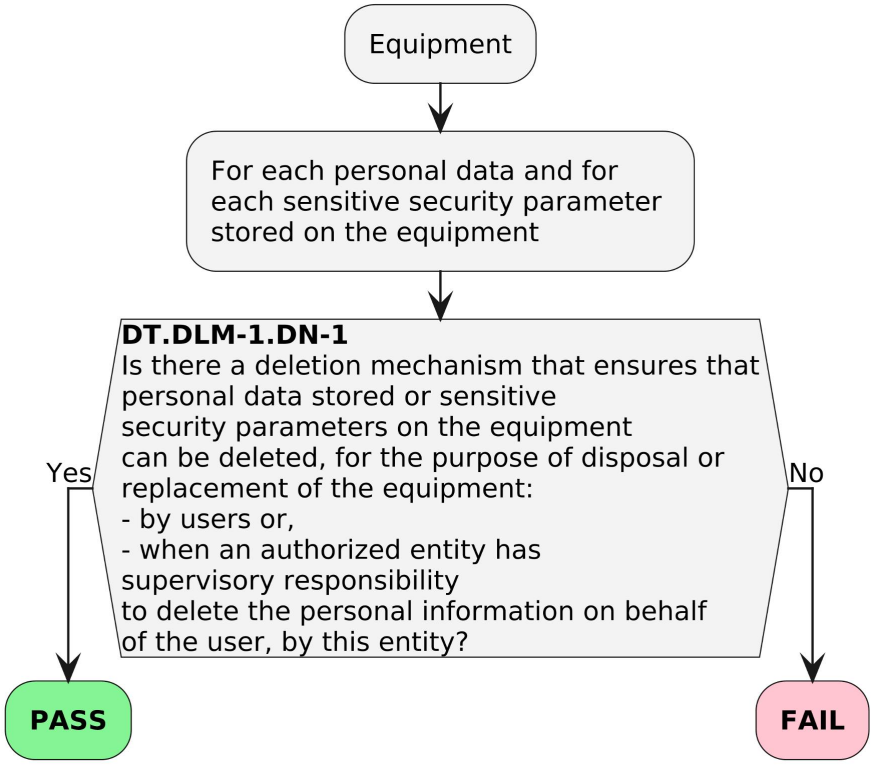

Figure - Decision tree for requirement DLM-1

Standard Terms	NO.	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
DL M-1	1	DT.DLM-1.DN-1	Is there a deletion mechanism that ensures that personal data stored or sensitive security parameters on the equipment can be deleted, for the purpose of disposal or replacement of the equipment: -by users or, -When an authorized entity has supervisory responsibility to delete the personal information on be half of the user, by this entity?	YES	Refer to 6.7.1.4.3 of EN18031-2 regulation. If there is a deletion mechanism that meets the requirements, the concept assessment passes, otherwise it fails.

Table - Conceptual assessment for DLM-1

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Remove device mechanism	PASS

4.7.1.2. Functional completeness assessment

Test Unit	Is it complete?	Compliance Conclusion
Remove device mechanism	yes	PASS

Table - Functional Conceptual assessment for DLM-1

4.7.1.3. Functional sufficiency assessment

Deletion mechanism	Expected Results	Actual Results
Remove device mechanism	Users can choose to unbind the bound device. After unbinding, the device's location data and other information will not be available.	Same as expected

Continued from the table above

Verdict	Supporting materials
PASS	to IXIT 4 - DLM 4 - 1

Table - Functional sufficiency assessment for DLM-1

4.8. UNM

4.8.1. UNM-1

The following table is a list of device notification mechanism information

Evaluation Unit	describe
Forgotten message notification	When the test device is forgotten somewhere and is out of range, the user will receive a notification
Notify when found	When the user turns on the "Found Notification" function, the test device is detected by another phone and the user will receive a found notification
Unwanted tracking notifications	When the test device is not associated with the user for a period of time, the user will receive this tracking prompt message

