



中国认可
国际互认
检测
TESTING
CNAS L4062



Test Report

Reference No...... : WTF26X07208074W
Applicant..... : Mid Ocean Brands B.V.
Address..... : Unit 711-716, 7/F., Tower A, 83 King Lam Street, Cheung Sha Wan,
Kowloon, Hong Kong.
Manufacturer : 118897
Address..... : 118897
Product Name : Smartwatch
Model No...... : MO2748
Standards : EN 18031-2:2024
Date of Receipt sample : 2026-07-15
Date of Test..... : 2026-07-15 to 2026-08-06
Date of Issue : 2026-08-14
Test Result..... : **PASS**

Remarks:

The results shown in this test report refer only to the sample(s) tested, this test report cannot be reproduced, except in full, without prior written permission of the company. The report would be invalid without specific stamp of test institute and the signatures of approver.

Prepared By:

Waltek Testing Group (Shenzhen) Co., Ltd.

Address: 1/F., Room 101, Building 1, Hongwei Industrial Park, Liuxian 2nd Road,
Block 70 Bao'an District, Shenzhen, Guangdong, China
Tel.: +86-755-33663308 Fax.: +86-755-33663309 Email: sem@waltek.com.cn

Tested by:

Fred Hou

Fred Hou

Approved by:

Rio Luo 2026.08

Rio Luo



Table of Contents

Revision History.....	3
1. Summary of Test Results	5
2. General Test Information	14
2.1. Description of EUT	14
2.2. Primary function of EUT	14
2.3. Physical Port of EUT	14
2.4. Document of EUT	14
2.5. Deviations of test standard	15
2.6. Test environment conditions	15
2.7. Test Equipment	15
2.8. Test structure.....	16
2.9. Test procedure	16
2.10. Test laboratory.....	17
3. TEST RESULT	18
3.1 [ACM] Access control mechanism	18
3.2 [AUM] Authentication mechanism.....	21
3.3 [SUM] Secure update mechanism.....	30
3.4 [SSM] Secure storage mechanism	35
3.5 [SCM] Secure communication mechanism.....	39
3.6 [LGM] Logging mechanism.....	47
3.7 [DLM] Deletion mechanism.....	51
3.8 [UNM] User notification mechanism	52
3.9 [CCK] Confidential cryptographic keys.....	54
3.10 [GEC] General equipment capabilities	57
3.11 [CRY] Cryptography	64
4. Assignment of verdict	66
Appendix I : Photos of the EUT	67



Test Report Declare

Applicant	Mid Ocean Brands B.V.
Address	Unit 711-716, 7/F., Tower A, 83 King Lam Street, Cheung Sha Wan, Kowloon, Hong Kong.
Manufacturer	118897
Address	118897
Equipment under Test	Smartwatch
Test Model No.	MO2748
Trade Mark	/

Test Standard Used:

EN 18031-1:2024 Common security requirements for radio equipment Part 1: Internet connected radio equipment.

We Declare:

The equipment described above is tested by Waltek Testing Group (Shenzhen) Co., Ltd. and in the configuration tested the equipment complied with the standards specified above. The test results are contained in this test report and Waltek Testing Group (Shenzhen) Co., Ltd. is assumed of full responsibility for the accuracy and completeness of these tests.

Report No.:	WTF26X07208074W		
Date of Receipt:	2026-07-15	Date of Test:	2026-07-15 to 2026-08-06

Note: This report applies to above tested sample only. This report shall not be reproduced in parts without written approval of Waltek Testing Group (Shenzhen) Co., Ltd



Revision History

Revision	Revisions	Issue Date	Revised By
V1.0	Initial released Issue	08/14/2026	Fred Hou

WALTEK



1. Summary of Test Results

By performing the Conceptual assessment, Functional completeness assessment, and Functional sufficiency assessment of ACM, AUM, SUM, SSM, SCM, RLM, NMM, TCM, CCK, GEC, and CRY, There are currently no remaining non-conformities..

Based on the above test results, the conclusion of this test is: **Pass**.

See below detailed test result:

Test items	Test content		Verdict
1	[ACM] Access Control Mechanism		
1.1	[ACM-1] Applicability of access control mechanisms	The equipment shall use access control mechanisms to manage entities' access to security assets and network assets	PASS
1.2	[ACM-2] Appropriate access control mechanisms	Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets	PASS
1.3	[ACM-3] Default Access Control for Children in Toys	When the device is a toy, for each child that has access to external content and the child's access to the privacy features managed by the access control mechanisms required by ACM-1, the access control mechanisms shall by default ensure that the child's access to external content through the privacy features is limited to content from authorised entities	N/A



1.4	[ACM-4] Default Access Controls to Children's Private Assets for Toys and Childcare Devices	When the device is a toy or childcare device, any ACM-1-required access control mechanisms for children's privacy features and personal information shall by default restrict access to children's privacy features and personal information processed by the device to any third party other than the child or the child's parent/guardian	N/A
1.5	[ACM-5] Parent/Guardian Access Control for Children in Toys	When the device is a toy, any ACM-1 required access control mechanisms to manage child access shall be configured by the authorised entity to restrict child access to protected security and privacy assets for each child-accessible security and privacy asset	N/A
1.6	[ACM-6] Parent/Guardian Access Controls for Access to Managed Children's Privacy Assets by Other Entities in Toys	When the device is a toy, for each child privacy asset that is accessible to entities other than the child and for which access is managed by an access control mechanism required by ACM-1, the access control mechanism shall be configured by the authorised entity to restrict access by other entities to the managed child privacy assets	N/A
2	[AUM] Authentication mechanism		
2.1	[AUM-1] Applicability of authentication mechanisms	[AUM-1-1] Shall use authentication mechanisms for managing entities' access via network interfaces	PASS
2.2		[AUM-1-2] Shall use authentication mechanisms for managing entities' access via user interfaces	PASS



2.3	[AUM-2] Appropriate authentication mechanisms	Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity's claim based on examining evidence from at least one element of the categories knowledge, possession and inheritance (one factor authentication)	PASS
2.4	[AUM-3] Authenticator Validation	Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use	PASS
2.5	[AUM-4] Change Authenticator	Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change	PASS
2.6	[AUM-5] Password strength	[AUM-5-1] If factory default passwords are used by an authentication mechanism that is required per AUM-1-1 or AUM-1-2, they shall: — be unique per equipment; and — follow best practice concerning strength; or — be enforced to be changed by the user before or on first use	PASS



2.7		[AUM-5-2]If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall: — be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or — be defined by an authorized entity within a network where access is limited to authorised entities; or — be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.	PASS
2.8	[AUM-6] Brute force breach protection	Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks	PASS
3	[SUM] Security Update Mechanism		
3.1	[SUM-1] Applicability of the updated mechanisms	The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or network assets	PASS
3.2	[SUM-2] Security updates	Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.	PASS
3.3	[SUM-3] Automatic updates	update mechanism that is required per SUM-1 shall be capable of updating the software	PASS
4	[SSM] Secure Storage Mechanism		
4.1	[SSM-1] Applicability of safe storage mechanisms	The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets	PASS



4.2	[SSM-2] Provide appropriate integrity protection for safe storage mechanisms	Secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently	PASS
4.3	[SSM-3] Provide adequate confidentiality protection for secure storage mechanisms	Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently	PASS
5	[SCM] Secure Communication Mechanism		
5.1	[SCM-1] Applicability of secure communication mechanisms	The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces	PASS
5.2	[SCM-2] Provide adequate integrity and authenticity protection for secure communication mechanisms	Shall apply best practices to protect the integrity and authenticity of the security assets and network assets communicated	PASS



5.3	[SCM-3] Provide adequate confidentiality protection for secure communication mechanisms	shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed	PASS
5.4	[SCM-4] Adequate replay protection for secure communication mechanisms	Shall apply best practices to protect the security assets and the network assets communicated against replay attacks	PASS
6	[LGM] Logging mechanism		
6.1	[LGM-1] Applicability of logging mechanisms	Devices should use logging mechanisms to record internal activities (called events) related to privacy assets and their protection	PASS
6.2	[LGM-2] Persistent storage of log data	The logging mechanism required by LGM-1 shall store log data of relevant events in the persistent storage of the device	PASS
6.3	[LGM-3] Minimum number of events in persistent storage	All log data stored in device persistent storage by the LGM-1-required logging mechanism shall include the minimum number of latest events, latest events	PASS



6.4	[LGM-4] Persistent storage of time-dependent information on log data	All log data stored in device persistent storage by the logging mechanism required by LGM-1 shall include timestamps or time-related information	PASS
7	[DLM] Deletion Mechanism		
7.1	[DLM-1] Applicability of the deletion mechanism	The device should provide a deletion mechanism that allows users to delete personal data and sensitive security parameters stored on the device	PASS
8	[UNM] User Notification Mechanism		
8.1	[UNM-1] Applicability of user notification mechanisms	The device should provide a user notification mechanism for notifying device users of changes that affect the protection or privacy of their personal information.	PASS
8.2	[UNM-2] Appropriate content of user notifications	The notification provided by the required UNM-1 user notification mechanism shall include, at a minimum, a description of the change and a description of how the change affects the protection and privacy of personal information.	PASS
9	[CCK] Confidential Cryptographic Key		
9.1	[CCK-1] Appropriate confidential encryption key	Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits	PASS



9.2	[CCK-2] Confidential cryptographic key generation mechanism	The generation of confidential cryptographic keys shall adhere to best practice cryptography	PASS
9.3	[CCK-3] Preventing Static Defaults for Preloaded Secret Encryption Keys	Preinstalled confidential cryptographic keys shall be practically unique per equipment	N/A
10	[GEC] General equipment capacity		
10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	The equipment shall not include publicly known exploitable vulnerabilities	PASS
10.2	[GEC-2] Restriction of service exposure through relevant network interfaces	In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces	PASS
10.3	[GEC-3] Configuration of optional services and associated public network interfaces	Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service	PASS



10.4	[GEC-4] Documentation of network interface exposures and services exposed through network interfaces	The equipment's user documentation shall contain a description of — all exposed network interfaces; and — all services exposed via network interfaces	PASS
10.5	[GEC-5] No unnecessary external interfaces	The equipment shall only expose physical external interfaces if they are necessary for its intended Functionality	PASS
10.6	[GEC-6] Input validation	The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets	PASS
10.7	[GEC-7] Documentation of external sensing capabilities	All external sensing capabilities of the device related to the privacy of the user or subscriber shall be logged to the user	PASS
11	[CRY] Cryptography		
11.1	[CRY-1] Best Practice Cryptography	The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets	PASS



2. General Test Information

2.1. Description of EUT

EUT Name	Smartwatch
Model	MO2748
EUT Function Description	The EUT is a smartwatch that connects to a mobile app via Bluetooth.
Bluetooth	BLE5.3
Hardware Configuration	AB5681
Communication Modules	BLE5.3
Operating System	FreeRTOS
Hardware Version	Z2950V1.0
Software Version	V1.00
Firmware Version	/
Communication Protocols	Bluetooth
Communication Module	/
Certification Report	/

Note: The information above are provided by the manufacturer of the EUT.

2.2. Primary function of EUT

Function	Description
Smartwatch	The EUT is a smartwatch that connects to a mobile app via Bluetooth.

2.3. Physical Port of EUT

Physical Port	Description
Touch menu	Touch menu is a screen that can be used to operate the device through touch.
Up button	The device can be woken up to access the menu by Up button; a long press allows you to choose Shutdown, Restart, or Reset.
Down button	Down button can wake up the device, turn off the screen, long press to enter sports mode
Sensor	The sensor can detect usage status, turning on the screen when the device is facing a person and turning off the screen when it is not.



Magnetic suction contact	Charging
--------------------------	----------

2.4.Document of EUT

1. User manual;

2.5.Deviations of test standard

No deviation.

2.6.Test environment conditions

During the measurement the environmental conditions were within the listed ranges:

Temperature range:	25.1°C~29.5°C
Humidity range:	53.5%RH~66.8%RH

Note: The specific temperature and humidity information of each test item refers to the temperature and humidity record in the corresponding test data.

2.7.Test Equipment

- 1) Equipment:

Fixed Asset Number	Hardware Environment		Software Environment
	Name/Model	Configuration (CPU/memory/hard drive)	
WTXW1105A1013	PC/ThinkPad P52	CPU: intel i5 Memory: 16GB Hard disk: 1TSSD	1. Windows 11 Home Chinese Edition/Client Operating System.
Network environment: LAN.			

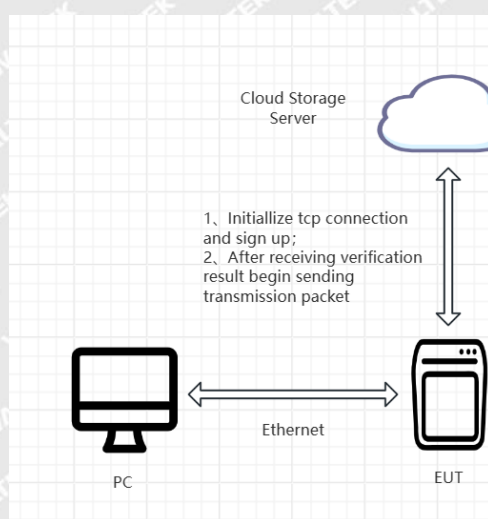
- 2) Tools:

Fixed Asset Number	Tool name	Version	Tool Usage	quantities
WTXW1105A1018	SecureCRT	9.7.2	Serial port debug	1



Fixed Asset Number	Tool name	Version	Tool Usage	quantities
WTXW1105A1019	Wireshark	V4.6.6	WIFI protocol analysis	1
WTXW1105A1020	Proxypin	v1.2.8	Packet capture	1
WTXW2108B0001	BTP	v1.14.0	BLE protocol analysis	1
WTXW2108B0002	NRF connect	4.29.1	BLE replay	1
WTXW2108B0003	Kali Linux	2026.1	DDOS attack Interface scan	1
WTXW2108B0005	Xray	6.18.13_r3	Vulnerabilities detection	1
WTXW2108B0005	Xray vulnerability database	vuln_library-6_2026-07-12	Vulnerabilities detection	1

2.8. Test structure



2.9. Test procedure



- (1) The EUT placement requires reference to the test block diagram and is placed on a non-metallic table.
- (2) Setup the EUT and assistant equipment as shown above block diagram and equipment list.
- (3) Finish the Conceptual assessment and Functional completeness assessment based on the materials and evidences collected from customer.

2.10. Test laboratory

Waltek Testing Group (Shenzhen) Co., Ltd.

1/F., Room 101, Building 1, Hongwei Industrial Park, Liuxian 2nd Road, Block 70 Bao'an District, Shenzhen, Guangdong, China

Tel.: +86-755-33663308 Fax.: +86-755-33663309 Email: sem@waltek.com.cn

WALTEK



3. TEST RESULT

3.1 [ACM] Access control mechanism

3.1.1 [ACM-1] Applicability of access control mechanisms

Conceptual assessment:

According to [E.Just.DT.ACM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

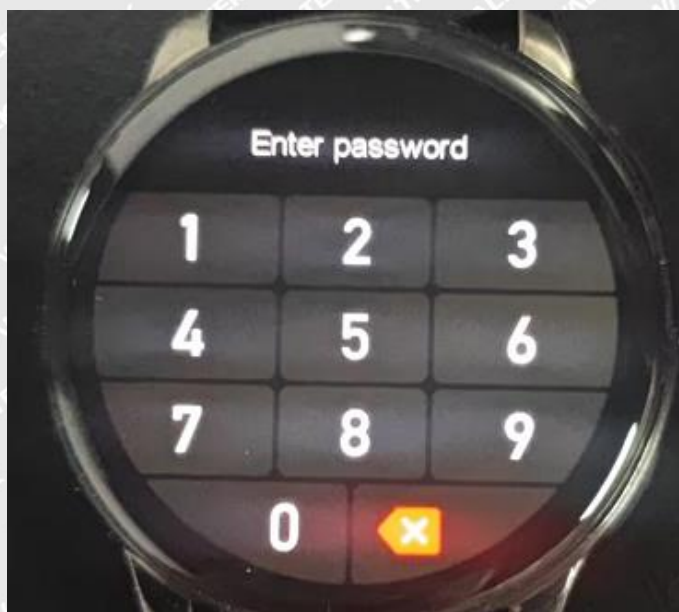
All security assets and network assets accessible by entities have been recorded in [E.Info.ACM-1.NetworkAsset] and [E.Info.ACM-1.SecurityAsset]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Access control mechanisms to manage the entity's use of assets existed and there was no evidence that they had not been implemented	EUT devices can have device locks set through the app, with access control in place. Bluetooth is also accessed and controlled via pairing packets using the SMP protocol.	PASS
Judgement (Verdict)	PASS	

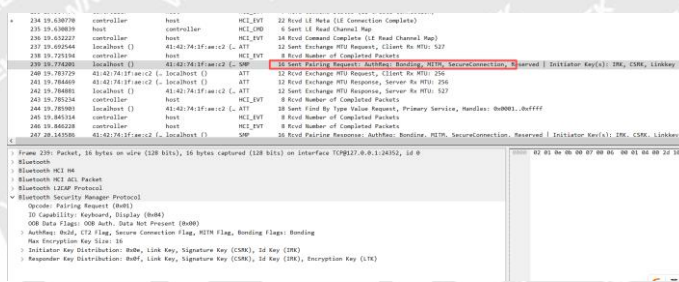


Device Lock



Evidence

Bluetooth Access Control



3.1.2 [ACM-2] Appropriate access control mechanisms

Conceptual assessment:

According to [E.Just.DT.ACM-2] in technical documentation, the verdict of this conceptual test is **PASS**.

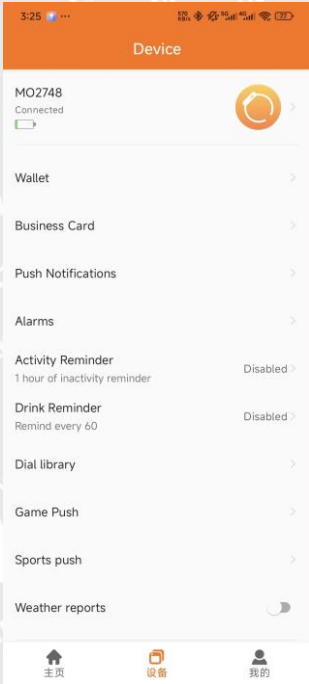
Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the access control mechanism. Therefore, this Functional completeness assessment is not required.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Roles assigned to each user have associated authorizations	Each EUT user has corresponding permissions.	PASS



Least privilege is associated with the role	Role permissions corresponding to each EUT user	PASS
Assets can only be accessed by authorized users given their role	Assets are only accessible to users who have been authenticated.	PASS
Only authorized users can change roles	EUT has only one permission role, which can be used directly after binding.	N/A
Judgement (Verdict)	PASS	
Evidence	 	

3.1.3 [ACM-3] Authenticator validation



The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.1.4 [ACM-4] Default access control to children's privacy assets for toys and childcare equipment

The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.1.5 [ACM-5] Parental/Guardian access controls for children in toys

The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.1.6 [ACM-6] Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys

The EUT is not a toy, therefore the verdict of this test is **NOT APPLICABLE**.

3.2 [AUM] Authentication mechanism

3.2.1 [AUM-1] Applicability of authentication mechanisms

[AUM-1-1] Requirement network interface

Conceptual assessment:

There is no authentication mechanism through the network interface that needs to be evaluated, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional completeness assessment

There are no authentication mechanism in user interface of the EUT. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
The authentication mechanism is implemented as specified in [E.Info.AUM-1-1.ACM.AuthenticationMechanism].	Implementing identity authentication through Bluetooth binding	PASS
Judgement (Verdict)	PASS	



Evidence

[AUM-1-2] Requirement user interface

Conceptual assessment:

According to [E.Just.DT.AUM-1-2] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

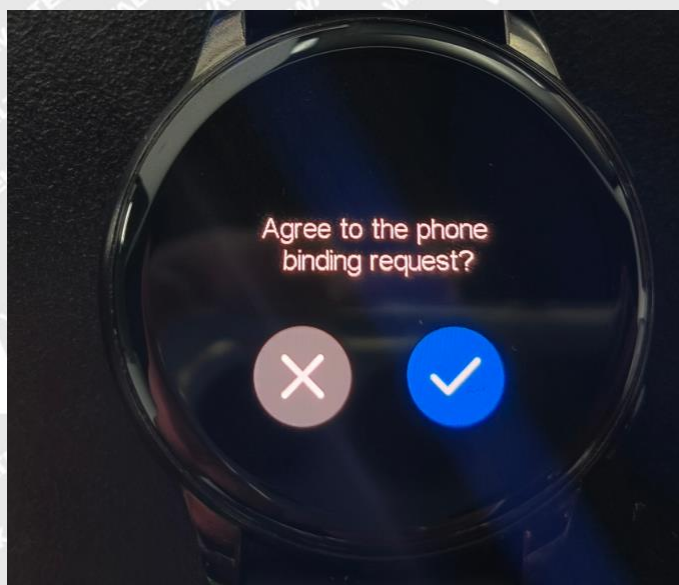
This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
The authentication mechanism is implemented as specified in [E.Info.AUM-1-2.ACM.AuthenticationMechanism].	The user interface authenticates identity through the screen lock, EUT can also verify identity when binding the app.	PASS
Judgement (Verdict)	PASS	



Evidence



3.2.2 [AUM-2] Appropriate authentication mechanisms

Conceptual assessment:

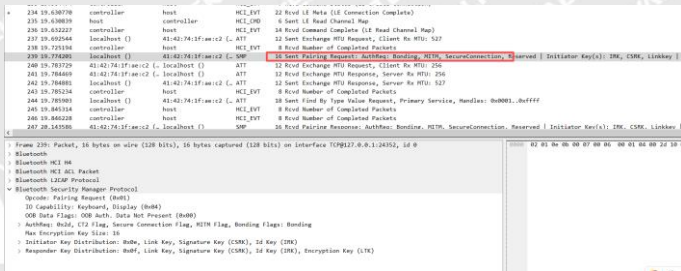
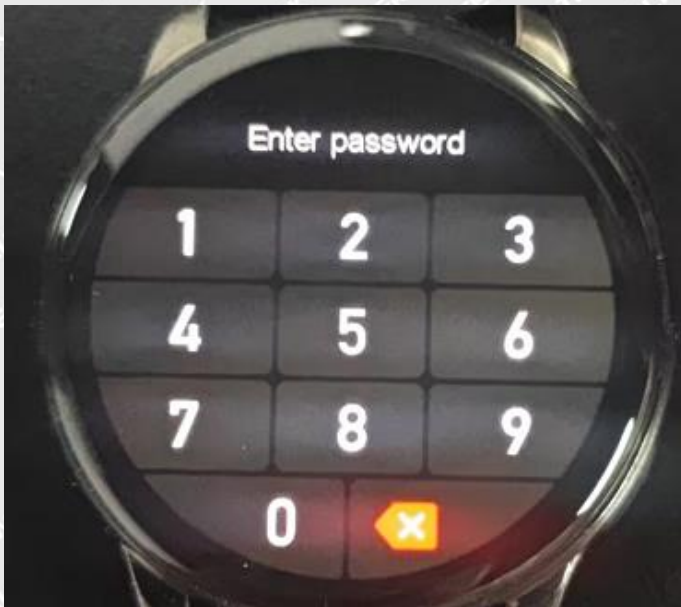
According to [E.Just.DT.AUM-2] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment



Descriptions	Test results	Verdict
Authentication is possible and the authentication mechanism is implemented as specified in [E.Info.AUM-2-1.AuthenticationMechanism].	1. After start-up, the EUT will sending pairing request. If the terminal app receive request and reply with response. The two device will begin pairing stage. The SMP is responsible for the pairing process between devices, ensuring that both parties can securely exchange keys and authentication information before establishing a connection. Through this pairing, devices can establish a secure connection to protect subsequent data transmission. 2. EUT authenticates multiple users through screen lock.	PASS
Judgement (Verdict)	PASS	
Evidence	Bluetooth  Device lock 	



3.2.3 [AUM-3] Authenticator validation

Conceptual assessment:

According to [E.Just.DT.AUM-3] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Incorrect validators cannot to used for successful validation	An incorrect password or PIN cannot pass verification	PASS
If not protected, the replay of recorded successful authentication attempts cannot be used for successful authentication	Bluetooth can prevent replay attacks by verifying the PIN code.	PASS
(If there exist or can create different user accounts) Passwords of other entities cannot be used for authentication	Each EUT user corresponds to a specific password, and a single user's password cannot verify other users.	PASS
Judgement (Verdict)	PASS	



The Bluetooth restrictions of EUT only allow connection through the FitCloudPro application; all other connection methods will fail.

No.	Time	Source	Destination	Protocol	Length	Info
301	12.986548	localhost ()	41:42:07:28:1f:02 ()	HTTP	24	Rcvd AT+VGS=15
302	12.986750	localhost ()	41:42:07:28:1f:02 ()	HTTP	20	Sent OK
303	12.988467	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
304	12.989470	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
305	12.992471	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
306	12.994413	41:42:07:28:1f:02 ()	localhost ()	L2CAP	21	Rcvd Configure Request (DCID: 0x0043)
307	12.994453	localhost ()	41:42:07:28:1f:02 ()	L2CAP	19	Sent Configure Response - Success (SCID: 0x00c8)
308	12.997772	41:42:07:28:1f:02 ()	localhost ()	L2CAP	23	Rcvd Configure Response - Success (SCID: 0x0043)
309	12.999459	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
310	13.000241	41:42:07:28:1f:02 ()	localhost ()	SDP	29	Rcvd Service Search Attribute Request : Phonebook Access Server: Attrib
311	13.000359	localhost ()	41:42:07:28:1f:02 ()	SDP	19	Sent Service Search Attribute Response
312	13.005476	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
313	13.029086	41:42:07:28:1f:02 ()	localhost ()	L2CAP	17	Rcvd Disconnection Request (LCID: 0x00c8, DCID: 0x0043, PSN: 0x0001, S
314	13.029032	localhost ()	41:42:07:28:1f:02 ()	L2CAP	17	Sent Disconnection Response (SCID: 0x00c8, DCID: 0x0043, PSN: 0x0001, S
315	13.034468	controller	host	HCI_EVT	8	Rcvd Number of Completed Packets
316	18.963833	controller	host	HCI_EVT	6	Rcvd Max Slots Change
317	18.964779	controller	host	HCI_EVT	6	Rcvd Max Slots Change

Evidence

The device lock in the EUT app does not authenticate when the password is wrong.



