Cybersecurity Test Report

Equipment	:	**Noise Cancelling Wireless Headphones**
Model Name	:	**Px8 S2, Px7 S3**
Applicant	:	**B&W Group Ltd.** **Dale Road, Worthing, West Sussex, BN11 2BH, United Kingdom**
Manufacturer	:	**B&W Group Ltd.** **Dale Road, Worthing, West Sussex, BN11 2BH, United Kingdom**
Standard	:	**EN 18031-1:2024** **EN 18031-2:2024**

The product was received on Feb. 24, 2025 and testing was performed from Feb. 25, 2025 to Apr. 17, 2025. We, Sporton International Inc. EMC & Wireless Communications Laboratory, would like to declare that the tested sample has been evaluated in accordance with the test procedures given in EN 18031:2024 and has been in compliance with the applicable technical standards.

The test results in this report apply exclusively to the tested model / sample. Without written approval from Sporton International Inc. EMC & Wireless Communications Laboratory, the test report shall not be reproduced except in full.

Joseph Chang

Approved by : Joseph Chang

Sporton International Inc. EMC & Wireless Communications Laboratory
No. 52, Huaya 1st Rd., Guishan Dist., Taoyuan City 333, Taiwan (R.O.C.)

TEL : 886-3-327-3456
FAX : 886-3-328-4978

Table of Contents

History of this test report

Report no.	Version	Description	Issue date
E1522432	Rev. 01	Initial issue of report	Jun. 04, 2025

Summary of Test Result

Requirements	Requirements	Assessment			Overall Verdict
		Conceptual	Functional completeness	Functional sufficiency	
Access control mechanism	ACM-1 Applicability of access control mechanisms	PASS	PASS	PASS	PASS
	ACM-2 Appropriate access control mechanisms	PASS	PASS	PASS	
	ACM-3 Default access control for children in toys	N/A	N/A	N/A	
	ACM-4 Default access control to children's privacy assets for toys and childcare equipment	N/A	N/A	N/A	
	ACM-5 Parental/Guardian access controls for children in toys	N/A	N/A	N/A	
	ACM-6 Parental/Guardian access controls for other entities' access to managed children's privacy assets in toys	N/A	N/A	N/A	
Authentication mechanism	AUM-1 Applicability of authentication mechanisms	PASS	PASS	PASS	PASS
	AUM-2 Appropriate authentication mechanisms	PASS	PASS	PASS	
	AUM-3 Authenticator Validation	PASS	PASS	PASS	
	AUM-4 Changing authenticators	PASS	PASS	PASS	
	AUM-5 Password strength	PASS	PASS	PASS	
	AUM-6 Brute force protection	PASS	PASS	PASS	

Secure update mechanism	**SUM-1** **Applicability of update mechanisms**	PASS	PASS	PASS	PASS
	SUM-2 **Secure updates**	PASS	PASS	PASS	
	SUM-3 **Automated updates**	PASS	PASS	PASS	
Secure storage mechanism	**SSM-1** **Applicability of secure storage mechanisms**	PASS	PASS	PASS	PASS
	SSM-2 **Appropriate integrity protection for secure storage mechanisms**	PASS	PASS	PASS	
	SSM-3 **Appropriate confidentiality protection for secure storage mechanisms**	PASS	PASS	PASS	
Secure communication mechanism	**SCM-1** **Applicability of secure communication mechanisms**	PASS	PASS	PASS	PASS
	SCM-2 **Appropriate integrity and authenticity protection for secure communication mechanisms**	PASS	PASS	PASS	
	SCM-3 **Appropriate confidentiality protection for secure communication mechanisms**	PASS	PASS	PASS	
	SCM-4 **Appropriate replay protection for secure communication mechanisms**	PASS	PASS	PASS	
Logging Mechanism	**LGM-1** **Applicability of logging mechanisms**	PASS	PASS	PASS	PASS
	LGM-2 **Persistent storage of log data**	N/A	N/A	N/A	
	LGM-3 **Minimum number of persistently stored events**	PASS	PASS	PASS	
	LGM-4	PASS	PASS	PASS	

	Time-related information of persistently stored dog data				
Resilience mechanism	**RLM-1** **Applicability and appropriateness of resilience mechanisms**	N/A	N/A	N/A	N/A
Deletion mechanism	**DLM-1** **Applicability of deletion mechanisms**	PASS	PASS	PASS	PASS
Network monitoring mechanism	**NMM-1** **Applicability and appropriateness of network monitoring mechanisms .**	PASS	PASS	PASS	PASS
Traffic control mechanism	**TCM-1** **Applicability of and appropriate traffic control mechanisms**	N/A	N/A	N/A	N/A
User notification mechanism	**UNM-1** **Applicability of user notification mechanisms**	N/A	N/A	N/A	N/A
	UNM-2 **Appropriate user notification content**	N/A	N/A	N/A	
Confidential cryptographic keys	**CCK-1** **Appropriate CCKs**	PASS	PASS	PASS	PASS
	CCK-2 **CCK generation mechanisms**	PASS	PASS	PASS	
	CCK-3 **Preventing static default values for preinstalled CCKs**	PASS	PASS	PASS	
General equipment capabilities	**GEC-1** **Up-to-date software and hardware with no publicly known exploitable vulnerabilities**	PASS	PASS	PASS	PASS
	GEC-2 **Limit exposure of services via related network interfaces**	PASS	PASS	PASS	
	GEC-3 **Configuration of optional services and the related exposed network interfaces**	PASS	PASS	PASS	
	GEC-4	N/A	N/A	N/A	

	Documentation of exposed network interfaces and exposed services via network interfaces				
	GEC-5 **No unnecessary external interfaces**	PASS	PASS	PASS	
	GEC-6 **Input validation**	PASS	PASS	PASS	
	GEC-7 **Documentation of external sensing capabilities**	N/A	N/A	N/A	
	GEC-8 **Equipment Integrity**	N/A	N/A	N/A	
Cryptography	**CRY-1** **Best practice cryptography**	PASS	PASS	PASS	PASS

Test item comparison table

EN 18031-1-2-3 Test item comparison table			
Project	EN 18031-1	EN 18031-2	EN 18031-3
2.1.1[ACM-1]	6.1.1 [ACM-1]	6.1.1 [ACM-1]	6.1.1 [ACM-1]
2.1.2[ACM-2]	6.1.2 [ACM-2]	6.1.2 [ACM-2]	6.1.2 [ACM-2]
2.1.3[ACM-3]	N/A	6.1.3 [ACM-3]	N/A
2.1.4[ACM-4]	N/A	6.1.4 [ACM-4]	N/A
2.1.5[ACM-5]	N/A	6.1.5 [ACM-5]	N/A
2.1.6[ACM-6]	N/A	6.1.6 [ACM-6]	N/A
2.2.1[AUM-1]	6.2.1 [AUM-1]	6.2.1 [AUM-1]	6.2.1 [AUM-1]
2.2.2[AUM-2]	6.2.2 [AUM-2]	6.2.2 [AUM-2]	6.2.2 [AUM-2]
2.2.3[AUM-3]	6.2.3 [AUM-3]	6.2.3 [AUM-3]	6.2.3 [AUM-3]
2.2.4[AUM-4]	6.2.4 [AUM-4]	6.2.4 [AUM-4]	6.2.4 [AUM-4]
2.2.5[AUM-5]	6.2.5 [AUM-5]	6.2.5 [AUM-5]	6.2.5 [AUM-5]
2.2.6[AUM-6]	6.2.6 [AUM-6]	6.2.6 [AUM-6]	6.2.6 [AUM-6]
2.3.1[SUM-1]	6.3.1 [SUM-1]	6.3.1 [SUM-1]	6.3.1 [SUM-1]
2.3.2[SUM-2]	6.3.2 [SUM-2]	6.3.2 [SUM-2]	6.3.2 [SUM-2]
2.3.3[SUM-3]	6.3.3 [SUM-3]	6.3.3 [SUM-3]	6.3.3 [SUM-3]
2.4.1[SSM-1]	6.4.1 [SSM-1]	6.4.1 [SSM-1]	6.4.1 [SSM-1]
2.4.2[SSM-2]	6.4.2 [SSM-2]	6.4.2 [SSM-2]	6.4.2 [SSM-2]
2.4.3[SSM-3]	6.4.3 [SSM-3]	6.4.3 [SSM-3]	6.4.3 [SSM-3]
2.5.1[SCM-1]	6.5.1 [SCM-1]	6.5.1 [SCM-1]	6.5.1 [SCM-1]
2.5.2[SCM-2]	6.5.2 [SCM-2]	6.5.2 [SCM-2]	6.5.2 [SCM-2]
2.5.3[SCM-3]	6.5.3 [SCM-3]	6.5.3 [SCM-3]	6.5.3 [SCM-3]
2.5.4[SCM-4]	6.5.4 [SCM-4]	6.5.4 [SCM-4]	6.5.4 [SCM-4]
2.6.1[LGM-1]	N/A	6.6.1 [LGM-1]	6.6.1 [LGM-1]
2.6.2[LGM-2]	N/A	6.6.2 [LGM-2]	6.6.2 [LGM-2]
2.6.3[LGM-3]	N/A	6.6.3 [LGM-3]	6.6.3 [LGM-3]
2.6.4[LGM-4]	N/A	6.6.4 [LGM-4]	6.6.4 [LGM-4]
2.7.1[RLM-1]	6.6.1 [RLM-1]	N/A	N/A
2.8.1[DLM-1]	N/A	6.7.1 [DLM-1]	N/A
2.9.1[NMM-1]	6.7.1 [NMM-1]	N/A	N/A
2.10.1[TCM-1]	6.8.1 [TCM-1]	N/A	N/A
2.11.1[UNM-1]	N/A	6.8.1 [UNM-1]	N/A

2.11.2[UNM-2]	N/A	6.8.2 [UNM-2]	N/A
2.12.1[CCK-1]	6.9.1 [CCK-1]	6.9.1 [CCK-1]	6.7.1 [CCK-1]
2.12.2[CCK-2]	6.9.2 [CCK-2]	6.9.2 [CCK-2]	6.7.2 [CCK-2]
2.12.3[CCK-3]	6.9.3 [CCK-3]	6.9.3 [CCK-3]	6.7.3 [CCK-3]
2.13.1[GEC-1]	6.10.1 [GEC-1]	6.10.1 [GEC-1]	6.8.1 [GEC-1]
2.13.2[GEC-2]	6.10.2 [GEC-2]	6.10.2 [GEC-2]	6.8.2 [GEC-2]
2.13.3[GEC-3]	6.10.3 [GEC-3]	6.10.3 [GEC-3]	6.8.3 [GEC-3]
2.13.4[GEC-4]	6.10.4 [GEC-4]	6.10.4 [GEC-4]	6.8.4 [GEC-4]
2.13.5[GEC-5]	6.10.5 [GEC-5]	6.10.5 [GEC-5]	6.8.5 [GEC-5]
2.13.6[GEC-6]	6.10.6 [GEC-6]	6.10.6 [GEC-6]	6.8.6 [GEC-6]
2.13.7[GEC-7]	N/A	6.10.7 [GEC-7]	6.8.7 [GEC-7]
2.13.8[GEC-8]	N/A	N/A	6.8.8 [GEC-8]
2.14.1[CRY-1]	6.11.1 [CRY-1]	6.11.1 [CRY-1]	6.9.1 [CRY-1]

The DUT in this case is a pair of Noise Cancelling Wireless Headphones, classified as a network-connected device with limited data processing capability. The device may interact with mobile applications via Bluetooth and support firmware updates, but it does not directly store or process personal or financial user data independently. Therefore, only RED d and e are applicable and need to be tested in this case. RED f is not applicable due to the absence of direct support for electronic transactions or financial data handling on the DUT itself.

- **RED d**: Security asset and network asset
- **RED e**: Security asset and privacy asset

Comments and explanations:
The product specifications of the Equipment Under Test (EUT) presented in this report are declared by the manufacturer, as in Appendix A, who shall take full responsibility for the authenticity. Note: The term EUT, Device Under Test (DUT) and device refer to the same.
Declaration of Conformity:
The test results with all measurement uncertainty excluded are presented in accordance with the regulation limits or requirements declared by manufacturers.

Test Engineer: Jason Hsu

1.General Description

1.1.Product Feature of Equipment Under Test

Product Feature		
DUT	Noise Cancelling Wireless Headphones	
Model Name	Px8 S2	Px7 S3
Hardware Version	DVT2	DVT2
Software Version	v6.0.7	v3.0.7
General Specs	Bluetooth 5.3	

1.1.Test Device Picture

Test Device Picture	
Px7 S3	Px8 S2
	

1.2.Usage of samples

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

Product	Model	Serial No.
Noise Cancelling Wireless Headphones	Px7 S3	#4_Series
Noise Cancelling Wireless Headphones	Px7 S3	#5_Series
Noise Cancelling Wireless Headphones	Px7 S3	#6_Series
Noise Cancelling Wireless Headphones	Px8 S2	#1_Main
Noise Cancelling Wireless Headphones	Px8 S2	#2_Main
Noise Cancelling Wireless Headphones	Px8 S2	#3_Main

1.3.Testing Facility

Test Site	Sporton International Inc. EMC & Wireless Communications Laboratory
Test Site Location	No.52, Huaya 1st Rd., Guishan Dist., Taoyuan City 333, Taiwan (R.O.C.) TEL: +886-3-327-3456 FAX: +886-3-328-4978
Test Site Number	TH03-HY

1.4.Test Equipment

Item	Equipment	Brand Name	Model Name	Operating System
1	Note book	ASUS	Asus Expertbook b1402cva	N/A
2	Router	Dlink	Dlink AX-3000	N/A

1.5.Test Software

Item	Software	Version	Configuration
1	Wireshark	4.42	Default
2	Charles	5.0	Default

1.6.Data provided by the client

The following data has been provided by the client:

1. EN 18031-1, -2 E-Info

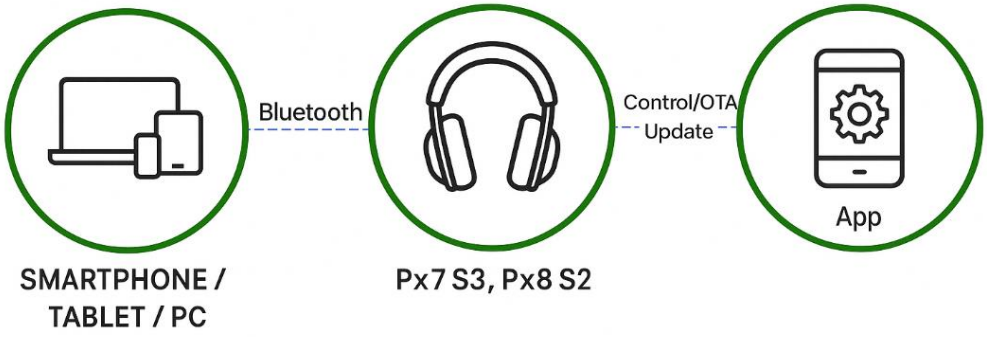
1.7.Applied Standards

i. EN 18031-1:2024.

ii. EN 18031-2:2024

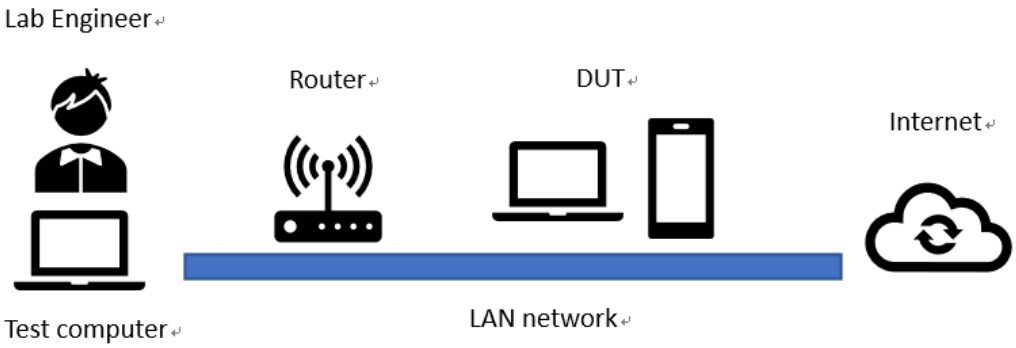
iii. NIST.SP.800-52r2

1.8.Connection Diagram of Test System



1.9.Test layout

IP: 192.168.137.110



2.Test result

2.1.[ACM] Access control mechanisms

2.1.1.[ACM-1] Applicability of access control mechanisms.