Table - User notification mechanism

4.8.1.1. Conceptual assessment

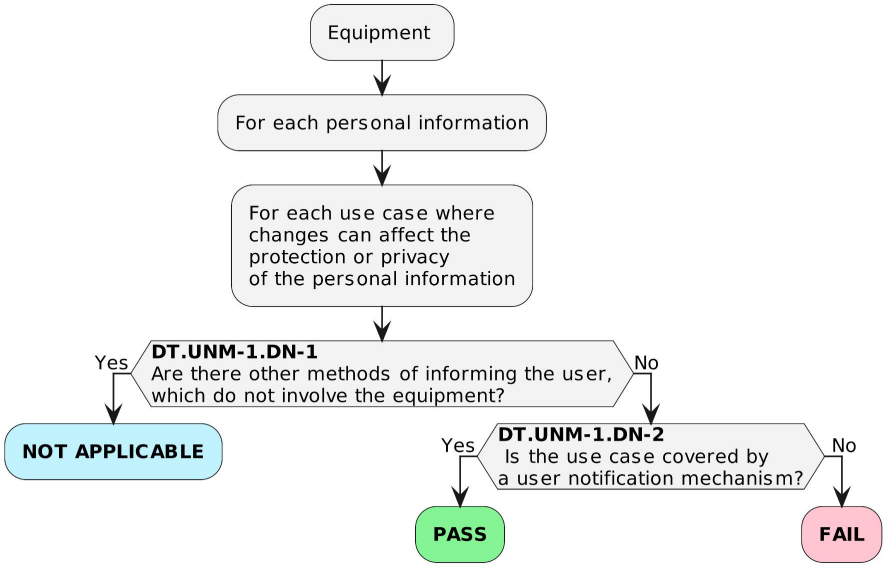

Figure - Decision tree for requirement UNM-1

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
UNM-1	1	DT.UNM-1.DN-1	Are there other methods of informing the user, which do not involve the equipment?	NO	Refer to 6.8.1.4.3 of EN18031-2. If there is no method that does not involve the device to notify the user, the concept assessment is passed, otherwise it goes to the next node.
	2	DT.UNM-1.DN-2	Is the use case covered by a user notification mechanism?	YES	Refer to 6.8.1.4.3 of EN18031-2 regulation. If the use case is covered by the user notification mechanism, it passes the concept assessment, otherwise it fails.

Table - Conceptual assessment for UNM-1

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Forgotten message notification	PASS
Notify when found	PASS
Unwanted tracking notifications	PASS

4.8.1.2. Functional completeness assessment

Evaluation Unit	Whether to record in Table - User notification mechanism	Compliance Conclusion
Forgotten message notification	yes	PASS
Notify when found	yes	PASS
Unwanted tracking notifications	yes	PASS

Table - Functional Conceptual assessment for UNM-1

4.8.1.3. Functional sufficiency assessment

Evaluation Unit	Expected Results	Actual Results
Forgotten message notification	When the test device is out of range from the user, the user will receive a notification	Same as expected
Notify when found	When a lost test device is brought close to another user, the lost user will receive a notification	Same as expected
Unwanted tracking notifications	When the test device moves with a non-bound user for a period of time, the user will receive a notification	Same as expected

Continued from the table above

Compliance Conclusion	Supporting materials
PASS	to IXIT 5 - UNM 5 - 1
PASS	to IXIT 5 - UNM 5 - 2
PASS	Reference IXIT 5 - UNM 5 - 3

Table - Functional sufficiency assessment for UNM-1

4.8.2. UNM-2

The following table describes the device notification mechanism information list in detail based on the table of UNM-1.

Notification content	Specific description
Forgotten message notification	The user receives a forgotten notification with a specific message that the user is out of range of the test device
Notify when found	The user receives a Found notification with the approximate geographic location of the test device
Unwanted tracking notifications	The user receives a tracking notification, which contains a message that the user is suspected of being tracked