3.2.4 [AUM-4] Changing authenticator

Conceptual assessment:

According to [E.Just.DT.AUM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

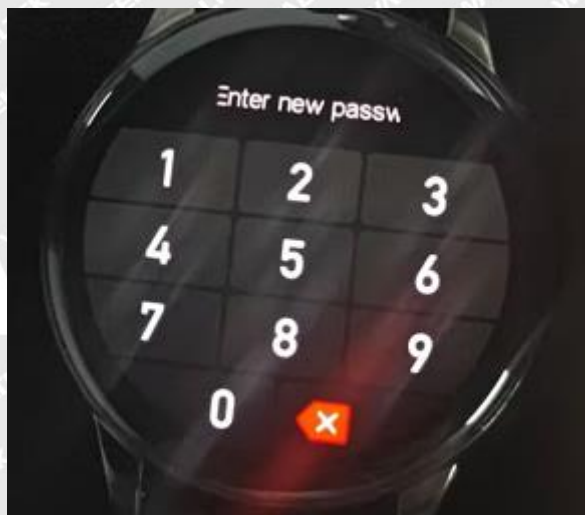
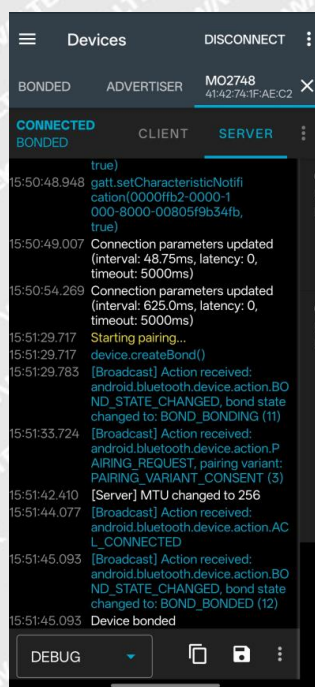


Descriptions	Test results	Verdict
Authenticators can be changed according to the instructions in [E.Info.AUM-4.AUM.AuthChange].	The Bluetooth connector of the EUT can be changed.The screen lock mechanism can be changed	PASS
Newly Assigned Authenticators Allow access to Secure, Private Assets on Every Route	Newly assigned authenticators can view the device and Internet information of the EUT through BLE and the EUT	PASS
Previous authenticator no longer allows access to secure, private assets via any path	Previous authenticator no longer allows subscribe request of the BLE	PASS
Judgement (Verdict)	PASS	

WALTEK



Evidence



3.2.5 [AUM-5] Password strength

Conceptual assessment:

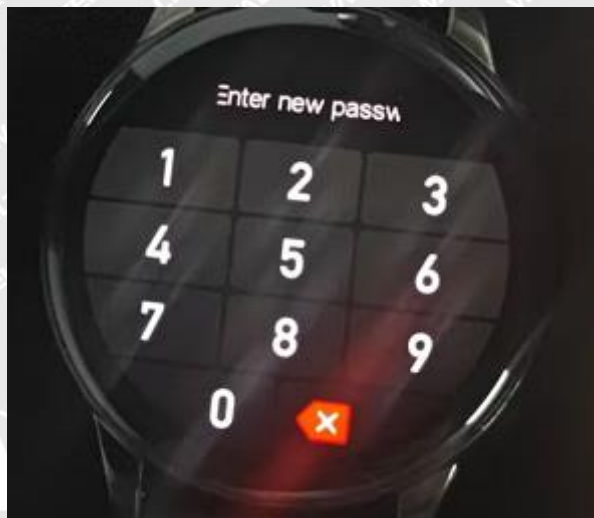
According to [E.Just.DT.AUM-5] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment



Descriptions	Test results	Verdict
factory default passwords must be set "before or on first use".	Bluetooth is not a password, and network interfaces do not use this mechanism.	NOT APPLICABLE
The non-factory default password must be set "before the device logically connects to the network".	Users can configure the screen lock mechanism, with a 4-digit code defined solely by authorized entities.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.2.6 [AUM-6] Applicability of access control mechanisms

Conceptual assessment:

According to [E.Just.DT.AUM-6] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



The number of consecutive failed attempts before the device blocks further attempts matches the value recorded in [E.Info.AUM-6.AUM.BFProtection	1. Each Bluetooth connection pairing requires manual confirmation on the EUT, so brute-force attacks are not possible.	PASS
	2. Since the target customer group of this product is elderly. Considering usability, The product cannot force enable screen lock when first use and screen locked due to multiple input errors. Therefore, this product does not support forcing screen lock at first use and Password lock mechanism.	N/A
Judgement (Verdict)	PASS	
Evidence		

3.3 [SUM] Secure update mechanism

3.3.1 [SUM-1] Applicability of update mechanisms

Conceptual assessment:

According to [E.Just.DT.SUM-1] in technical documentation, the verdict of this conceptional test is **PASS**.



Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Update (SW-a) Installation was successful and relevant software components were effectively updated	EUT can update by clicking on the version in the app.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.3.2 [SUM-2] Secure updates

Conceptual assessment:

According to [E.Just.DT.SUM-2] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

**Functional sufficiency assessment**

Descriptions	Test results	Verdict
It is implemented according to the SCM using secure communication mechanism	The connection between the EUT and the cloud server using AES_128_GCM to avoid illegal update package.	PASS
Unauthorized software updates not installed	The TLS protocol uses SHA256 hashing to prevent tampering by man-in-the-middle attacks.	PASS
Secure communication channels do not allow man-in-the-middle attacks to impersonate authorized software update sources.	Secure communication channels do not allow man-in-the-middle attacks to impersonate authorized software update sources.	PASS
Software updates that were not installed and were altered during communication	Software updates that were not installed and were altered during communication.	PASS
Judgement (Verdict)	PASS	



TLS Protocol

No.	Time	Source	Destination	Protocol	Length	Info
330	35.079643900	192.168.137.208	47.106.210.56	TLSv1.2	528	Seq=518 Ack=518 Win=0 Len=0
331	35.079644000	192.168.137.208	47.106.210.56	TLSv1.2	575	Client Hello (SHA256WithRSAEncryption)
332	35.130471600	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=518 Win=0 Len=0
333	35.130471700	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=518 Win=0 Len=0
334	35.134123100	47.106.210.56	192.168.137.208	TLSv1.2	1514	Server Hello
335	35.136744700	47.106.210.56	192.168.137.208	TLSv1.2	1413	Certificate, Server Key Exchange, Server Hello Done
336	35.186092000	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
337	35.186094700	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
338	35.190395500	192.168.137.208	47.106.210.56	TLSv1.2	151	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
339	35.234646600	192.168.137.208	47.106.210.56	TLSv1.2	123	Application Data
340	35.234646700	192.168.137.208	47.106.210.56	TLSv1.2	123	Application Data
341	35.234647000	192.168.137.208	47.106.210.56	TLSv1.2	111	Application Data
342	35.284902700	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
343	35.284907000	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
344	35.429700600	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=1461 Win=0 Len=0
345	35.509615900	192.168.137.208	47.106.210.56	TLSv1.2	675	Application Data, Application Data, Application Data
346	35.539562100	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=1461 Win=0 Len=0

Frame 331: Packet, 575 bytes on wire (4608 bits) on interface \Device\NPF{...} (0x00000000-00000000-00000000-00000000) (16:ab:c5:32:a5:e6 (16:ab:c5:32:a5:e6))

Ethernet II, Src: 1a:da:25:7e:32:84 (1a:da:25:7e:32:84), Dst: 16:ab:c5:32:a5:e6 (16:ab:c5:32:a5:e6)

Internet Protocol Version 4, Src: 192.168.137.208, Dst: 47.106.210.56

Transmission Control Protocol, Src Port: 39078, Dst Port: 443, Seq: 1, Ack: 1, Len: 527

Transport Layer Security

Handshake Type: Client Hello (1)

Length: 508

Version: TLS 1.2 (0x0003)

Random: ef42a171047a77e714342503e7a085f84b7392ab5374a13d1c8da02a5609

GMT Unix Time: Mar 15, 2007 07:13:27.000000000 中国标准时间

Random Bytes: 03479ac714342503e7a085f84b7392ab5374a13d1c8da02a5609

A man-in-the-middle attack can cause an upgrade to fail

330	35.079643900	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=518 Win=0 Len=0
331	35.079644000	192.168.137.208	47.106.210.56	TLSv1.2	575	Client Hello (SHA256WithRSAEncryption)
332	35.130471600	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=518 Win=0 Len=0
333	35.130471700	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=518 Win=0 Len=0
334	35.134123100	47.106.210.56	192.168.137.208	TLSv1.2	1514	Server Hello
335	35.136744700	47.106.210.56	192.168.137.208	TLSv1.2	1413	Certificate, Server Key Exchange, Server Hello Done
336	35.186092000	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
337	35.186094700	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
338	35.190395500	192.168.137.208	47.106.210.56	TLSv1.2	151	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
339	35.234646600	192.168.137.208	47.106.210.56	TLSv1.2	123	Application Data
340	35.234646700	192.168.137.208	47.106.210.56	TLSv1.2	123	Application Data
341	35.234647000	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
342	35.284902700	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
343	35.284907000	192.168.137.208	47.106.210.56	TCP	58	Seq=518 Ack=1461 Win=0 Len=0
344	35.429700600	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=1461 Win=0 Len=0
345	35.509615900	192.168.137.208	47.106.210.56	TLSv1.2	675	Application Data, Application Data, Application Data
346	35.539562100	47.106.210.56	192.168.137.208	TCP	54	Seq=518 Ack=1461 Win=0 Len=0

Handshake Type: Certificate (11)

Length: 2098

Certificate Length: 2098

Certificate (2098 bytes)

Version: v3 (2)

Signature: sha256WithRSAEncryption

Signature (2098 bytes)

Algorithm: sha256WithRSAEncryption

Subject: CN=...

Algorithm: sha256WithRSAEncryption

Evidence

Updating the feature requires binding the EUT, and binding the EUT requires confirmation on the EUT.

Device

Sports push	>
Weather reports	>
Raise to Wake	Enabled >
Automatic Health Monitor	Disabled >
Find Watch	>
When you find the watch, it will vibrate	>
Wrist Preference	Left hand >
Hour Style	Hour Style 24 >
Frequent Contacts	>
Shake Photograph	>
Restore Factory Settings	>
Device Version	8269.0000.100 >



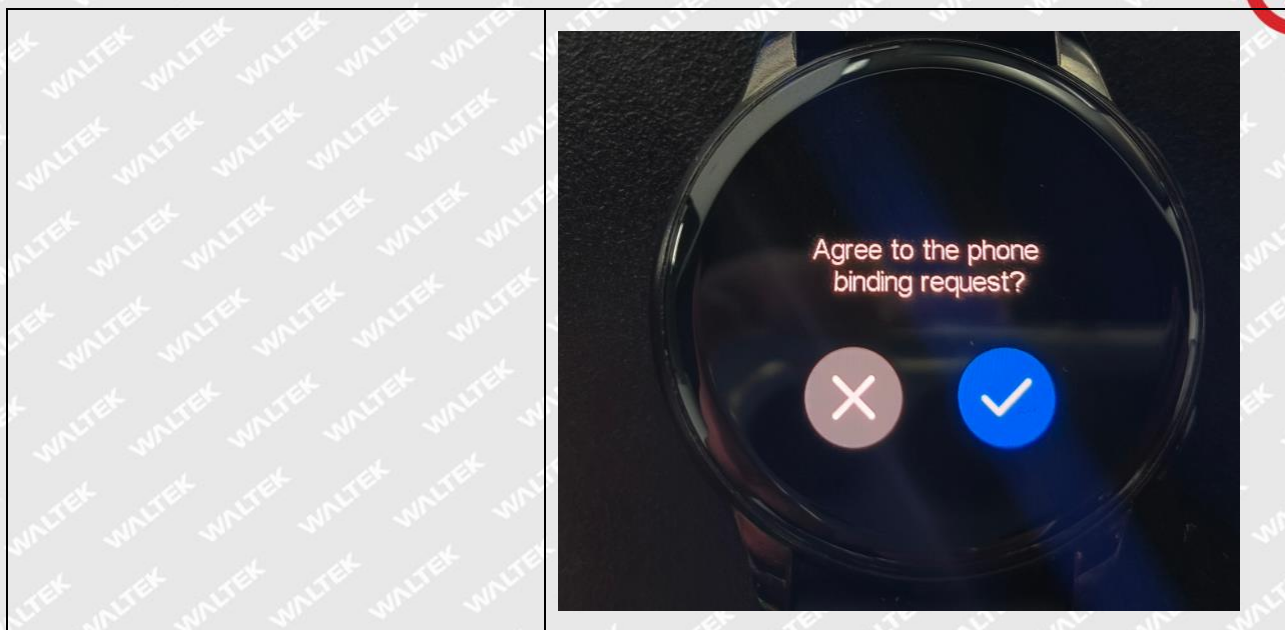
主页



设备



我的



3.3.3 [SUM-3] Automated updates

Conceptual assessment:

According to [E.Just.DT.SUM-3] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

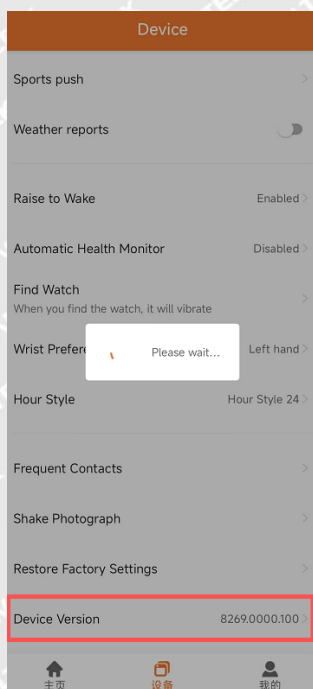
Functional sufficiency assessment

Descriptions	Test results	Verdict
The device can install updates "without human intervention on the device" or "by scheduling the installation of updates with human approval" or "by triggering the installation of updates with human approval". Successful update of relevant software components	The device can install updates by triggering the installation of updates with human approval.	PASS
Judgement (Verdict)	PASS	



Evidence

Requires the user to manually click to “Device Version”



3.4 [SSM] Secure storage mechanism

3.4.1 [SSM-1] Applicability of secure storage mechanisms

Conceptual assessment:

Wi-Fi credentials, which are protected by multiple security mechanisms. Physically, as a household product, the device enjoys basic environmental security; its storage chip is wrapped in a solid shell to resist direct contact under non-destructive disassembly. At the interface level, the device does not reserve any available physical debugging ports, thus cutting off the path to directly access internal storage through hardware. At the logical level, all high-risk remote network services (such as SSH) have been disabled, effectively preventing unauthorized network access. Therefore, the verdict of this conceptional test is **NOT APPLICABLE**.

Functional completeness assessment

There are no assets accessible by entities. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



Security, network assets are "persistently stored only through the secure storage mechanism documented in [E.Info.SSM-1.SecurityAsset.SSM]"	EUT stores data using cloud servers. Cloud storage prevents unauthorized access via the TLS protocol.	PASS
Judgement (Verdict)	PASS	
Evidence	Cloud storage	

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

Conceptual assessment:

According to the SSM-1 Conceptual assessment, there are no assets are accessible by entities, therefore the verdict of this conceptional test is **NOT APPLICABLE**.

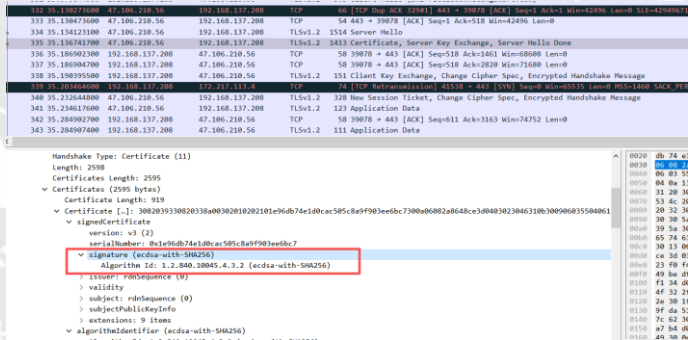
Functional completeness assessment

According to SSM-1 functional completeness assessment. The verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Secure storage mechanism "implemented in accordance with [E.Info.SSM-2.SSM.AccessControl]"	Entities can only access sensitive and confidential assets through access control.	PASS
Deny unauthorised modification of stored security, network assets	EUT ensures data integrity through the ecdsa-with-SHA256 signature algorithm.	PASS



Judgement (Verdict)	PASS
	Access Control  Evidence Ecdsa-with-SHA256 signature algorithm 

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

Conceptual assessment:

According to the SSM-1 Conceptual assessment, there are no assets are accessible by entities, therefore the verdict of this conceptual test is **PASS**.

Functional completeness assessment

According to SSM-1 functional completeness assessment. The verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment



Descriptions	Test results	Verdict
Secure storage mechanism "implemented in accordance with [E.Info.SSM-3.SSM.AccessControl]"	Screen Lock mechanism are implemented to protect the assets.	PASS
Deny unauthorised access to stored confidential security, network assets	If the authorized user denies the request, the EUT will fail to bind and will not be able to access the assets.	PASS
Judgement (Verdict)	PASS	
Evidence	Screen Lock  Deny unauthorised access to stored confidential security, private assets 	



3.5 [SCM] Secure communication mechanism

3.5.1 [SCM-1] Applicability of secure communication mechanisms

Conceptual assessment:

According to [E.Just.DT.SCM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

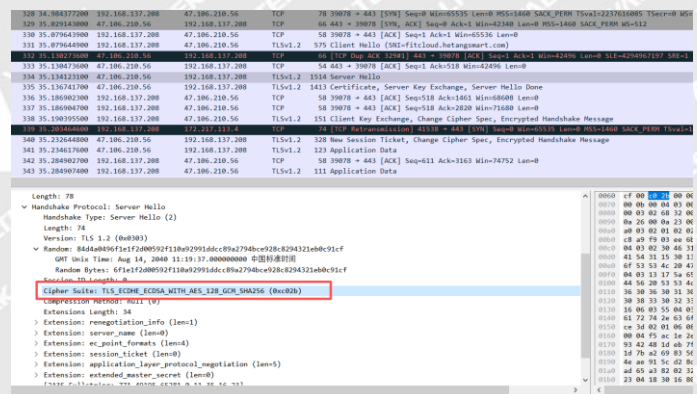
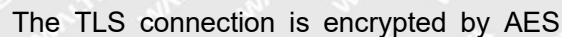
Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.SCM-1.NetworkAsset] and [E.Info.SCM-1.SecurityAsset]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
As described in [E.Info.SCM-1.SCM], a communication mechanism exists for communicating this security asset	1. According to the official Bluetooth documentation, Bluetooth Low Energy employs AES-CCM encryption for encrypted communication. 2. Once connected to the Internet, the device communicates with the cloud platform using the TLS encryption protocol to ensure a secure communication mechanism.	PASS
Judgement (Verdict)	PASS	

Evidence



Page 40 of 40

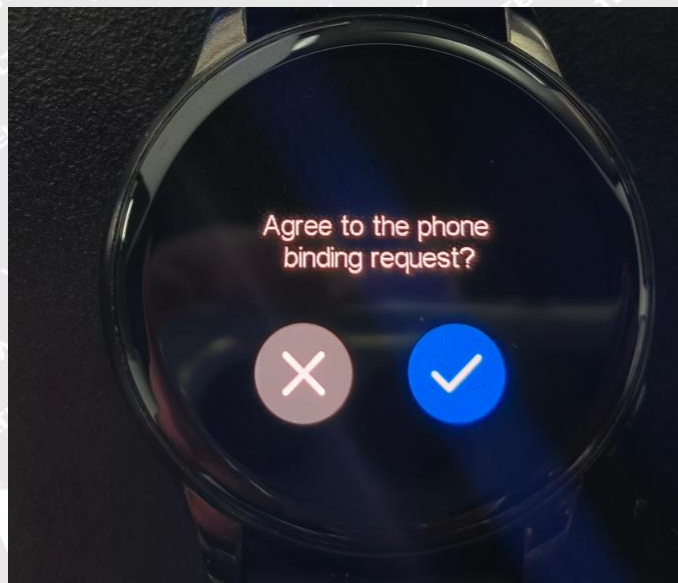


Functional sufficiency assessment

Descriptions		Test results	Verdict
Secrets used to protect authenticity and integrity cannot be intercepted and misused		The EUT can initiate a Bluetooth connection request ,which uses AES-CCM as encryption algorithm. The EUT communicate with Internet by TLS, which is encrypted with AES algorithm respectively.	PASS
Tampered with information is not considered complete information		The cloud platform service connection uses the HTTPS protocol, ensuring secure transmission through the TLS (Transport Layer Security) protocol, preventing man-in-the-middle interception of communication requests.	PASS
Unauthorised messages not accepted as authentic		Unauthorised messages not accepted as authentic	PASS
Successful man-in-the-middle attacks are not possible when using channel-based communication		TLS are used to prevent MITM attack. A Bluetooth man-in-the-middle attack requires the EUT to click 'agree' to connect on the user interface; if the EUT does not agree, the connection cannot be established.	PASS
Judgement (Verdict)	PASS		P A S S

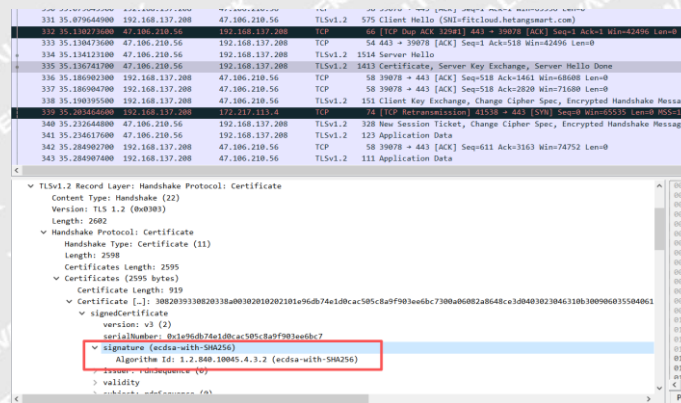


Bluetooth man-in-the-middle attack requires the EUT to click 'agree'.



Evidence

TLS uses SHA256 to prevent MITM attack







		t e d a n d m i s s u e d
--	--	---

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

Conceptual assessment:

According to [E.Just.DT.SCM-3] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

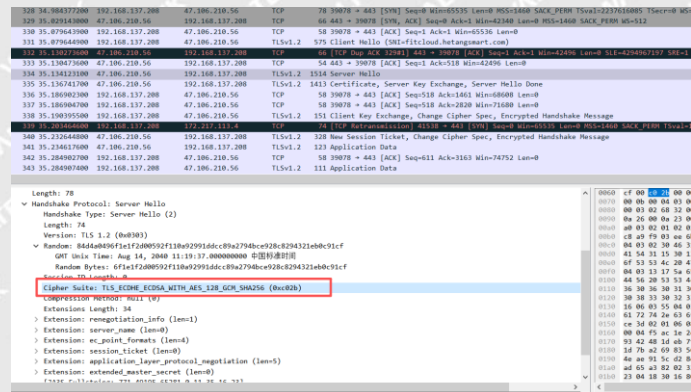
This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

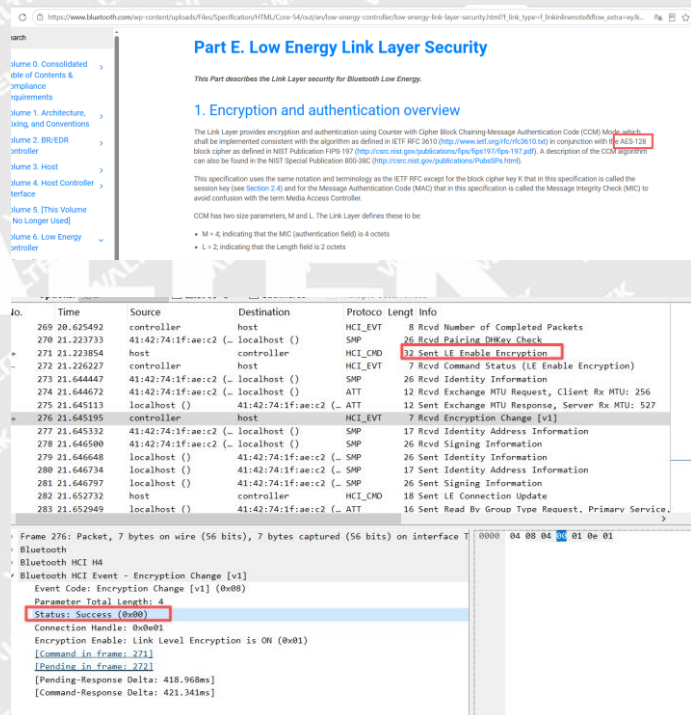
Descriptions	Test results	Verdict
The key used to encrypt the payload in the message must not be compromised	Using TLS and cellular authorization as protection of the key.	PASS
Communication security, network assets cannot be tapped	The security assets and network assets captured by Wireshark and are encrypted.	PASS

**Judgement (Verdict)****PASS**

The data connection to the cloud platform is transmitted via the TLS protocol, and the connection between the EUT and the Cloud Platform is encrypted using AES_128_GCM.



BLE link key is encrypted with AES-CCM 128bits

Evidence

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

Conceptual assessment:

According to [E.Just.DT.SCM-4] in technical documentation, the verdict of this conceptual test is **PASS**.



Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

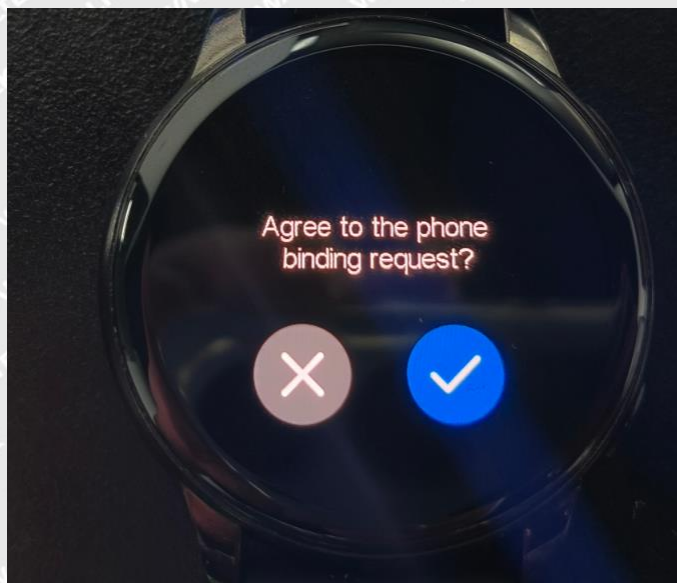
Descriptions	Test results	Verdict
No longer accepts copies (binary copies) of accepted information (part of secure, private asset communications)	1. Bluetooth data requests require the EUT to click 'Agree' on the interface; repeated attacks are ineffective. 2. TLS generates unique random numbers through the handshake, records sequence numbers and timestamps for verification, so that replayed old ciphertexts cannot pass session and timing verification, thereby defending against replay attacks.	PASS
Judgement (Verdict)	PASS	

WALTEK



Evidence

Sending repeat BLE request, unauthorised messages not accepted as authentic.



The data connection to the cloud platform is transmitted via the TLS protocol, and the connection between the EUT and the Cloud Platform is encrypted using AES_128_GCM.