Security Flaw	Unauthorized access to security and network assets Unauthorized access to security and privacy assets Unauthorized entities gaining access to protected security and financial assets**.**	
Affected Essential Requirements	This security flaw allows unauthorized entities to access assets, compromising essential security requirements per 3.3(d) (e) (f).	
Typical Attack	Exploitation of unsecured access points to gain access to sensitive security or network assets. Exploitation of unsecured access points to gain access to sensitive security or privacy assets. Exploitation of unsecured access points to gain access to sensitive security or financial assets.	
Covered by Requirement?	EN 18031-1: 6.1.1 [ACM-1] Applicability of access control mechanisms. The equipment shall use access control mechanisms to manage access to security and network assets unless excluded by public accessibility, physical/logical measures, or legal restrictions. EN 18031-2:6.1.1[ACM-1]Applicability of access control mechanisms. Access control mechanisms shall be used to manage access to security and privacy assets, except where exclusions apply (public access, physical/logical restrictions, or legal implications).	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment determines: - The assets in scope - Access mechanism is present - Physical/logical measures in place	
Objectively Verifiable and Reproducible?	- Reliable documentation required	PASS
	- Complete and structured assessment	PASS
	- Reliable assessment results requested	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence

Documentation on access control mechanisms, including descriptions of public accessibility, physical/logical measures, legal justifications, and access control configurations.

According to the E.info-ACM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☑PASS ☐ FAIL ☐ N/A
●Functional sufficiency assessment:
verdict ☑PASS ☐ FAIL ☐ N/A

According the E.info-ACM-1, there are four kinds of ACM: RBAC, MAC, DAC and generic, each asset has its own access control mechanism, describe in the following table:

ACM	Asset Identifier	Description
MAC	SecurityAsset1	Pairing Keys
	SecurityAsset2	Encryption Keys
	SecurityAsset3	Bluetooth Link Keys
	SecurityAsset4	Firmware Images
	SecurityAsset5	OTA Update Mechanism
DAC	NetworkAsset1	Bluetooth Communication

1. Security Asset Protection (MAC)

The following security assets are protected using Mandatory Access Control (MAC) to ensure that only authorized system processes can access them. These assets include:

1.1 Pairing Keys (SecurityAsset1)

Pairing keys are generated during the initial Bluetooth pairing process and stored securely.

Only system-level processes with SMP (Security Manager Protocol) permissions can manage pairing keys.

	Unauthorized devices attempting to connect will be denied, protecting the integrity of the paired connection. MAC Enforcement: Pairing keys are protected by system-enforced policies and cryptographic authentication mechanisms. 1.2 Encryption Keys (SecurityAsset2) Encryption keys are generated during Bluetooth communication to ensure secure data transmission. AES-CCM (Counter with CBC-MAC) encryption is used to protect communication between paired devices. Only system processes and Bluetooth services can handle encryption keys. MAC Enforcement: Encryption keys are strictly controlled by the Bluetooth stack and cannot be accessed by unauthorized applications. 1.3 Bluetooth Link Keys (SecurityAsset3) Link keys enable secure reconnection between previously paired devices. These keys are managed through the Link Key Generation process during device pairing. Unauthorized access to link keys is denied through system-level enforcement. MAC Enforcement: Link keys are stored securely and are protected by Bluetooth link security mechanisms. 1.4 Firmware Images (SecurityAsset4) Firmware update images are signed and verified, and the **update process is limited to system-level processes** only. **Access to write firmware partitions**

	is restricted via system-level permissions and enforced through mandatory access controls (e.g., SELinux) to prevent unauthorized flashing or tampering. 1.5 OTA Update Mechanism (SecurityAsset5) The OTA update mechanism is only accessible by the authorized vendor application. **Access to the OTA trigger and firmware write APIs is controlled via UID checks and role-based policies**, ensuring that only authenticated processes can initiate updates. 2. Network Interface Tests (DAC) The following network asset is protected using Discretionary Access Control (DAC) to allow authorized devices to manage Bluetooth connections. 2.1 Bluetooth Communication (NetworkAsset1) Bluetooth communication is restricted to paired and authorized devices only. LE Secure Connections (LESC) is used to establish encrypted communication between the earphones and paired devices. Users have control over enabling or disabling Bluetooth functionality and can manage device connections. DAC Enforcement: Bluetooth pairing requires explicit user authorization. Communication between devices is protected by encryption, ensuring secure data transfer. Conclusion: The system enforces security policies by implementing **MAC, DAC** access control mechanisms. Security assets (pairing keys, encryption keys, link keys, firmware, and OTA updates) are protected through **MAC**, while Bluetooth communication is regulated by **DAC**. These integrated security measures ensure that the system meets all **ACM-1** requirements. Result: **PASS**

2.1.2. [ACM-2] Appropriate access control mechanisms.

Security Flaw	Unauthorized entities gaining access to protected security and network assets. Unauthorized entities gaining access to protected security and privacy assets. Unauthorized access to security and financial assets.	
Affected Essential Requirements	The security flaw allows unauthorized entities to access protected assets, related to clause 3.3(d) (e) .	
Typical Attack	Exploitation of weak or inappropriate access control mechanisms to gain unauthorized access to security or network assets. Exploitation of weak or inappropriate access control mechanisms to gain unauthorized access to security or privacy assets. Exploitation of weak or absent access control mechanisms to gain unauthorized access to sensitive security or financial assets.	
Covered by Requirement?	EN 18031-1: 6.1.2 [ACM-2] Appropriate access control mechanisms. Access control mechanisms that are required per ACM-1 must ensure only authorized entities have access to protected assets. EN 18031-2: 6.1.2 [ACM-2] Appropriate access control mechanisms. Access control mechanisms that are required per ACM-1 must ensure only authorized entities have access to protected security and privacy assets.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Review of entities access to assets - Review of authorization roles and identities. - Consideration of environmental factors and operational use cases. The assessment includes: - Assessment of implemented access control mechanisms. - Review of authorization roles and identities. - Functionality tests for denying unauthorized access to security and financial assets.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	PASS
	- Complete and structured assessment:	PASS
	- Reliable assessment results requested	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation on access control mechanisms, including detailed descriptions of how each control denies unauthorized access, role assignments, and functional tests. Documentation of access control mechanisms and processes, including roles, identities, permissions, and records of system functionality tests demonstrating the denial of unauthorized access to security or financial assets.	

According to the E.info-ACM-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

According the E.info-ACM-2, there are four kinds of ACM, describes as following:

Category	Details
IC.ACM-2.RBAC	The methods to validate the appropriateness of the access control mechanism solely rely on role-based access control.
IC.ACM-2.DAC	The methods to validate the appropriateness of the access control mechanism solely rely on discretionary access control.
IC.ACM-2.MAC	The methods to validate the appropriateness of the access control mechanism solely rely on mandatory access control.
IC.ACM-2.Generic	The methods to validate the appropriateness of the access control mechanism do not solely rely on any of the methods described in ACM-2-DAC or ACM-2-MAC.

The Px8 S2 / Px7 S3 utilizes secure Bluetooth pairing and encrypted key management to safeguard access to security and network assets. Access to the device's assets is granted only through validated Bluetooth pairing and secure key exchange.

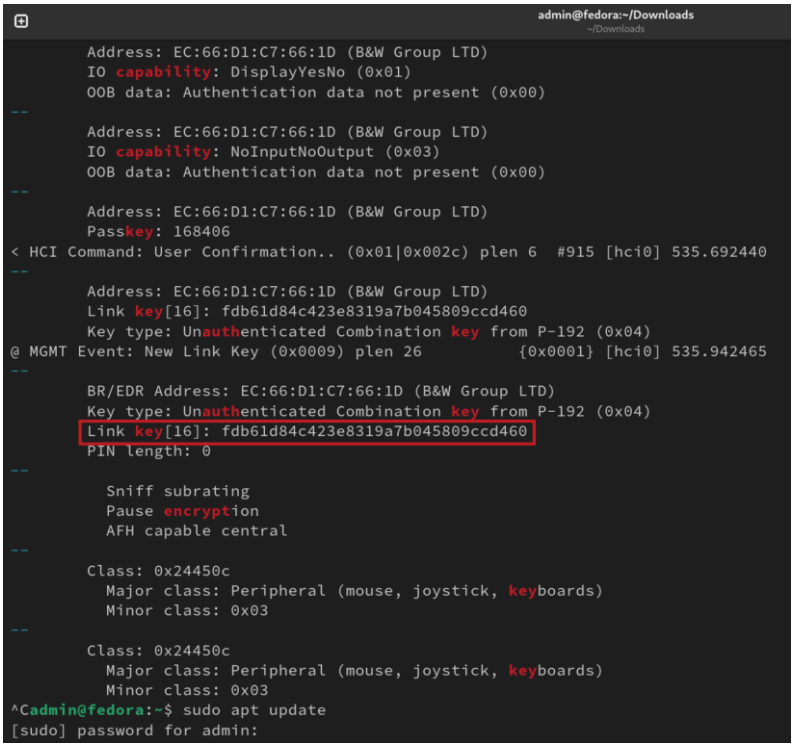


Figure 1:pairing key

Px8 S2 / Px7 S3 implements robust, multi-layered access control mechanisms for Bluetooth functionalities. By enforcing strict pairing procedures, secure link key generation, and encrypted reconnection, it ensures that every operation adheres to the principle of least privilege and is executed only with legitimate authorization. These measures effectively safeguard user data and security assets, thereby fully meeting the EN 18031 ACM-2 requirements for exemplifying a high standard of security protection. Therefore, the result of this conceptual test is: PASS.

Result: **PASS**

2.1.3. [ACM-3] Default access control for children in toys

Security Flaw	Unauthorized entities gaining access to external content through privacy functions meant for children.
Affected Essential Requirements	The security flaw allows unauthorized access to external content, particularly compromising children's privacy.

Typical Attack	Exploitation of weak or inappropriate access control mechanisms, allowing unauthorized content or interactions to be accessed by children through privacy functions.	
Covered by Requirement?	EN 18031-2:2024 6.1.3 [ACM-3] Default access control for children in toys. Access control mechanisms must ensure that children's access to external content via privacy functions is restricted to authorized entities by default.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Review of privacy functions that allow children to access external content - Evaluation of access control mechanisms for appropriateness - Consideration of external content sources.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	N/A
	- Complete and structured assessment:	N/A
	- Reliable assessment results requested	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation on access control mechanisms, including descriptions of how children's access to content from authorized entities is restricted, role assignments, and functional tests. **According to the E.info-ACM-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** The equipment is a Noise Cancelling Wireless Headphones, this requirement is not applicable Result:**N/A**	

2.1.4.[ACM-4] Default Access Control to Children's Privacy Assets for Toys and Childcare Equipment

Security Flaw	Unauthorized third-party access to children's privacy functions and personal information processed by toys and childcare equipment.

Affected Essential Requirements	The security flaw allows unauthorized third parties to access children's privacy functions or personal information, related to clause 3(3)e.	
Typical Attack	Exploitation of inappropriate access control settings, leading to unauthorized third-party access to children's personal information or privacy assets.	
Covered by Requirement?	EN 18031-2: 6.1.4 [ACM-4] Default access control to children's privacy assets. By default, access control mechanisms must restrict third-party access to children's privacy functions and personal information, except where necessary for the equipment's intended functionality.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Review of privacy functions and personal information accessible by third parties - Evaluation of access control mechanisms for appropriateness - Identification of authorized third-party access.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	N/A
	- Complete and structured assessment:	N/A
	- Reliable assessment results requested	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation on access control mechanisms, including detailed descriptions of how third-party access is restricted to necessary functionality, role assignments, and functional tests. **According to the E.info-ACM-4，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** The equipment is a Noise Cancelling Wireless Headphones, this requirement is not applicable Result:**N/A**	

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

Security Flaw	Unauthorized access by children to protected security and privacy assets.
Affected Essential Requirements	The security flaw allows children unauthorized access to assets, concerns 3(3)e

Typical Attack	Exploitation of weak or absent access controls allowing children unauthorized access to sensitive security or privacy assets.	
Covered by Requirement?	EN 18031-2: 6.1.5 [ACM-5] Parental/Guardian access controls. Access control mechanisms must allow authorized entities (parents/guardians) to configure and restrict children's access to protected security and privacy assets.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Review of security and privacy assets accessible by children. - Evaluation of access control mechanisms configurable by authorized entities (parents/guardians). - Consideration of ease of configuration and effectiveness in restricting access.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	N/A
	- Complete and structured assessment:	N/A
	- Reliable assessment results requested	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation on access control mechanisms, including descriptions of how authorized entities restrict children's access, role assignments, and configuration processes. **According to the E.info-ACM-5，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** The equipment is a Noise Cancelling Wireless Headphones, this requirement is not applicable Result:**N/A**	

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

Security Flaw	Unauthorized access by third parties to children's privacy assets

Affected Essential Requirements	The security flaw allows unauthorized entities access to children's privacy assets, concerns 3(3)e	
Typical Attack	Exploitation of weak or absent access controls allowing third-party access to sensitive children's privacy assets	
Covered by Requirement?	EN 18031-2:6.1.6 [ACM-6] Parental/Guardian access controls.Access control mechanisms must allow authorized entities (parents/guardians) to configure and restrict third-party access to children’s privacy assets	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Review of children's privacy assets accessible by third parties - Evaluation of access control mechanisms configurable by authorized entities (parents/guardians) - Consideration of ease of configuration and effectiveness in restricting access.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	N/A
	- Complete and structured assessment:	N/A
	- Reliable assessment results requested	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation on access control mechanisms, including descriptions of how authorized entities restrict third-party access to children’s privacy assets, role assignments, and configuration processes **According to the E.info-ACM-6，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** The equipment is a Noise Cancelling Wireless Headphones, this requirement is not applicable Result:**N/A**	

2.2. [AUM] Authentication mechanism

2.2.1. [AUM-1] Applicability of authentication mechanisms

Security Flaw	Unauthorized access to network functions and security parameters due to weak or absent authentication mechanisms.