Table - Specific description of the equipment use case list

4.8.2.1. Conceptual assessment

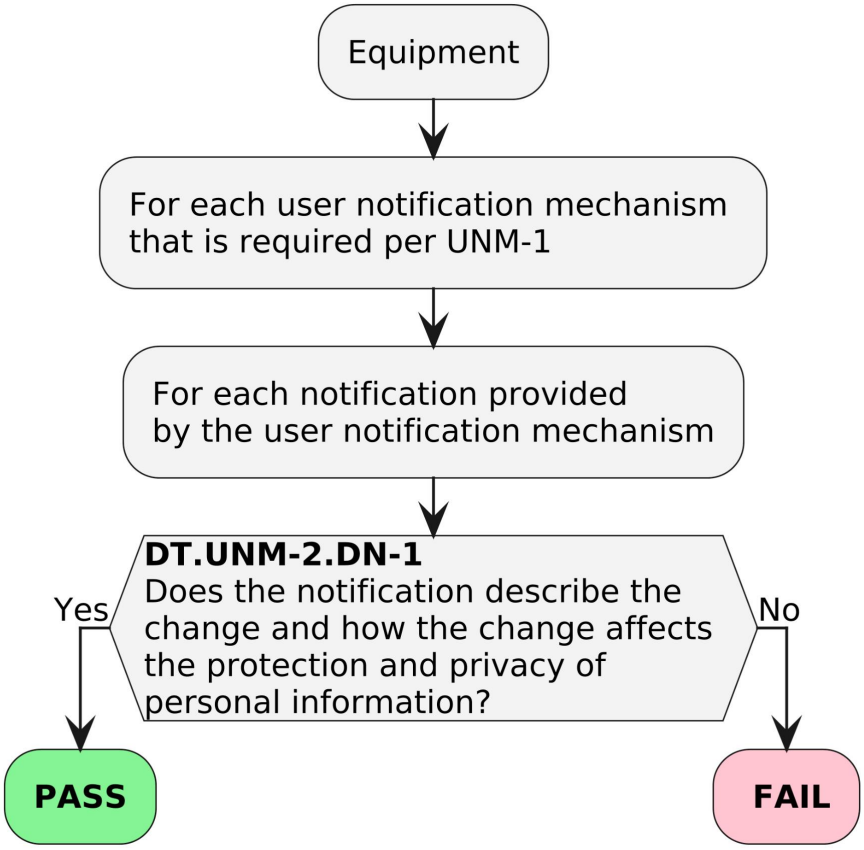

Figure - Decision tree for requirement UNM-2

Standard Terms	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
UN M-2	DT. UN M-2. DN-1	Does the notification describe the change and how the change affects the protection and privacy of personal information?	YES	Refer to 6.8.2.4.3 of EN18031-2. If the change and its impact on personal information protection and privacy are described, the concept assessment passes. Otherwise, it fails.

Table - Conceptual assessment for UNM-2

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Forgotten message notification	PASS
Notify when found	PASS
Unwanted tracking notifications	PASS

4.8.2.2. Functional completeness assessment

According to EN18031-2 clause 6.8.2.4.5, please refer to Functional sufficiency assessment.

4.8.2.3. Functional sufficiency assessment

Notification Items	Expected Notification Items	Actual notification items
Forgotten message notification	The test device has gone out of detection range and may lose the reminder notification	Similar to expected results
Notify when found	The lost test device is located somewhere, prompting the user to find the test device there	Similar to expected results
Unwanted tracking notifications	It is suspected that there is a test device tracking the user. Please check whether you are being illegally tracked.	Similar to expected results

Continued from the table above

Verdict	Supporting materials
PASS	Reference IXIT 5 - UNM 5 - 4
PASS	Reference IXIT 5 - UNM 's 5 - 5
PASS	to IXIT 5 - UNM 5 - 6
PASS	to IXIT 5 - UNM 5 - 7

Table - Functional sufficiency assessment for UNM-2

4.9. CCK

4.9.1. CCK-1

The following table describes the device encryption mechanism in detail.

Evaluation Unit	describe
Binding Key	When the test device is bound to the user's software, a pair of keys is generated through end-to-end encryption. The private key will be

	stored in the software on the user's phone, and the public key will be stored in the test device.
Broadcast data encryption	The Bluetooth signal broadcast by the test device periodically contains a dynamically generated key that is changed regularly to prevent tracking

Table - Encryption mechanism

4.9.1.1. Conceptual assessment

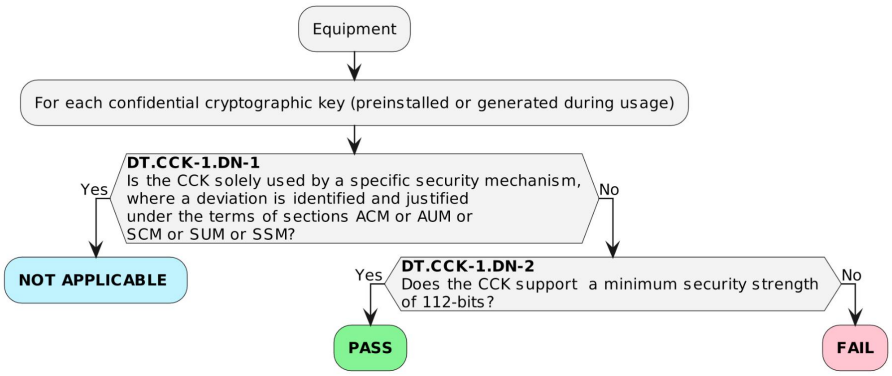

Figure - Decision tree for requirement CCK-1

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
CCK-1	1	DT.CCK-1.DN-1	Is the CCK solely used by a specific security mechanism,where a deviation is identified and justified under the terms of secti o ns ACM or AUM or SCM or SUM or SSM?	NO	Refer to 6.9.1.4.3 of EN18031-2 regulation. If the evaluation unit is only used for a specific safety mechanism, it does not apply. Otherwise, go to the next node.
	2	DT.CCK-1.DN-2	Does the CCK support a minimum security strength of 112-bits?	YES	Refer to 6.9.1.4.3 of EN18031-2 regulation. If the evaluation unit supports at least 112 bits of security strength, the concept evaluation passes. Otherwise, it fails.