3.6 [LGM] Logging mechanism

3.6.1[LGM-1]Applicability and appropriateness of logging mechanisms

Conceptual assessment:

According to [E.Just.DT.LGM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

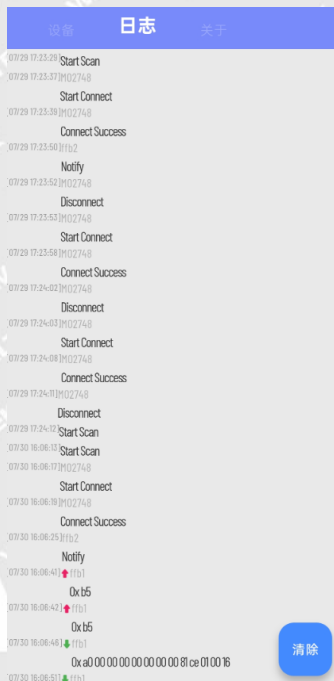
Functional completeness assessment

The verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



This event can be generated as documented in [E.Info.LGM-1.PrivacyAssetEvent.	The logs of the EUT are stored in the connected mobile phone.	PASS
Log data can be accessed as described in [E.Info.LGM-1.PrivacyAssetEvent.	Device log can be accessed	PASS
Judgement (Verdict)	PASS	
Evidence		

3.6.2 [LGM-2] Persistent storage of log data

Conceptual assessment:

According to [E.Just.DT.LGM-2] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Log data of relevant events (i.e. test items) exists in the device memory	EUT can store logs in the Phone for a long period.	N/A



Judgement (Verdict)	N/A
Evidence	

3.6.3 [LGM-3] Minimum number of persistently stored events

Conceptual assessment:

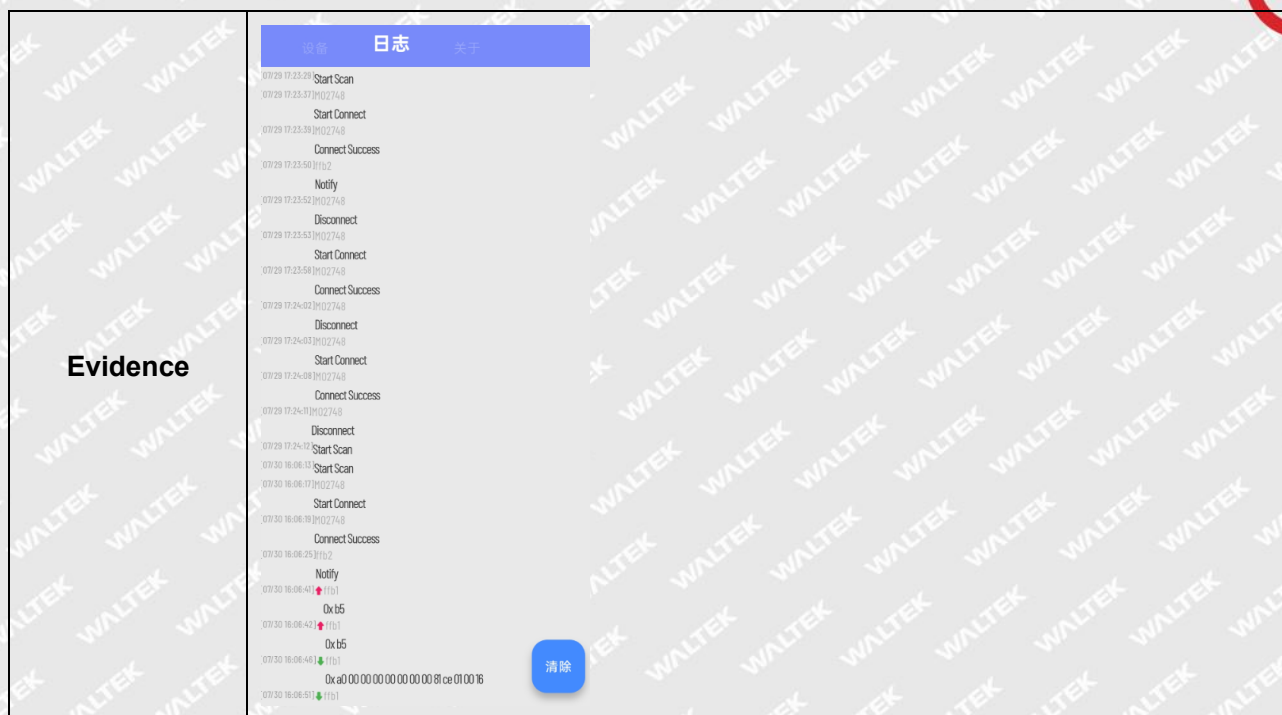
According to [E.Just.DT.LGM-3] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Generates the number of logging events recorded in [E.Info.LGM-3.Quantity].	EUT log storage is external, and the number of logs stored depends on the phone's capacity.	PASS
Judgement (Verdict)	PASS	



3.6.4 [LGM-4] Time-related information of persistently stored log data

Conceptual assessment:

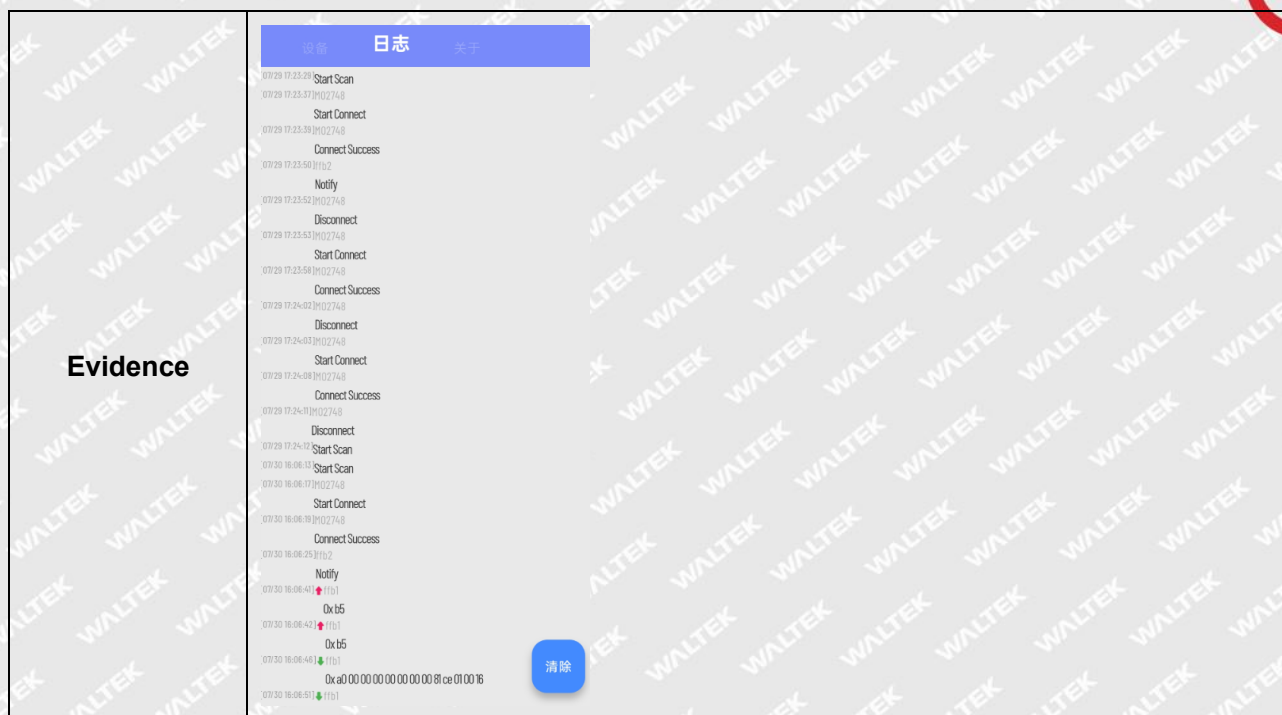
According to [E.Just.DT.LGM-4] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
When real-time information is not available, "Log data stored continuously on the device includes time-related information recorded in [E.Info.LGM-4.LGM.Timerelated].	Log data stored continuously on the device includes time-related	PASS
Judgement (Verdict)	PASS	



3.7 [DLM] Deletion mechanism

3.7.1 [DLM-1] Applicability of deletion mechanisms

Conceptual assessment:

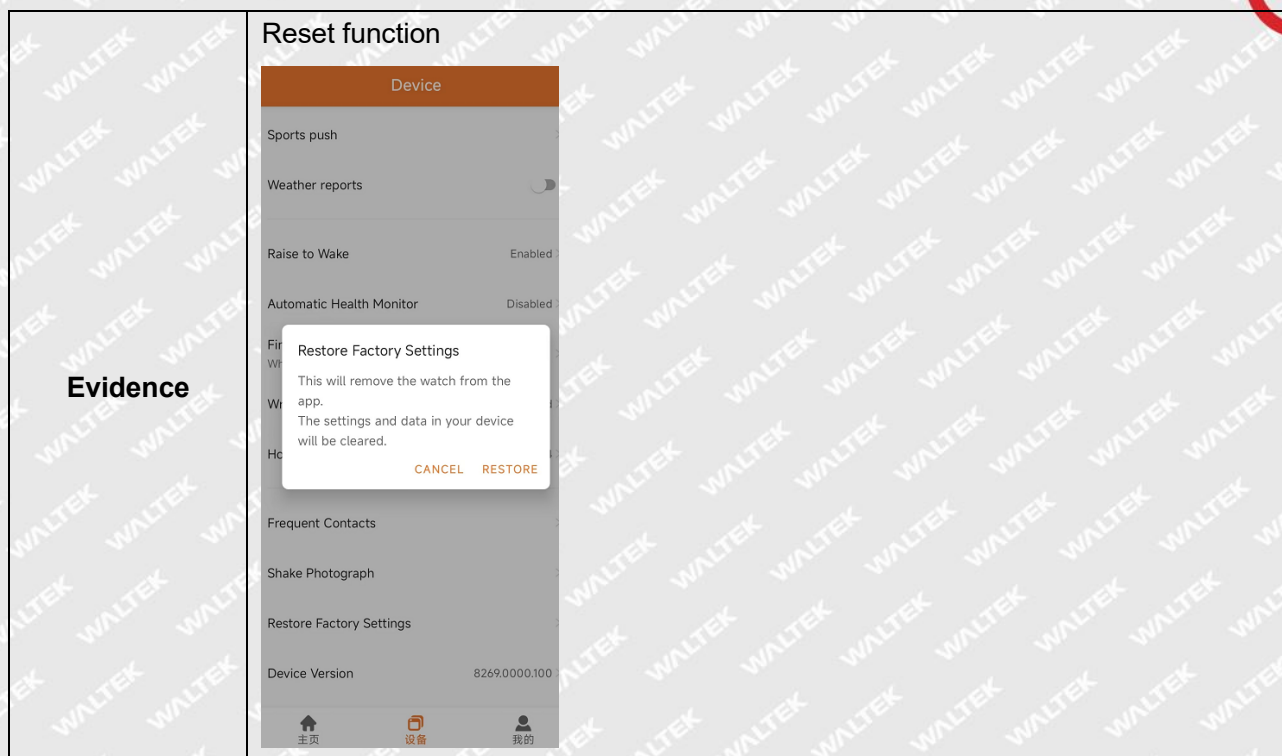
According to [E.Just.DT.DLM-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and privacy assets accessible by entities have been recorded in [E.Info.DLM-1.PrivacyAsset] and [E.Info.DLM-1.SecurityAsset]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Personal information may be deleted through the deletion mechanism recorded in [E.Info.DLM-1.DLM].	The EUT has a factory reset function.	PASS
Judgement (Verdict)	PASS	



Evidence

3.8 [UNM] User notification mechanism

3.8.1 [UNM-1] Applicability of user notification mechanisms

Conceptual assessment:

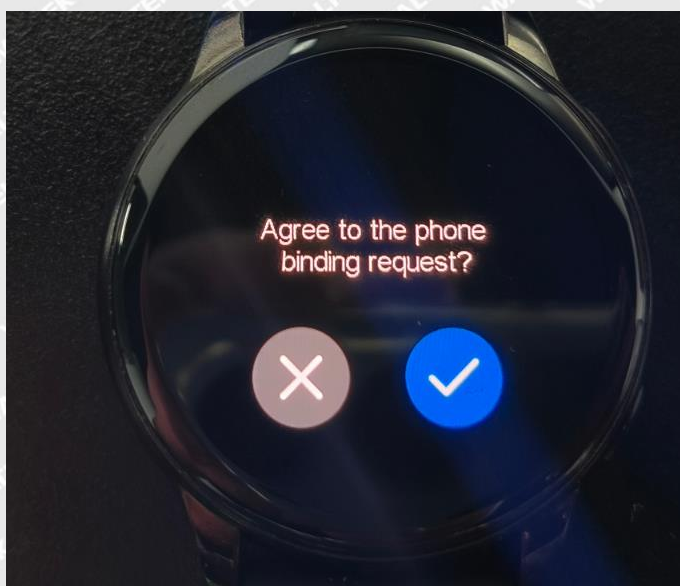
According to [E.Just.DT.UNM-1] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

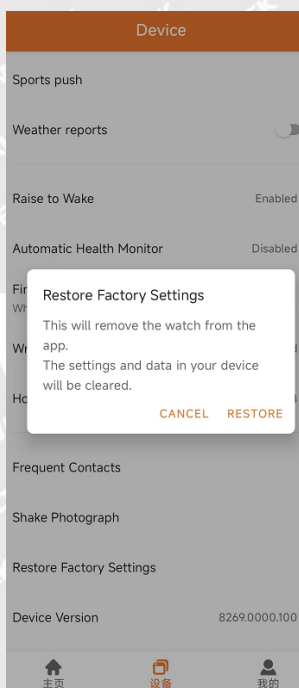
All security assets and privacy assets accessible by entities have been recorded in [E.Info.UNM-1]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
This test item "Each use case documented in [E.Info.UNM-1.PersonalInformation.UseCase.Notification] has at least one user notification mechanism"	A prompt will appear asking whether to agree to the binding when the EUT is first bound, and a prompt will appear asking whether to agree when restoring to factory settings.	PASS
Judgement (Verdict)	PASS	



Evidence



3.8.2 [UNM-2] Appropriate user notification content

Conceptual assessment:

According to [E.Just.DT.UNM-2] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

This Functional completeness assessment is covered by the Functional sufficiency assessment of the applicability of the certification scheme. Therefore, this Functional completeness assessment is not required. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment



Descriptions	Test results	Verdict
The content of each notification for the test item is as described in [E.Info.UNM-2.Notifications.UseCase.Content]	The notification content includes a description of the changes and their impact on users.	PASS
Judgement (Verdict)	PASS	
Evidence		

3.9 [CCK] Confidential cryptographic keys

3.9.1 [CCK-1] Appropriate CCKs

Conceptual assessment:

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

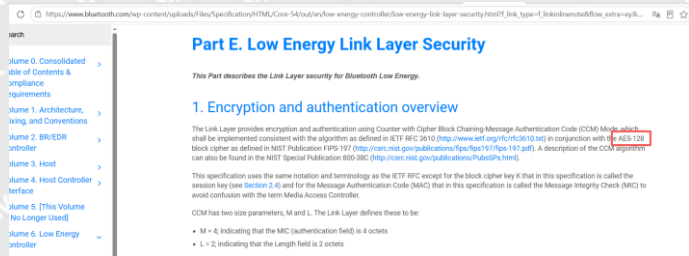
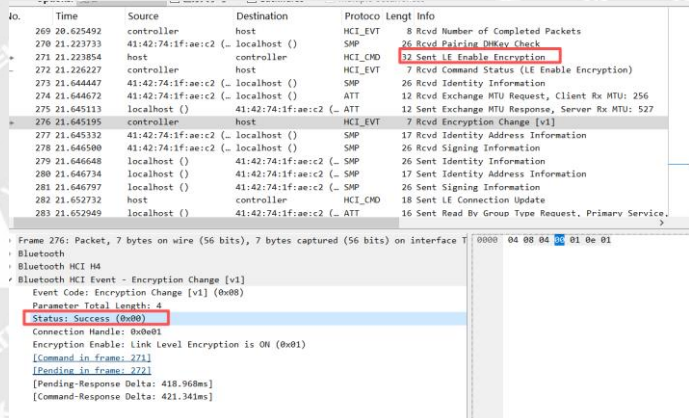
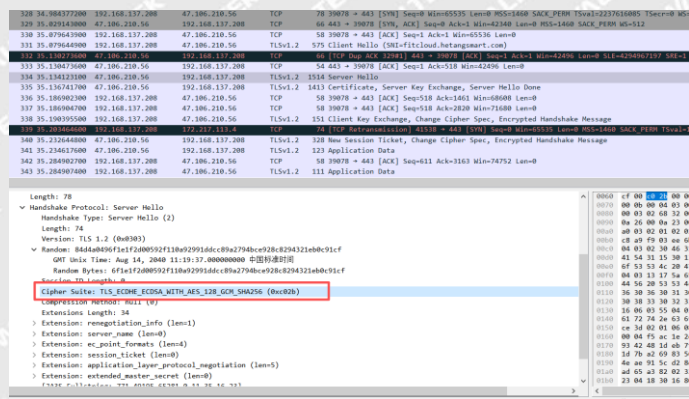
Functional completeness assessment

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



The CCK lengths recorded in [E.Info.CCK-1.CCK] are realized according to [E.Info.CCK-1.CCK.SecurityStrength	1.Blutetooth connection request ,which uses AES-CCM as encryption algorithm with AES-CCM 128bit key. 2.The connection EUT and Cloud Plat form is encrypted with 128bit key.	PASS
Judgement (Verdict)	PASS	
Evidence	BLE link key is encrypted with AES-CCM 128bit key  Part E. Low Energy Link Layer Security This Part describes the Link Layer security for Bluetooth Low Energy. 1. Encryption and authentication overview The Link Layer provides encryption and authentication using Counter with Cipher Block Chaining Message Authentication Code (CCM) mode. The CCM mode shall be implemented consistent with the algorithm as defined in IEEE 802.15.4-2015 (http://www.ieee.org/10.1109/802.15.4-2015) in conjunction with the AES-128 block cipher as defined in NIST Publication FIPS 197 (http://csrc.nist.gov/publications/fips/fips197/fips197.pdf). A description of the CCM mode can also be found in the NIST Special Publication 800-38C (http://csrc.nist.gov/publications/PubsSPs.html). This specification uses the same notation and terminology as the IEEE 802.15.4-2015 for the block cipher key K that in this specification is called the session key (see Section 2.4) and for the Message Authentication Code (MAC) that in this specification is called the Message Integrity Check (MIC) to avoid confusion with the term Media Access Control. CCM has two size parameters, M and L. The Link Layer defines these to be: • M = 4, indicating that the MIC (authentication field) is 4 octets • L = 2, indicating that the Length field is 2 octets  io. Time Source Destination Protocol Length Info 269 20.625492 controller host HCI_EVT 8 Rcvd Number of Completed Packets 270 21.223733 41:42:74:1f:ae:c2 (-. local host ()) SMP 26 Rcvd Pairing Done/AV-Check 271 21.223854 host controller HCI_CMD 32 Sent LE Enable Encryption 272 21.226227 controller host HCI_EVT 7 Rcvd Command Status (LE Enable Encryption) 273 21.644447 41:42:74:1f:ae:c2 (-. local host ()) SMP 26 Rcvd Identity Information 274 21.644672 41:42:74:1f:ae:c2 (-. local host ()) ATT 12 Rcvd Exchange MTU Request, Client Rx MTU: 256 275 21.645113 local host () 41:42:74:1f:ae:c2 (-. ATT 12 Sent Exchange MTU Response, Server Rx MTU: 527 276 21.645195 controller host HCI_EVT 7 Rcvd Encryption Change [v1] 277 21.645332 41:42:74:1f:ae:c2 (-. local host ()) SMP 17 Rcvd Identity Address Information 278 21.646500 41:42:74:1f:ae:c2 (-. local host ()) SMP 26 Rcvd Signing Information 279 21.646648 local host () 41:42:74:1f:ae:c2 (-. SMP 26 Sent Identity Information 280 21.646734 local host () 41:42:74:1f:ae:c2 (-. SMP 17 Sent Identity Address Information 281 21.646797 local host () 41:42:74:1f:ae:c2 (-. SMP 26 Sent Signing Information 282 21.652732 host controller HCI_CMD 18 Sent LE Connection Update 283 21.652949 local host () 41:42:74:1f:ae:c2 (-. ATT 16 Sent Read By Group Type Request, Primary Service... Frame 276: Packet, 7 bytes on wire (56 bits), 7 bytes captured (56 bits) on interface T 0000 04 08 04 01 0e 01 Bluetooth Bluetooth HCI H4 Bluetooth HCI Event - Encryption Change [v1] Event Code: Encryption Change [v1] (0x08) Parameter Total Length: 4 Status: Success (0x00) Connection Handle: 0x0001 Encryption Enable: Link Level Encryption is ON (0x01) [Command in frame: 271] [Pending in frame: 272] [Pending-Response Delta: 418.968ms] [Command-Response Delta: 421.341ms] The connection EUT and Cloud Platform is encrypted with 128bit key  128 34.98437200 192.168.137.200 47.106.210.56 TCP 76 39078 → 443 [SYN] Seq=65535 Len=0 MSS=6408 SACK_PERM TSval=223761888 TSecr=0 129 35.82914300 47.106.210.56 192.168.137.200 TCP 60 443 → 39078 [SYN, ACK] Seq=0 Ack=65535 Len=0 MSS=6408 SACK_PERM TSval=0 TSecr=223761888 130 35.87964300 192.168.137.200 47.106.210.56 TCP 58 39078 → 443 [ACK] Seq=1 Ack=1 Min=65536 Len=0 131 35.87964300 192.168.137.200 47.106.210.56 TLSv1.2 575 Client Hello (001-FitzCloud.Hetangmart.com) 132 35.87964300 47.106.210.56 192.168.137.200 TLS 441 [ChangeCipherSpec] ChangeCipherSpec (001) 133 35.13817100 47.106.210.56 192.168.137.200 TCP 54 443 → 39078 [ACK] Seq=1 Ack=518 Min=65536 Len=0 134 35.13817100 47.106.210.56 192.168.137.200 TLSv1.2 1514 Server Hello 135 35.13674100 47.106.210.56 192.168.137.200 TLSv1.2 1413 Certificate, Server Key Exchange, Server Hello Done 136 35.13690200 192.168.137.200 47.106.210.56 TCP 58 39078 → 443 [ACK] Seq=518 Ack=1413 Min=60008 Len=0 137 35.13690200 192.168.137.200 47.106.210.56 TCP 58 39078 → 443 [ACK] Seq=518 Ack=2820 Min=71680 Len=0 138 35.13693500 192.168.137.200 47.106.210.56 TLSv1.2 355 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message 139 35.13693500 47.106.210.56 192.168.137.200 TLS 74 [ChangeCipherSpec] ChangeCipherSpec (001) 140 35.23264800 47.106.210.56 192.168.137.200 TLSv1.2 328 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message 141 35.23461700 47.106.210.56 192.168.137.200 TLSv1.2 123 Application Data 142 35.28490700 192.168.137.200 47.106.210.56 TCP 58 39078 → 443 [ACK] Seq=611 Ack=3163 Min=74752 Len=0 143 35.28490700 192.168.137.200 47.106.210.56 TLSv1.2 111 Application Data Length: 78 Handshake Protocol: Server Hello Handshake Type: Server Hello (2) Length: 74 Version: TLS 1.2 (0x0303) Random: 844d4806f1e1f080932f138a2991d6c8ba2784bc928c8294321ebbc91cf GMT Unix Time: Aug 14, 2040 11:19:17.000000000 0285938278 Random Bytes: 6f1ef2080932f138a2991d6c8ba2784bc928c8294321ebbc91cf Compression Method: null (0) Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc030) Extensions Length: 34 Extension: renegotiation_info (len=1) Extension: server_name (len=0) Extension: ec_point_formats (len=4) Extension: session_ticket (len=0) Extension: application_layer_protocol_negotiation (len=5) Extension: extended_master_secret (len=0) 2556 23.04 18 30 16 86	



3.9.2 [CCK-2] CCK Generation Mechanisms

Conceptual assessment:

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional completeness assessment

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptual test is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
There is significant complexity surrounding the validation of cryptographic key generation mechanisms and typically they will be implemented by a third party with significant cryptographic expertise, who is unlikely to share details of such key generation processes. Given these considerations, no functional sufficiency assessment is provided for this requirement	1.The data being transferred by BLE using AES-CCM cryptography to encrypt the method by which the keys are exchange	PASS
	2.The TLS key is stored in the cloud, and it is connected between the mobile phone and the cloud, unrelated to the EUT.	N/A
Judgement (Verdict)	PASS	
Evidence	BLE Link key generation mechanism <pre> graph TD PIN --> E2 E2 --> LinkKey[Link Key] LinkKey --> UnitKey[Unit key] LinkKey --> CombKey[Combination key] LinkKey --> MasterKey[Master key] LinkKey --> E3 E3 --> EncKey[Encryption Key] LinkKey -- "For Authentication Procedure" --> AuthProc[] EncKey -- "For Encryption Procedure" --> EncProc[] </pre>	



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

Conceptual assessment:

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptional test is **NOT APPLICABLE**.

Functional completeness assessment

The device does not have a pre-installed key when it leaves the factory, and the encryption key generation mechanism is not used yet. Therefore, the verdict of this conceptional test is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
comparing the CCKs and confirming that they are not the same and there is no obvious way to derive one from the other	There are no preinstalled CCKs in the EUT	NOT APPLICABLE
Judgement (Verdict)	NOT APPLICABLE	
Evidence	N/A	

3.10 [GEC] General equipment capabilities

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

Conceptual assessment:

According to [E.Just.DT.GEC-1] in technical documentation, the verdict of this conceptional test is **PASS**.

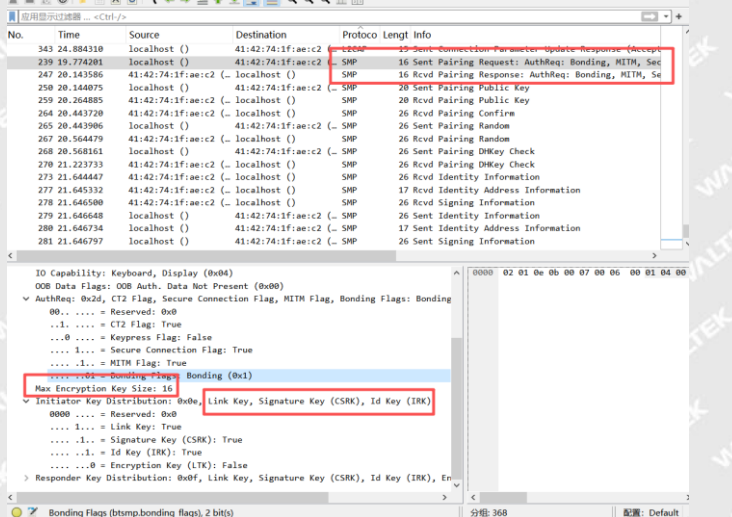
Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-1]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
--------------	--------------	---------



Measures have been taken as described in [E.Info.GEC-1.ListOfVulnerabilities] to ensure that assets cannot be affected if test items are utilized	The EUT only enables Bluetooth services. By capturing and analyzing the Bluetooth SMP pairing traffic, it is observed that the BLE device under test negotiates with the communication terminal to use the LE Secure Connections (SMP v2) security connection mechanism. Both parties complete key negotiation based on the ECDH elliptic curve algorithm. The negotiation process includes standard secure connection exchange messages such as public key exchange and DH key check. In the pairing negotiation messages, the AuthReq field simultaneously enables the Bonding flag, MITM protection flag, and Secure Connections mandatory flag. The communication link uses AES-128 encryption key length, and the protocol layer refuses to downgrade to the traditional SMP v1 pairing process. After the negotiation is complete, the device normally distributes key materials such as the IRK identity resolving key and CSRK signing key, and supports the bonding reconnection mechanism. It is determined that the EUT does not have any known publicly exploitable vulnerabilities.	PASS
Judgement (Verdict)	PASS	
Evidence		



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

Conceptual assessment:

According to [E.Just.DT.GEC-2] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-2]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Functionally assess whether there are further network interfaces or services (via network interfaces) exposed in factory default state, which are not listed in [E.Info.GEC-2.NetworkInterface.Exposure] or which are not required for setup according to [E.Info.GEC-2.Setup] or to operate the equipment in basic operation.	EUT only enables Bluetooth services, that is necessary.	PASS
Judgement (Verdict)	PASS	
Evidence	5.4. Call records You can save the latest 10 call records. 5.5. Voice Bluetooth Call Bluetooth: Divided into "call audio" and "media audio" switch. Call audio: It is used to switch to call by wireless connection. Media audio: It is used to switch to play media audio. (Disabled by default.) 1) You can turn on the media audio only when the voice audio is enabled. 2) When "media audio" is on, turn off "call audio", media audio switch will be closed simultaneously. 3) In the case of (2), turn on "call audio", and the "media audio" switch will be opened synchronously. 5.6. Speed dial	

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

Conceptual assessment:



According to [E.Just.DT.GEC-3] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-3]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Test items are configurable	Bluetooth is configurable.	PASS
Only authorized users can configure the [test project] settings (i.e., access control mechanisms and authentication mechanisms have been established)	Authorized users can change the status of BLE to Disabled by click 'Shutdown'.	PASS
Judgement (Verdict)	PASS	
Evidence		

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

Conceptual assessment:

According to [E.Just.DT.GEC-4] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment



All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-4]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
The equipment's user documentation shall contain a description of — all exposed network interfaces; and — all services exposed via network interfaces	The network interface is published in the user manual.	PASS
Judgement (Verdict)	PASS	
Evidence	5.4. Belgeschiedenis Bewaar de laatste 10 oproepgegevens. 5.5. Spraak-Bluetooth Bluetooth voor bellen is onderverdeeld in twee schakelaars: "gespreksgeluid" en "media-audio". Gespreksgeluid: Wordt gebruikt voor draadloos bellen. Media-audio: Wordt gebruikt voor het afspelen van mediageluid (standaard uitgeschakeld). 1) Media-audio kan alleen worden ingeschakeld als gespreksgeluid is ingeschakeld. 2) Wanneer "media-audio" is ingeschakeld en je "gespreksgeluid" uitschakelt, wordt "media-audio" automatisch ook uitgeschakeld. 3) In het geval van situatie (2), als je "gespreksgeluid" weer inschakelt, wordt de schakelaar voor "media-audio" automatisch ook weer ingeschakeld. 5.6. Sportgegevens	

3.10.5 [GEC-5] No unnecessary external interfaces

Conceptual assessment:

According to [E.Just.DT.GEC-5] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-5]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Is the physical external interface necessary for the intended functionality	The physical external interfaces of the EUT are all necessary	PASS
Judgement (Verdict)	PASS	



Evidence

2. Charging

Use the provided cable for charging. Charging time is more than 2 hours. If the watch is not used for a long time, make sure to turn off the watch and keep charging once a month.