	Unauthorized access to network functions, privacy assets, or security parameters due to weak or absent authentication mechanisms Unauthorized access to financial or security assets via network, user, or machine interfaces due to lack of authentication mechanisms.	
Affected Essential Requirements	The security flaw could result in unauthorized access to confidential or sensitive network configurations, affecting EN 18031-1 The security flaw could result in unauthorized access to confidential or sensitive personal, privacy, or security assets, affecting EN 18031-2 The security flaw may expose confidential financial data, security parameters, or sensitive financial function configurations, violating requirements of access control and security.	
Typical Attack	Exploitation of inadequate authentication mechanisms to access or modify sensitive security parameters or network functions. Exploitation of inadequate authentication mechanisms to access or modify sensitive personal, privacy, or security assets Exploitation of missing or weak authentication mechanisms to gain unauthorized access, modify financial or security assets, or use unauthorized functions.	
Covered by Requirement?	EN 18031-1:2024 6.2.1 [AUM-1] Applicability of authentication mechanisms. Authentication mechanisms must be used for access control over network and user interfaces that handle confidential or sensitive assets, except when absence is justified by functionality or environmental measures.. EN 18031-2:2024 6.2.1 [AUM-1] Applicability of authentication mechanisms. Authentication mechanisms must be used for access control over network and user interfaces that handle confidential or sensitive assets, except when absence is justified by functionality or environmental measures	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment involves: - Review of authentication mechanisms in network and user interfaces - Verification of managed access control - Evaluation of environmental measures where authentication is absent. - Review of access control and authentication mechanisms. - Verification of access via different interfaces (network, user, or machine).	
Objectively Verifiable and Reproducible?	- Reliable documentation required	PASS
	- Complete and structured assessment	PASS
	- Reliable assessment results requested	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence

Documentation of authentication mechanisms, including managed access over network and user interfaces, decision tree paths, and justification of absent authentication where applicable.

Documentation of authentication mechanisms implemented for managing access, including processes and logs showing restricted access to financial and security assets.

According to the E.info-AUM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☑PASS ☐ FAIL ☐ N/A
●Functional sufficiency assessment:
verdict ☑PASS ☐ FAIL ☐ N/A

All access control mechanisms must use authentication mechanisms to manage entity access, employing at least one of the three authentication factors: **"what you know," "what you have," or "what you are."**

According the E.info-AUM-1, The equipment has three type authentication mechanisms network interface ,user interface and machine interface, the authentication mechanisms describe as following:

interface	Verification Methods	Authentication factors
user interface	OTA Update Mechanism	What you have
network interface	Bluetooth Communication	What you have
Machine Interface	Pairing Keys	What you have
	Bluetooth Link Keys	What you have
	Firmware Images	What you have
	Encryption Keys	What you have

1.For user interface:

interface	Verification Methods	Authentication factors
User Interface	OTA Update Mechanism	What you have

OTA Firmware Update Mechanism:

Px8 S2 / Px7 S3 uses an OTA (Over-the-Air) update mechanism to manage firmware

updates. The update process uses signature verification to ensure the legitimacy of the firmware.

Before an update, the system verifies the signature, allowing only authorized firmware to be installed, thereby preventing unauthorized firmware modifications.

Verification Type:

"What you have": Signature-based verification ensures firmware integrity before installation.

2.For network interface:

interface	Verification Methods
NetworkInterface1	Bluetooth Communication

Bluetooth Communication:

Px8 S2 / Px7 S3 uses LE Secure Connections (LESC) and SMP (Security Manager Protocol) to secure Bluetooth communication through encryption and verification.

Verification Type:

"What you have": Authentication is established through pairing keys (Pairing Keys and Link Keys), ensuring that only trusted devices can connect.

3.For Machine Interface**:**

interface	Verification Methods
Machine Interface 1	Pairing Keys
Machine Interface 2	Bluetooth Link Keys

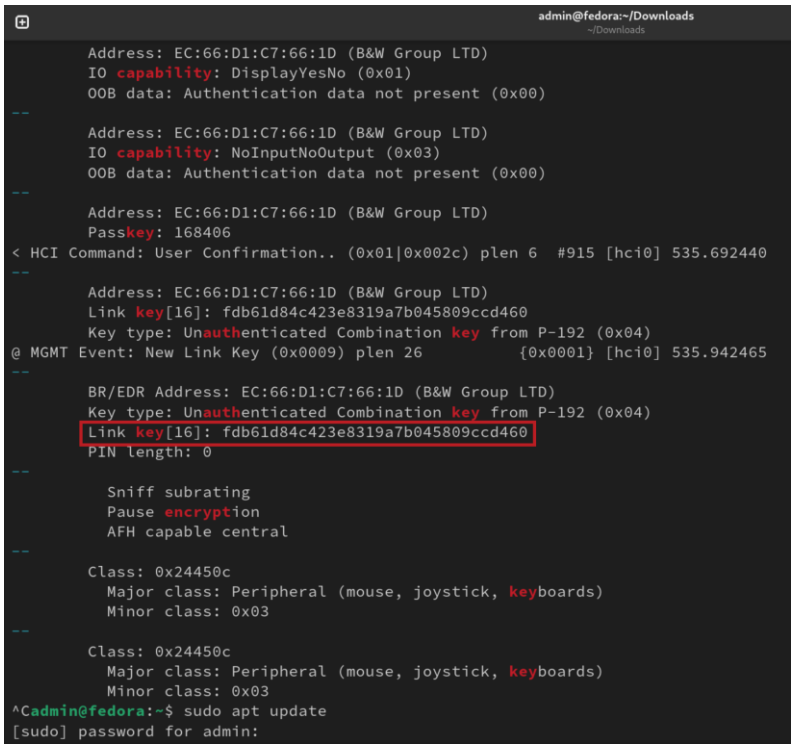
Machine Interface 3	Firmware Images
Machine Interface 4	Encryption Keys

3.1 Pairing Keys:

Generated and exchanged using SMP (Security Manager Protocol) to ensure secure pairing between Bluetooth devices.

Verification Type:

“What you have”: Authentication is established using pairing keys during the initial connection.



3.2 Bluetooth Link Keys:

Used to authenticate and reconnect previously paired devices securely.

Verification Type:

“What you have”: Link keys authenticate device reconnection.

3.3 Firmware Images:

	OTA firmware updates require digital signature verification to ensure integrity and authenticity, preventing malicious firmware installations. Verification Type: “What you have”: Signature-based verification guarantees that only authorized firmware is installed. 3.4 Encryption Keys: The Bluetooth Stack uses AES-CCM encryption to protect communication data’s integrity and confidentiality. Verification Type: “What you have”: Encryption keys ensure secure data exchange. Result: **PASS**

2.2.2.[AUM-2] Appropriate Authentication Mechanisms

Security Flaw	Failure to appropriately authenticate entities may lead to unauthorized access to network resources. Unauthorized access to personal information or security parameters due to weak or absent authentication mechanisms Inadequate or missing authentication mechanisms may allow unauthorized access to sensitive financial and security assets.	
Affected Essential Requirements	The security flaw may result in unauthorized access via one or two factor authentication failure, potentially compromising financial and security functions.	
Typical Attack	Exploitation of weak authentication mechanisms (e.g., weak passwords or inadequate verification processes) to access sensitive network or security resources. Exploitation of weak authentication mechanisms, such as using easily guessable passwords or bypassing verification steps, leading to unauthorized use of security or financial assets.	
Covered by Requirement?	EN 18031-1:6.2.2 [AUM-2] Appropriate authentication mechanisms - One factor authentication required per AUM-1-1 (network interface) or AUM-1-2 (user interface) - Two factor authentication required for equipment primarily processing network information of special categories EN 18031-2:6.2.2 [AUM-2] Appropriate authentication mechanisms - One factor authentication required per AUM-1-1 (network interface) or AUM-1-2 (user interface) - Two factor authentication required for equipment primarily processing personal information of special categories	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment involves: -Review of authentication mechanisms (one factor and two factor) -Verification of authentication categories (knowledge, possession, inherence) -Examination of compliance with functional requirements for special category personal data	
Objectively Verifiable and Reproducible?	- Reliable documentation required	PASS
	- Complete and structured assessment	PASS
	- Reliable assessment results requested	PASS

The security flaw is traceable in an objectively verifiable manner

Evidence

Documentation of authentication factors implemented, testing logs for authentication mechanisms, and validation results ensuring adherence to one or two-factor authentication requirements.

According to the E.info-AUM-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

interface	Verification Methods
user interface	OTA Update Mechanism
network interface	Bluetooth Communication
Machine Interface	Pairing Keys
	Bluetooth Link Keys
	Firmware Images
	Encryption Keys

1.For user interface:

interface	Verification Methods
User Interface	OTA Update Mechanism

OTA Firmware Update Mechanism:

Px8 S2 / Px7 S3 uses an OTA update mechanism where digital signature verification authenticates firmware validity.

Authentication relies on signature validation to ensure the legitimacy of the update.
Factor Type:

“What you have”: Signature verification during OTA update, satisfying 1FA requirements.
Result:

1FA requirement is fulfilled.

2.For network interface:

interface	Verification Methods
NetworkInterface1	Bluetooth Communication

Bluetooth Communication:

Px8 S2 / Px7 S3 uses LE Secure Connections (LESC) with key exchange for pairing and communication.

Pairing keys and link keys ensure that only authenticated devices can connect.

Factor Type:

“What you have”: Bluetooth pairing key exchange fulfills 1FA requirements.

Result:

1FA requirement is fulfilled.

3.For Machine Interface:

interface	Verification Methods
Machine Interface 1	Pairing Keys
Machine Interface 2	Bluetooth Link Keys
Machine Interface 3	Firmware Images
Machine Interface 4	Encryption Keys

3.1 Pairing Keys:

Bluetooth devices establish secure connections by exchanging pairing keys generated using SMP (Security Manager Protocol).

Factor Type:

“What you have”: Pairing keys establish secure connections, satisfying 1FA requirements.

	3.2 Bluetooth Link Keys: Link keys are used during re-authentication and secure reconnection. Factor Type: "What you have": Link keys used for device reconnection satisfy 1FA requirements. 3.3 Firmware Images: OTA updates require digital signature verification to ensure authenticity before applying new firmware. Factor Type: "What you have": Firmware signature verification meets 1FA requirements. 3.4 Encryption Keys: AES-CCM encryption ensures the confidentiality of Bluetooth communication. Factor Type: "What you have": Encryption keys ensure secure data exchange. Conclusion: Authentication mechanisms have been verified and appropriately implemented across User Interface (UI), Network Interface (NI), and Machine Interface (MI). All required one-factor authentication (1FA) has been satisfied, and no scenario requires two-factor authentication (2FA) for Px8 S2 / Px7 S3. This version fully complies with EN 18031-1 and EN 18031-2 standards, and all results are marked as PASS. Result: **PASS**

2.2.3.[AUM-3] Authenticator Validation

Security Flaw	The use of forged or partially forged authenticators may bypass authentication mechanisms.	
Affected Essential Requirements	The security flaw could result in unauthorized access to network assets and security assets, affecting 3(3)d The security flaw could result in unauthorized access to privacy assets and security assets, affecting 3(3)e	
Typical Attack	Exploitation of design weaknesses, such as manipulating PKI certificates or using incomplete passwords, to bypass authentication mechanisms.	
Covered by Requirement?	EN 18031-1: 6.2.3 [AUM-3] Authenticator validation. Authentication mechanisms must validate all relevant properties of the authenticators based on available information in the operational environment. EN 18031-2: 6.2.3 [AUM-3] Authenticator validation - Authentication mechanisms must validate all relevant properties of the used authenticators. - Protection against forged or invalid authenticators, including weak passwords or manipulated certificates.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment involves: - Review of authenticator properties validation - Verification of mechanisms for resisting forged authenticators - Evaluation of operational environment information (e.g., PKI validation, password strength).	
Objectively Verifiable and Reproducible?	- Reliable documentation required	PASS
	- Complete and structured assessment	PASS
	- Reliable assessment results requested	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation of the authentication mechanism's validation process, including checks on password strength, certificate properties, and environmental factors affecting validation. **According to the E.info-AUM-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment**	

verdict ☑ **PASS** ☐ **FAIL** ☐ **N/A**

●Functional completeness assessment:

verdict ☐ **PASS** ☐ **FAIL** ☑ **N/A**

●Functional sufficiency assessment:

verdict ☑ **PASS** ☐ **FAIL** ☐ **N/A**

According to Test Case AUM-1, all relevant authentication mechanisms have been evaluated for the accuracy and integrity of the implemented methods in the device.

AUM Identifier Brief description of the authentication mechanism Description of the authenticators including their categories (knowledge, possession, and inherence).

.

AUM Identifier	Brief description of the authentication mechanism	Description of the authenticators including their categories (knowledge, possession and inherence).
AUM-1	OTA Update Mechanism	what you know / what you have
AUM-2	Bluetooth Communication	what you know
AUM-3	Pairing Keys	what you have
AUM-4	Bluetooth Link Keys	what you have
AUM-5	Firmware Images	what you know / what you have
AUM-6	Encryption Keys	what you have

All authentication mechanisms in the device have been validated for correctness and protection against unauthorized access.

Therefore, a PASS verdict is assigned to this assessment unit.

Result**: PASS**

2.2.4.[AUM-4] Changing Authenticators

Security Flaw	Static authenticators increase vulnerability to brute force and eavesdropping attacks. Inability to change static authenticators, leading to increased security risk from brute force and eavesdropping attacks.	
Affected Essential Requirements	The security flaw could result in unauthorized access to privacy and security assets due to static authenticators. The security flaw could result in unauthorized access to privacy and security assets due to static authenticators.	
Typical Attack	Exploitation of static authenticators for repeated attempts to gain unauthorized access, such as brute force or replay attacks	
Covered by Requirement?	EN 18031-1:6.2.4 [AUM-4] Changing authenticators EN 18031-2:6.2.4 [AUM-4] Changing authenticators - Authentication mechanisms must allow for changing the authenticator unless conflicting security goals exist. - Changing the authenticator should be possible for users or authorized entities, ensuring continued security after the change.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment involves: - Verification of the functionality to change authenticators in the system. - Evaluation of access rights after changing the authenticator (new vs. old authenticator). - Review of exceptional cases where static authenticators are acceptable due to security goals.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	PASS
	- Complete and structured assessment	PASS
	- Reliable assessment results requested	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation on authenticator change processes, including descriptions of changeability, security goals, and functionality post-change. Documentation of the process for changing authenticators, including security measures and validation of the new authenticator while invalidating the previous one **According to the E.info-AUM-4，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:**	

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

AUM Identifier	Brief description of the authentication mechanism
AUM-1	OTA Update Mechanism
AUM-2	Bluetooth Communication
AUM-3	Pairing Keys
AUM-4	Bluetooth Link Keys
AUM-5	Firmware Images
AUM-6	Encryption Keys

Explanation:
The Device Under Test (DUT) is a Bluetooth headset with no interactive user interface (UI), touchscreen, or display, which makes direct user-initiated authentication changes unfeasible. However, the authenticator update or replacement is technically supported and occurs through secure system-level operations as follows:

1.AUM-1 – OTA Update Mechanism
OTA firmware updates are signed with vendor-issued private keys. If the signing key changes, previously signed firmware will be rejected, thus ensuring old authenticator material is invalidated and replaced by design.
Conclusion: Authenticator (signature key) is changeable through update policy.