Table - Conceptual assessment for CCK-1

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Binding Key	PASS
Broadcast data encryption	PASS

4.9.1.2. Functional completeness assessment

Evaluation Unit	Is it recorded in Table - Encryption mechanism	Compliance Conclusion
Binding Key	yes	PASS
Broadcast data encryption	yes	PASS

Table - Functional completeness assessment for CCK-1

4.9.1.3. Functional sufficiency assessment

Evaluation Unit	Expected Results	Actual Results
Binding Key	Key derivation is based on the NIST P-256 elliptic curve algorithm (ECDSA/ECDH), which complies with the hardware specifications of the Apple Find My network.	Same as expected
Broadcast data encryption	Dynamically generate AES-128 keys	Same as expected

Continued from the table above

Compliance Conclusion	Supporting materials
PASS	to IXIT 6 - UNM 6 - 1
PASS	to IXIT 6 - UNM 6 - 2

Table - Functional sufficiency assessment for CCK-1

4.9.2. CCK-2

The following table describes the generation method/derivation algorithm of the device encryption mechanism in detail.

Evaluation Unit	describe
Binding key generation mechanism	Bluetooth pairing is generated through ECDH-P256 protocol and encrypted with AES-128
Broadcast data	Dynamically generated (based on timestamp and device ID), encrypted broadcast

encryption generation mechanism	signal via AES-128

Table - Required information for CCK-2

4.9.2.1. Conceptual assessment

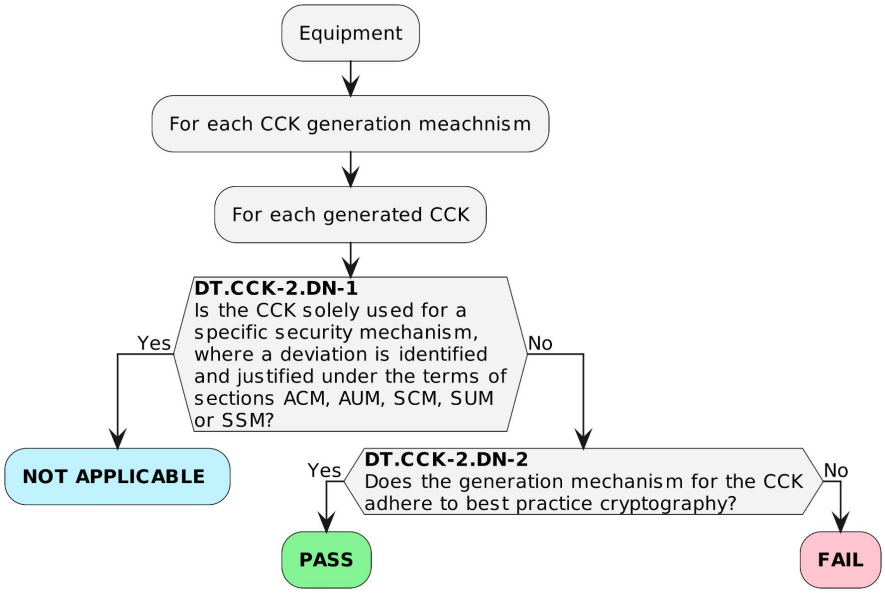

Figure - Decision tree for requirement CCK-2

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
CCK-2	1	DT.CCK-2.DN-1	Is the CCK solely used for a specific security mechanism,where a deviation is identified and justified under the terms of section s ACM,AUM,SCM,SUM or SSM?	NO	Refer to 6.9.2.4.3 of EN18031-2 regulation, when the evaluation unit is only used for a specific safety mechanism,
	2	DT.CCK-2.DN-2	Does the generation mechanism for the CCK adhere to best practice cryptography?	YES	Refer to 6.9.2.4.3 of EN18031-2 regulation. If the evaluation unit meets the best practice encryption, it passes the concept evaluation. Otherwise, it fails.

Table - Conceptual assessment for CCK-2

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results

Binding key generation mechanism	PASS
Broadcast data encryption generation mechanism	PASS

4.9.2.2. Functional completeness assessment

Evaluation Unit	Is it recorded in Table - Required information for CCK-2?	Compliance Conclusion
Binding key generation mechanism	√	PASS
Broadcast data encryption generation mechanism	√	PASS

Table - Functional completeness assessment for CCK-2

4.9.2.3. Functional sufficiency assessment

None

4.9.3. CCK-3

Evaluation Unit	describe
Binding Key	The test device generates a pair of keys through end-to-end encryption when binding with the user software