1. Touch menu
2. Up button
3. Down button
4. Sensor
5. Magnetic suction contact

3.10.6 [GEC-6] Input validation

Conceptual assessment:

According to [E.Just.DT.GEC-6] in technical documentation, the verdict of this conceptual test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.GEC-6]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions		Test results	Verdict
Test items against (relevant) "attacks related to input mechanisms"		Bluetooth interface refuses input	PASS
Judgement (Verdict)	PASS		



Evidence	Bluetooth input 07/30 16:06:17]M02748 Start Connect 07/30 16:06:19]M02748 Connect Success 07/30 16:06:25]ffb2 Notify 07/30 16:06:41]ffb1 Ox b5 07/30 16:06:42]ffb1 Ox b5 07/30 16:06:46]ffb1 Ox a0 00 00 00 00 00 00 00 81 ce 01 00 16 07/30 16:06:51]ffb1 清除
----------	--

3.10.7 [GEC-7] Documentation of external sensing capabilities

Conceptual assessment:

According to [E.Just.DT.GEC-7] in technical documentation, the verdict of this conceptional test is **NOT APPLICABLE**.

Functional completeness assessment

There is no non-network external interfaces that may affect the privacy of users or subscribers. Therefore the verdict of this Functional completeness assessment is **NOT APPLICABLE**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Does the user documentation mention the sensor	The user documentation mentions the sensor.	PASS
Judgement (Verdict)	PASS	

**Evidence****2. Charging**

Use the provided cable for charging. Charging time is more than 2 hours. If the watch is not used for a long time, make sure to turn off the watch and keep charging once a month.



1. Touch menu
2. Up button
3. Down button
4. Sensor
5. Magnetic suction contact

3.11 [CRY] Cryptography**3.11.1 [CRY-1] Best practice cryptography****Conceptual assessment:**

According to [E.Just.DT.CRY-1] in technical documentation, the verdict of this conceptional test is **PASS**.

Functional completeness assessment

All security assets and network assets accessible by entities have been recorded in [E.Info.CRY-1]. Therefore the verdict of this Functional completeness assessment is **PASS**.

Functional sufficiency assessment

Descriptions	Test results	Verdict
Mechanisms using encryption are implemented as described, with no indication of any deviation from the documentation	1. Bluetooth connection request uses AES-CCM as the encryption algorithm 2. The update package is protected by TLS.	PASS
Judgement (Verdict)	PASS	



Evidence

1. Encryption and authentication overview

This specification uses the same notation and terminology as the IEEE RFC except for the block cipher key K that in this specification is called the session key (see [Section 2.4](#)) and for the Message Authentication Code (MAC) that in this specification is called the Message Integrity Check (MIC) to avoid confusion with the term Media Access Controller.

CCM has two size parameters, M and L . The Link Layer defines these to be

- M = 4; indicating that the MIC (authentication field) is 4 octets
- L = 2; indicating that the Length field is 2 octets

No.	Time	Source	Destination	Protocol	Length	Info
269	20.425492	controller	192.168.1.8	HTTP	8	26 Rcvd Number of Completed Packets
270	21.223793	41:42:74:1fafe:c2 (local host)	local host	SMTP	26	26 Rcvd Local DMMX Check
271	21.223854	host	controller	HCI_CMD	32	32 Sent If Enable Encryption
272	21.226227	controller	host	HCI_EVT	7	7 Rcvd Command Status (If Enable Encryption)
273	21.644447	41:42:74:1fafe:c2 (local host)	local host	SMTP	26	26 Rcvd Identity Information
274	21.644672	41:42:74:1fafe:c2 (local host)	local host	ATT	12	12 Rcvd Exchange MTU Request, Client Rx MTU: 256
275	21.645113	local host	41:42:74:1fafe:c2 (local host)	ATT	12	12 Sent Exchange MTU Response, Server Rx MTU: 527
276	21.645195	controller	host	HCI_EVT	7	7 Rcvd Encryption Change [v1]
277	21.645332	41:42:74:1fafe:c2 (local host)	local host	SMTP	17	17 Rcvd Identity Address Information
278	21.646500	41:42:74:1fafe:c2 (local host)	local host	SMTP	26	26 Rcvd Signing Information
279	21.646648	local host	41:42:74:1fafe:c2 (local host)	SMTP	17	17 Sent Identity Information
280	21.646734	local host	41:42:74:1fafe:c2 (local host)	SMTP	17	17 Sent Identity Address Information
281	21.646797	local host	41:42:74:1fafe:c2 (local host)	SMTP	26	26 Sent Signing Information
282	21.652732	host	controller	HCI_CMD	18	18 Sent LE Connection Update
283	21.652949	local host	41:42:74:1fafe:c2 (local host)	ATT	18	18 Sent Read By Group Type Request, Primary Service

Frame 276: Packet, 7 bytes on wire (56 bits), 7 bytes captured (56 bits) on interface T 0000 04 08 04 00 01 0e 01

```
Bluetooth
Bluetooth HCI H4
Bluetooth HCI Event - Encryption Change [v1]
Event Code: Encryption Change [v1] (0x00)
Parameter Total Length: 4
Status: Success (0x00)
Connection Handle: 0x0001
Encryption Enable: Link Level Encryption is ON (0x01)
[Command in frame: 271]
[Pending in frame: 272]
[Pending-Response Delta: 418.968ms]
[Command-Response Delta: 421.341ms]
```

[illegible]

```
length: 78  
Handshake Protocol: Server Hello  
Version: TLSv1.2 (0x0003)  
Random: f6daeb9f2ef17e005f1f3d92991dd6;cf2978abcf3fb2c93412bbdcf3f  
GOT User Info: Aug 14, 2040 11:19:37.000000000 中国香港  
Random Bytes: cf2ef17e005f1f3d92991dd6;cf2978abcf3fb2c93412bbdcf3f  
Random.X.Length=38  
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)  
compression_method=none  
Extension Length: 84  
Extension: renegotiation_info (len=1)  
Extension: server_name (len=0)  
Extension: ec_point_formats (len=0)  
Extension: session_ticket (len=0)  
Extension: application_layer_protocol_negotiation (len=5)  
Extension: extended_master_secret (len=0)  
EXTENSION_DATA_LEN=0x00000000
```



4. Assignment of verdict

Tests may be judged as "PASS" or "FAIL" or "NOT APPLICABLE".

- If there is no evidence that the documented security mechanism has not been implemented, the judgement is "PASS";
- If there is evidence that the documented security mechanism has not been implemented, the judgement is "FAIL";
- The verdict "NOT APPLICABLE" for the assessment case is assigned otherwise.

WALTEK



Appendix I : Photos of the EUT



[END OF REPORT]



中国认可
国际互认
检测
TESTING
CNAS L6478



TEST REPORT

Reference No. : WTF25F06152819W001
Applicant..... : Mid Ocean Brands B.V.
Address..... : Unit 711-716, 7/F., Tower A, 83 King Lam Street, Cheung Sha Wan,
Kowloon, Hong Kong.
Manufacturer : 118897
Address..... : ---
Product Name..... : Smart watch
Model No..... : MO2748
Test specification..... : ETSI EN 300 328 V2.2.2 (2019-07)
Date of Receipt sample : 2025-06-17
Date of Test..... : 2025-06-24
Date of Issue..... : 2025-06-28
Test Report Form No. : WEW-300328A-01B
Test Result..... : Pass

Remarks:

The results shown in this test report refer only to the sample(s) tested, this test report cannot be reproduced, except in full, without prior written permission of the company. The report would be invalid without specific stamp of test institute and the signatures of approver.

Prepared By:

Waltek Testing Group (Foshan) Co., Ltd.

Address: 1/F., Building 19, Sunlink Machinery City, Xingye 4 Road,
Guanglong Industrial Park, Chihua Neighborhood Committee, Chencun,
Shunde District, Foshan, Guangdong, China

Tel:+86-757-23811398

Fax:+86-757-23811381

E-mail:info@waltek.com.cn

Tested by:

Roy Hong

Approved by:

Danny Zhou



1 Test Summary

Radio Spectrum			
Test	Test Requirement	Limit / Severity	Result
RF output power	ETSI EN 300 328 V2.2.2	≤20dBm	Pass
Power Spectral Density	ETSI EN 300 328 V2.2.2	≤10dBm/MHz	Pass
Duty Cycle, Tx-sequence, Tx-gap	ETSI EN 300 328 V2.2.2	Duty Cycle≤manufacturer declare value Tx-sequence:3.5~10ms Tx-gap:3.5~10ms	N/A
Medium Utilization	ETSI EN 300 328 V2.2.2	≤10%	N/A
Adaptivity	ETSI EN 300 328 V2.2.2	Clause 4.3.1.7	N/A
Occupied Channel Bandwidth	ETSI EN 300 328 V2.2.2	Within the band 2400-2483.5MHz	Pass
Transmitter unwanted in the OOB domain	ETSI EN 300 328 V2.2.2	Figure 3	Pass
Transmitter unwanted emissions in the spurious domain	ETSI EN 300 328 V2.2.2	Table 12	Pass
Receiver spurious emissions	ETSI EN 300 328 V2.2.2	Table 13	Pass
Receiver Blocking	ETSI EN 300 328 V2.2.2	Clause 4.3.2.11.4.2	Pass

Remark:

Pass Test item meets the requirement

N/A Not Applicable



2 Contents

	Page
1 TEST SUMMARY	2
2 CONTENTS	3
3 GENERAL INFORMATION	4
3.1 GENERAL DESCRIPTION OF E.U.T.	4
3.2 TECHNICAL SPECIFICATION	4
3.3 STANDARDS APPLICABLE FOR TESTING	5
3.4 TEST FACILITY	5
3.5 SUBCONTRACTED	5
3.6 ABNORMALITIES FROM STANDARD CONDITIONS	5
3.7 DISCLAIMER	5
4 EQUIPMENT USED DURING TEST	6
4.1 EQUIPMENT LIST	6
4.2 SOFTWARE LIST	7
4.3 SPECIAL ACCESSORIES AND AUXILIARY EQUIPMENT	7
4.4 MEASUREMENT UNCERTAINTY	7
4.5 DECISION RULE	7
5 TEST CONDITIONS AND TEST MODE	8
5.1 RF CHANNEL AND FREQUENCY	8
5.2 INDEPENDENT OPERATION MODES	8
5.3 TEST ENVIRONMENT CONDITION	8
6 RF REQUIREMENTS	9
6.1 RF OUTPUT POWER	9
6.2 POWER SPECTRAL DENSITY	18
6.3 OCCUPIED CHANNEL BANDWIDTH	23
6.4 TRANSMITTER UNWANTED EMISSIONS IN THE OUT-OF-BAND DOMAIN	26
6.5 TRANSMITTER UNWANTED EMISSIONS IN THE SPURIOUS DOMAIN	33
6.6 RECEIVER SPURIOUS EMISSIONS	35
6.7 RECEIVER BLOCKING	37
7 PHOTOGRAPHS - TEST SETUP	42
7.1 PHOTOGRAPH - SPURIOUS EMISSIONS TEST SETUP	42
8 PHOTOGRAPHS – EUT CONSTRUCTIONAL DETAILS	43



3 General Information

3.1 General Description of E.U.T.

Product Name : Smart watch
Model No. : MO2748
Remark : ---
Rating : Input: DC 5V
Battery Capacity : 3.8V, 300mAh, 1.14Wh
Adapter Model..... : ---

3.2 Technical Specification

Bluetooth Version : Bluetooth LE
Frequency Range : 2402-2480MHz
Maximum RF Output Power : 2.47 dBm (EIRP)@1Mbps
Type of Modulation : GFSK
Quantity of Channels : 40
Channel Separation..... : 2MHz
Data Rate : 1Mbps, 2Mbps
Antenna Type..... : Wire Antenna
Antenna Gain : -1.8dBi
Receiver Category : 2

Receiver Category	Description
1	Adaptive equipment with a maximum RF output power greater than 10 dBm e.i.r.p.
2	non-adaptive equipment with a Medium Utilization (MU) factor greater than 1 % and less than or equal to 10 % (irrespective of the maximum RF output power); or equipment (adaptive or non-adaptive) with a maximum RF output power greater than 0 dBm e.i.r.p. and less than or equal to 10 dBm e.i.r.p.
3	non-adaptive equipment with a maximum Medium Utilization (MU) factor of 1 % (irrespective of the maximum RF output power) or equipment (adaptive or non-adaptive) with a maximum RF output power of 0 dBm e.i.r.p.



3.3 Standards Applicable for Testing

The tests were performed according to following standards:

ETSI EN 300 328 V2.2.2 (2019-07)	Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the RED Directive.
-------------------------------------	---

3.4 Test Facility

The test facility has a test site registered with the following organizations:

- **ISED – Registration No.: 21895**

Waltek Testing Group (Foshan) Co., Ltd. has been registered and fully described in a report filed with the Innovation, Science and Economic Development Canada (ISED). The acceptance letter from the ISED is maintained in our files. Registration ISED number: 21895, March 12, 2019

- **FCC – Registration No.: 820106**

Waltek Testing Group (Foshan) Co., Ltd. EMC Laboratory has been registered and fully described in a report filed with the (FCC) Federal Communications Commission. The acceptance letter from the FCC is maintained in our files. Registration 820106, August 16, 2018

- **NVLAP – Lab Code: 600191-0**

Waltek Testing Group (Foshan) Co., Ltd. EMC Laboratory is accredited by the National Voluntary Laboratory Accreditation Program (NVLAP/NIST). NVLAP Code: 600191-0.

This report must not be used by the client to claim product certification, approval, or endorsement by NVLAP, NIST, or any agency of the Federal Government.

3.5 Subcontracted

Whether parts of tests for the product have been subcontracted to other labs:

☐ Yes ☒ No

If Yes, list the related test items and lab information:

Test items:---

Lab information:---

3.6 Abnormalities from Standard Conditions

None.

3.7 Disclaimer

The antenna gain information is provided by the customer. The laboratory is not responsible for the accuracy of the antenna gain information.



4 Equipment Used during Test

4.1 Equipment List

☒ 3m Semi-anechoic Chamber for Spurious Emission						
Item	Equipment	Manufacturer	Model No.	Serial No.	Last Calibration Date	Calibration Due Date
1	3m Semi-anechoic Chamber	CHANGCHUANG	9m×6m×6m	-	2024-01-05	2027-01-04
2	EMI TEST RECEIVER	RS	ESR7	101566	2025-01-06	2026-01-05
3	Spectrum Analyzer	Agilent	N9020A	MY48011796	2025-01-06	2026-01-05
4	Trilog Broadband Antenna	SCHWARZBECK	VULB9162	9162-117	2025-01-12	2026-01-11
5	Coaxial Cable (below 1GHz)	Times Microwave Systems	RG223-NMNM-10M	-	2025-01-07	2026-01-06
6	Coaxial Cable (below 1GHz)	Times Microwave Systems	RG223-NMNM-3M	-	2025-01-07	2026-01-06
7	Broad-band Horn Antenna	SCHWARZBECK	BBHA 9120 D	01561	2025-01-13	2026-01-12
8	Broadband Preamplifier (Above 1GHz)	Lunar E M	LNA1G18-40	20160501002	2025-01-06	2026-01-05
9	Coaxial Cable (above 1GHz)	Times-Microwave	CBL5-NN	-	2025-01-06	2026-01-05
☒ RF Conducted test						
Item	Equipment	Manufacturer	Model No.	Serial No.	Last Calibration Date	Calibration Due Date
1	Environmental Chamber	GERUI	GR-HWS-1000L	GR24061818	2024-07-02	2025-07-01
2	Spectrum Analyzer	Agilent	N9020A	MY48011796	2025-01-06	2026-01-05
3	EXG Analog Signal Generator	Agilent	N5181A	MY48180720	2025-01-06	2026-01-05
4	RF Control Unit	TONSCEND	JS0806-2	-	2025-01-08	2026-01-07
5	USB Wideband Power Sensor	KEYSIGHT	U2021XA	MY56510008	2025-01-08	2026-01-07

☐: Not Used☒: Used



4.2 Software List

Description	Manufacturer	Model	Version
EMI Test Software (Radiated Emission)	FARATRONIC	EZ-EMC	RA-03A1-2
RF Conducted Test	TONSCEND	JS1120-2	2.6

4.3 Special Accessories and Auxiliary Equipment

Item	Equipment	Technical Data	Manufacturer	Model No.	Serial No.
1.	/	/	/	/	/

4.4 Measurement Uncertainty

Parameter	Uncertainty	Note
RF Output Power	$\pm 2.2\text{dB}$	(1)
Occupied Bandwidth	$\pm 1.5\%$	(1)
Transmitter Spurious Emission	$\pm 3.8\text{dB}$ (for 25MHz-1GHz)	(1)
	$\pm 5.0\text{dB}$ (for 1GHz-18GHz)	(1)

(1) This uncertainty represents an expanded uncertainty expressed at approximately the 95% confidence level using a coverage factor of $k=2$.

4.5 Decision Rule

Compliance or non-compliance with a disturbance limit shall be determined in the following manner.

If U_{LAB} is less than or equal to U_{cispr} , then

- Compliance is deemed to occur if no measured disturbance level exceeds the disturbance limit;
- Non-compliance is deemed to occur if any measured disturbance level exceeds the disturbance limit.

If U_{LAB} is greater than U_{cispr} , then

- Compliance is deemed to occur if no measured disturbance level, increased by $(U_{\text{LAB}} - U_{\text{cispr}})$, exceeds the disturbance limit;
- Non-compliance is deemed to occur if any measured disturbance level, increased by $(U_{\text{LAB}} - U_{\text{cispr}})$, exceeds the disturbance limit.



5 Test Conditions and Test mode

The equipment under test (EUT) was configured to measure its highest possible emission/immunity level. The test modes were adapted according to the operation manual for use, the EUT was operated in the continuous transmitting mode that was for the purpose of the measurements, more detailed description as follows:

5.1 RF Channel and Frequency

The lowest, middle and highest channel were tested as representatives.

BLE							
Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)	Channel	Frequency (MHz)
00	2402	10	2422	20	2442	30	2462
01	2404	11	2424	21	2444	31	2464
02	2406	12	2426	22	2446	32	2466
03	2408	13	2428	23	2448	33	2468
04	2410	14	2430	24	2450	34	2470
05	2412	15	2432	25	2452	35	2472
06	2414	16	2434	26	2454	36	2474
07	2416	17	2436	27	2456	37	2476
08	2418	18	2438	28	2458	38	2478
09	2420	19	2440	29	2460	39	2480

5.2 Independent Operation Modes

Test Mode	Description	Test Channel
A.1	Wireless with BLE mode, Transmitting	Lowest Channel, Middle Channel, Highest Channel
A.2	Wireless with BLE mode, Receiving	Lowest Channel, Highest Channel
B	Operating Normal mode with BLE connecting	/

5.3 Test Environment Condition

Test Condition	Temperature (°C)	Relative Humidity (%)	ATM Pressure (kPa)
Normal	22	45 %	101.2kPa
LTVN	-10	---	---
HTNV	+50	---	---



6 RF Requirements

6.1 RF Output power

6.1.1 Standard Applicable

According to Section 4.3.1.2.3, The maximum RF output power for adaptive Frequency Hopping equipment shall be equal to or less than 20 dBm. The maximum RF output power for non-adaptive Frequency Hopping equipment, shall be declared by the supplier. The maximum RF output power for this equipment shall be equal to or less than the value declared by the supplier. This declared value shall be equal to or less than 20 dBm.

According to Section 4.3.2.2.3, For adaptive equipment using wide band modulations other than FHSS, the maximum RF output power shall be 20 dBm. The maximum RF output power for non-adaptive equipment shall be declared by the supplier and shall not exceed 20 dBm. For non-adaptive equipment using wide band modulations other than FHSS, the maximum RF output power shall be equal to or less than the value declared by the supplier.

6.1.2 Test Procedure

According to section 5.4.2.2.1.2 of the standard EN 300328, the test procedure shall be as follows:

Step 1:

- Use a fast power sensor with a minimum sensitivity of -40 dBm and capable of minimum 1 MS/s.
 - Use the following settings:
 - Sample speed 1 MS/s or faster.
 - The samples shall represent the RMS power of the signal.
 - Measurement duration: For non-adaptive equipment: equal to the observation period defined in clause 4.3.1.3.2 or clause 4.3.2.4.2. For adaptive equipment, the measurement duration shall be long enough to ensure a minimum number of bursts (at least 10) is captured.
- For adaptive equipment, to increase the measurement accuracy, a higher number of bursts may be used.

Step 2:

- For conducted measurements on devices with one transmit chain:
 - Connect the power sensor to the transmit port, sample the transmit signal and store the raw data. Use these stored samples in all following steps.
- For conducted measurements on devices with multiple transmit chains:
 - Connect one power sensor to each transmit port for a synchronous measurement on all transmit ports.
 - Trigger the power sensors so that they start sampling at the same time. Make sure the time difference between the samples of all sensors is less than 500 ns.
 - For each individual sampling point (time domain), sum the coincident power samples of all ports and store them. Use these summed samples as the new stored data set.

**Step 3:**

- Find the start and stop times of each burst in the stored measurement samples.

The start and stop times are defined as the points where the power is at least 30 dB below the highest value of the stored samples in step 2.

In case of insufficient sensitivity of the power sensor (e.g. in case of radiated measurements), the value of 30 dB may need to be reduced appropriately.

Step 4:

- Between the start and stop times of each individual burst calculate the RMS power over the burst using the formula below. The start and stop points shall be included. Save these P_{burst} values, as well as the start and stop times for each burst.

$$P_{burst} = \frac{1}{k} \sum_{n=1}^k P_{sample}(n)$$

with k being the total number of samples and n the actual sample number.

Step 5:

- The highest of all P_{burst} values (value A in dBm) will be used for maximum e.i.r.p. calculations.

Step 6:

- Add the (stated) antenna assembly gain G in dBi of the individual antenna.
- In case of smart antenna systems operating in mode with beamforming (see clause 5.3.2.2.4), add the additional beamforming gain Y in dB.
- If more than one antenna assembly is intended for this power setting, the maximum overall antenna gain (G or $G + Y$) shall be used..
- The RF Output Power (P_{out}) shall be calculated using the formula below: $P_{out} = A + G + Y$
- This value, which shall comply with the limit given in clause 4.3.1.2.3 or clause 4.3.2.2.3, shall be recorded in the test report.

6.1.3 Test Condition

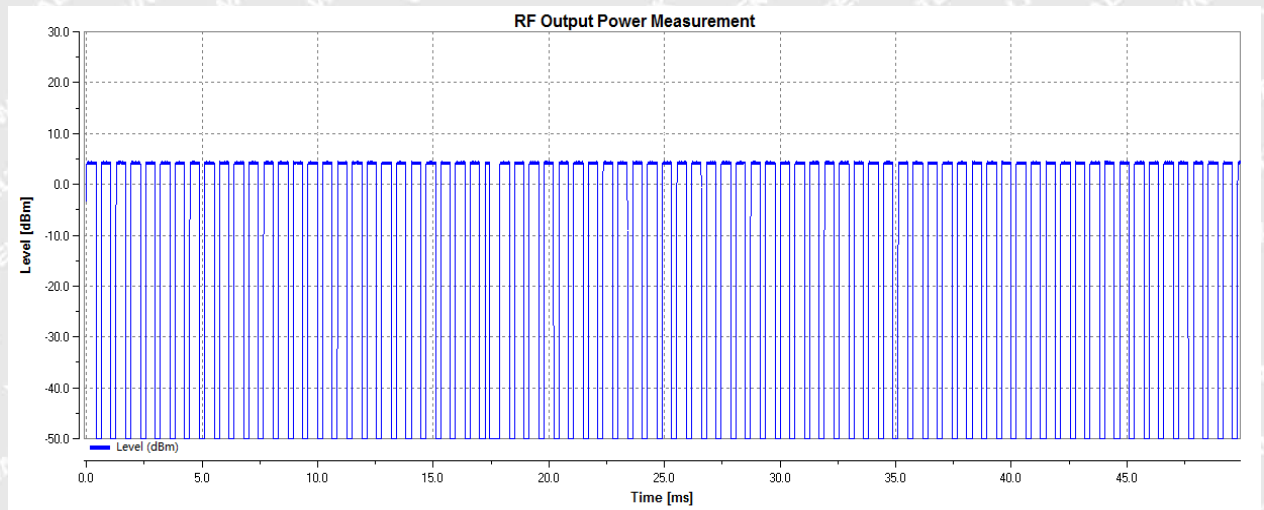
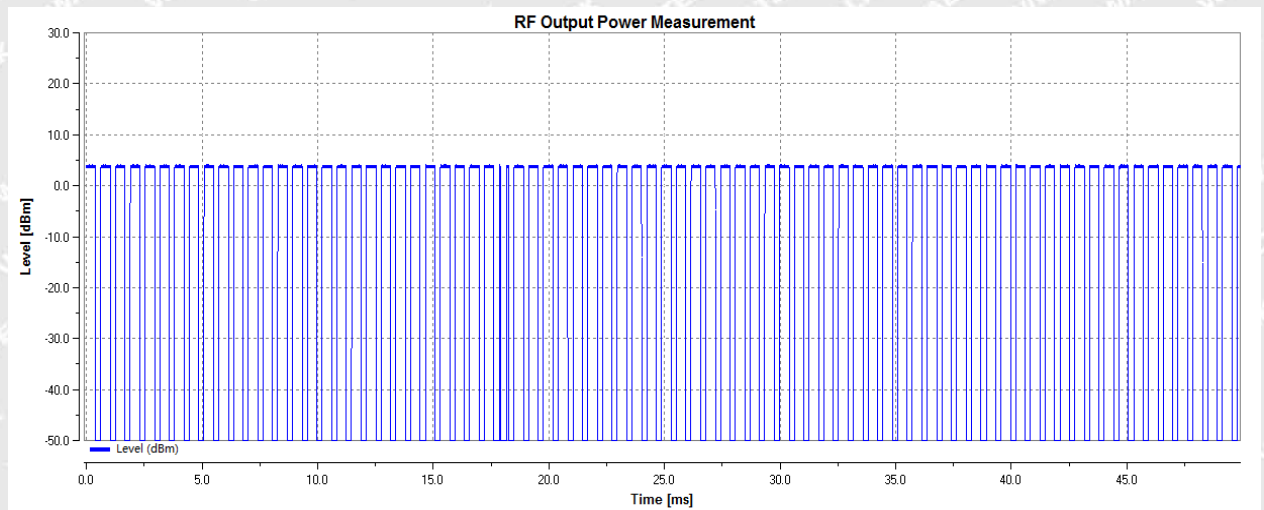
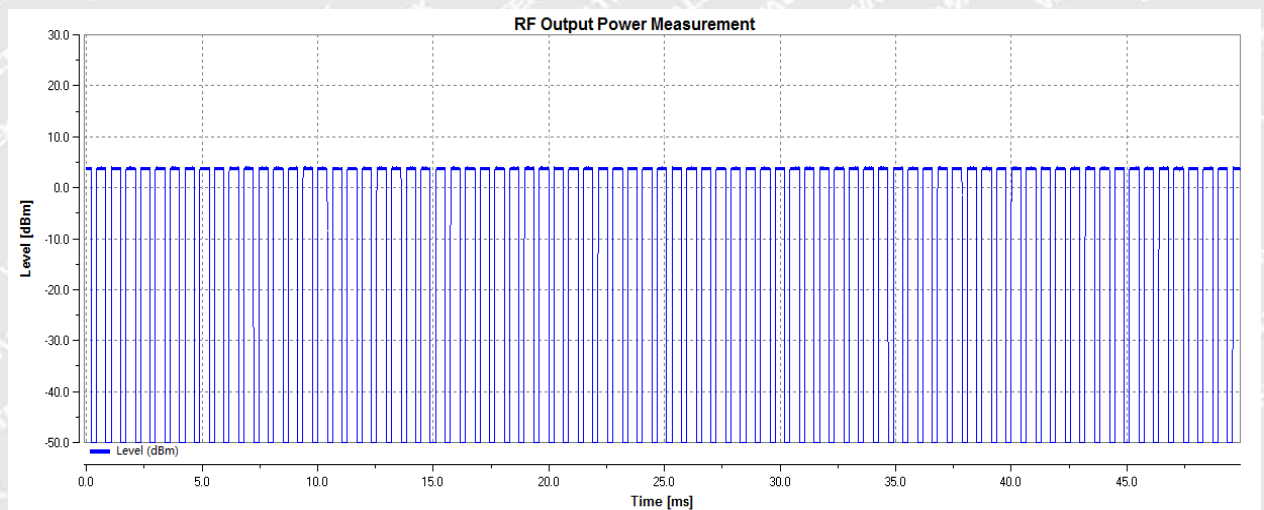
Operating Mode	A.1
Test Environment	Normal Condition, Extreme Condition
Test Voltage	DC 3.3V (power to control panel)
Ambient temperature	22°C
Humidity	54%RH
Atmospheric Pressure	101.2kPa