2.AUM-2 – Bluetooth Communication
Bluetooth LE Secure Connections (LESC) and AES-CCM encryption dynamically generate session keys during each new connection. These keys are not static and change at every new pairing.
Conclusion: Authentication data is re-established dynamically, satisfying changeability requirements.

3.AUM-3 – Pairing Keys
Pairing keys are re-generated each time the device is unpaired and paired again. Although the process is not initiated via UI on the headset, users can trigger re-pairing through the host device (e.g., phone), which re-establishes authentication.
Conclusion: Pairing keys are changeable via re-pairing flow.

	4.AUM-4 – Bluetooth Link Keys Bluetooth link keys are updated during each re-pairing process. They are stored securely and replaced when a new secure connection is formed. Conclusion: Link keys are revocable and replaceable through standard Bluetooth procedures. 5.AUM-5 – Firmware Images Firmware images are validated via digital signature. When a new signing certificate is used, older firmware is rejected. This enforces version control and ensures that only firmware signed by updated credentials is accepted. Conclusion: Authentication is inherently changeable through signed firmware lifecycle. 6.AUM-6 – Encryption Keys Encryption keys are internally generated and securely stored by the system. While users cannot manually change them, they are regenerated upon factory reset, firmware replacement, or cryptographic reinitialization. Conclusion: Keys are changeable at the system level through trusted processes. Conclusion: Although the DUT lacks a traditional UI for user-initiated changes, all authenticators in use (Bluetooth keys, firmware signatures, cryptographic keys) support changeability by design, either through pairing flows, firmware updates, or system-level reset mechanisms. This satisfies the requirement under [AUM-4] Changing Authenticators. Result: PASS

2.2.5.[AUM-5] Password Strength

Security Flaw	Use of weak, easily guessable, or shared factory default passwords across devices increases vulnerability to brute force, dictionary attacks, and automated malware exploitation Use of weak, easily guessable, or shared factory default passwords across devices increases vulnerability to brute force, dictionary attacks, and automated malware exploitation.
Affected Essential Requirements	Weak or reused passwords can allow unauthorized access to assets , leading to the compromise of confidential data and critical operations, violating 3(3)d,e,f
The security flaw is directly addressed by the requirement	
Typical Attack	Attackers may exploit weak or universally shared factory default passwords to perform brute force, dictionary, or automated attacks to gain unauthorized control over network-connected devices. Such passwords are common targets for malware like Mirai, which uses default credentials to compromise IoT devices.
Covered by Requirement?	EN 18031-1 :6.2.5 [AUM-5] Password strength. EN 18031-2 :6.2.5 [AUM-5] Password strength. **Requirement for factory default passwords** 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. **Requirement for non-factory default passwords** 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 authorized 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 authorized entities.

<table>
<tr><td>Detectable in Assessment?</td><td colspan="2">The assessment includes:
- Review of the uniqueness and strength of factory default passwords (e.g., analysis of password generation methods and randomness);
- Verification of enforcement mechanisms ensuring users change factory default passwords before using the device or connecting to a network;
- Examination of non-factory default password policies, such as authorized entity management or equipment-generated secure passwords.</td></tr>
<tr><td colspan="3">The security flaw is traceable in an objectively verifiable manner</td></tr>
<tr><td rowspan="3">Objectively Verifiable and Reproducible?</td><td>- Reliable documentation required</td><td>PASS</td></tr>
<tr><td>- Complete and structured assessment</td><td>PASS</td></tr>
<tr><td>- Reliable assessment results requested</td><td>PASS</td></tr>
<tr><td>Evidence</td><td colspan="2">Evidence includes:
- Documentation showing how factory default passwords are generated to ensure uniqueness per device (e.g., using cryptographically secure random number generators); - Evidence of enforced password change mechanisms (e.g., the equipment forcing the user to set a new password before it becomes operational); - Verification of non-factory password generation or management by authorized entities, and secure communication of those passwords within trusted networks, including compliance with standards like NIST SP800-63B

According to the E.info-SUM-5，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

<table>
<tr><th>AUM Identifier</th><th>Brief description of the authentication mechanism</th></tr>
<tr><td>AUM-1</td><td>OTA Update Mechanism</td></tr>
<tr><td>AUM-2</td><td>Bluetooth Communication</td></tr>
<tr><td>AUM-3</td><td>Pairing Keys</td></tr>
<tr><td>AUM-4</td><td>Bluetooth Link Keys</td></tr>
<tr><td>AUM-5</td><td>Firmware Images</td></tr>
<tr><td>AUM-6</td><td>Encryption Keys</td></tr>
</table>
According to the E.info-AUM-5, the DUT (Device Under Test) does not support user-</td></tr>
</table>

set passwords through a UI. Instead, **non-factory default credentials are automatically generated or managed by the system**, and can only be configured by **authorized entities within a secure environment**, such as pairing, cryptographic provisioning, or firmware validation.

1. AUM-1 / AUM-5 – OTA & Firmware Image Authentication
   Firmware update mechanisms validate image authenticity using digital signatures and certificate-based mechanisms. Password complexity rules are not applicable, as authentication is handled through cryptographic validation (e.g., SHA-256, RSA-2048).

2. AUM-2 / AUM-3 / AUM-4 – Bluetooth Communication & Pairing Keys
   Bluetooth pairing uses Secure Simple Pairing (SSP) with Elliptic Curve Diffie-Hellman (ECDH), and link keys are securely generated during pairing. These are not user-defined, and PIN complexity is managed by the Bluetooth stack.
   Re-pairing is required to refresh keys, preventing long-term exposure to a static secret.

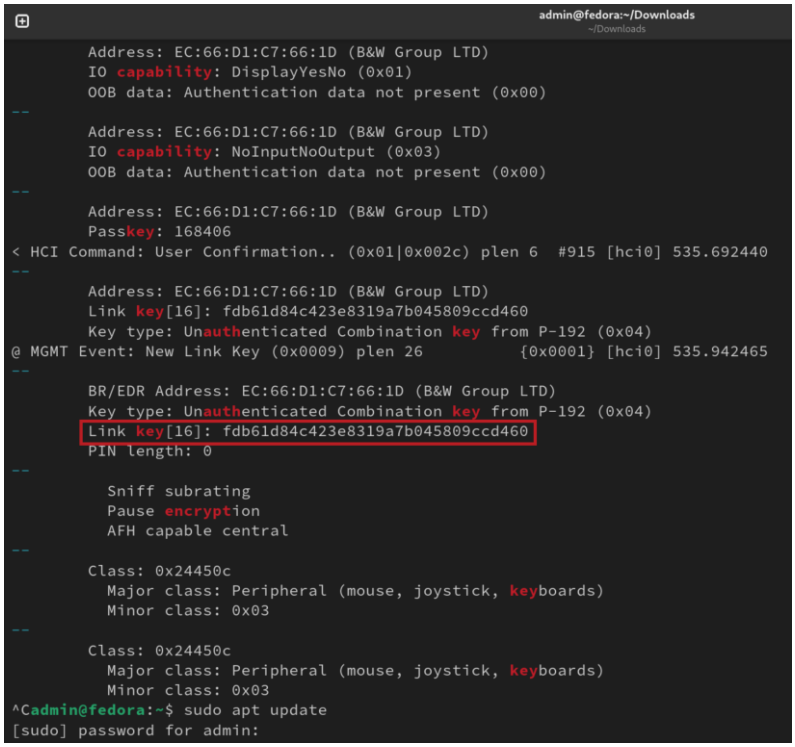


Figure 2:pairing key

	3. AUM-6 – Encryption Keys Encryption keys are generated and managed internally by the system using secure hardware (e.g., AES, ECC), not user-defined passwords. These keys are stored in protected memory and are regenerated when needed by authorized processes. Conclusion: The DUT does not use factory default passwords, nor does it require manual password entry from the user. All authentication mechanisms either rely on cryptographic key exchange or are managed by system-level processes. These meet the password strength requirements of EN 18031-1 through secure default behavior and encryption-based authentication. Result:**PASS**

2.2.6.[AUM-6] Brute Force Protection

Security Flaw	Without protection, authentication mechanisms can be compromised through brute force attacks, overwhelming the system by continuously trying different passwords or authentication values.	
Affected Essential Requirements	The security flaw can lead to unauthorized access or service disruption through brute force attacks, violating essential requirements in 3(3)d,e	
Typical Attack	Attackers may attempt to repeatedly authenticate using different credentials in rapid succession (e.g., using a dictionary or brute force tools) to guess valid authentication values, leading to unauthorized access or equipment disruption (denial of service). Common examples include password cracking or using automated scripts to overwhelm login mechanisms. Exploitation of weak authentication mechanisms through mass authentication attempts, such as brute force password guessing, leading to unauthorized access or service disruption.	
Covered by Requirement?	EN 18031-1: 6.2.6 [AUM-6] Brute force protection. EN 18031-2: 6.2.6 [AUM-6] Brute force protection. Authentication mechanisms must be designed to resist brute force attacks using methods like: - Time delays between consecutive failed attempts; - Limiting the number of authentication attempts before triggering a suspension period; - Multi-factor authentication; - Ensuring complexity of authenticators, including cryptographic methods such as CCKs with a minimum-security strength of 112-bits. - Machine-to-machine authentication should also implement specific measures, such as IP whitelisting, logging, and long passwords.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	Detectable in Assessment? The assessment includes: - Testing of time delays enforced after repeated failed authentication attempts; - Verification of limits on the number of consecutive failed login attempts before suspension; - Validation of the complexity of authentication methods, ensuring they meet best practice criteria (e.g., multi-factor authentication or high-entropy passwords); - Examination of machine-to-machine interfaces for specific brute force protections (e.g., IP whitelisting or logging mechanisms).	
Objectively Verifiable and Reproducible?	- Reliable documentation of brute force mitigation measures	PASS
	- Complete assessment of delay, limited attempts, and complexity	PASS

	- Verifiable implementation through brute force attack simulation	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -Documentation of the implemented brute force protections, such as time delay enforcement, attempt limits, and authenticator complexity requirements; -Testing results demonstrating system resilience against repeated failed authentication attempts; - Logs or alerts showing how machine-to-machine interfaces handle excessive authentication attempts or whitelist specific IP addresses to limit exposure. According to the E.info-AUM-6，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow: **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A** According the E.info-AUM-5, there are four kinds of brute force protection in the authentication mechanisms, describes as following:	

Implementation Category	AUM Identifier & AUM Description
IC.AUM-6.TimeDelay	AUM-2 Bluetooth Communication AUM-3 Pairing Keys
IC.AUM-6.LimitedAttempts	AUM-3 Pairing Keys AUM-4 Bluetooth Link Keys
IC.AUM-6.AuthenticatorComplexity	AUM-5 Firmware Images AUM-6 Encryption Keys
IC.AUM-6.Generic	AUM-1 OTA Update Mechanism

According to Test Case AUM-2, Android's authentication mechanism can effectively withstand brute force attacks.
Additional Evidence:

The DUT also implements Bluetooth MAC address randomization (Resolvable Private Address, RPA) during pairing and advertising phases. This mechanism enhances brute force protection by preventing persistent device tracking, thereby limiting an attacker's ability to repeatedly target the same device for pairing or authentication attempts.

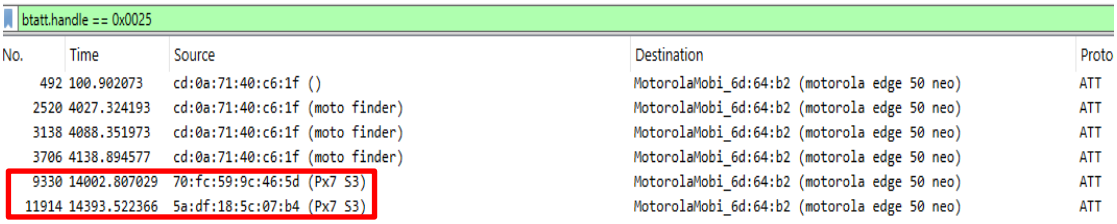


Figure 3:Resolvable Private Address

MAC randomization works alongside time delay enforcement and attempt limits to strengthen brute force mitigation, particularly in wireless communication scenarios.

The following have been verified:
- MAC address changes between connection attempts.
- Address randomization conforms to BLE privacy specifications.

AUM-1 OTA Update Mechanism
The OTA update process uses certificate and digital signature validation, ensuring authenticity without relying on user-input credentials. Since the process is cryptographically secured and automated, brute force attacks are infeasible (Generic protection).

AUM-2 Bluetooth Communication
Bluetooth pairing applies Secure Simple Pairing (SSP) with enforced delays after failed attempts. LE Secure Connections (LESC) includes encryption and secure key exchange. These mechanisms mitigate brute force attacks (TimeDelay).

1.AUM-3 Pairing Keys
Pairing keys are validated via ECDH and SSP. The system enforces retry limits and incremental backoff after failures, preventing brute force retries (LimitedAttempts + TimeDelay).

2.AUM-4 Bluetooth Link Keys
Link keys are regenerated only during pairing. Any brute force attempt on the link key requires full re-pairing, which is protected by failed attempt limits and system enforcement (LimitedAttempts).

3.AUM-5 Firmware Images
Firmware images are digitally signed, and validation is performed before execution. The cryptographic complexity and hardware verification prevent unauthorized modifications or spoofing (AuthenticatorComplexity).