Table - Required information for CCK-3

4.9.3.1. Conceptual assessment

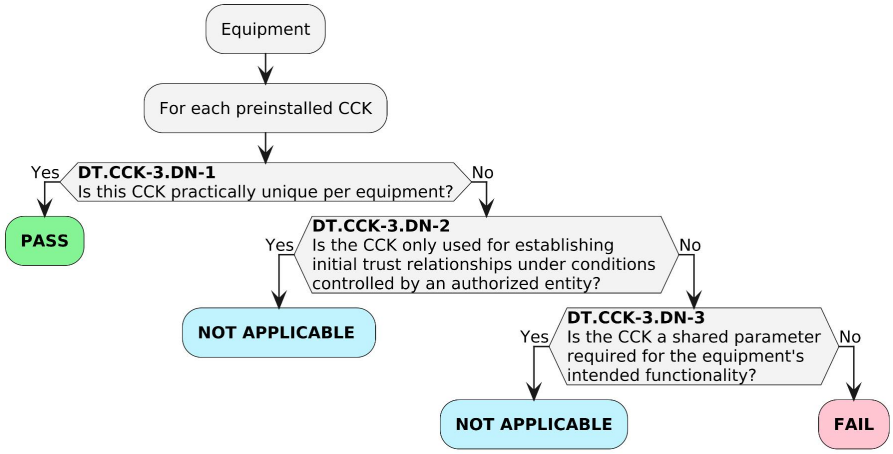

Figure - Decision tree for requirement CCK-3

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
CCK-3	1	DT.CCK-3.DN-1	Is this CCK practically unique per equipment?	YES	Refer to 6.9.3.4.3 of EN18031-2 regulation. If the evaluation unit is unique in each device, the concept evaluation is passed, otherwise it goes to the next node.
	2	DT.CCK-3.DN-2	Is the CCK only used for establishing initial trust relationships under conditions controlled by an authorized entity?		Refer to 6.9.3.4.3 of EN18031-2 regulation. If the evaluation unit is used only to establish the initial trust relationship under the conditions controlled by the authorized entity, it does not apply. Otherwise, go to the next node.
	3	DT.CCK-3.DN-3	Is the CCK a shared parameter equipped for the equipment's intended functionality?		Refer to 6.9.3.4.3 of EN18031-2 regulation. When the evaluation unit is a shared parameter required for the intended function of the equipment, it does not apply, otherwise it fails.

Table - Conceptual assessment for CCK-3

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Binding Key	PASS

4.9.3.2. Functional completeness assessment

Evaluation Unit	Is it recorded in Table - Required information for CCK-3?	Compliance Conclusion
Binding Key	√	PASS

Table - Functional completeness assessment for CCK-3

4.9.3.3. Functional sufficiency assessment

Evaluation Unit	Expected Results	Actual Results
Binding Key	Generate a unique key for each device	Same as expected