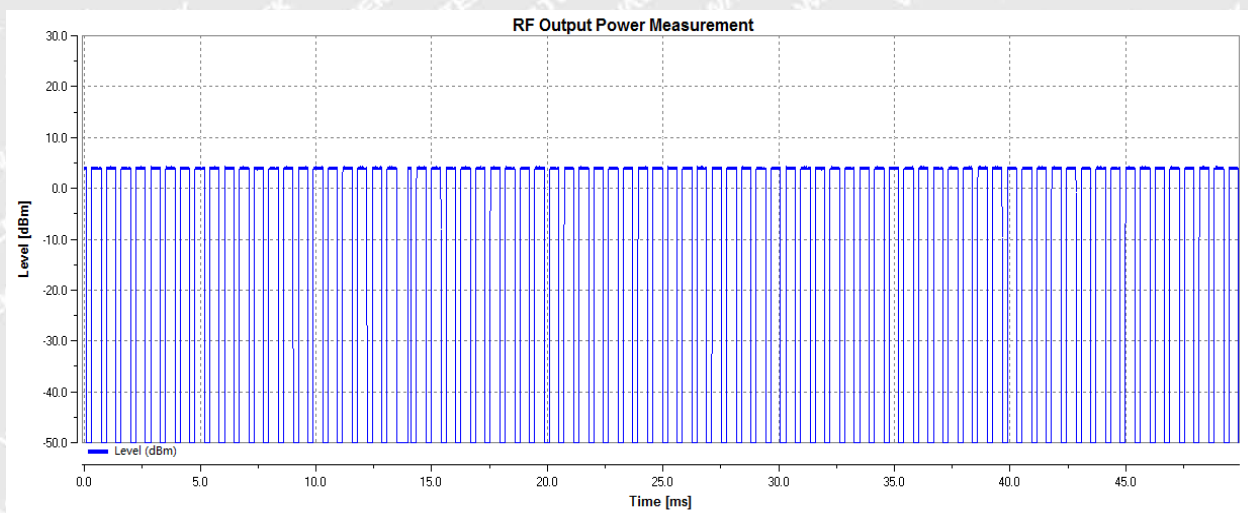
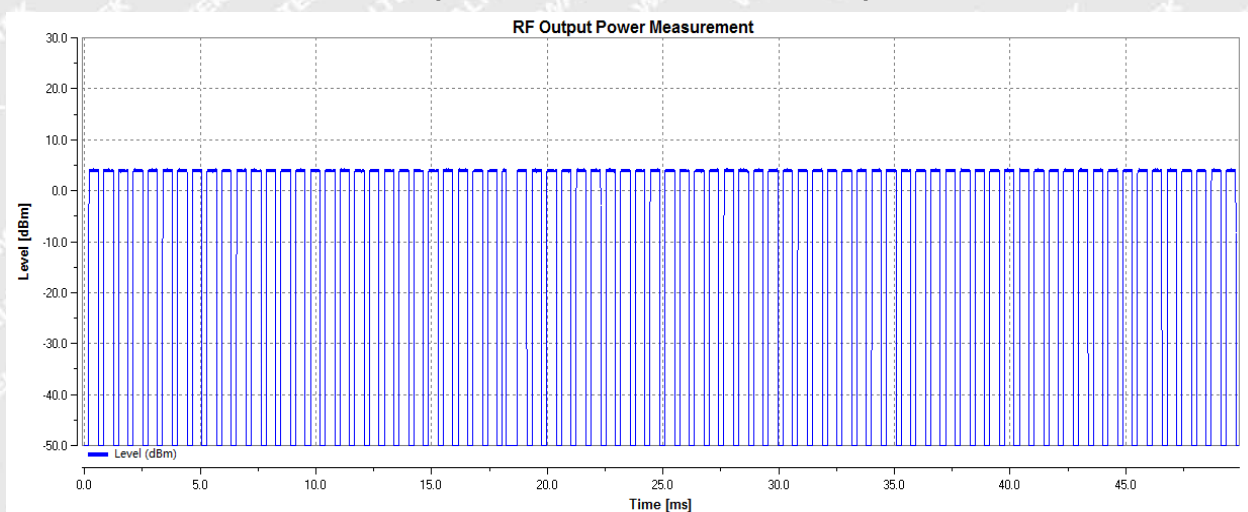
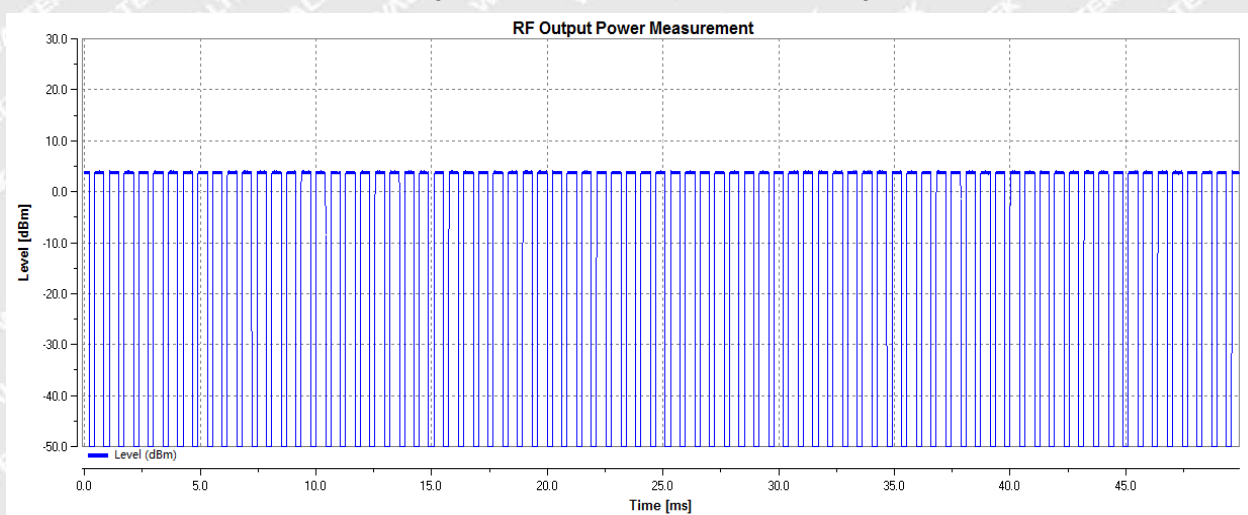


6.1.4 Test Result

Test Mode	Test Condition	Test Channel (MHz)	EIRP (dBm)	Limit (dBm)	Verdict
BLE (1Mbps)	TLVN	2402	2.47	<=20	Pass
	TNVN	2402	2.04	<=20	Pass
	THVN	2402	2.00	<=20	Pass
	TLVN	2440	2.20	<=20	Pass
	TNVN	2440	2.19	<=20	Pass
	THVN	2440	2.16	<=20	Pass
	TLVN	2480	2.46	<=20	Pass
	TNVN	2480	2.47	<=20	Pass
	THVN	2480	2.04	<=20	Pass
BLE (2Mbps)	TLVN	2402	2.45	<=20	Pass
	TNVN	2402	2.44	<=20	Pass
	THVN	2402	2.43	<=20	Pass
	TLVN	2440	1.99	<=20	Pass
	TNVN	2440	2.05	<=20	Pass
	THVN	2440	1.95	<=20	Pass
	TLVN	2480	2.10	<=20	Pass
	TNVN	2480	2.09	<=20	Pass
	THVN	2480	2.10	<=20	Pass

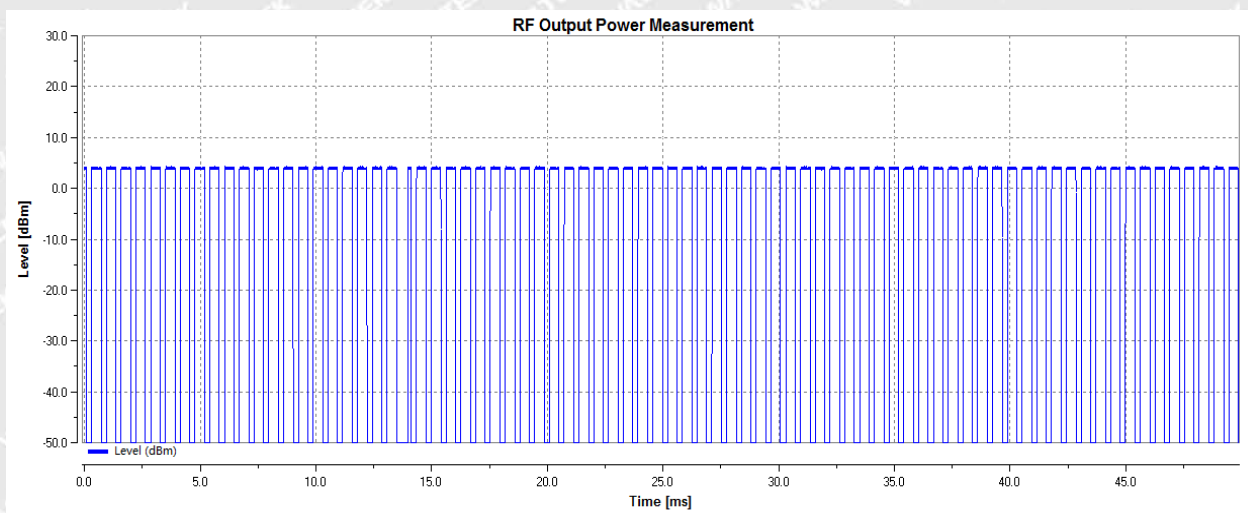
Remark: EIRP=Conducted power+ ANT gain

**Test Graphs:****RF Output Power_TLVN_BLE_2402_1Mbps****RF Output Power_TNVN_BLE_2402_1Mbps****RF Output Power_THVN_BLE_2402_1Mbps**

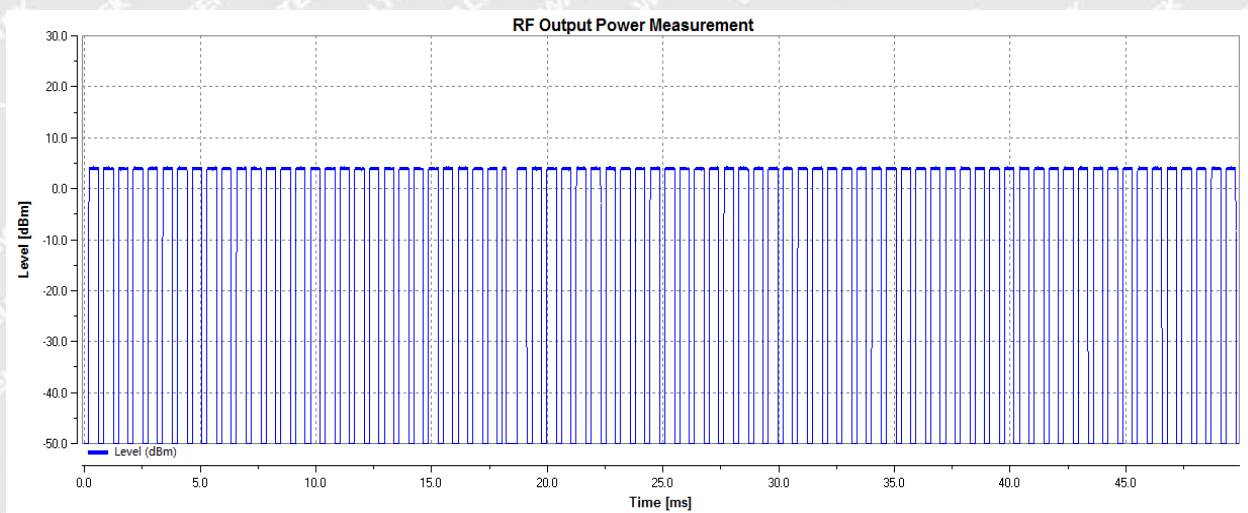
**RF Output Power_TLVN_BLE_2440_1Mbps****RF Output Power_TNVN_BLE_2440_1Mbps****RF Output Power_THVN_BLE_2440_1Mbps**



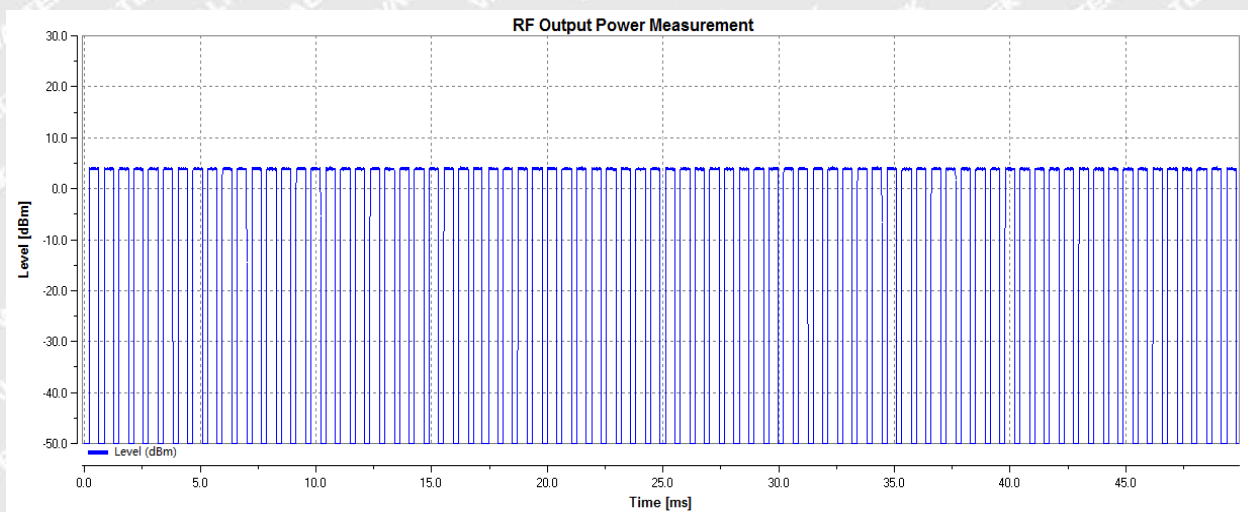
RF Output Power_TLVN_BLE_2480_1Mbps

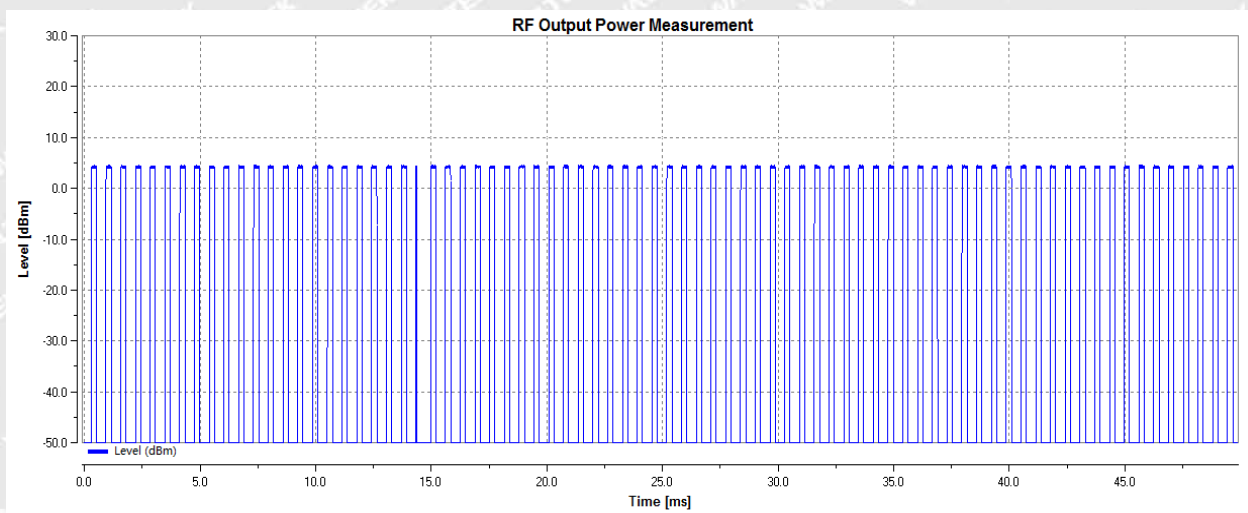
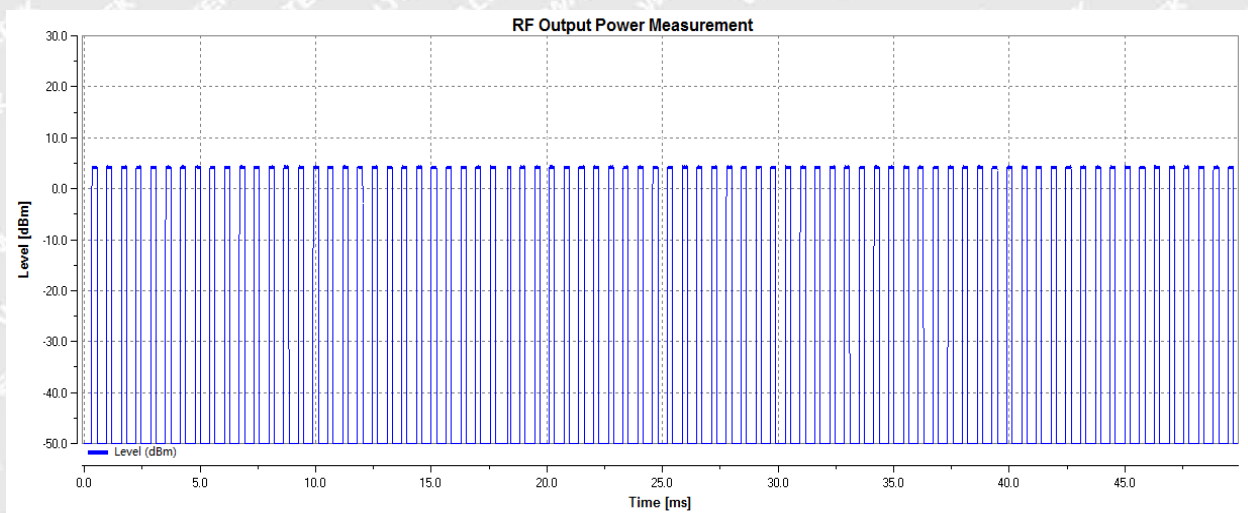
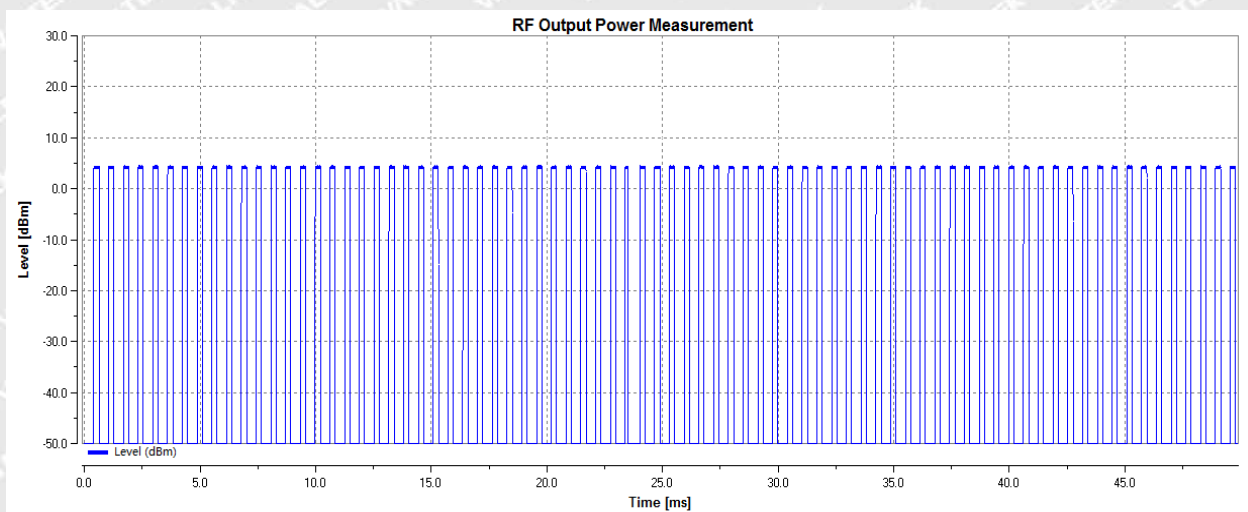


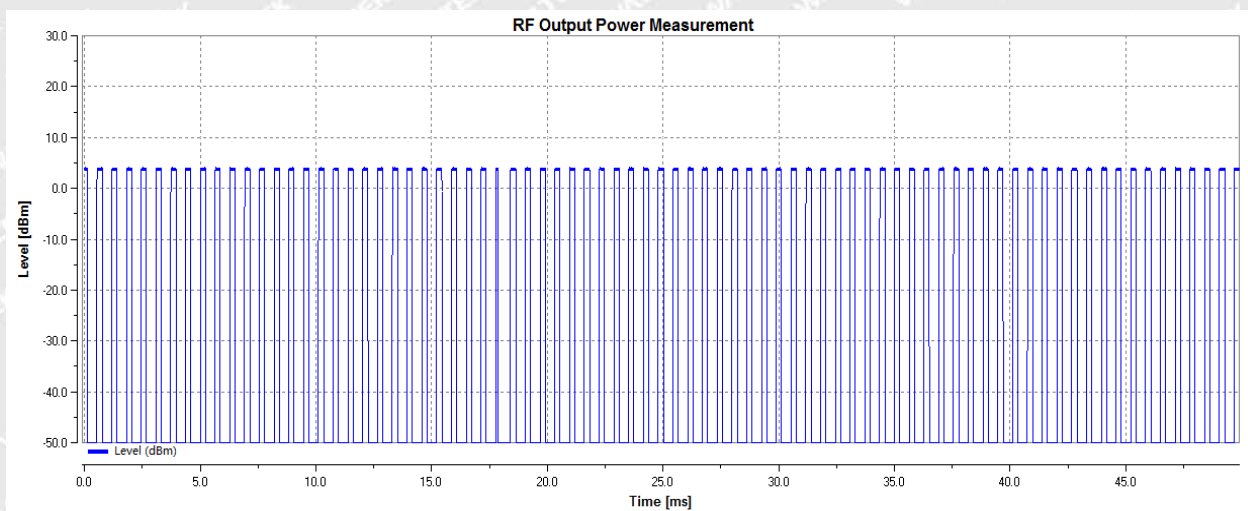
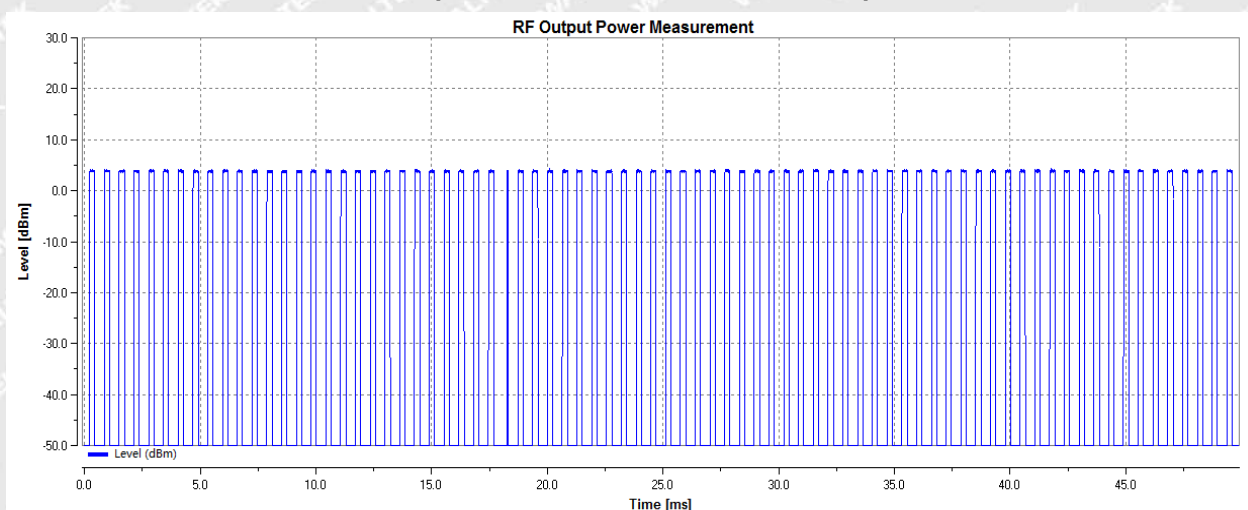
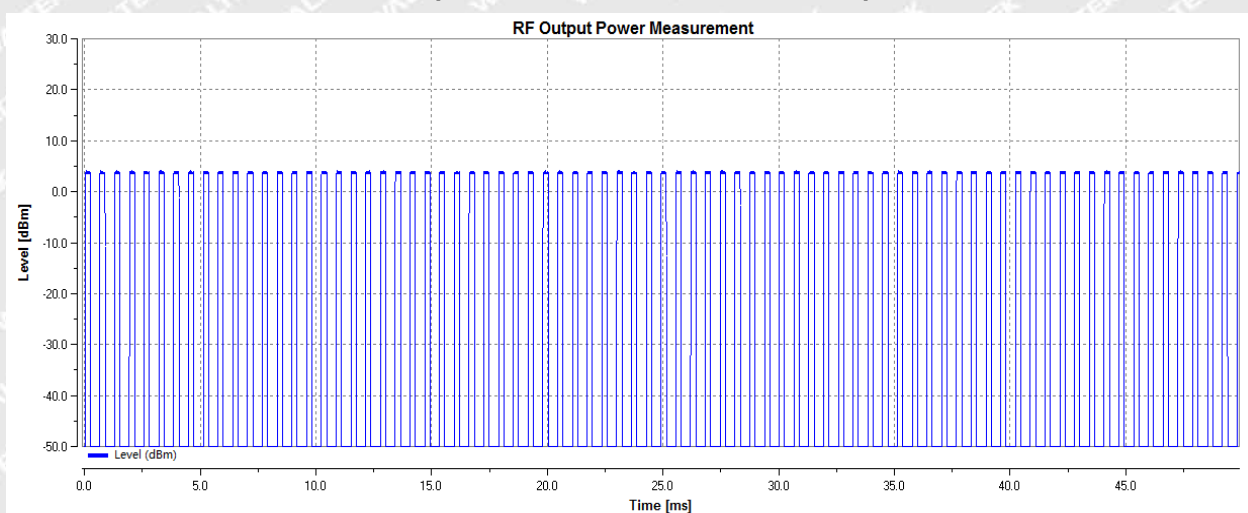
RF Output Power_TNVN_BLE_2480_1Mbps