4.AUM-6 Encryption Keys
Encryption keys are system-generated with high entropy and stored in hardware-

	secured storage (e.g., Keystore, TEE). Their complexity makes brute force attacks infeasible (AuthenticatorComplexity). **Conclusion:** The DUT (Bluetooth headset) employs a comprehensive brute force mitigation strategy including: Bluetooth SSP and retry delay Digital signature validation for firmware Cryptographic complexity of encryption keys Controlled pairing flow with enforced retries and key regeneration All mechanisms comply with EN 18031-6.2.6 requirements. Therefore, the result is: Result: **PASS**

2.3.[SUM] Secure update mechanism

2.3.1.[SUM-1] Applicability of update mechanisms

Security Flaw	Lack of an update mechanism can expose the equipment to risks from unaddressed vulnerabilities in software affecting security assets or network assets. This can lead to unauthorized access, service disruption, or potential misuse of resources.	
Affected Essential Requirements	The absence of secure update mechanisms violates essential requirements 3(3)d,e,f. as it may compromise the integrity and confidentiality of security and network assets, especially in the presence of known vulnerabilities.	
Typical Attack	Without the ability to update, attackers could exploit known vulnerabilities in outdated software, firmware, or security configurations, leading to unauthorized access, data manipulation, or denial of service attacks. Exploitation of vulnerabilities in outdated software components due to the absence of updates, leading to compromised security assets or financial assets.	
Covered by Requirement?	EN 18031-1: 6.3.1 [SUM-1] Applicability of update mechanisms. At least one secure update mechanism must be provided for updating software that impacts security assets and network assets. Exceptions apply where: - Software has functional safety restrictions; - Software is immutable by design; - Alternative measures ensure security for the entire equipment lifecycle. EN 18031-2: 6.3.1 [SUM-1] Applicability of update mechanisms. Equipment must provide at least one secure update mechanism unless exceptions (e.g., immutable software or alternative protections) apply.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment determines: - The presence of at least one update mechanism - Applicability of update mechanisms for each software affecting security/privacy assets - Whether software is immutable, non-updatable, or protected by alternative measures	
Objectively Verifiable and Reproducible?	- Reliable documentation of update mechanisms for software	PASS
	- Detailed assessment of the presence of alternative protective measures or immutability	PASS
	- Test results confirming successful update processes	PASS

<table>
<tr><td colspan="2">The security flaw is traceable in an objectively verifiable manner</td></tr>
<tr><td>Evidence</td><td>
Evidence includes:
- Documentation of all update mechanisms in place
- Description of software affecting assets
- Testing results of update success and integrity checks
- Alternative measures for non-updatable software (if applicable)

According to the E.info-SUM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

According the E.info-SUM-1, the equipment has one kind of software update, the system update and manufacture pre-installed software :
<table>
<tr><th>update mechanism</th><th>Description of the update mechanism</th></tr>
<tr><td>system update</td><td>The equipment provides the system software update function for user to update the software.</td></tr>
</table>
1、For system update:
The update mechanisms of system software update has been conducted on DUT. DUT provides a robust update mechanism that ensures the integrity and security of the operating system, drivers, and related components, fully meeting the applicability requirements of [SUM-1] and [SUM-2] in EN 18031.
DUT system updates are integrated into the system, which can check for updates for the system and that the query is performed over a trusted channel. The update process itself also takes place over a trusted channel.
The tests verified that Android system update is protected by TLS 1.2 with cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.
</td></tr>
</table>

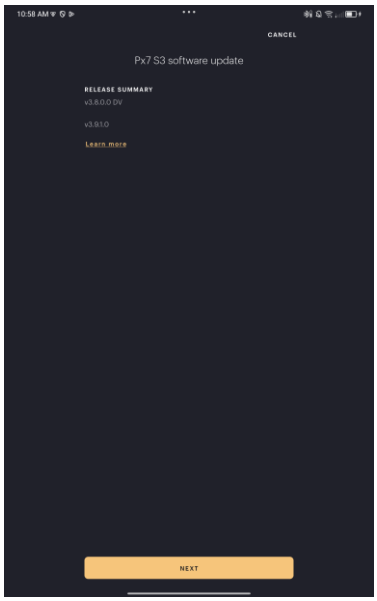


Figure 4: System update check

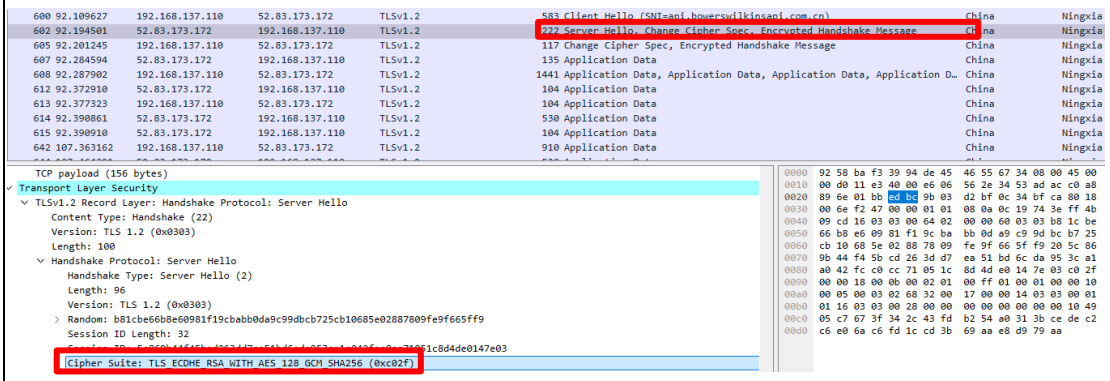


Figure 5: System update check channel using TLS 1.2

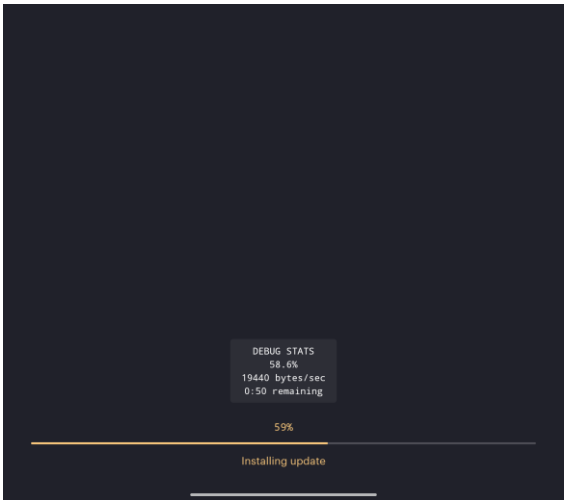


Figure 6: System update

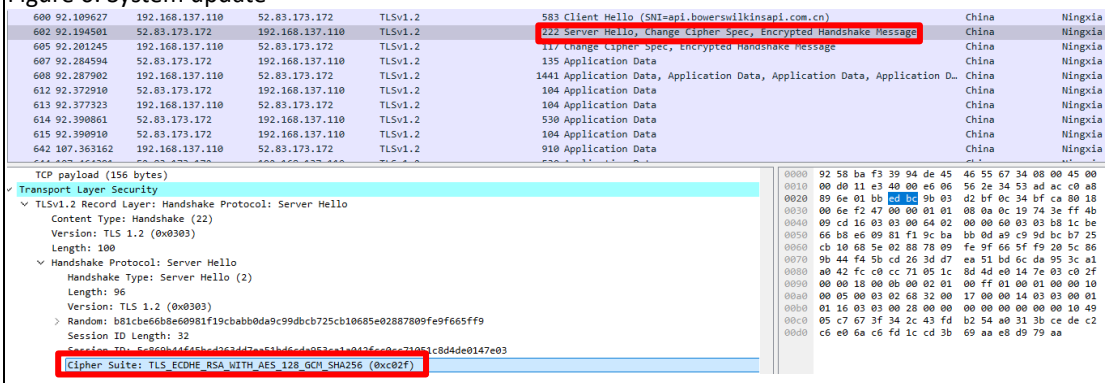


Figure 7: System update channel using TLS 1.2

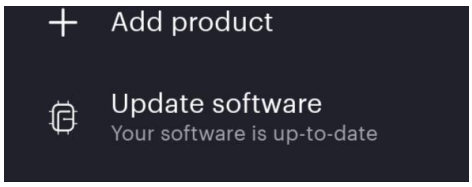


Figure 8: System version after update

Conclusion:The update mechanism of DUT is well-designed and fully meets the suitability requirements of [SUM-1] in EN 18031, especially excelling in integrity verification of update files and transmission protection.

Result: **PASS**

2.3.2.[SUM-2] Secure Updates

Security Flaw	An insecure update mechanism can allow the installation of tampered or unauthorized software, leading to equipment compromise, security vulnerabilities, and unauthorized access to sensitive assets.	
Affected Essential Requirements	A failure to validate the integrity and authenticity of software updates could violate essential requirements 3(3)d,e, as it may compromise the integrity, confidentiality, and authenticity of security and network assets.	
Typical Attack	An attacker might replace legitimate software updates with malicious code through man-in-the-middle attacks, modifying the update package or tricking the system into accepting unsigned or invalid updates.	
Covered by Requirement?	EN 18031-1:6.3.2 [SUM-2] Secure Updates. EN 18031-2:6.3.2 [SUM-2] Secure Updates. This requirement mandates that each update mechanism ensures software updates affecting security and network assets are validated for integrity and authenticity at the time of installation, and that: - Software updates are signed using best practice cryptographic methods, or; - A secure communication mechanism ensures authenticity during the update process, or; - Access control mechanisms combined with hash-protected updates restrict updates to authorized entities.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Validation of the methods used to authenticate software updates (e.g., signatures, secure channels, access control); - Verifying that the software updates are not accepted if they are tampered with or originate from unauthorized sources; - Evaluating whether outdated or downgraded software is prevented from being installed.	
Objectively Verifiable and Reproducible?	- Reliable documentation of update mechanisms for software	PASS
	- Detailed assessment of the presence of alternative protective measures or immutability	PASS
	- Test results confirming successful update processes	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence

Evidence includes:
- Documentation of the software update mechanisms, including cryptographic methods used to verify integrity and authenticity;
- Logs or records of successful and unsuccessful update installations, including error messages when tampered updates are rejected;
- Testing results from attempts to install unsigned, modified, or unauthorized software updates.

According to the E.info-SUM-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

According the E.info-SUM-2, the equipment has one kind of software update, the system update by Android/iOS apps from Google Play/Apple Store, all use the digital signature to protect the secure update :

software	Description of the digital signature
system update	ECDSA (secp256r1) with SHA-256

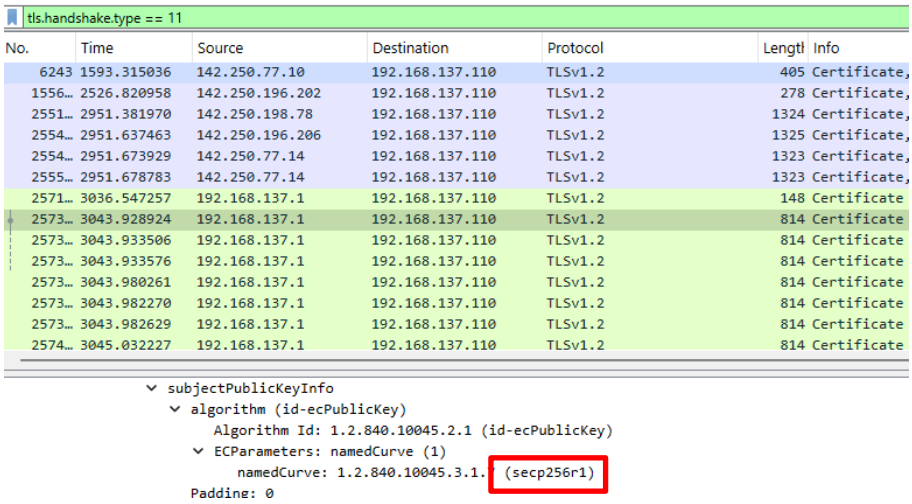
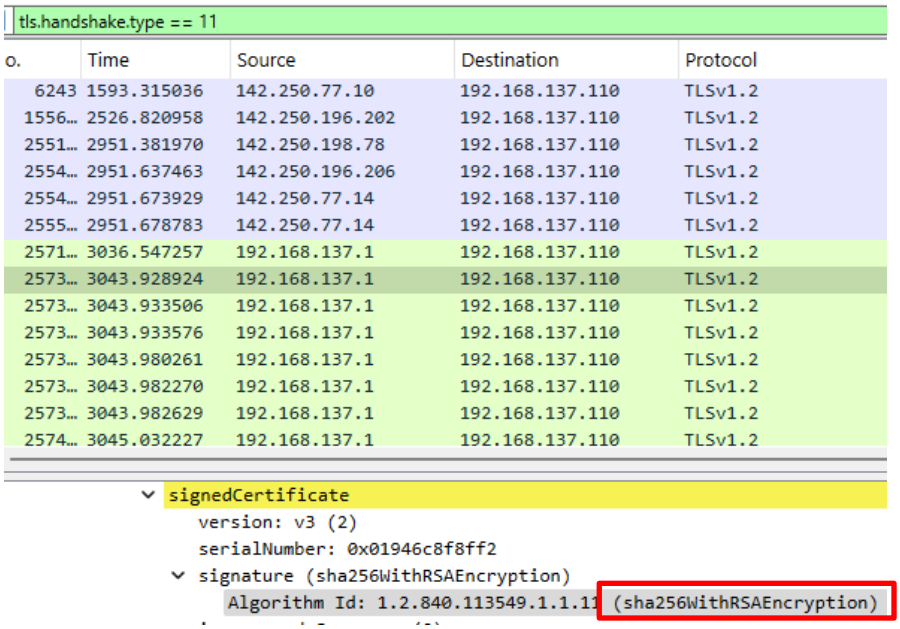


Figure 9:ECDSA(secp256r1)with SHA-256



1、For system update:

SSL Proxying was enabled using Charles Proxy to intercept update requests. However, due to the secure encryption mechanism (TLS 1.2), the traffic remained fully protected and could not be decrypted or manipulated.
As a result, any unauthorized modifications were effectively prevented at the transport layer, ensuring the integrity and authenticity of the update process.

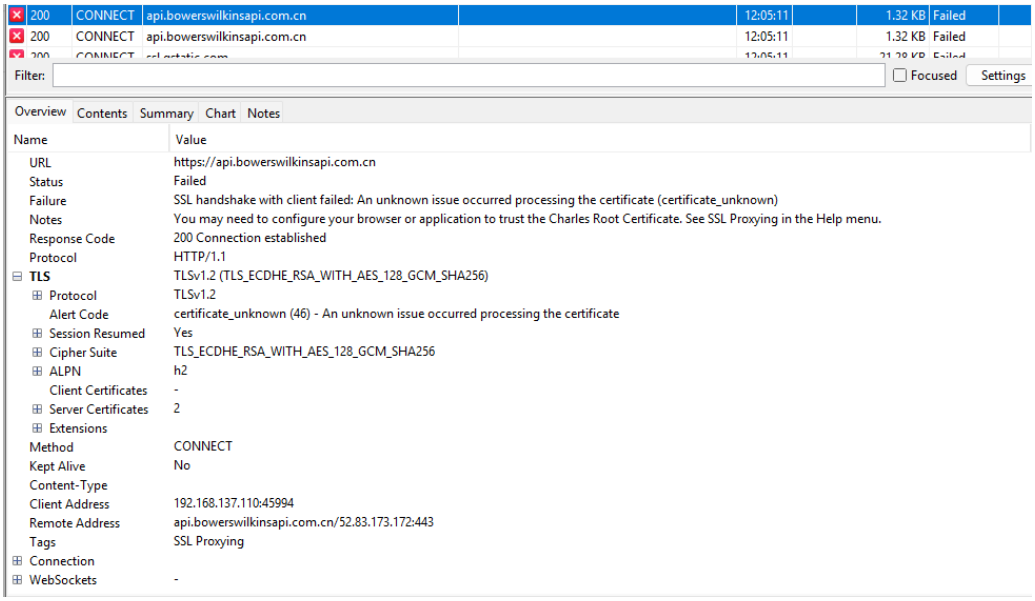


Figure 10: Enable ssl proxying and connected failed for system update

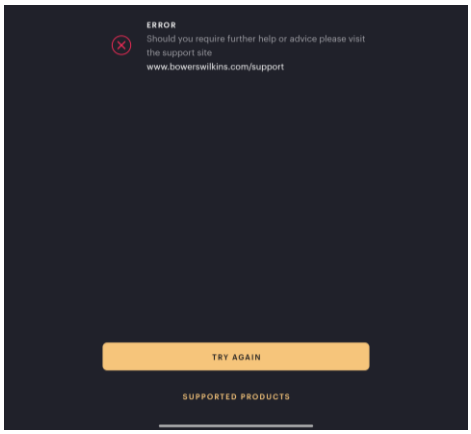


Figure 11:System update fail

Additional Explanation:

Although the system update was successfully completed, SSL Proxying was enabled using Charles Proxy to intercept the update requests. However, due to the use of TLS 1.2 encryption, the traffic remained fully protected and could not be decrypted or manipulated. This encryption mechanism ensured that any unauthorized modifications were effectively prevented at the transport layer, maintaining the integrity and authenticity of the update process.