Continued from the table above

Compliance Conclusion	Supporting materials
PASS	to IXIT 6 - UNM 6 - 3

Table - Functional sufficiency assessment for CCK-3

4.10. GEC

4.10.1. GEC-1

4.10.1.1. Conceptual assessment

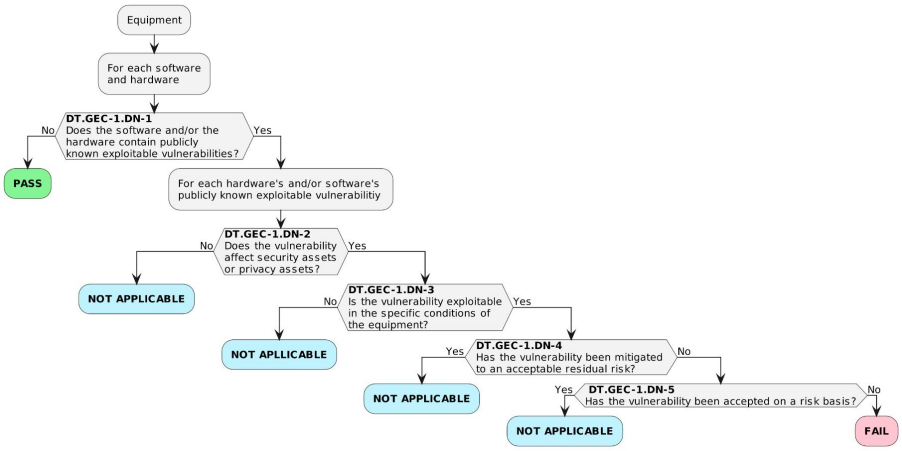

Figure - Decision tree for requirement GEC-1

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
GEC-1	1	DT.GEC-1.DN-1	Does the software and/or hardware contain publicly known exploitable vulnerabilities?	NO	Refer to 6.10.1.4.3 of EN18031-2 regulation. If the software or hardware of the device does not contain known vulnerabilities, it passes the concept assessment, otherwise it goes to the next node.
	2	DT.GEC-1.DN-2	Does the vulnerability affect security assets or privacy assets?		Refer to 6.10.1.4.3 of EN18031-2 regulation. If the software or hardware vulnerability does not affect the security assets or network assets, it does not apply. Otherwise, go to the next node.
	3	DT.GEC-1.DN-3	Is the vulnerability exploitable in the specific conditions of the equipment?		Refer to 6.10.1.4.3 of EN18031-2 regulation. If the vulnerability can be exploited under certain equipment conditions, it will go to the next node. Otherwise, it is not applicable.
	4	DT.GEC-1.DN-4	Has the vulnerability been mitigated to an acceptable residual risk?		Refer to 6.10.1.4.3 of EN18031-2. If the vulnerability has been mitigated to an acceptable residual risk, it is not applicable. Otherwise, proceed to the

					next node.
	5	DT.GEC-1.DN-5	Has the vulnerability been accepted on a risk basis?		Refer to 6.10.1.4.3 of EN18031-2 regulation. If the vulnerability is acceptable based on risk, it is not applicable. Otherwise, it fails.

Table - Conceptual assessment for GEC-1

4.10.1.2. Functional completeness assessment

The device uses the latest software and hardware versions and has no known exploitable vulnerabilities, so a functional integrity assessment is not necessary.

4.10.1.3. Functional sufficiency assessment

Evaluation Unit	Expected Results	Actual Results
Hardware vulnerability testing	All components meet the test requirements and have no vulnerabilities	As expected
Software vulnerability testing	All components are the latest version and have no vulnerabilities	As expected

Continued from the table above

Compliance Conclusion	Supporting materials
PASS	to IXIT 7 - UNM 7 - 1
PASS	to IXIT 7 - UNM 7 - 2

Table - Functional sufficiency assessment for GEC-1

4.10.2. GEC-2

Evaluation Unit	describe
GATT Services	Bluetooth low energy core data exchange protocol
BLE Services	Functional modules of Bluetooth low energy devices

Table - Required information for GEC-2

4.10.2.1. Conceptual assessment

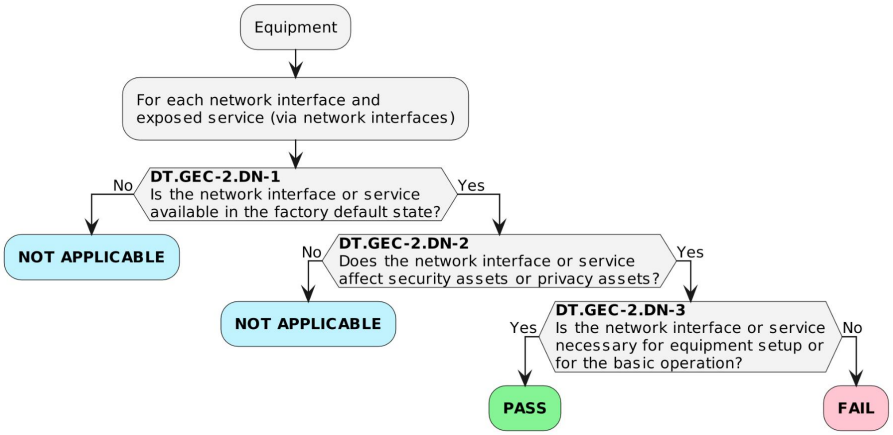

Figure - Decision tree for requirement GEC-2

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
GEC-2	1	DT.GEC-2.DN-1	Is the network interface or service available in the factory default state?	YES	Refer to 6.10.2.4.3 of EN18031-2 regulation. If the evaluation unit is available in the factory default state, go to the next node. Otherwise, it is not applicable.
	2	DT.GEC-2.DN-2	Does the network interface or service affect security assets or privacy assets?	YES	Refer to 6.10.2.4.3 of EN18031-2 regulation. When the evaluation unit affects the safety asset or network asset, it goes to the next node. Otherwise, it does not apply.
	3	DT.GEC-2.DN-3	Is the network interface or service necessary for equipment setup or for the basic operation?	YES	Refer to 6.10.2.4.3 of EN18031-2 regulation. If the evaluation unit is necessary for the equipment or basic operation, it passes the concept evaluation, otherwise it fails.