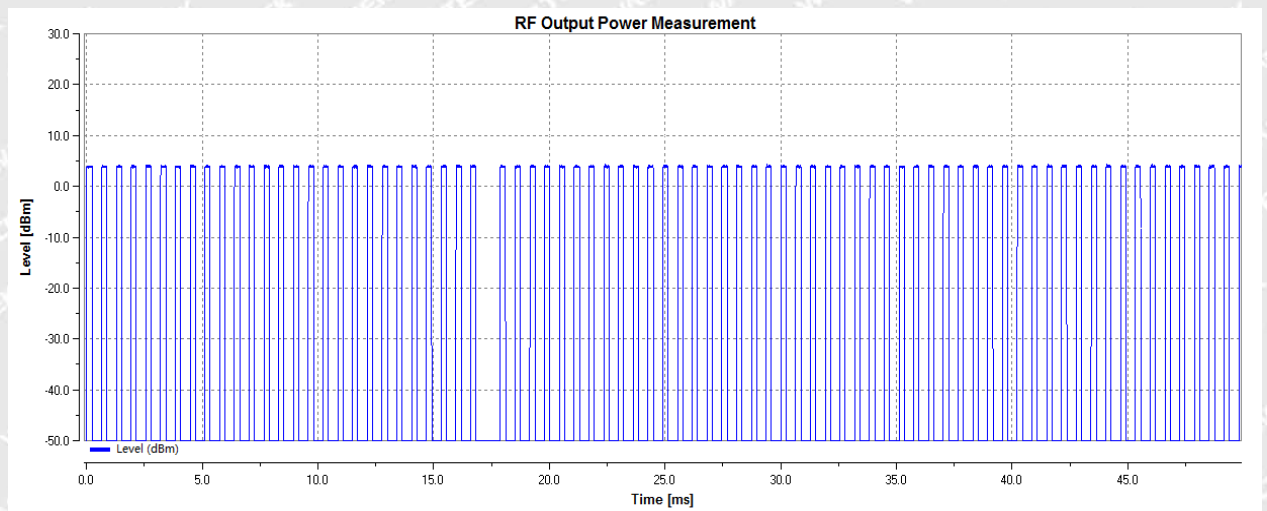
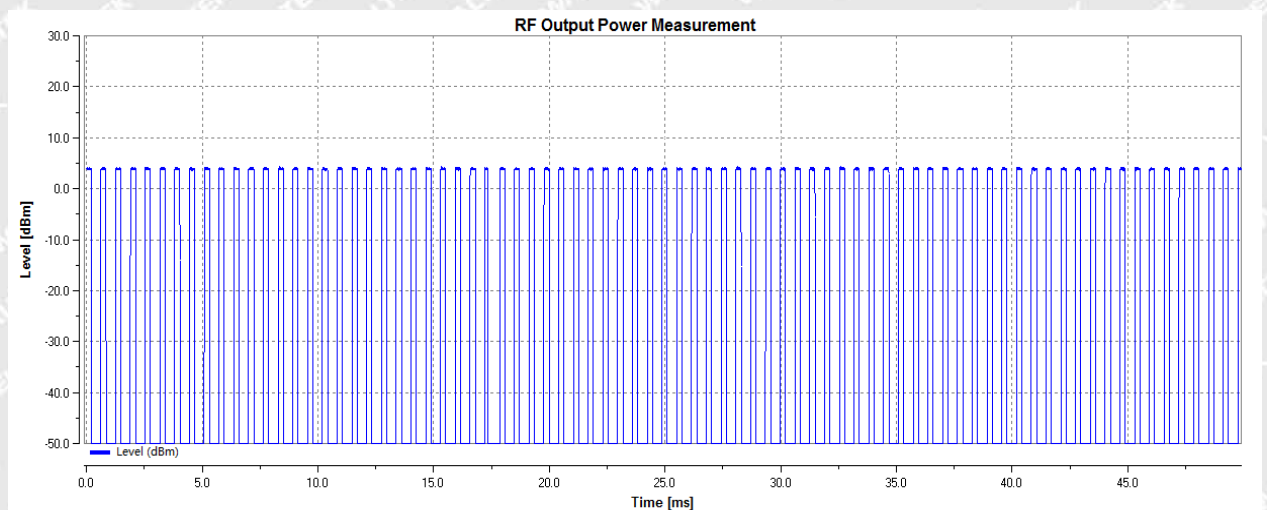
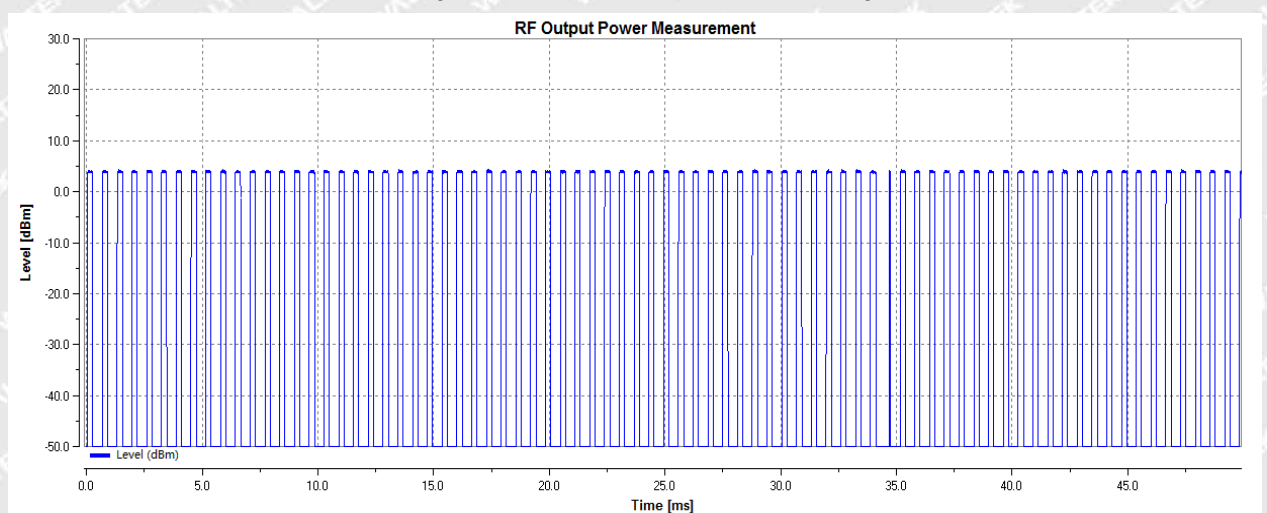


RF Output Power_THVN_BLE_2480_1Mbps



**RF Output Power_TLVN_BLE_2402_2Mbps****RF Output Power_TNVN_BLE_2402_2Mbps****RF Output Power_THVN_BLE_2402_2Mbps**

**RF Output Power_TLVN_BLE_2440_2Mbps****RF Output Power_TNVN_BLE_2440_2Mbps****RF Output Power_THVN_BLE_2440_2Mbps**

**RF Output Power_TLVN_BLE_2480_2Mbps****RF Output Power_TNVN_BLE_2480_2Mbps****RF Output Power_THVN_BLE_2480_2Mbps**

*Remark: The antenna gain is not considered in the result plot.



6.2 Power Spectral Density

6.2.1 Standard Applicable

According to Section 4.3.2.3.3, For equipment using wide band modulations other than FHSS, the maximum Power Spectral Density is limited to 10 dBm per MHz.

6.2.2 Test Procedure

According to section 5.4.3.2.1 of the standard EN 300328, the test procedure shall be as follows:

Step 1:

Connect the UUT to the spectrum analyser and use the following settings:

- Start Frequency: 2 400 MHz
- Stop Frequency: 2 483,5 MHz
- Resolution BW: 10 kHz
- Video BW: 30 kHz
- Sweep Points: > 8 350; for spectrum analysers not supporting this number of sweep points, the frequency band may be segmented
- Detector: RMS
- Trace Mode: Max Hold
- Sweep time:

For non-continuous transmissions: $2 \times \text{Channel Occupancy Time} \times \text{number of sweep points}$.

For non-adaptive equipment use the maximum TX-sequence time in the formula above instead of the Channel Occupancy Time.

For continuous transmissions: 10 s; the sweep time may be increased further until a value where the sweep time has no further impact anymore on the RMS value of the signal.

For non-continuous signals, wait for the trace to stabilize.

Save the data (trace data) set to a file.

Step 2:

For conducted measurements on smart antenna systems using either operating mode 2 or operating mode 3 (see clause 5.3.2.2), repeat the measurement for each of the transmit ports. For each sampling point (frequency domain), add up the coincident power values (in mW) for the different transmit chains and use this as the new data set.

Step 3:

Add up the values for power for all the samples in the file using the formula below.

$$P_{\text{Sum}} = \sum_{n=1}^k P_{\text{sample}}(n)$$

with 'k' being the total number of samples and 'n' the actual sample number

**Step 4:**

Normalize the individual values for power (in dBm) so that the sum is equal to the RF Output Power (e.i.r.p.) measured in clause 5.4.2 and save the corrected data. The following formulas can be used:

$$C_{Corr} = P_{Sum} - P_{e.i.r.p.}$$

$$P_{Samplecorr}(n) = P_{Sample}(n) - C_{Corr}$$

with 'n' being the actual sample number

Step 5:

Starting from the first sample PSamplecorr(n) (lowest frequency), add up the power (in mW) of the following samples representing a 1 MHz segment and record the results for power and position (i.e. sample #1 to sample #100). This is the Power Spectral Density (e.i.r.p.) for the first 1 MHz segment which shall be recorded.

Step 6:

Shift the start point of the samples added up in step 5 by one sample and repeat the procedure in step 5 (i.e. sample #2 to sample #101).

Step 7:

Repeat step 6 until the end of the data set and record the Power Spectral Density values for each of the 1 MHz segments.

From all the recorded results, the highest value is the maximum Power Spectral Density (PSD) for the UUT. This value, which shall comply with the limit given in clause 4.3.2.3.3, shall be recorded in the test report. RBW/VBW=10/30 kHz

6.2.3 Test Condition

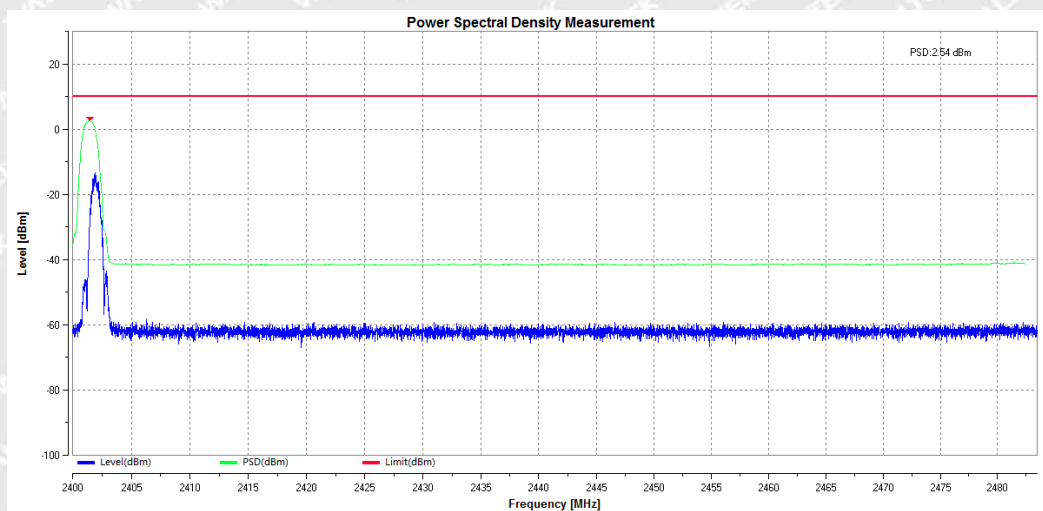
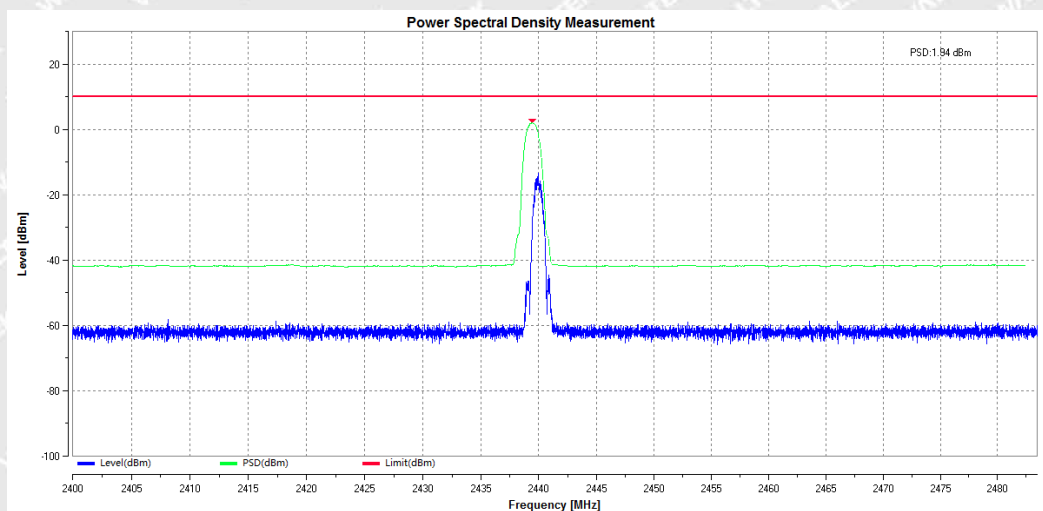
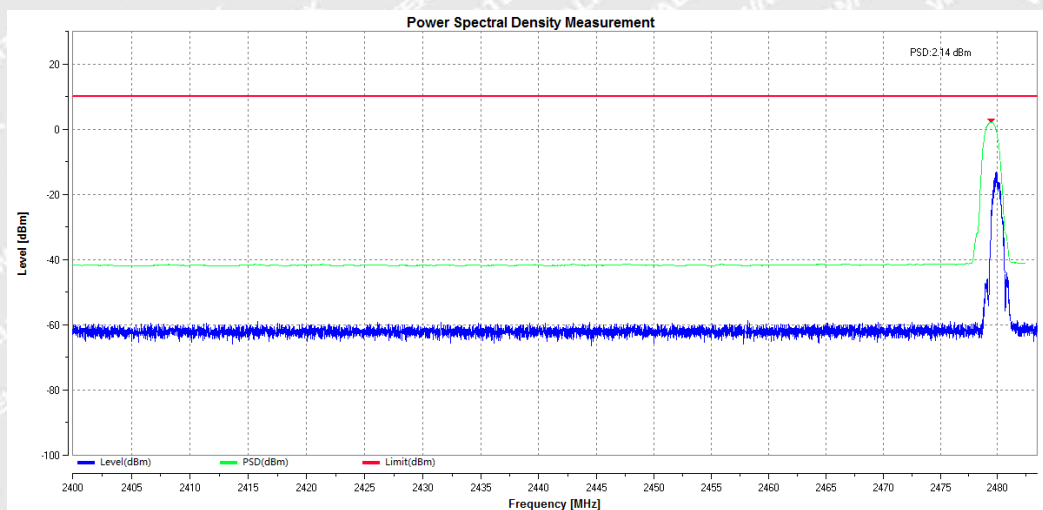
Operating Mode	A.1
Test Environment	Normal Condition
Test Voltage	DC 3.3V (power to control panel)
Ambient temperature	22°C
Humidity	54%RH
Atmospheric Pressure	101.2kPa

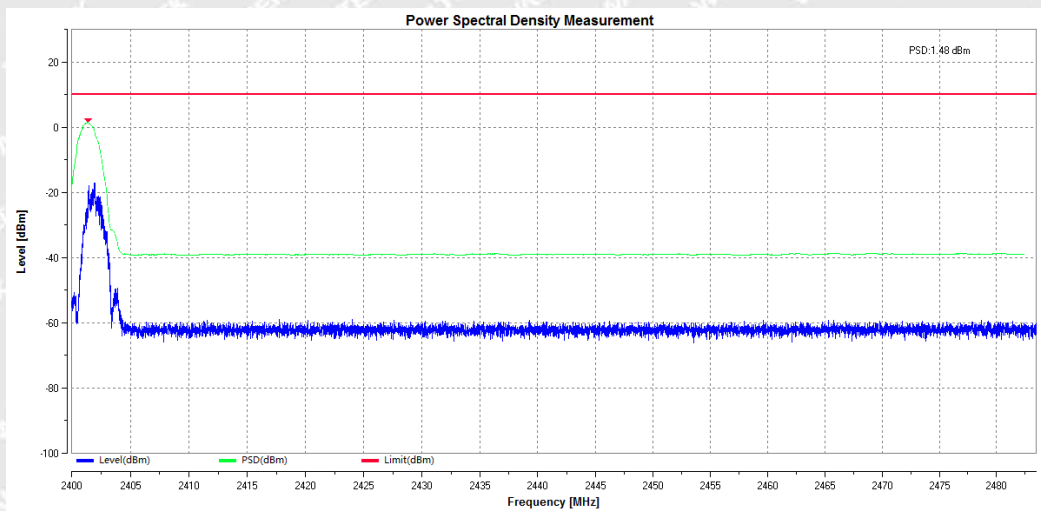
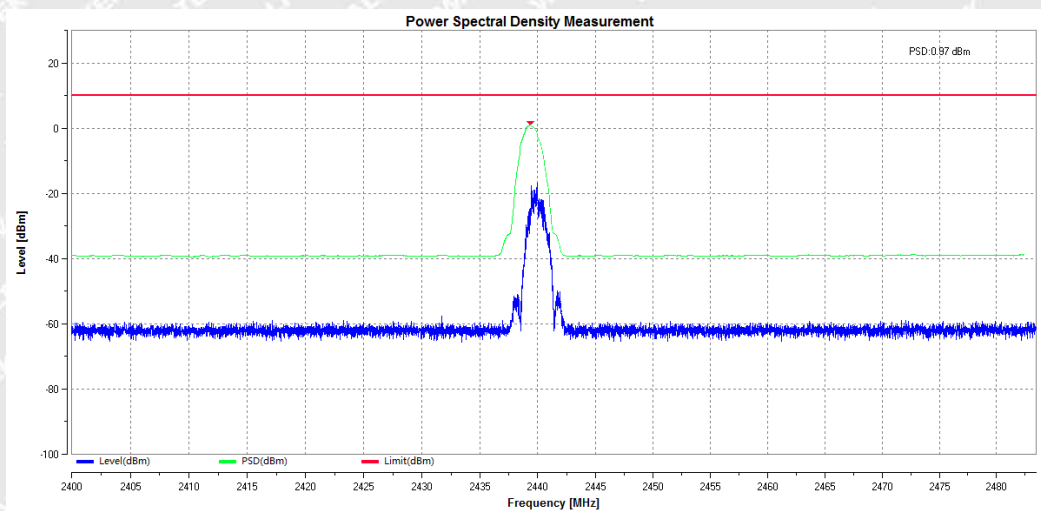
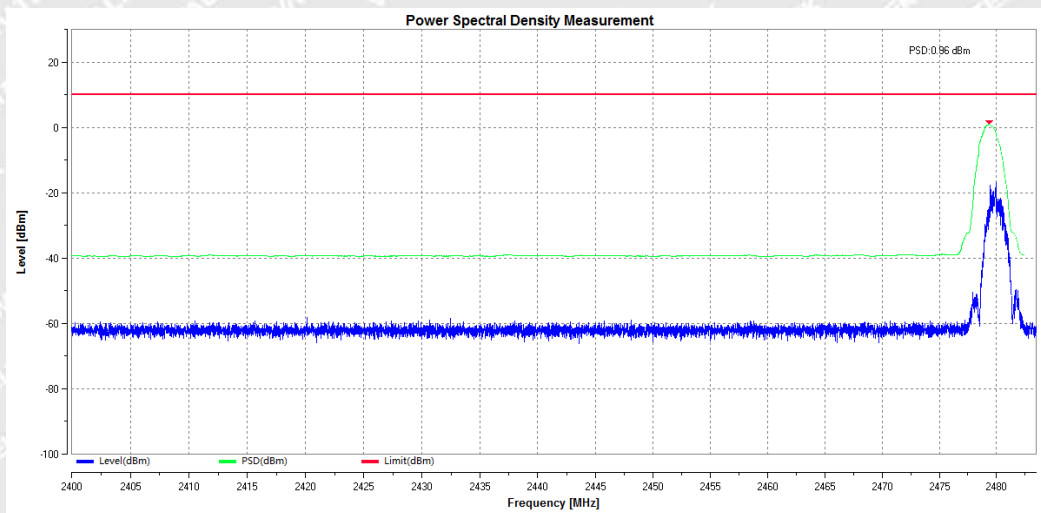


6.2.4 Test Result

Test Mode	Test Condition	Test Channel	PSD (dBm)	Limit (dBm)	Verdict
BLE (1Mbps)	NTNV	2402	2.54	<=10	Pass
	NTNV	2440	1.94	<=10	Pass
	NTNV	2480	2.14	<=10	Pass
BLE (2Mbps)	NTNV	2402	1.48	<=10	Pass
	NTNV	2440	0.97	<=10	Pass
	NTNV	2480	0.96	<=10	Pass

WALTEK

**Test Graphs:****Power Spectral Density_NTNV_BLE_2402_1Mbps****Power Spectral Density_NTNV_BLE_2440_1Mbps****Power Spectral Density_NTNV_BLE_2480_1Mbps**

**Power Spectral Density_NTNV_BLE_2402_2Mbps****Power Spectral Density_NTNV_BLE_2440_2Mbps****Power Spectral Density_NTNV_BLE_2480_2Mbps**



6.3 Occupied Channel Bandwidth

6.3.1 Standard Applicable

According to section 4.3.1.8.3. The Occupied Channel Bandwidth for each hopping frequency shall fall completely within the band given in clause 1.

For non-adaptive Frequency Hopping equipment with e.i.r.p greater than 10 dBm, the Occupied Channel Bandwidth for every occupied hopping frequency shall be equal to or less than the value declared by the supplier.

This declared value shall not be greater than 5 MHz.

According to section 4.3.2.7.3. The Occupied Channel Bandwidth shall fall completely within the band given in clause 1. In addition, for non-adaptive systems using wide band modulations other than FHSS and with e.i.r.p greater than 10 dBm, the occupied channel bandwidth shall be less than 20 MHz.

6.3.2 Test Procedure

According to the section 5.4.7.2.1, the measurement procedure shall be as follows:

Step 1:

Connect the UUT to the spectrum analyser and use the following settings:

- Centre Frequency: The centre frequency of the channel under test
- Resolution BW: $\sim 1\%$ of the span without going below 1%
- Video BW: $3 \times \text{RBW}$
- Frequency Span: $2 \times \text{Nominal Channel Bandwidth}$
- Detector Mode: RMS
- Trace Mode: Max Hold
- Sweep time: 1 s

Step 2:

Wait for the trace to stabilize.

Find the peak value of the trace and place the analyser marker on this peak.

Step 3:

Use the 99 % bandwidth function of the spectrum analyser to measure the Occupied Channel Bandwidth of the UUT. This value shall be recorded.