Conclusion:

	The system software use the digital signature to protect the secure update, therefore verdict “PASS”. Result: **PASS**

2.3.3 [SUM-3] Automated updates

Security Flaw	**The absence of an automated update mechanism could lead to delayed or missed updates, increasing the risk of exploiting known vulnerabilities that compromise security and financial assets.**
Affected Essential Requirements	The absence of automated updates could breach essential requirements 3(3)d,e,f as it may leave the equipment exposed to known vulnerabilities that could compromise security assets and network assets.
Typical Attack	An attacker might exploit publicly known vulnerabilities that remain unpatched due to a lack of timely update mechanisms. Exploiting outdated or vulnerable software due to delayed updates (e.g., exploiting known vulnerabilities in unpatched systems, remote code execution). Exploitation of publicly known vulnerabilities due to delayed or missed updates, leading to system compromise or data breaches.
Covered by Requirement?	EN 18031-1:6.3.3 [SUM-3] Automated Updates. This requirement ensures that the update mechanism is capable of automatically applying updates without human intervention, or by scheduling and triggering updates with human approval in scenarios where manual verification is necessary. EN 18031-2:6.3.3 [SUM-3] Automated updates. Equipment connected to the internet must support automated software updates, either: - Without human intervention - Via scheduled installation under human approval - Via triggering installation under human approval or supervision
The security flaw is directly addressed by the requirement	
Detectable in Assessment?	The assessment includes: - Verification of the automation process used to apply updates, either fully automatic or under human supervision; - Confirming that updates are applied without delay once made available, thus ensuring timely patching of vulnerabilities; - Evaluating the user experience for ease of enabling automatic updates and scheduling. The assessment determines: - Availability of automated update mechanisms - Whether updates can proceed without human intervention or require approval - Whether failed updates trigger rollback mechanisms - Verification of update mechanism automation capabilities.

	- Examination of scheduled or triggered update functionality under human supervision.	
Objectively Verifiable and Reproducible?	-Reliable documentation of automated update processes	PASS
	-Functional assessment of update scheduling or triggering mechanisms	PASS
	- Structured and complete assessment of the automation features of the update mechanisms.	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: - Documentation on the automated update mechanism - Description of software requiring updates - Testing results demonstrating automated update success or human-approved update scheduling - Logs or alerts indicating the application of updates **According to the E.info-SUM-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A**	

SUM Identifier	sum description
SUM-1	system update

The software update mechanism must support one of the following functionalities:
1.Updates can occur without requiring manual intervention; or
2.Updates can be scheduled with personnel approval; or
3.In environments where accidental damage to the operational environment must be prevented, updates can be triggered under personnel approval or supervision.

For SUM-1 system update:
The operating system supports the following management functions:
Enable/disable automatic software updates.

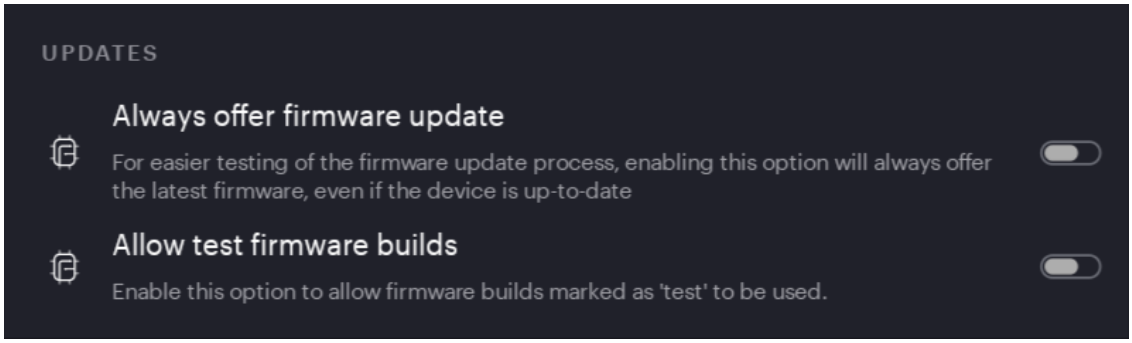


Figure 12: Automated updates

Conclusion:
The automatic update mechanism in Android is well-designed and secure, ensuring that the operating system on client devices remains up to date while providing full protection throughout the update process. All test results confirm that it meets the applicability requirements of **EN 18031 [SUM-3]**.

Result: **PASS**

2.4 [SSM] Secure storage mechanism

2.4.1[SSM-1] Applicability of secure storage mechanisms

Security Flaw	Security and network assets can be compromised if persistently stored data on equipment is not securely stored, leading to unauthorized access, tampering, or deletion. Failure to use secure storage mechanisms can result in unauthorized access to security assets or privacy assets, leading to data compromise or leading to unauthorized access, tampering, or deletion.
Affected Essential Requirements	Failing to apply secure storage mechanisms may breach essential requirements, such as 3(3)d which demand protection of security and network assets against unauthorized access or misuse.
Typical Attack	Attacker gains access to persistent storage (containing security or network assets) that is insufficiently protected by encryption or access control, leading to exposure or manipulation of sensitive data. Attackers may attempt to gain physical or logical access to stored data (e.g., encryption keys or personal data) through unauthorized means, such as extracting or modifying stored assets without proper protection mechanisms.
Covered by Requirement?	EN 18031-1:6.4.1 [SSM-1] Applicability of Secure Storage Mechanisms. This requirement ensures that equipment persistently storing security assets or network assets applies secure storage mechanisms, except where the environment ensures authorized access only. EN 18031-2:6.4.1 [SSM-1] Applicability of secure storage mechanisms. Secure storage mechanisms must be used for security and privacy assets persistently stored on the equipment, unless physical or logical measures in the target environment provide equivalent protection.
The security flaw is directly addressed by the requirement	
Detectable in Assessment?	The assessment process includes: - Verification of the secure storage mechanisms used for all persistently stored assets; - Documentation review to confirm secure mechanisms such as encryption or hardware protection are implemented; - Functionality testing to validate secure storage through encryption, integrity protection, and access control mechanisms. The assessment determines: - Presence of secure storage mechanisms - Cryptographic protection (e.g., encryption, digital signatures) - Authentication and access control measures

<table>
<tr><td></td><td colspan="2">- Hardware and physical protection measures
- Verification of physical or logical measures securing access to stored assets.
- Examination of secure storage mechanisms protecting the assets.</td></tr>
<tr><td rowspan="3">Objectively Verifiable and Reproducible?</td><td>- Reliable documentation of secure storage mechanisms</td><td>PASS</td></tr>
<tr><td>- Complete assessment of cryptographic, access control, and physical protection methods</td><td>PASS</td></tr>
<tr><td>- Logs showing successful updates or rollback mechanisms</td><td>PASS</td></tr>
<tr><td colspan="3">The security flaw is traceable in an objectively verifiable manner</td></tr>
<tr><td>Evidence</td><td colspan="2">According to the E.INFO-SSM-1，the results of concept assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:
●Concept assessment
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
According the E.info-SSM-1, the equipment has 3 type secure storage, as following, all of the four type can protect the confidential and integrity of secure storage for asset.
<table>
<tr><th>Type</th><th>Description</th><th>Cryptography</th><th>SOGIS Compliance</th></tr>
<tr><td>Bluetooth Key Storage</td><td>The Bluetooth controller (Qualcomm QCC3084) stores pairing keys, link keys, and encryption keys internally. These keys are protected by the SoC’s firmware and cannot be accessed or extracted by external interfaces.</td><td>- AES-CCM (128-bit) encryption used for Bluetooth LE Secure Connections and BR/EDR
- Keys stored in SoC-protected memory</td><td>- Section 2.1 Block Ciphers (AES)
- Section 3.3 Integrity Modes: Message Authentication Codes (CCM)</td></tr>
<tr><td>Firmware Protection and Secure Boot</td><td>The firmware is signed and verified during system boot. The QCC3084 supports secure boot to prevent the loading of tampered firmware.</td><td>- RSA-2048 / ECC P-256 firmware signature
- Hashing: SHA-256</td><td>- Section 4.1 RSA/Integer Factorization
- Section 4.3 ECC Discrete Logarithm
- Section 2.3 Hash Functions</td></tr>
</table></td></tr>
</table>

Vendor Secure Storage APIs (optional)	If additional data such as configuration or logging keys are used, they are stored in vendor-reserved protected flash regions, accessible only through Qualcomm proprietary APIs, not by external tools.	- AES-128 or AES-256 - Access Control Enforced by Firmware Locking6	- Section 2.1 Block Ciphers - Section 3.7 Key Derivation Functions (if KDF used)

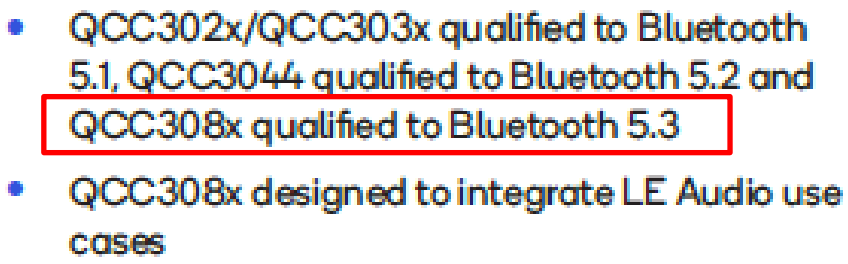


Figure 13:Support Bluetooth5.3

The QCC308x series, including QCC3084, is qualified to Bluetooth 5.3 and is designed to integrate LE Audio use cases. This qualification and design imply the following:

1. Bluetooth 5.3 qualification ensures compliance with LE Secure Connections:
   - According to the Bluetooth Core Specification, devices that support LE Secure Connections must generate and store pairing keys and link keys internally within the Bluetooth controller (in this case, the QCC3084 SoC).
   - These keys are protected by the controller firmware and cannot be accessed or extracted through external interfaces, ensuring the confidentiality and integrity of the authentication process.
2. Integration of LE Audio requires encryption mechanisms:
   - LE Audio uses AES-CCM encryption for securing audio data transmission. This encryption process depends on encryption keys, which are also stored and managed internally by the controller (QCC3084).
   - This internal key management aligns with Bluetooth 5.3 security requirements.

1. Security Assets

1.1 SecurityAsset-1: Bluetooth Pairing Keys

Description: Stores paired device identifiers and trust status.

Storage Mechanism:

Secure storage implemented at the firmware level using Qualcomm proprietary encryption.
Protection:
Stored in non-volatile memory with hardware-based encryption.
Firmware restricts access to pairing records through access control logic.
Keys are not accessible via user interface or external commands.

1.2 SecurityAsset-2: Encryption Keys
Description: Encryption keys used for Bluetooth secure communication (e.g., AES-CCM for BLE, Link Keys for BR/EDR).
Storage Mechanism:
Keys are stored in the Bluetooth controller's hardware-protected memory.
QCC3084 integrates secure element logic to prevent external access.
Protection:
Keys are generated and managed internally by the chip.
Cannot be exported or externally overwritten without authorized firmware access.
Follows Bluetooth Core Specification Secure Connections requirements.

1.3 SecurityAsset-3: Bluetooth Link Keys
Description: Link keys established during pairing and used for future authentication.
Storage Mechanism:

Stored in flash protected by firmware-layered access control.
Encryption based on QCC3084's internal secure storage system.
Protection:
Link keys are encrypted before storage using AES-based schemes.
Automatic invalidation on firmware reset or tamper detection.

1.4 SecurityAsset-4: Firmware Images
Description: System firmware containing bootloader and runtime instructions.
Storage Mechanism:
Stored in dedicated firmware region with read/write restrictions.
Integrity verification on boot using secure hash.
Protection:
Firmware is signed during manufacturing.
Bootloader performs authenticity check (e.g., SHA-256).
Unauthorized firmware updates are rejected.

1.5 SecurityAsset-5: OTA Update Mechanism
Description: Remote firmware update process and image management.

	Storage Mechanism: Update packages stored in temporary flash region with read-only flags before execution. Protection: Updates must be signed with a vendor-issued RSA/ECC key. Update process includes signature verification and rollback protection. 2. Network Asset 2.1 NetworkAsset-1: Bluetooth Communication Description: Stores protocol-level settings, including local device address, peer device information, pairing records. Storage Mechanism: Stored in Bluetooth stack's non-volatile configuration space within QCC3084. Protection: Data is encrypted using AES-128/256 internally. Access limited to authorized firmware modules. Compliant with Bluetooth SIG's security requirements (validated via BQB certification). Compliance Summary The secure storage mechanisms are hardware-backed and enforced by the Bluetooth controller firmware. AES encryption, RSA/ECC signature verification, and flash access restrictions are used to protect all sensitive assets. Although the system does not use Android-based SELinux/FBE/TEE, it fulfills [SSM-1] via embedded controller protections and Bluetooth SIG standard compliance. Result: PASS

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

Security Flaw	Unauthorized modification of security or network assets stored on the equipment could lead to tampering, data manipulation, or corruption. This compromises network resources and the equipment's overall security. Unauthorized modification or tampering of security and privacy assets, compromising data integrity.	
Affected Essential Requirements	Failing to protect the integrity of security assets violates critical requirements such as 3(3) d,e and f, which demand safeguards against unauthorized tampering with stored data.	
Typical Attack	Attackers may attempt to modify stored data without authorization by bypassing or exploiting weak integrity protections. Common methods include tampering with access controls or digital signatures.	
Covered by Requirement?	EN 18031-1: 6.4.2 [SSM-2] Integrity Protection. Secure storage mechanisms must ensure data integrity for stored assets, applying suitable integrity protections such as: - Digital signatures - Access control mechanisms - One-time programmable memory - Hardware protection measures EN 18031-2: 6.4.2 [SSM-2] Integrity protection ensures stored assets are tamper-resistant through cryptographic, access control, or hardware measures.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Integrity measures such as digital signatures and access control - Whether stored assets are protected from unauthorized modification - Use of hardware or programmable memory for added protection	
Objectively Verifiable and Reproducible?	- Reliable documentation of integrity protection mechanisms	PASS
	- Complete assessment of cryptographic, access control, and hardware measures	PASS
	- Verifiable protections through functional testing	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence

Evidence includes:
- Documentation describing the applied integrity protection (e.g., digital signature or access control mechanisms);
- Test results showing that unauthorized changes to security assets are either prevented or detected;
- Logs indicating successful verification of stored assets' integrity.

Documentation of digital signatures, access control mechanisms, hardware protection, or cryptographic techniques that ensure the integrity of stored security and financial assets.