Table - Conceptual assessment for GEC-2

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
GATT Services	PASS
BLE Services	PASS

4.10.2.2. Functional completeness assessment

Evaluation Unit	Is it recorded in Table - Required information for GEC-2	Compliance Conclusion

GATT Services	√	PASS
BLE Services	√	PASS

Table - Functional completeness assessment for GEC-2

4.10.2.3. Functional sufficiency assessment

None

4.10.3. GEC-2

4.10.3.1. Conceptual assessment

The service interface of the test device itself will not affect the user's privacy assets, the GEC-3 standard is not applicable, and no concept evaluation is required

4.10.3.2. Functional completeness assessment

The test equipment is not subject to GEC-3 standards and does not need to be evaluated for functional integrity

4.10.3.3. Functional sufficiency assessment

The test equipment is not subject to GEC-3 standards and does not need to be evaluated for functional adequacy

4.10.4. GEC-4

Evaluation Unit	describe
Test Equipment User Manual	Detailed description of all services for testing equipment

Table - Required information for GEC-4

4.10.4.1. Conceptual assessment

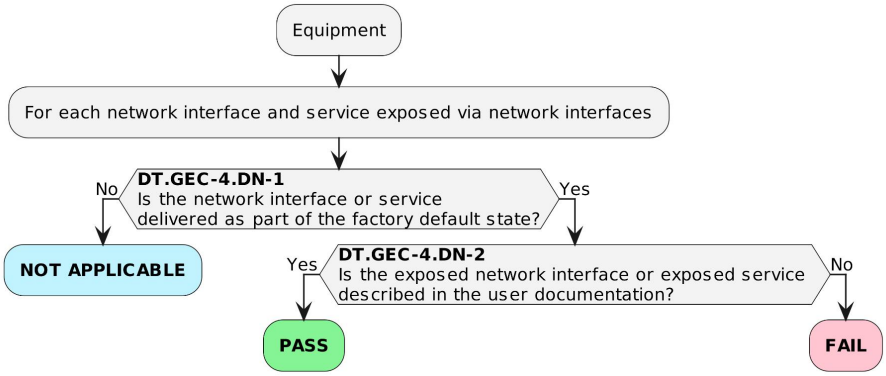

Figure - Decision tree for requirement GEC-4

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
GEC-4	1	DT.GEC-4.DN-1	Is the network interface or service delivered as part of the factory default state?	YES	Refer to 6.10.4.4.3 of EN18031-2 regulation. When the evaluation unit is part of the factory default state, go to the next node. Otherwise, it does not apply.
	2	DT.GEC-4.DN-2	Is the exposed network interface or exposed described in the user documentation?	YES	Refer to 6.10.4.4.3 of EN18031-2 regulation. If the content of the evaluation unit is described in the user documentation, the concept evaluation is passed, otherwise it fails.

Table - Conceptual assessment for GEC-4

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Test Equipment User Manual	PASS

4.10.4.2. Functional completeness assessment

Evaluation Unit	Is it recorded in Table - Required information for GEC-4?	Compliance Conclusion
Test Equipment User Manual	√	PASS

Table - Functional completeness assessment for GEC-4

4.10.4.3. Functional sufficiency assessment

None

4.10.5. GEC-5

The following table describes the interfaces and their uses based on the product documentation provided by the manufacturer.

Evaluation Unit	describe
Pairing mode button	Users need to physically touch the test device to turn it on and off

Table - Required information for GEC-5

4.10.5.1. Conceptual assessment

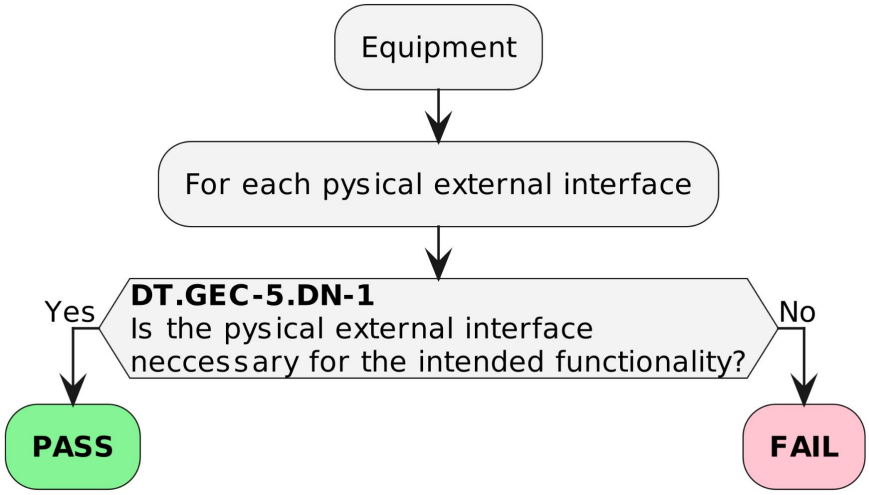

Figure - Decision tree for requirement GEC-5

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
GEC-5	1	DT.GEC-5.DN-1	Is the physical external interface neccessary for the intended functionality?	YES	Refer to 6.10.5.4.3 of EN18031-2 regulation. If the evaluation unit is necessary for the expected result, the concept evaluation is passed, otherwise it fails.