6.3.3 Test Condition

Operating Mode : A.1

Test Environment : Normal Condition

Test Voltage : DC 3.3V (power to control panel)

Ambient temperature : 22°C

Humidity : 54%RH

Atmospheric Pressure : 101.2kPa

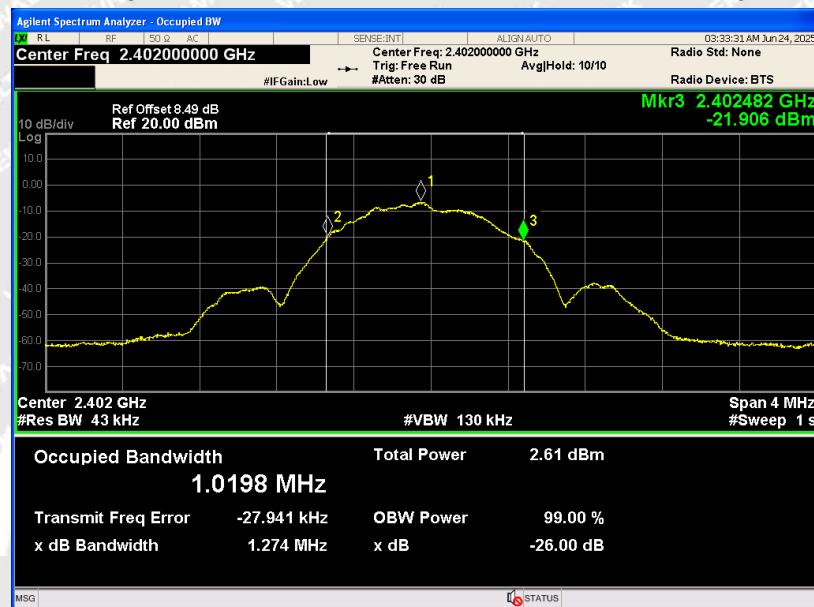


6.3.4 Test Result

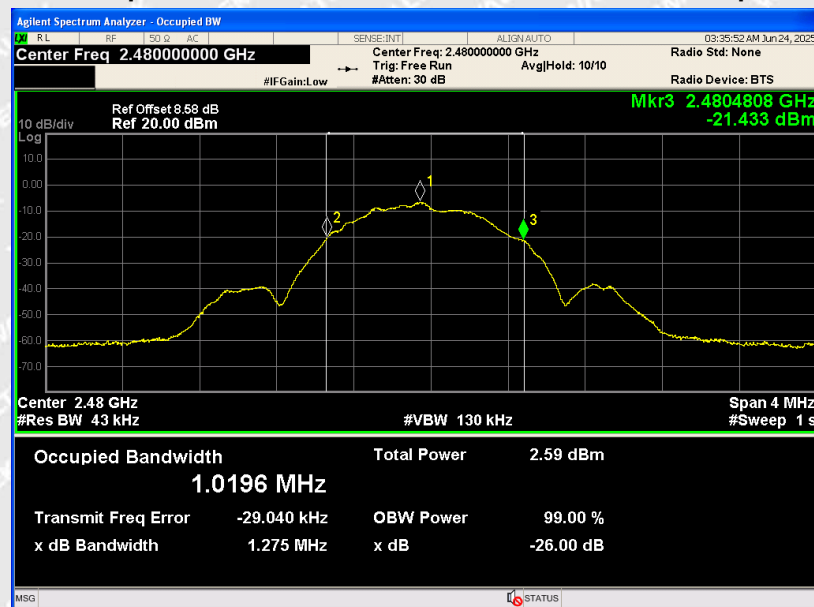
Test Mode	Test Condition	Channel	OCB (MHz)	FL(MHz)	FH(MHz)	Limit(MHz)	Verdict
BLE (1Mbps)	NTNV	2402	1.0198	2401.46	2402.48	2400 to 2483.5	Pass
		2480	1.0196	2479.46	2480.48	2400 to 2483.5	Pass
BLE (2Mbps)	NTNV	2402	2.0209	2400.97	2402.99	2400 to 2483.5	Pass
		2480	2.0196	2478.97	2480.99	2400 to 2483.5	Pass

Test Graphs:

Occupied Channel Bandwidth_NTNV_BLE_2402_1Mbps

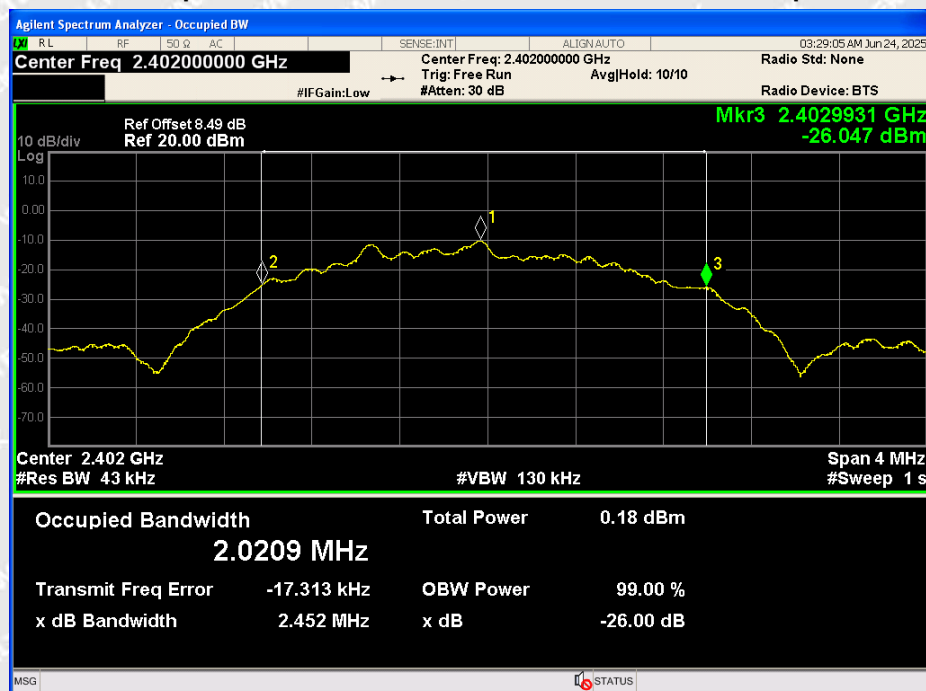


Occupied Channel Bandwidth_NTNV_BLE_2480_1Mbps

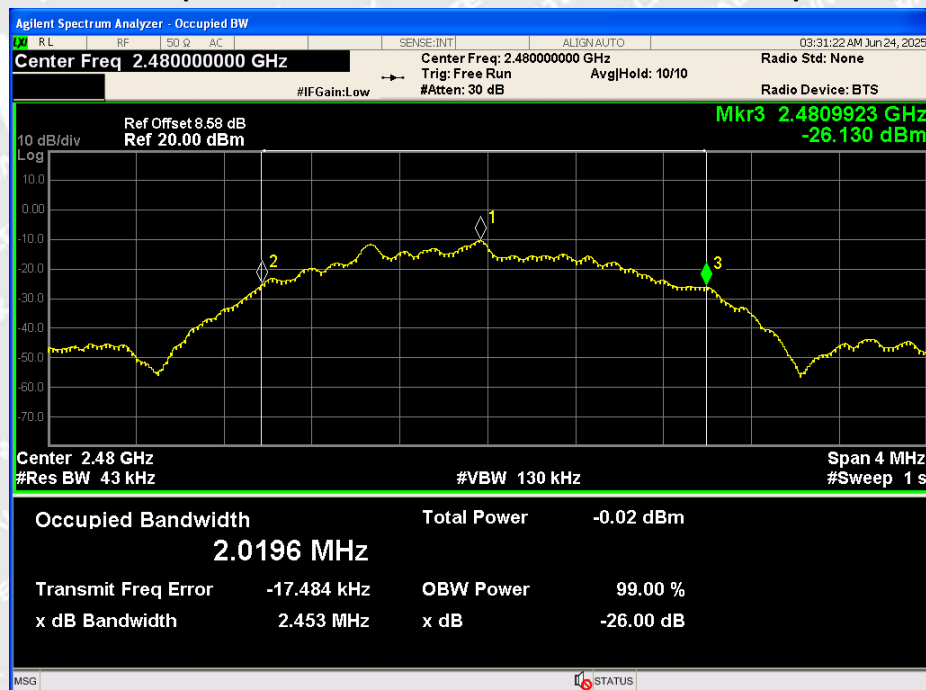




Occupied Channel Bandwidth_NTNV_BLE_2402_2Mbps



Occupied Channel Bandwidth_NTNV_BLE_2480_2Mbps

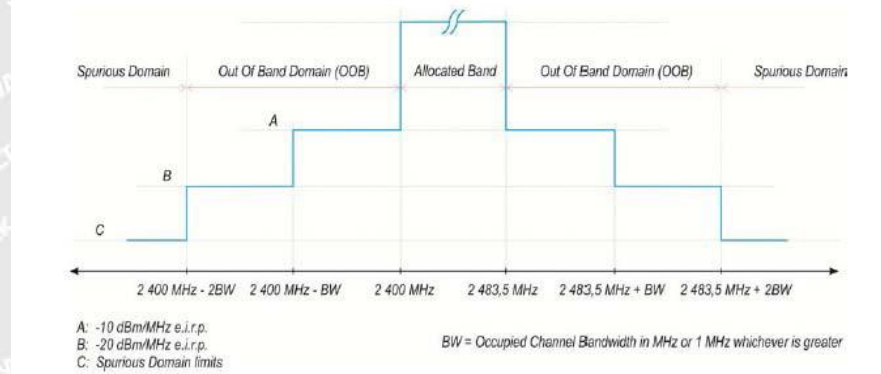




6.4 Transmitter unwanted emissions in the out-of-band domain

6.4.1 Standard Applicable

According to section 4.3.1.9.3&4.3.2.8.3, The transmitter unwanted emissions in the out-of-band domain but outside the allocated band, shall not exceed the values provided by the mask in figure below



Within the 2 400 MHz to 2 483,5 MHz band, the Out-of-band emissions are fulfilled by compliance with the Occupied Channel Bandwidth requirement

6.4.2 Test Procedure

According to the section 5.4.8.2.1, the measurement procedure shall be as follows:

The Out-of-band emissions within the different horizontal segments of the mask provided in figure 1 and figure 3 shall be measured using the procedure in step 1 to step 6 below. This method assumes the spectrum analyser is equipped with the Time Domain Power option.

Step 1:

• Connect the UUT to the spectrum analyser and use the following settings:

- Measurement Mode: Time Domain Power
- Centre Frequency: 2 484 MHz
- Span: Zero Span
- Resolution BW: 1 MHz
- Filter mode: Channel filter
- Video BW: 3 MHz
- Detector Mode: RMS
- Trace Mode: Max Hold
- Sweep Mode: Single Sweep
- Sweep Points: Sweep time [μ s] / (1 μ s) with a maximum of 30 000
- Trigger Mode: Video
- Sweep Time: > 120 % of the duration of the longest burst detected during the measurement of the RF Output Power

Step 2 (segment 2 483,5 MHz to 2 483,5 MHz + BW):

- The measurement shall be performed and repeated while the trigger level is increased until no triggering takes place.
- For FHSS equipment operating in a normal hopping mode, the different hops will result in signal bursts with different power levels. In this case the burst with the highest power level shall be selected.
- Set a window (start and stop lines) to match with the start and end of the burst and in which the RMS power shall be measured using the Time Domain Power function.
- Select RMS power to be measured within the selected window and note the result which is the RMS power



within this 1 MHz segment (2 483,5 MHz to 2 484,5 MHz). Compare this value with the applicable limit provided by the mask.

- Increase the centre frequency in steps of 1 MHz and repeat this measurement for every 1 MHz segment within the range 2 483,5 MHz to 2 483,5 MHz + BW. The centre frequency of the last 1 MHz segment shall be set to 2 483,5 MHz + BW - 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 3 (segment 2 483,5 MHz + BW to 2 483,5 MHz + 2 BW):

- Change the centre frequency of the analyser to 2 484 MHz + BW and perform the measurement for the first 1 MHz segment within range 2 483,5 MHz + BW to 2 483,5 MHz + 2 BW. Increase the centre frequency in 1 MHz steps and repeat the measurements to cover this whole range. The centre frequency of the last 1 MHz segment shall be set to 2 483,5 MHz + 2 BW - 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 4 (segment 2 400 MHz - BW to 2 400 MHz):

- Change the centre frequency of the analyser to 2 399,5 MHz and perform the measurement for the first 1 MHz segment within range 2 400 MHz - BW to 2 400 MHz. Reduce the centre frequency in 1 MHz steps and repeat the measurements to cover this whole range. The centre frequency of the last 1 MHz segment shall be set to 2 400 MHz - BW + 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 5 (segment 2 400 MHz - 2 BW to 2 400 MHz - BW):

- Change the centre frequency of the analyser to 2 399,5 MHz - BW and perform the measurement for the first 1 MHz segment within range 2 400 MHz - 2 BW to 2 400 MHz - BW. Reduce the centre frequency in 1 MHz steps and repeat the measurements to cover this whole range. The centre frequency of the last 1 MHz segment shall be set to 2 400 MHz - 2 BW + 0,5 MHz (which means this may partly overlap with the previous 1 MHz segment).

Step 6:

- In case of conducted measurements on equipment with a single transmit chain, the declared antenna assembly gain G in dBi shall be added to the results for each of the 1 MHz segments and compared with the limits provided by the mask given in figure 1 or figure 3. If more than one antenna assembly is intended for this power setting, the antenna with the highest gain shall be considered.
- In case of conducted measurements on smart antenna systems (equipment with multiple transmit chains), the measurements need to be repeated for each of the active transmit chains. The declared antenna assembly gain G in dBi for a single antenna shall be added to these results. If more than one antenna assembly is intended for this power setting, the antenna with the highest gain shall be considered. Comparison with the applicable limits shall be done using any of the options given below:
 - Option 1: the results for each of the transmit chains for the corresponding 1 MHz segments shall be added. The additional beamforming gain Y in dB shall be added as well and the resulting values compared with the limits provided by the mask given in figure 1 or figure 3.
 - Option 2: the limits provided by the mask given in figure 1 or figure 3 shall be reduced by $10 \times \log_{10}(A_{ch})$ and the additional beamforming gain Y in dB. The results for each of the transmit chains shall be individually compared with these reduced limits.

NOTE: A_{ch} refers to the number of active transmit chains.

It shall be recorded whether the equipment complies with the mask provided in figure 1 or figure 3.

RBW=1MHz VBW=3MHz

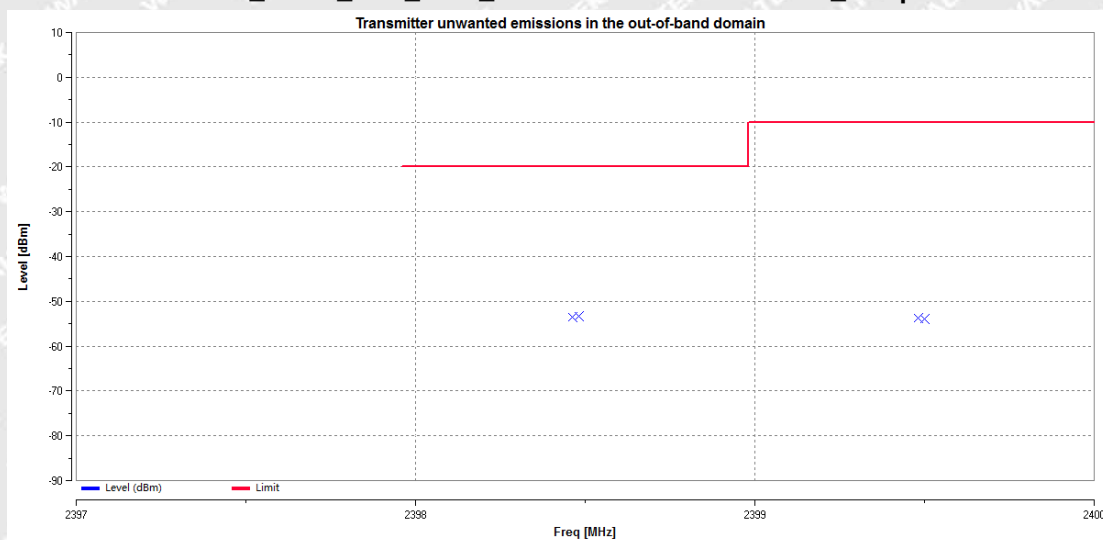
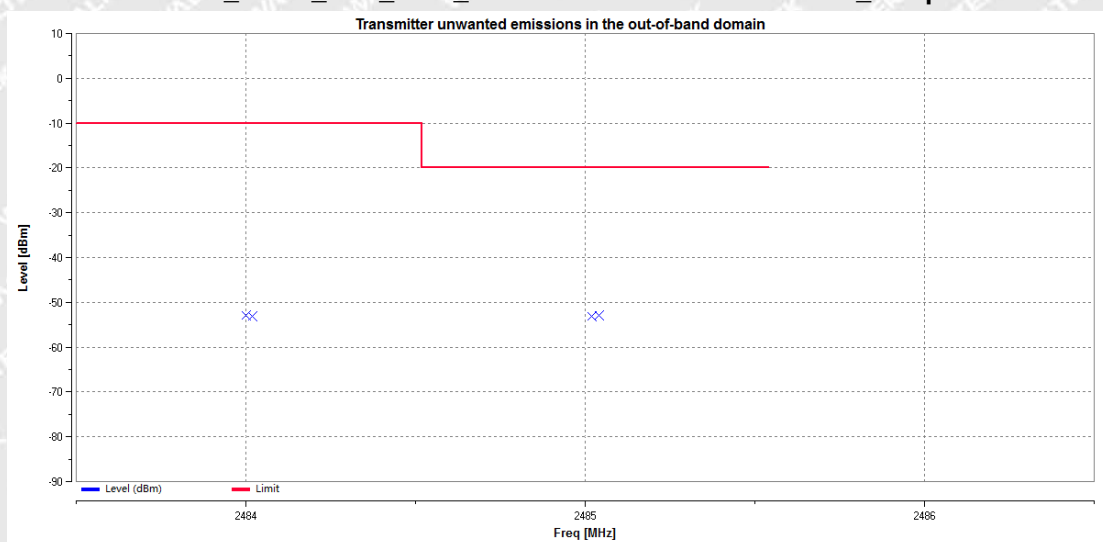


6.4.3 Test Condition

Operating Mode : A.1
Test Environment : Normal Condition
Test Voltage : DC 3.3V (power to control panel)
Ambient temperature : 22°C
Humidity : 54%RH
Atmospheric Pressure : 101.2kPa

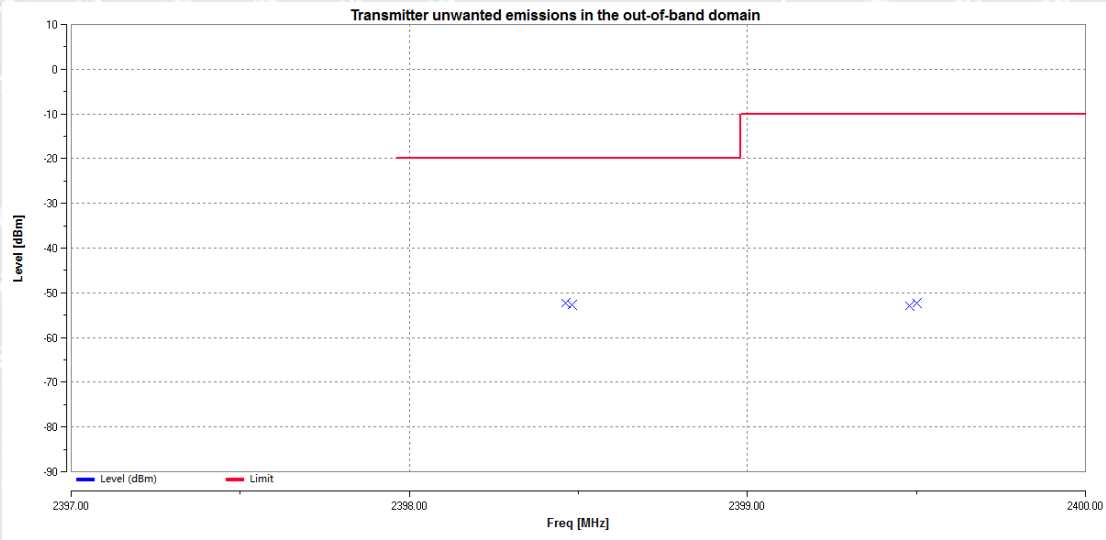
6.4.4 Test Result

Test Mode	Test Channel	Test Segment (MHz)	Max. Emissions Reading (dBm)	Limit (dBm)	Verdict
BLE (1Mbps)	Low	2400-2BW to 2400-BW	-53.40	<=-20	Pass
		2400-BW to 2400	-53.68	<=-10	Pass
		2483.5 to 2483.5+BW	-52.91	<=-10	Pass
		2483.5+BW to 2483.5+2BW	-52.90	<=-20	Pass
	High	2400-2BW to 2400-BW	-52.33	<=-20	Pass
		2400-BW to 2400	-52.25	<=-10	Pass
		2483.5 to 2483.5+BW	-41.91	<=-10	Pass
		2483.5+BW to 2483.5+2BW	-44.35	<=-20	Pass
BLE (2Mbps)	Low	2400-2BW to 2400-BW	-46.96	<=-20	Pass
		2400-BW to 2400	-40.63	<=-10	Pass
		2483.5 to 2483.5+BW	-31.50	<=-10	Pass
		2483.5+BW to 2483.5+2BW	-52.72	<=-20	Pass
	High	2400-2BW to 2400-BW	-52.10	<=-20	Pass
		2400-BW to 2400	-53.04	<=-10	Pass
		2483.5 to 2483.5+BW	-51.71	<=-10	Pass
		2483.5+BW to 2483.5+2BW	-52.51	<=-20	Pass
Note: The data just list the worst case.					

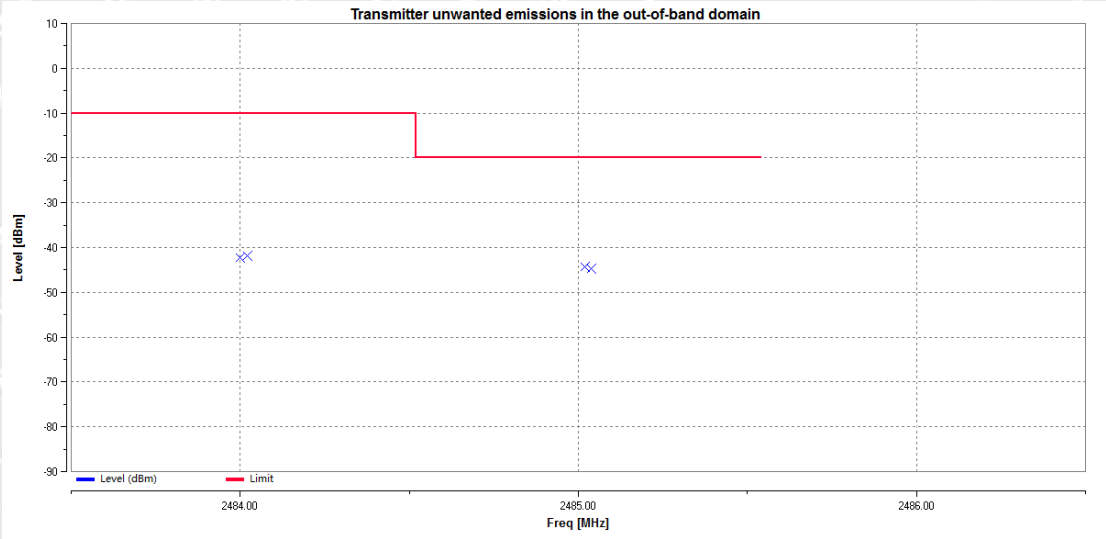
**Test Graphs:****OOB_NTNV_BLE_2402_2400MHz-2BW to 2400MHz_1Mbps****OOB_NTNV_BLE_2402_2483.5MHz to 2483.5MHz+2BW_1Mbps**



OOB_NTNV_BLE_2480_2400MHz-2BW to 2400MHz_1Mbps

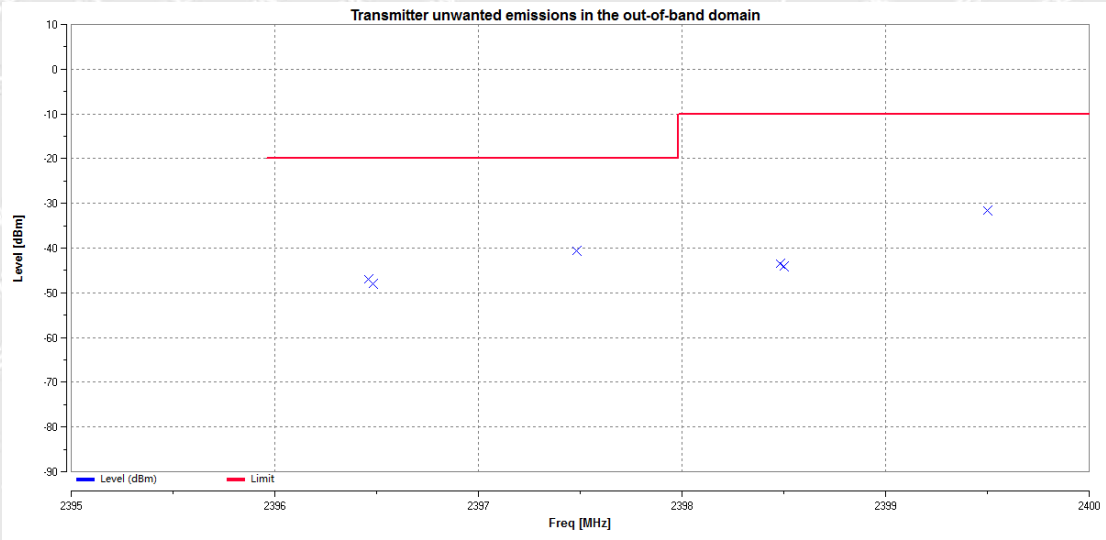


OOB_NTNV_BLE_2480_2483.5MHz to 2483.5MHz+2BW_1Mbps

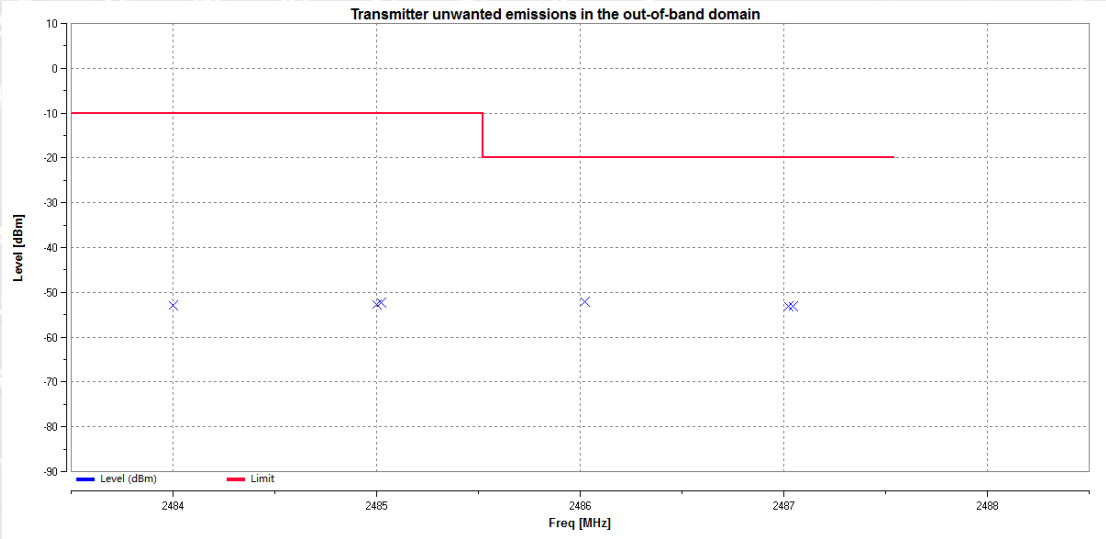




OOB_NTNV_BLE_2402_2400MHz-2BW to 2400MHz_2Mbps

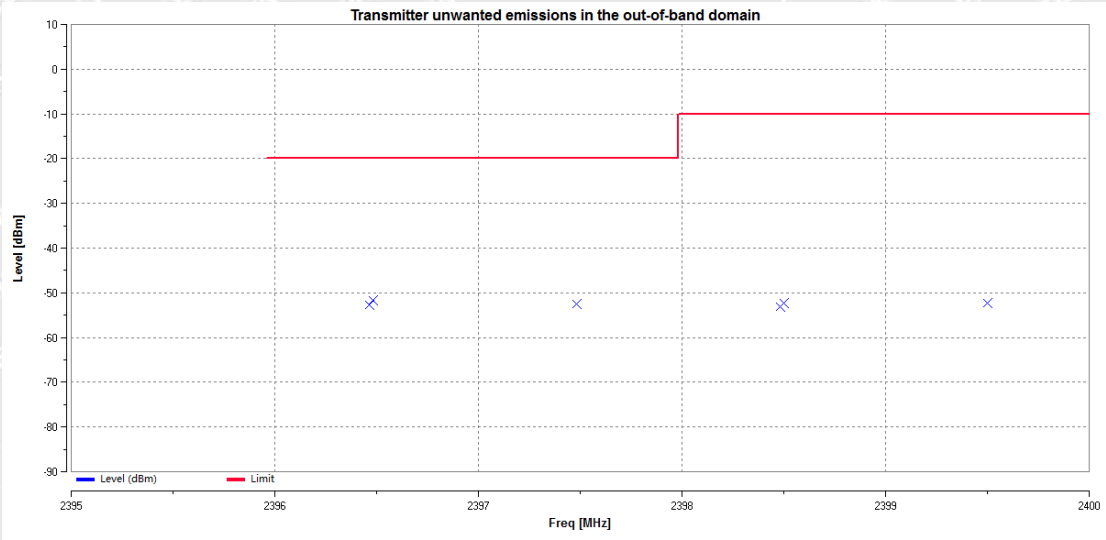


OOB_NTNV_BLE_2402_2483.5MHz to 2483.5MHz+2BW_2Mbps

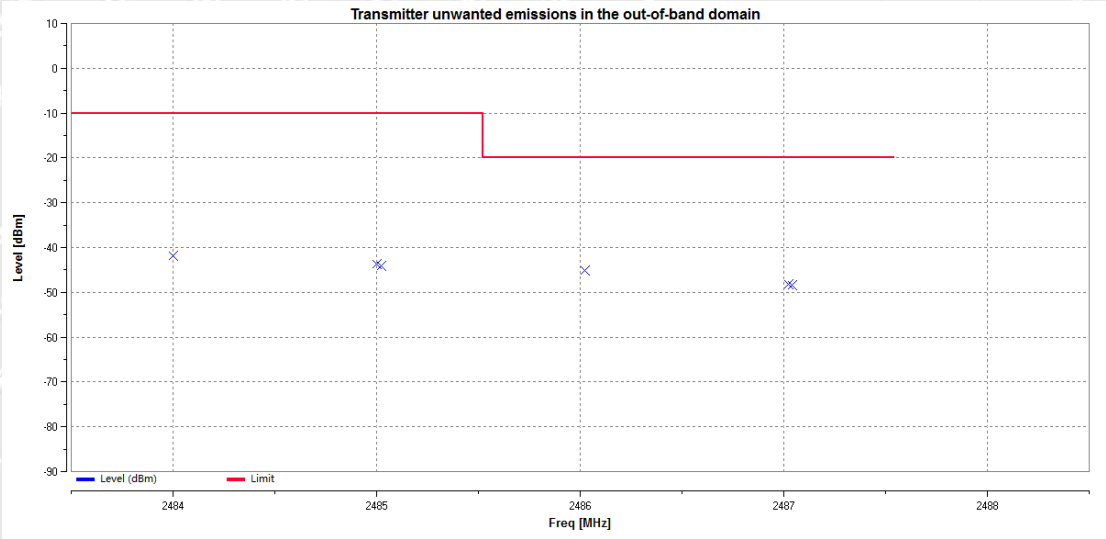




OOB_NTNV_BLE_2480_2400MHz-2BW to 2400MHz_2Mbps



OOB_NTNV_BLE_2480_2483.5MHz to 2483.5MHz+2BW_2Mbps





6.5 Transmitter unwanted emissions in the spurious domain

6.5.1 Standard Applicable

According to section 4.3.1.10.3& 4.3.2.9.3

The transmitter unwanted emissions in the spurious domain shall not exceed the values given in the following table.