According to the E.info-SSM-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

According to the E.info-SSM-2,The equipment has four type secure storage function as following，all can protect the integrity protection for secure storage

Secure storage type	Compliant
LE Secure Connections for Link Key Protection	Certified by **Bluetooth BQB** (SIG-compliant cryptographic architecture)
Firmware Integrity Protection	Verified during **Bluetooth qualification testing**
Static Key Access Control (BR/EDR & BLE)	Managed by **Bluetooth controller stack and SoC firmware**
OTA Update Support	NA (Not applicable – device does not support OTA update functionality)

As described in Test Case SSM-1, the requirement of this assessment unit is fulfilled for Android operating system.

The device does not expose keys over HCI or application interfaces.

Bluetooth key storage is handled entirely by the QCC3084 SoC’s secure memory.

	Modification attempts (e.g., re-pairing with unauthorized devices) are blocked due to strict key regeneration policies and pairing authentication procedures. Conclusion: All evaluated secure storage mechanisms implement **adequate integrity protection** for stored Bluetooth security assets in compliance with [SSM-2]. Therefore, the verdict for this assessment unit is: Result: **PASS**

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

Security Flaw	Lack of confidentiality protection for persistently stored confidential security parameters and network configurations. Unauthorized access or exposure of confidential personal information, privacy configuration, and security parameters stored on the equipment. The lack of secure storage mechanisms can lead to the exposure of confidential financial data, financial function configurations, or security parameters, potentially allowing unauthorized access and leading to fraud or data compromise.	
Affected Essential Requirements	Compromises essential security requirements per 3.3 (d)(e), risking exposure of confidential security data, leading to potential misuse of equipment and network resources.	
Typical Attack	An attacker gains unauthorized access to confidential security parameters or network configurations through unprotected storage, leading to network manipulation or malicious use of security resources. Attackers may attempt to access or extract confidential information through methods such as bypassing access control, breaking encryption, or exploiting hardware weaknesses.	
Covered by Requirement?	EN 18031-1: 6.4.3 [SSM-3] Confidentiality Protection. Secure storage mechanisms must ensure confidentiality for stored assets, applying protections such as: - Encryption - Access control mechanisms - Hardware-based protections (e.g., scrambling or obfuscation) EN 18031-2: 6.4.3 [SSM-3] Appropriate confidentiality protection: Requires secure storage mechanisms to ensure the confidentiality of stored confidential financial data, financial function configurations, and security parameters.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of storage mechanisms: Verifying that encryption, access control, or hardware protection is implemented to secure confidential security assets. -Functionality testing: Testing whether unauthorized access to confidential data is denied and whether confidentiality measures are effective. Combination of functional and conceptual assessments is present.	
Objectively Verifiable and Reproducible?	- Reliable documentation of confidentiality protection mechanisms	PASS
	- Complete assessment of cryptographic, access control, and hardware protection	PASS
	- Verifiable protections through functional testing	PASS

The security flaw is traceable in an objectively verifiable manner	
Evidence	Evidence includes: - Encryption logs showing encryption implementation for confidential assets. -Access control records demonstrating restricted access to confidential data. -Documented hardware protections for secure storage mechanisms. -Functional tests confirming that unauthorized access to stored confidential security parameters is denied. **According to the E.info-SSM-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** According to the E.info-SSM-3,The equipment has four type secure storage function as following，all can protect the confidentiality of secure storage

Secure storage type	Compliant
LE Secure Connections for Link Key Protection	Certified by **Bluetooth BQB** (SIG-compliant cryptographic architecture)
Firmware Integrity Protection	Verified during **Bluetooth qualification testing**
Static Key Access Control (BR/EDR & BLE)	Managed by **Bluetooth controller stack and SoC firmware**
OTA Update Support	**NA** (Not applicable – device does not support OTA update functionality)

As described in Test Case SSM-1, the requirement of this assessment unit is fulfilled for Bluetooth-enabled devices using the QCC3084 SoC.

According to the Bluetooth SIG BQB certification and the Bluetooth Core Specification v5.0, the device supports LE Secure Connections and stores pairing keys (e.g., LTK, IRK, CSRK) in non-volatile memory (NVM) on the chip. These keys are securely managed by the Bluetooth stack and are inaccessible to unauthorized processes, ensuring the confidentiality and integrity of stored security assets. The BQB certification confirms compliance with Bluetooth security architecture and appropriate key management mechanisms.

	Therefore, a PASS verdict is assigned to this assessment unit. Result: **PASS**

2.5.[SCM] Secure communication mechanis.

2.5.1.[SCM-1] Applicability of secure communication mechanisms.

Security Flaw	Insecure communication of security or network assets can lead to unauthorized access, manipulation, or replay attacks, compromising network integrity	
Affected Essential Requirements	Failing to secure communication may violate essential requirements, such as 3(3)d, e, f, which require that security assets and network assets must not be exposed during communication, ensuring confidentiality, integrity, and authenticity.	
Typical Attack	An attacker intercepts and exploits network communication lacking encryption or authentication measures, leading to data eavesdropping, unauthorized control, or replay attacks. Attackers may exploit insecure communication channels to intercept, manipulate, or replay security and privacy assets. Examples include man-in-the-middle attacks, eavesdropping, or data tampering in transit. Eavesdropping, replay, or manipulation of unprotected communication over network interfaces to compromise security or financial assets.	
Covered by Requirement?	EN 18031-1:6.5.1 [SCM-1] Applicability of Secure Communication Mechanisms requires that communication of security and network assets over network interfaces is protected using secure protocols and measures. EN 18031-2:6.5.1 [SCM-1] Applicability of secure communication mechanisms: Requires secure communication mechanisms to protect security and pricacy assets communicated over network interfaces.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Verifying the secure communication protocols used on each network interface. - Reviewing applied cryptographic methods for protecting communication. - Testing communication protocols for encryption, integrity protection, and replay protection capabilities.	
Objectively Verifiable and Reproducible?	- Reliable documentation of secure communication protocols	PASS
	- Complete assessment of encryption, authentication, and integrity protections	PASS
	- Verifiable implementation through secure communication testing	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence

Evidence includes:
- Logs or tests showing secure communication (e.g., TLS/SSL encryption) for network and security assets;
- Documentation describing secure protocols and configuration for each network interface;
- Test results verifying protection against common attack vectors such as replay, eavesdropping, or manipulation.

According to the E.info-SCM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☑PASS ☐ FAIL ☐ N/A
●Functional sufficiency assessment:
verdict ☑PASS ☐ FAIL ☐ N/A

According to the E.info-SCM-1， the equipment has 3 network interfaces as following:

Network interface identifier	Description
NetworkInterface1	Bluetooth Communication

The TL will test secure communication of the above network interface as following:

According to **Test Case SUM-1**, the Android **system update** and **Google Play system update** is protected by TLS 1.2 with cipher suite TLS_ECDHE RSA _WITH_AES_128_GCM_SHA256, and this cipher suit complies with [NIST SP 800-52].

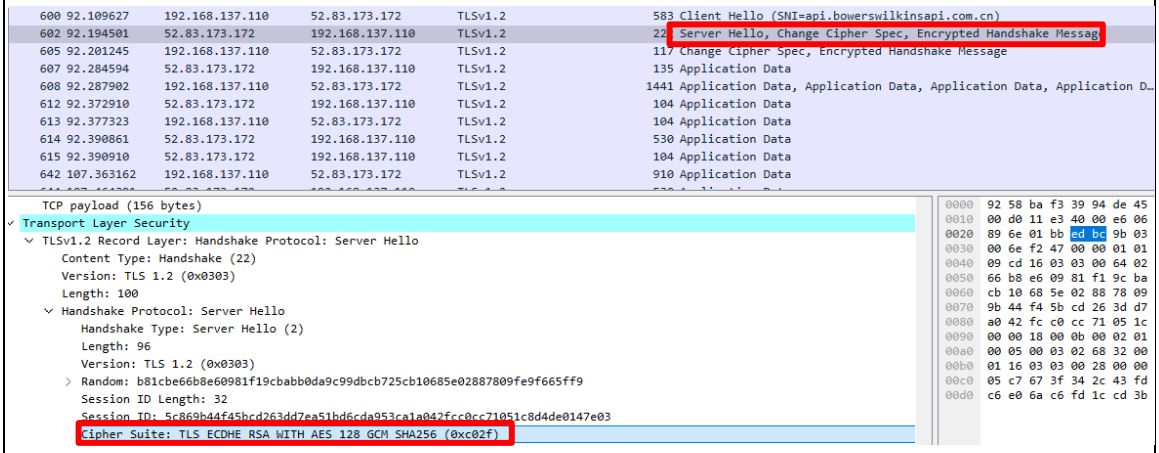
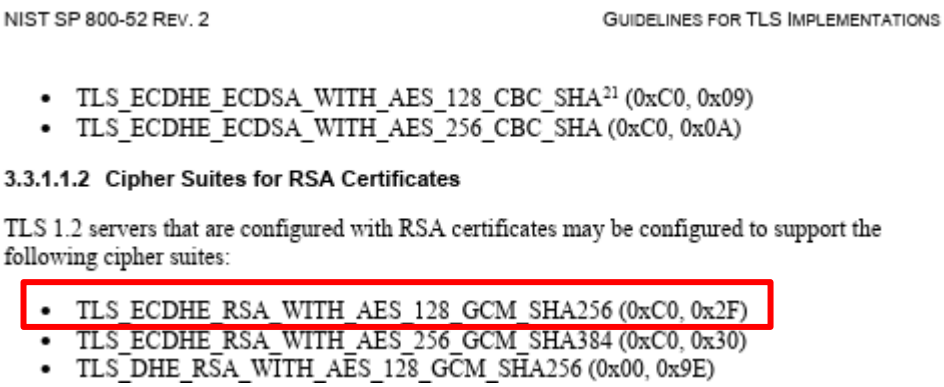


Figure 14: System update update is protected by TLS 1.2



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

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA[21] (0xC0, 0x09)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC0, 0x0A)

3.3.1.1.2 Cipher Suites for RSA Certificates

TLS 1.2 servers that are configured with RSA certificates may be configured to support the following cipher suites:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC0, 0x2F)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xC0, 0x30)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x00, 0x9E)

Figure 15: Cipher suit requirement in NIST SP 800-52

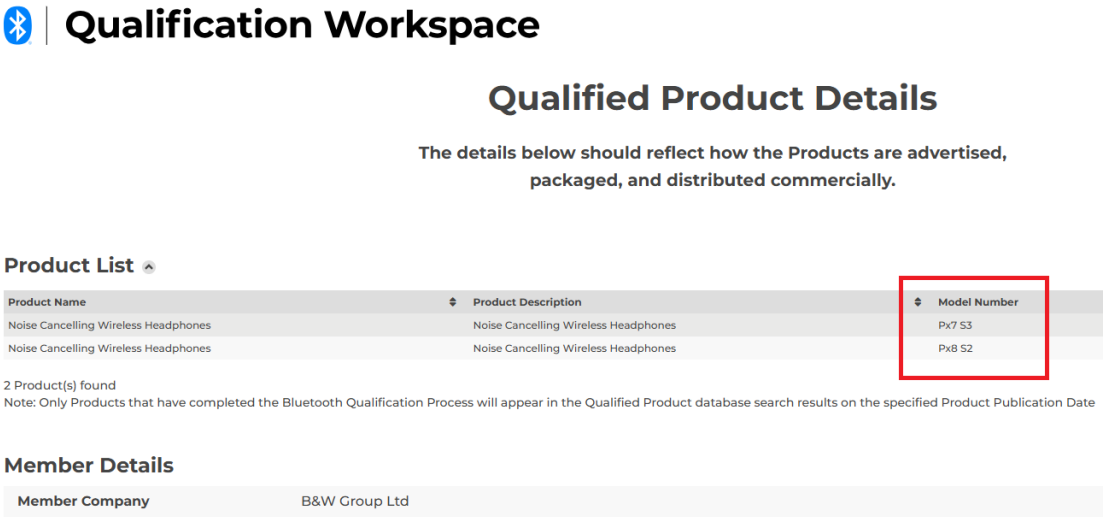
According to the official Bluetooth Qualification Body (BQB) listing published by the Bluetooth SIG:

- The DUT supports Bluetooth 5.0 with LE Privacy 1.2 and AES-CCM encryption for Bluetooth Low Energy (BLE);
- It also supports Secure Simple Pairing (SSP), AES-CCM encryption, and Link Key Generation for BR/EDR (Classic Bluetooth).

These encryption and privacy mechanisms are mandatory features defined in the Bluetooth Core Specification v5.0+, and are validated during BQB qualification.

The product is officially registered and certified under the Bluetooth SIG Qualification Program, which confirms its conformance with secure Bluetooth communication standards.

This ensures that Bluetooth communication on the DUT meets EN 18031 [SCM-1] requirements for confidentiality, integrity, and authenticity of network assets.



Qualification Workspace

Qualified Product Details

The details below should reflect how the Products are advertised, packaged, and distributed commercially.

Product List

Product Name	Product Description	Model Number
Noise Cancelling Wireless Headphones	Noise Cancelling Wireless Headphones	Px7 S3
Noise Cancelling Wireless Headphones	Noise Cancelling Wireless Headphones	Px8 S2

2 Product(s) found
Note: Only Products that have completed the Bluetooth Qualification Process will appear in the Qualified Product database search results on the specified Product Publication Date

Member Details

Member Company	B&W Group Ltd

Conclusion: The DUT has been certified under the Bluetooth BQB program. Bluetooth BQB certification includes verification of essential encryption and security protocols. Since the DUT only supports Bluetooth as its sole communication interface, and Bluetooth is protected by AES-CCM, LE Privacy, and SSP (as required in the Bluetooth spec and verified via BQB certification), it satisfies [SCM-1] requirements.

Result: **PASS**

2.5.2.[SCM-2] Appropriate integrity and authenticity protection for secure communication Mechanisms.

Security Flaw	The absence of integrity and authenticity protection for secure communication mechanisms can result in unauthorized access, tampering, or manipulation of communicated security assets and financial assets.	
Affected Essential Requirements	Failing to implement adequate integrity and authenticity protection mechanisms may violate essential security and privacy standards such as 3(3)d, e.	
Typical Attack	A man-in-the-middle (MitM) attack or message tampering can result in malicious manipulation of sensitive communications if proper integrity and authenticity mechanisms are not applied.	
Covered by Requirement?	EN 18031-1: 6.5.2 [SCM-2] Appropriate Integrity and Authenticity Protection for Secure Communication Mechanisms Requires integrity and authenticity protection using best practices (e.g., MAC, digital signatures) for all assets communicated via network interfaces. EN 18031-2:6.5.1 [SCM-1] Applicability of secure communication mechanisms: Requires secure communication mechanisms to protect security and pricacy assets communicated over network interfaces.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: - Integrity checks: Confirm the use of MAC, digital signatures, or other mechanisms for integrity protection in communication protocols. - Authentication checks: Validate methods such as PKI or secret exchange for authenticity verification. - Verification of cryptographic mechanisms protecting communication integrity. - Examination of communication protocols ensuring secure transmission of assets.	
Objectively Verifiable and Reproducible?	- Use of cryptographic message authentication codes (MAC) or equivalent methods	PASS
	- Verification through message integrity and authenticity testing, including scenarios involving secret keys or certificates	PASS
	- Functional evaluation of protocol implementation	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: - Logs showing communication integrity checks (MAC, signature validation); - Documentation of security measures (encryption, authentication, and integrity mechanisms used);	

- Test results verifying integrity and authenticity protection against tampering or manipulation.