Table - Conceptual assessment for GEC-5

The following are the results of the concept assessment of all assessment units

Evaluation Unit	Decision Tree Results
Pairing mode button	PASS

4.10.5.2. Functional completeness assessment

None

4.10.5.3. Functional sufficiency assessment

None

4.10.6. GEC-6

4.10.6.1. Conceptual assessment

Because the test equipment does not accept input, GEC-6 standards do not apply and no concept evaluation is required

4.10.6.2. Functional completeness assessment

The test equipment is not subject to GEC-6 standards and does not need to be evaluated for functional integrity

4.10.6.3. Functional sufficiency assessment

The test equipment is not subject to GEC-6 standards and does not need to be evaluated for functional adequacy

4.10.7. GEC-7

4.10.7.1. Conceptual assessment

The test device does not have any perceived functionality that could affect the privacy of the user or subscriber, so the GEC-7 standard is not applicable and no concept assessment is required

4.10.7.2. Functional completeness assessment

Because the test equipment is not subject to GEC-7 standards, no functional integrity assessment is required

4.10.7.3. Functional sufficiency assessment

None

4.11. CRY

4.11.1. CRY-1

The following table shows the asset items and corresponding protection mechanisms obtained by integrating equipment assets.

Evaluation Unit	describe
AES-128 encryption	For BLE data encryption

Table - Required information for CRY-1

4.11.1.1. Conceptual assessment

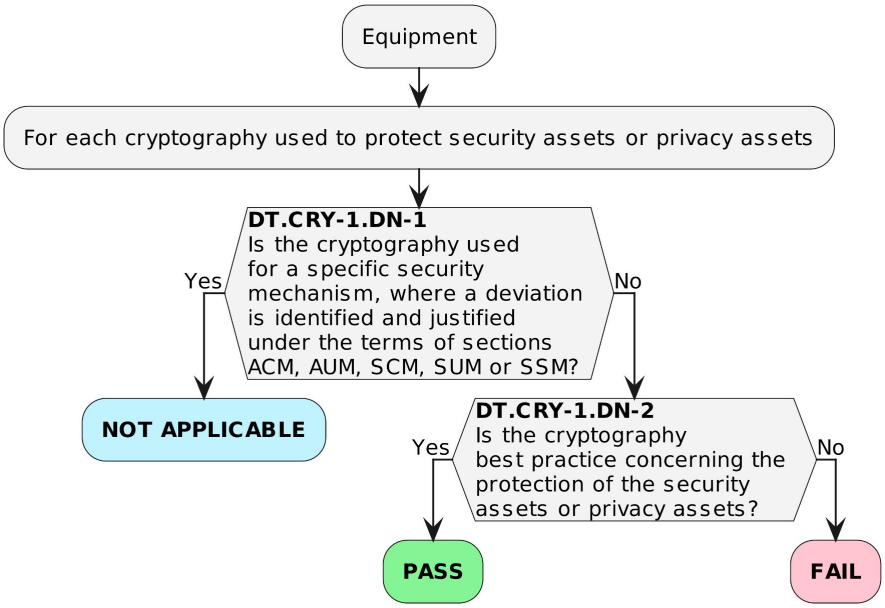

Figure - Decision tree for requirement CRY-1

Standard Terms	NO .	Decision Tree Node Name	Decision Tree Description	YES / NO	Judgment description
CRY-1	1	DT.CRY-1.DN-1	Is the cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM, AUM, SCM, SUM or SSM?	NO	Refer to 6.10.6.4.3 of EN18031-2 regulation. If the evaluation unit belongs to a specific safety mechanism, it is not applicable. Otherwise, go to the next node.
	2	DT.CRY-1.DN-2	Is the cryptography best practice concerning the protection of the security assets or privacy assets?	YES	Refer to 6.10.6.4.3 of EN18031-2 regulation. If the evaluation unit meets the best practices for protecting security assets or privacy assets, it passes the concept evaluation. Otherwise, it fails.

Table - Conceptual assessment for CRY-1

4.11.1.2. Functional completeness assessment

Evaluation Unit	Is it recorded in Table - Required information for CRY-1	Compliance Conclusion
AES-128 encryption	√	PASS

Table - Functional completeness assessment for CRY-1

4.11.1.3. Functional sufficiency assessment

Evaluation Unit	Expected Results	Actual Results
AES-128 encryption	Verify that the device is transmitting data via AES-128 encryption when in use	Same as expected

Continued from the table above

Compliance Conclusion	Supporting materials
PASS	to IXIT8-UNM8-1

Table - Functional sufficiency assessment for CRY-1

5. EQUIPMENT UNDER TEST

5.1. Product Photo

5.2. Photographs of The Eut

END OF REPORT