Frequency Range	Maximum Power	Bandwidth
30 MHz to 47 MHz	-36 dBm	100 kHz
47 MHz to 74 MHz	-54 dBm	100 kHz
74 MHz to 87,5 MHz	-36 dBm	100 kHz
87,5 MHz to 118 MHz	-54 dBm	100 kHz
118 MHz to 174 MHz	-36 dBm	100 kHz
174 MHz to 230 MHz	-54 dBm	100 kHz
230 MHz to 470 MHz	-36 dBm	100 kHz
470 MHz to 694 MHz	-54 dBm	100 kHz
694 MHz to 1 GHz	-36 dBm	100 kHz
1 GHz to 12,75 GHz	-30 dBm	1 MHz

6.5.2 Test Procedure

The device under test has an integral antenna and the radiated measurement shall apply to the device, using the method of measurement as described in the EN300328 section 5.4.9.2.

RBW=100kHz VBW=300kHz 30MHz-1GHz

RBW=1MHz VBW=3MHz 1GHz-12.75GHz

6.5.3 Test Condition

Operating Mode	A.1
Test Environment	Normal Condition
Test Voltage	Battery 3.8V
Ambient temperature	22°C
Humidity	54%RH
Atmospheric Pressure	101.2kPa



6.5.4 Test Result

Frequency (MHz)	Receiver Reading (dBμV)	Turn table Angle (°)	RX Antenna		Substituted			Absolute Level (dBm)	Limit (dBm)	Margin (dB)
			Height (m)	Polar (H/V)	SG Level (dBm)	Cable (dB)	Antenna Gain (dB)			
TX_BLE_Low Channel_1Mbps										
362.92	30.99	283	1.1	H	-74.46	0.16	0.00	-74.30	-36	-38.30
362.92	31.73	315	1.9	V	-73.15	0.16	0.00	-72.99	-36	-36.99
1974.50	44.47	317	1.5	H	-49.12	0.31	10.40	-59.21	-30	-29.21
1974.50	47.52	134	1.8	V	-45.31	0.31	10.40	-55.40	-30	-25.40
4638.13	40.91	126	1.8	H	-49.78	2.61	12.70	-59.87	-30	-29.87
4638.13	39.84	156	1.6	V	-49.84	2.61	12.70	-59.93	-30	-29.93
TX_BLE_High Channel_1Mbps										
80.46	35.19	255	1.4	H	-72.05	0.15	0.00	-71.90	-36	-35.90
80.46	34.64	144	1.2	V	-72.21	0.15	0.00	-72.06	-36	-36.06
4019.00	41.86	205	1.1	H	-49.41	2.49	12.60	-59.52	-30	-29.52
4019.00	44.25	109	1.5	V	-45.66	2.49	12.60	-55.77	-30	-25.77
5732.52	44.26	157	1.4	H	-45.03	2.87	12.90	-55.06	-30	-25.06
5732.52	39.72	318	1.1	V	-48.72	2.87	12.90	-58.75	-30	-28.75

Frequency (MHz)	Receiver Reading (dBμV)	Turn table Angle (°)	RX Antenna		Substituted			Absolute Level (dBm)	Limit (dBm)	Margin (dB)
			Height (m)	Polar (H/V)	SG Level (dBm)	Cable (dB)	Antenna Gain (dB)			
TX_BLE_Low Channel_2Mbps										
828.46	23.44	167	1.5	H	-72.07	0.22	0.00	-71.85	-36	-35.85
828.46	22.60	254	1.6	V	-73.06	0.22	0.00	-72.84	-36	-36.84
3704.01	44.89	112	1.3	H	-46.39	2.37	12.50	-56.52	-30	-26.52
3704.01	42.12	314	1.2	V	-47.43	2.37	12.50	-57.56	-30	-27.56
3777.80	41.70	145	1.7	H	-49.58	2.37	12.50	-59.71	-30	-29.71
3777.80	40.56	250	1.8	V	-48.99	2.37	12.50	-59.12	-30	-29.12
TX_BLE_High Channel_2Mbps										
514.02	27.98	114	1.5	H	-71.78	0.18	0.00	-71.60	-54	-17.60
514.02	26.80	243	1.0	V	-74.30	0.18	0.00	-74.12	-54	-20.12
2506.58	44.12	160	1.6	H	-49.54	0.43	10.60	-59.71	-30	-29.71
2506.58	44.21	194	1.0	V	-45.73	0.43	10.60	-55.90	-30	-25.90
5002.09	43.47	160	1.6	H	-45.95	2.79	12.70	-55.86	-30	-25.86
5002.09	43.40	279	1.1	V	-45.55	2.79	12.70	-55.46	-30	-25.46



6.6 Receiver spurious emissions

6.6.1 Standard Applicable

According to section 4.3.1.11.3&4.3.2.10.3, The spurious emissions of the receiver shall not exceed the values given in table below

NOTE: In case of equipment with antenna connectors, these limits apply to emissions at the antenna port (conducted) and to the emissions radiated by the cabinet. In case of integral antenna equipment (without temporary antenna connectors), these limits apply to emissions radiated by the equipment. Spurious emission limits for receivers

Frequency Range	Maximum Power	Bandwidth
30 MHz to 1 GHz	-57 dBm	100 kHz
1 GHz to 12,75 GHz	-47 dBm	1 MHz

6.6.2 Test Procedure

The device under test has an integral antenna and the radiated measurement shall apply to the device, using the method of measurement as described in the EN300328 section 5.4.10.2.

RBW=100kHz VBW=300kHz 30MHz-1GHz

RBW=1MHz VBW=3MHz 1GHz-12.75GHz

6.6.3 Test Condition

Operating Mode : A.2
Test Environment : Normal Condition
Test Voltage : Battery 3.8V
Ambient temperature : 22°C
Humidity : 54%RH
Atmospheric Pressure : 101.2kPa



6.6.4 Test Result

Frequency (MHz)	Receiver Reading (dBμV)	Turn table Angle (°)	RX Antenna		Substituted			Absolute Level (dBm)	Limit (dBm)	Margin (dB)
			Height (m)	Polar (H/V)	SG Level (dBm)	Cable (dB)	Antenna Gain (dB)			
RX_BLE_Low Channel_1Mbps										
117.92	33.01	264	1.7	H	-74.18	0.15	0.00	-74.03	-57	-17.03
117.92	32.44	257	1.0	V	-74.24	0.15	0.00	-74.09	-57	-17.09
2535.88	44.30	221	2.0	H	-49.36	0.43	10.60	-59.53	-47	-12.53
2535.88	42.06	121	1.9	V	-47.88	0.43	10.60	-58.05	-47	-11.05
4707.04	42.80	169	1.9	H	-48.10	2.61	12.70	-58.19	-47	-11.19
4707.04	40.72	134	1.0	V	-48.21	2.61	12.70	-58.30	-47	-11.30
RX_BLE_High Channel_1Mbps										
630.24	28.30	104	1.7	H	-71.25	0.20	0.00	-71.05	-57	-14.05
630.24	27.09	303	1.9	V	-71.97	0.20	0.00	-71.77	-57	-14.77
5292.56	41.26	132	1.7	H	-48.34	2.81	12.80	-58.33	-47	-11.33
5292.56	38.91	226	1.3	V	-49.91	2.81	12.80	-59.90	-47	-12.90
5998.32	39.58	161	1.8	H	-48.89	2.90	12.90	-58.89	-47	-11.89
5998.32	39.71	165	1.9	V	-48.53	2.90	12.90	-58.53	-47	-11.53

Frequency (MHz)	Receiver Reading (dBμV)	Turn table Angle (°)	RX Antenna		Substituted			Absolute Level (dBm)	Limit (dBm)	Margin (dB)
			Height (m)	Polar (H/V)	SG Level (dBm)	Cable (dB)	Antenna Gain (dB)			
RX_BLE_Low Channel_2Mbps										
456.98	26.69	244	1.7	H	-75.02	0.16	0.00	-74.86	-57	-17.86
456.98	32.50	315	1.3	V	-70.25	0.16	0.00	-70.09	-57	-13.09
2211.24	44.36	225	1.9	H	-47.16	0.38	10.50	-57.28	-47	-10.28
2211.24	40.33	163	1.1	V	-48.45	0.38	10.50	-58.57	-47	-11.57
3535.10	44.63	294	1.3	H	-47.89	2.34	12.40	-57.95	-47	-10.95
3535.10	42.22	212	1.5	V	-48.39	2.34	12.40	-58.45	-47	-11.45
RX_BLE_High Channel_2Mbps										
615.18	26.91	261	1.5	H	-72.47	0.20	0.00	-72.27	-57	-15.27
615.18	26.99	204	1.3	V	-72.01	0.20	0.00	-71.81	-57	-14.81
1722.73	45.61	237	1.5	H	-49.99	0.30	9.40	-59.09	-47	-12.09
1722.73	47.56	230	1.8	V	-47.77	0.30	9.40	-56.87	-47	-9.87
3475.32	45.28	140	1.8	H	-47.65	2.34	12.40	-57.71	-47	-10.71
3475.32	44.49	239	2.0	V	-46.54	2.34	12.40	-56.60	-47	-9.60



6.7 Receiver Blocking

6.7.1 Standard Applicable

According to section 4.3.2.11.2, Receiver blocking is a measure of the ability of the equipment to receive a wanted signal on its operating channel without exceeding a given degradation in the presence of an unwanted signal (blocking signal) at frequencies other than those of the operating band.

Load Based Equipment not using any of the mechanisms referenced above shall comply with the following minimum set of requirements :

The minimum performance criterion shall be a PER less than or equal to 10 %. The manufacturer may declare alternative performance criteria as long as that is appropriate for the intended use of the equipment (see clause 5.4.1.t)).

While maintaining the minimum performance criteria as defined in clause 4.3.2.11.3, the blocking levels at specified frequency offsets shall be equal to or greater than the limits defined for the applicable receiver category 1, 2 and 3 provided in table 14, table 15 or table 16.

Receiver category 1

Adaptive equipment with a maximum RF output power greater than 10 dBm e.i.r.p. shall be considered as receiver category 1 equipment.

Table 14: Receiver Blocking parameters for Receiver Category 1 equipment

Wanted signal mean power from companion device (dBm) (see notes 1 and 4)	Blocking signal frequency (MHz)	Blocking signal power (dBm) (see note 4)	Type of blocking signal
(-133 dBm + 10 × log ₁₀ (OCBW)) or -68 dBm whichever is less (see note 2)	2 380 2 504	-34	CW
(-139 dBm + 10 × log ₁₀ (OCBW)) or -74 dBm whichever is less (see note 3)	2 300 2 330 2 360 2 524 2 584 2 674		

NOTE 1: OCBW is in Hz.

NOTE 2: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative test may be performed using a wanted signal up to $P_{\min} + 26$ dB where $P_{\min}$ is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal.

NOTE 3: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative test may be performed using a wanted signal up to $P_{\min} + 20$ dB where $P_{\min}$ is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal.

NOTE 4: The level specified is the level at the UUT receiver input assuming a 0 dBi antenna assembly gain. In case of conducted measurements, this level has to be corrected for the (in-band) antenna assembly gain (G). In case of radiated measurements, this level is equivalent to a power flux density (PFD) in front of the UUT antenna with the UUT being configured/positioned as recorded in clause 5.4.3.2.2.



Receiver category 2

Non-adaptive equipment with a Medium Utilization (MU) factor greater than 1 % and less than or equal to 10 % or adaptive equipment with a maximum RF output power of 10 dBm e.i.r.p. shall be considered as receiver category 2 equipment.

Table 15: Receiver Blocking parameters for Receiver Category 2 equipment

Wanted signal mean power from companion device (dBm) (see notes 1 and 3)	Blocking signal frequency (MHz)	Blocking signal power (dBm) (see note 3)	Type of blocking signal
(-139 dBm + $10 \times \log_{10}(\text{OCBW}) + 10 \text{ dB}$) or (-74 dBm + 10 dB) whichever is less (see note 2)	2 380 2 504 2 300 2 584	-34	CW
NOTE 1: OCBW is in Hz. NOTE 2: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative test may be performed using a wanted signal up to $P_{\text{min}} + 26 \text{ dB}$ where P_{min} is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal. NOTE 3: The level specified is the level at the UUT receiver input assuming a 0 dBi antenna assembly gain. In case of conducted measurements, this level has to be corrected for the (in-band) antenna assembly gain (G). In case of radiated measurements, this level is equivalent to a power flux density (PFD) in front of the UUT antenna with the UUT being configured/positioned as recorded in clause 5.4.3.2.2.			

Receiver category 3

Non-adaptive equipment with a maximum Medium Utilization (MU) factor of 1 % or adaptive equipment with a maximum RF output power of 0 dBm e.i.r.p. shall be considered as receiver category 3 equipment.

Table 16: Receiver Blocking parameters for Receiver Category 3 equipment

Wanted signal mean power from companion device (dBm) (see notes 1 and 3)	Blocking signal frequency (MHz)	Blocking signal power (dBm) (see note 3)	Type of blocking signal
(-139 dBm + $10 \times \log_{10}(\text{OCBW}) + 20 \text{ dB}$) or (-74 dBm + 20 dB) whichever is less (see note 2)	2 380 2 504 2 300 2 584	-34	CW
NOTE 1: OCBW is in Hz. NOTE 2: In case of radiated measurements using a companion device and the level of the wanted signal from the companion device cannot be determined, a relative the test may be performed using a wanted signal up to $P_{\text{min}} + 30 \text{ dB}$ where P_{min} is the minimum level of wanted signal required to meet the minimum performance criteria as defined in clause 4.3.1.12.3 in the absence of any blocking signal. NOTE 3: The level specified is the level at the UUT receiver input assuming a 0 dBi antenna assembly gain. In case of conducted measurements, this level has to be corrected for the (in-band) antenna assembly gain (G). In case of radiated measurements, this level is equivalent to a power flux density (PFD) in front of the UUT antenna with the UUT being configured/positioned as recorded in clause 5.4.3.2.2.			



6.7.2 Test Procedure

Step 1: • For non-frequency hopping equipment, the UUT shall be set to the lowest operating channel.

Step 2: • The blocking signal generator is set to the first frequency as defined in the appropriate table corresponding to the receiver category and type of equipment.

Step 3: • With the blocking signal generator switched off, a communication link is established between the UUT and the associated companion device using the test setup shown in figure 6. The variable attenuator is set to a value that achieves the minimum performance criteria as specified in clause 4.3.1.12.3 or clause 4.3.2.11.3 with a resolution of at least 1 dB. The resulting level for the wanted signal at the input of the UUT is Pmin. This value shall be measured and recorded in the test report.

• The signal level is increased by the value provided in the table corresponding to the receiver category and type of equipment.

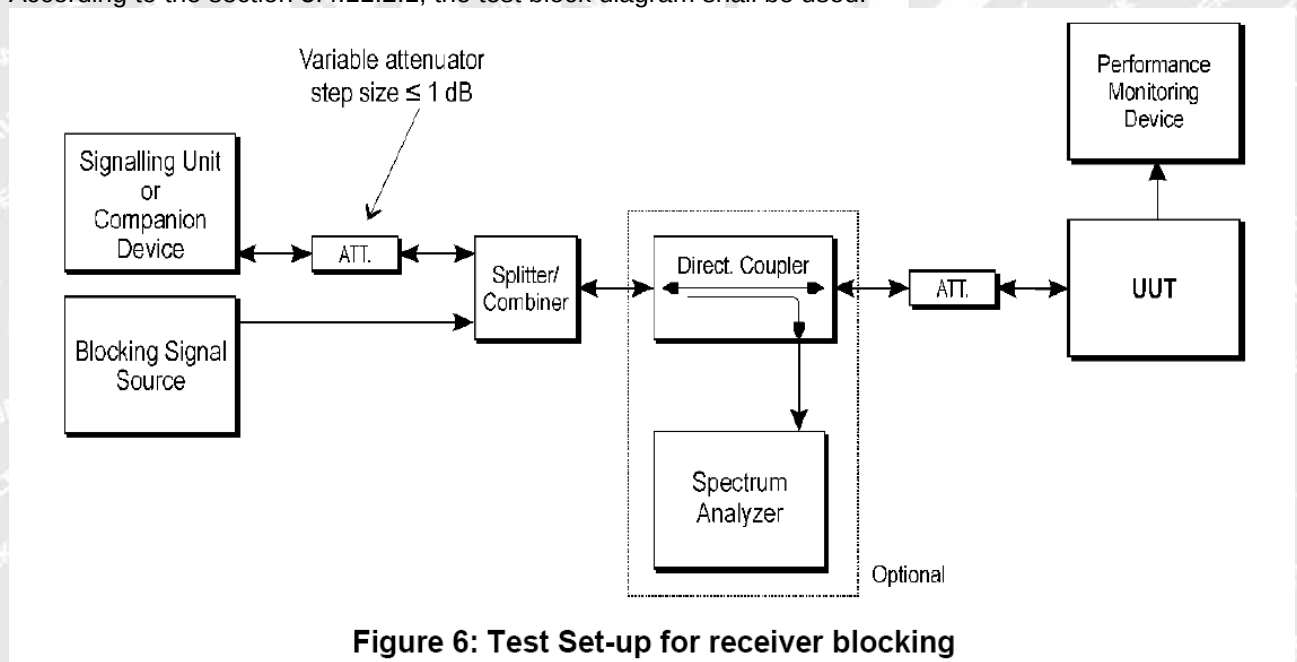
Step 4: • The blocking signal at the UUT is set to the level provided in the table corresponding to the receiver category and type of equipment. It shall be verified and recorded in the test report that the performance criteria as specified in clause 4.3.1.12.3 or clause 4.3.2.11.3 is met.

Step 5: • Repeat step 4 for each remaining combination of frequency and level for the blocking signal as provided in the table corresponding to the receiver category and type of equipment.

Step 6: • For non-frequency hopping equipment, repeat step 2 to step 5 with the UUT operating at the highest operating channel.

6.7.3 Test Setup

According to the section 5.4.11.2.1, the test block diagram shall be used.



All test procedure is carried to the section 5.4.11.2.1
RBW/VBW=8MHz/30MHz



6.7.4 Test Condition

Operating Mode : B
Test Environment : Normal Condition
Test Voltage : DC 3.3V (power to control panel)
Ambient temperature : 22°C
Humidity : 54%RH
Atmospheric Pressure : 101.2kPa

6.7.5 Test Result

GFSK_1Mbps						
Receiver Blocking Categories 2						
Wanted signal meanpower from companion device (dBm)	OCBW (Hz)	Blocking signal frequency (MHz)	Blocking signal power(dBm) CW	PER (%)	Limit	Results
-68.92	1019600	2380	-34	3.9	≤10%	Pass
		2504	-34	1.0		
		2300	-34	3.8		
		2584	-34	2.9		
NOTE 1: For equipment that supports a PER or FER test to be performed, the minimum performance criterion shall be a PER or FER less than or equal to 10 %.						
NOTE 2: For equipment that does not support a PER or a FER test to be performed, the minimum performance criterion shall be no loss of the wireless transmission function needed for the intended use of the equipment.						
NOTE 3: The smallest channel bandwidth and the lowest data rate for this channel bandwidth which still allows the equipment to operate as intended shall be used. This mode of operation shall be aligned with the performance criteria defined in clause 4.3.1.12.3 or clause 4.3.2.11.3 and shall be described in the test report.						



GFSK_2Mbps						
Receiver Blocking Categories 2						
Wanted signal meanpower from companion device (dBm)	OCBW (Hz)	Blocking signal frequency (MHz)	Blocking signal power(dBm) CW	PER (%)	Limit	Results
-65.95	2019600	2380	-34	1.7	≤10%	Pass
		2504	-34	3.9		
		2300	-34	4.9		
		2584	-34	5.2		

NOTE 1: For equipment that supports a PER or FER test to be performed, the minimum performance criterion shall be a PER or FER less than or equal to 10 %.

NOTE 2: For equipment that does not support a PER or a FER test to be performed, the minimum performance criterion shall be no loss of the wireless transmission function needed for the intended use of the equipment.

NOTE 3: The smallest channel bandwidth and the lowest data rate for this channel bandwidth which still allows the equipment to operate as intended shall be used. This mode of operation shall be aligned with the performance criteria defined in clause 4.3.1.12.3 or clause 4.3.2.11.3 and shall be described in the test report.

WALTEK



7 Photographs - Test Setup

7.1 Photograph - Spurious Emissions Test Setup

Below 1GHz



Above 1GHz





8 Photographs – EUT Constructional Details

Please refer to “ANNEX” (Reference No. WTF25F06152819W).

=====End of Report=====

WALTEK



中国认可
国际互认
检测
TESTING
CNAS L6478



TEST REPORT

Reference No. : WTF25F06152819W002
Applicant : Mid Ocean Brands B.V.
Address : Unit 711-716, 7/F., Tower A, 83 King Lam Street, Cheung Sha Wan, Kowloon, Hong Kong.
Manufacturer : 118897
Address : ---
Product Name : Smart watch
Model No. : MO2748
Test specification : EN 62479:2010
EN 50663:2017
Date of Receipt sample : 2025-06-17
Date of Test : 2025-06-24
Date of Issue : 2025-06-28
Test Report Form No. : WEW-62479A-01B
Test Result : Pass

Remarks:

The results shown in this test report refer only to the sample(s) tested, this test report cannot be reproduced, except in full, without prior written permission of the company. The report would be invalid without specific stamp of test institute and the signatures of approver.

Prepared By:

Waltek Testing Group (Foshan) Co., Ltd.

Address: 1/F., Building 19, Sunlink Machinery City, Xingye 4 Road,
Guanglong Industrial Park, Chihua Neighborhood Committee, Chencun,
Shunde District, Foshan, Guangdong, China

Tel:+86-757-23811398

Fax:+86-757-23811381

E-mail:info@waltek.com.cn

Tested by:

Approved by:

Roy Hong

Danny Zhou



1 Test Summary

HEALTH			
Test	Test Method	Class / Severity	Result
RF Exposure	EN 62479:2010 EN 50663:2017	-	Pass

Remark:

Pass Test item meets the requirement

N/A Not Applicable

WALTEK



2 Contents

	Page
1 TEST SUMMARY	2
2 CONTENTS	3
3 GENERAL INFORMATION	4
3.1 GENERAL DESCRIPTION OF E.U.T.	4
3.2 TECHNICAL SPECIFICATION	4
3.3 STANDARDS APPLICABLE FOR TESTING	4
3.4 DISCLAIMER	4
4 RF EXPOSURE BASIC RESTRICTIONS	5
4.1 LIMITS STANDARD APPLICABLE	5
4.2 EVALUATION METHODS	6
4.3 EVALUATION RESULTS	6
5 PHOTOGRAPHS – EUT CONSTRUCTIONAL DETAILS	7

WALTEK



3 General Information

3.1 General Description of E.U.T.

Product Name : Smart watch
Model No. : MO2748
Remark : ---
Rating : Input: DC 5V
Battery Capacity : 3.8V, 300mAh, 1.14Wh
Adapter Model..... : ---

3.2 Technical Specification

Bluetooth Version : Bluetooth LE
Frequency Range : 2402-2480MHz
Maximum RF Output Power : 2.47 dBm (EIRP)@1Mbps
Type of Modulation : GFSK
Quantity of Channels : 40
Channel Separation..... : 2MHz
Data Rate : 1Mbps, 2Mbps
Antenna Type..... : Wire Antenna
Antenna Gain : -1.8dBi

3.3 Standards Applicable for Testing

The tests were performed according to following standards:

EN 62479:2010	Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz - 300 GHz)
EN 50663:2017	Generic standard for assessment of low power electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (10 MHz - 300 GHz)

3.4 Disclaimer

The antenna gain information is provided by the customer. The laboratory is not responsible for the accuracy of the antenna gain information.



4 RF EXPOSURE BASIC RESTRICTIONS

4.1 Limits Standard Applicable

According to EN 62479:2010, Assessment of the compliance of low power electronic and electrical equipment with the basic restrictions related to human exposure to electromagnetic fields (10 MHz to 300 GHz).

Low-power exclusion level $P_{\max}$ based on considerations of SAR

When SAR is the basic restriction, a conservative minimum value for $P_{\max}$ can be derived, equal to the localized SAR limit ($SAR_{\max}$) multiplied by the averaging mass (m):

$$P_{\max} = SAR_{\max} m \quad (A.1)$$

Example values of $P_{\max}$ according to Equation (A.1) are provided in Table A.1 for cases described by the ICNIRP guidelines [1], IEEE Std C95.1-1999 [2] and IEEE Std C95.1-2005 [3] where SAR limits are defined. Other exposure guidelines or standards may be applicable depending on national regulations.

Table A.1 – Example values of SAR-based $P_{\max}$ for some cases described by ICNIRP, IEEE Std C95.1-1999 and IEEE Std C95.1-2005

Guideline / Standard	SAR limit, $SAR_{\max}$ W/kg	Averaging mass, m g	$P_{\max}$ mW	Exposure tier ^a	Region of body ^a
ICNIRP [1]	2	10	20	General public	Head and trunk
	4	10	40	General public	Limbs
	10	10	100	Occupational	Head and trunk
	20	10	200	Occupational	Limbs
IEEE Std C95.1-1999 [2]	1,6	1	1,6	Uncontrolled environment	Head, trunk, arms, legs
	4	10	40	Uncontrolled environment	Hands, wrists, feet and ankles
	8	1	8	Controlled environment	Head, trunk, arms, legs
	20	10	200	Controlled environment	Hands, wrists, feet and ankles
IEEE Std C95.1-2005 [3]	2	10	20	Action level	Body except extremities and pinnae
	4	10	40	Action level	Extremities and pinnae
	10	10	100	Controlled environment	Body except extremities and pinnae
	20	10	200	Controlled environment	Extremities and pinnae

^a Consult the appropriate standard for more information and definitions of terms.



4.2 Evaluation Methods

Based on the above standard limit, the basic restriction at frequency between 10MHz to 300GHz is on localized SAR in the head. Any device with output power below 20mW cannot produce an exposure exceeding this restriction under the most pessimistic exposure conditions.

The basic restriction is 2W/Kg for general public device, so any unit which supplies less than 20mW from it's antenna port, averaged over 6 minutes, will meet the basic restriction.

4.3 Evaluation Results

Maximum Average Output Power

Frequency (MHz)	RF Output Power (dBm)	RF Output Power (mW)	Limit (mW)	Result
2402	2.47	1.766	20	Pass

Remark: The details of RF output power refer to report No.WTF25F06152819W001.

Since average output power at worst case is: 1.766 mW which cannot exceed the exempt condition, 20mW specified in EN 62479. It is deemed to full fit the requirement of RF exposure basic restriction specified in EC Council Recommendation (1999/519/EC).

WALTEK



5 Photographs – EUT Constructional Details

Please refer to “ANNEX” (Reference No. WTF25F06152819W).

=====End of Report=====

WALTEK