Documentation of secure communication mechanisms used, including cryptographic measures, message authentication codes (MACs), and integrity protection for secure communication of security and financial assets.

According to the E.info-SCM-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A
●Functional sufficiency assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A

According the E.info，the equipment has five network interfaces ,and the protocol of these interfaces are described in the following table,all of the protocols used by the interfaces can protect the integrity and authenticity protection for secure communication Mechanisms.

networkinterface description	The communication protocols implemented .
Bluetooth Communication	LE Secure Connections / LE Privacy

As described in Test Case SCM-1, the requirement of this assessment unit is fulfilled for the device under test. it implements TLS 1.2 with the cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F), which is recommended by NIST SP 800-52r2 and widely accepted in industry. This configuration ensures authenticated encryption and forward secrecy. Therefore, the secure communication mechanism complies with SCM-1, and integrity/authenticity protection is provided in line with SCM-2.

Result: **PASS**

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

Security Flaw	Eavesdropping or interception of communicated security assets or network assets, leading to disclosure or misuse of sensitive information. Unauthorized eavesdropping on communicated security and privacy assets. The lack of confidentiality protection for communication mechanisms may result in eavesdropping or unauthorized access to communicated financial and security assets.	
Affected Essential Requirements	A lack of confidentiality protection could result in violations of essential security requirements such as 3(3)d , e and f -Best practice cryptography must be used to protect the confidentiality of communicated security and network assets. -Eavesdropping protection: Ensure all assets communicated are encrypted and resistant to unauthorized interception. -Deviations from best practices (e.g., for interoperability) must have compensating measures to maintain security.	
Typical Attack	Eavesdropping or man-in-the-middle attacks, where an unauthorized party gains access to sensitive data by intercepting communications. Eavesdropping on communication channels to intercept confidential financial or security data.	
Covered by Requirement?	EN 18031-1: 6.5.3 [SCM-3] Appropriate Confidentiality Protection for Secure Communication Mechanisms EN 18031-2: 6.5.3 [SCM-3] Appropriate Confidentiality Protection for Secure Communication Mechanisms Mandates the use of best practice cryptographic methods to ensure confidentiality of network, security, privacy and financial assets during communication.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: -Encryption methods: Validate encryption methods like symmetric encryption schemes or authenticated encryption (AE) for ensuring confidentiality during communication. -Protocol evaluation: Evaluate the cryptographic protocols used, ensuring compliance with best practices. -Testing covers cryptographic protections, encryption methods, and resilience against eavesdropping or unauthorized access.	
Objectively Verifiable and Reproducible?	- Use of symmetric/asymmetric encryption for message confidentiality	PASS
	- Verification of key exchange mechanisms and encrypted communication channels	PASS
	- Functional evaluation of cryptographic protocol implementation	PASS

The security flaw is traceable in an objectively verifiable manner	
Evidence	Evidence includes: - Logs showing encrypted communication; - Documentation of cryptographic algorithms and key exchange methods; - Test results verifying protection against eavesdropping. **According to the E.info-SCM-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A** According to the E.info-SCM-3,the equipment has three network interfaces, the message encryption can protect the integrity of secure communication.

Description	Capabilities	MessageEnc
Bluetooth Communication	Uses AES-128 for secure pairing and ECDH for key exchange	Key generated via ECDH and encrypted with AES-128.

Use adb logat | findstr -I “Bond” to find Bond log

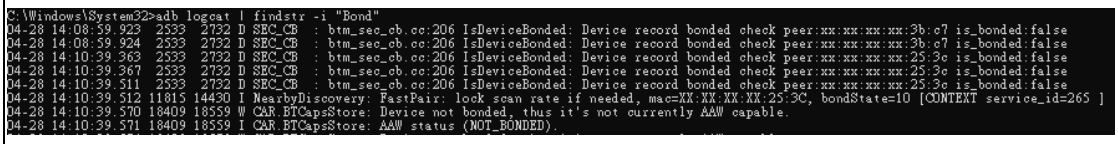


Figure 16: Find Bond log

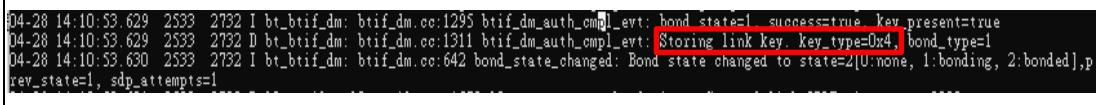
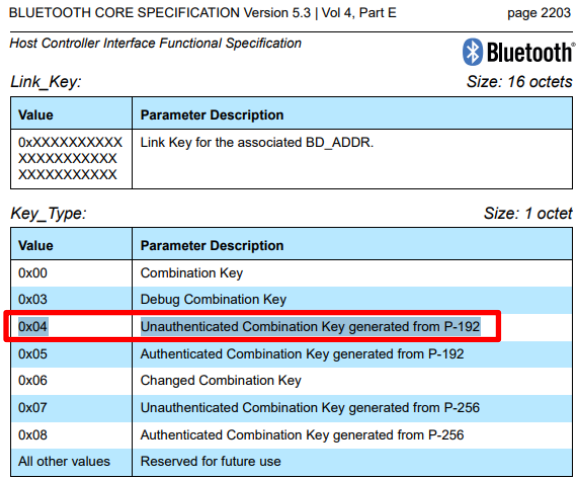


Figure 17:key_type=0x4



BLUETOOTH CORE SPECIFICATION Version 5.3 | Vol 4, Part E page 2203

Host Controller Interface Functional Specification

Link_Key: *Size: 16 octets*

Value	Parameter Description
0xXXXXXXXXXX XXXXXXXXXX XXXXXXXXXX	Link Key for the associated BD_ADDR.

Key_Type: *Size: 1 octet*

Value	Parameter Description
0x00	Combination Key
0x03	Debug Combination Key
0x04	Unauthenticated Combination Key generated from P-192
0x05	Authenticated Combination Key generated from P-192
0x06	Changed Combination Key
0x07	Unauthenticated Combination Key generated from P-256
0x08	Authenticated Combination Key generated from P-256
All other values	Reserved for future use

Figure 18:BLUETOOTH CORE SPECIFICATION Version 5.3

It can be confirmed that during the Bluetooth pairing process, a link key with key_type=0x04 was generated and stored.

Referring to the Bluetooth Core Specification 5.3 (Volume 4, Part E, Table 2.2: Link Key Types):

- key_type=0x04 corresponds to **Unauthenticated Combination Key generated from P-192**.
- The key is generated using **Elliptic Curve Diffie-Hellman (ECDH)** key exchange.
- The resulting link key is encrypted using **AES-128**.

Thus, the Bluetooth communication implements:

- **ECDH key exchange** during the pairing process, and
- **AES-128 encryption** for protecting the generated link key and subsequent communication sessions.

Conclusion:
Based on the log evidence and official Bluetooth specification, it is confirmed that the Bluetooth communication uses AES-128 for secure pairing and ECDH for key exchange, satisfying the security requirements stated in:

SCM-3 Appropriate Confidentiality Protection for Secure Communication Mechanisms (EN 18031-1 / EN 18031-2).

Result：**PASS**

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

Security Flaw	Replay attacks may allow attackers to maliciously repeat valid data transmissions, potentially leading to unauthorized actions, such as replaying authentication data or control commands.	
Affected Essential Requirements	If replay protection is not applied, attackers could exploit this weakness to gain unauthorized access or execute unauthorized commands. This relates to clause 3(3)d,e,f on communication protection.	
Typical Attack	An attacker captures and retransmits legitimate communication (e.g., login credentials, control commands) to manipulate or hijack system operations. Methods include session hijacking and replaying data.	
Covered by Requirement?	EN 18031-1:6.5.4 [SCM-4] Replay Protection. Secure communication mechanisms must apply replay protection techniques such as: - Sequence numbers - Timestamps - One-time encryption keys EN 18031-2:6.5.4 [SCM-4] Replay Protection. Secure communication mechanisms must apply replay protection techniques such as: - Sequence numbers - Timestamps - One-time encryption keys	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: -Message tracking: Use unique identifiers such as sequence numbers or timestamps. -Replay prevention: Ensure that retransmitted messages (e.g., duplicated data packets) are rejected.	
Objectively Verifiable and Reproducible?	- Reliable documentation of replay protection methods in place	PASS
	- Complete assessment of sequence numbers, timestamps, or key-based protections	PASS
	- Functional testing results	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Documentation of secure communication mechanisms, including replay protection methods such as sequence numbers, timestamps, or one-time encryption keys, ensuring protection against replay attacks. **According to the E.info-SCM-4，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A**	

●**Functional sufficiency assessment:**

verdict ☑ **PASS** ☐ **FAIL** ☐ **N/A**

According the E.info-SCM-4, the three network interfaces all can protect the replay attack of secure communication.

Description	Capabilities	Replay Attack Protection
Bluetooth Communication	Uses AES-128 for secure pairing and ECDH for key exchange	Bluetooth Secure Connections use a combination of ECDH key exchange and session-specific keys, along with challenge-response authentication, to prevent replaying pairing or data exchange attempts.

As documented in [SCM-4], TLS 1.2 is applied using the cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xC02F). The selected TLS 1.2 cipher suite provides authenticated encryption with associated data (AEAD) and incorporates per-session keys and implicit replay protection through the use of secure sequence numbering.

Therefore, it is considered that best practices are applied to protect the communicated asset against replay attacks.

As documented in Test Case SCM-1, the use of TLS 1.2 and the selected cipher suite has been verified in connection.

A PASS verdict is assigned.

Result：**PASS**

2.6.[LGM] Logging mechanism

2.6.1.[LGM-1] Applicability of logging mechanisms

Security Flaw	Lack of proper logging for privacy asset-related activities, leading to undetected security breaches or unauthorized actions. Lack of logging mechanisms can prevent the detection of unauthorized activities and security breaches related to financial assets.	
Affected Essential Requirements	Incomplete or missing logs of critical internal activities could result in difficulty detecting and responding to security breaches, potentially violating data protection laws. Related to clause 3(3)e,f on data logging. The security flaw may hinder the ability to detect security breaches and unusual activities that affect financial assets, potentially violating essential requirement 3(3)d.	
Typical Attack	Attackers manipulate or perform unauthorized actions (e.g., access to privacy assets) without detection due to the absence or failure of logging mechanisms. Examples include tampering with logs or preventing log entries. Attacks exploiting the absence of logs for unauthorized access, changes to financial assets, or failure to track important security-related events, making it harder to identify and respond to breaches.	
Covered by Requirement?	EN 18031-2:6.6.1 [LGM-1] Logging Mechanism. All internal activities relevant to privacy assets and protection must be logged unless legally prohibited. Example events: - Access, add, edit, or delete privacy assets - Unauthorized access attempts	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Implementation of logging mechanisms for privacy asset activities - Availability and completeness of logs for relevant internal activities - Review of logged events for activities involving financial assets and security-related actions. - Verification of logging configuration and SIEM integration. - Examination of logs for events like adding, editing, or deleting financial assets and attempts to access or modify them.PASS	
Objectively Verifiable and Reproducible?	- Reliable documentation of the logging mechanism implementation	PASS
	- Complete assessment of log data for relevant internal activities	PASS
	- Functional testing of logging mechanisms	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence

Evidence includes:
- Description of the logging mechanism and events logged
- Logs of privacy asset-related activities (e.g., add, edit, delete)
- Test results showing the effectiveness of logging mechanisms

Documentation of logging mechanisms for financial assets, including types of events logged (e.g., access, modification, or unauthorized access), and logs sent to security information and event management (SIEM) systems.

According to the E.info-LGM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment

verdict ☑ PASS ☐ FAIL ☐ N/A

●Functional completeness assessment:

verdict ☑ PASS ☐ FAIL ☐ N/A

●Functional sufficiency assessment:

verdict ☑ PASS ☐ FAIL ☐ N/A

Use adb logat | findstr -I "Bond" to find Bond log

```
C:\Windows\System32>adb logcat | findstr -i "Bond"
04-28 14:08:59.923  2533  2732 D SEC_CB  : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:3b:c7 is_bonded:false
04-28 14:08:59.924  2533  2732 D SEC_CB  : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:3b:c7 is_bonded:false
04-28 14:10:39.363  2533  2732 D SEC_CB  : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:25:3c is_bonded:false
04-28 14:10:39.367  2533  2732 D SEC_CB  : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:25:3c is_bonded:false
04-28 14:10:39.511  2533  2732 D SEC_CB  : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:25:3c is_bonded:false
04-28 14:10:39.512 11815 14430 I NearbyDiscovery: FastPair: lock scan rate if needed, mac=XX:XX:XX:XX:25:3C, bondState=10 [CONTEXT service_id=265 ]
04-28 14:10:39.570 18409 18559 W CAR.BTCapsStore: Device not bonded, thus it's not currently AAW capable.
04-28 14:10:39.571 18409 18559 I CAR.BTCapsStore: AAW status (NOT_BONDED).
```

Figure 19: Find Bond log

1. Bluetooth Pairing Process Initiation

Use **adb logat | findstr -I "Bond"**

Log Output**:**

```
04-28 14:10:49.449  2533  2732 I bt_btif_dm: btif_dm.cc:642 bond_state_changed: Bond state changed to state=1[0:none, 1:bonding, 2:bonded],p
rev_state=0, sdp_attempts=0
04-28 14:10:49.449  2533  2732 D bt_bta_dm_sec: bta_dm_sec.cc:159 bta_dm_bond: Bonding with peer device:xx:xx:xx:xx:66:1d type:public transp
ort:BT_TRANSPORT_AUTO type:BR_EDR
```

Figure 20: Bluetooth Pairing Initiation (Bonding Start)

Explanation:
This log confirms that the device (MAC: XX:XX:XX:66:1D) transitions from none to bonding state, indicating that the Bluetooth pairing process has been initiated using BR/EDR transport. This satisfies LGM-1 requirements for establishing a secure pairing process.

2. Encryption & Key Exchange During Pairing

Log Output:

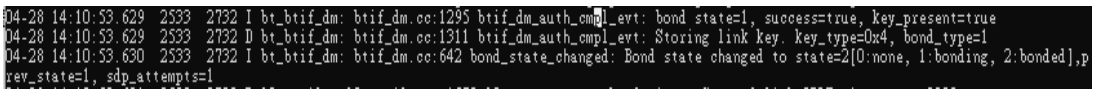


Figure 21:Key Exchange and Storage

Explanation:
This log confirms that the pairing process has successfully completed, transitioning to the bonded state, with a link key generated and stored. The key type 0x4 (commonly P-192 or P-256 ECDH) ensures encryption and secure key exchange, meeting LGM-1 encryption and key management requirements.

3. Bonding State Transition

Log Output:

Figure 22: Pairing State Transition Completed (Bonded)

Explanation:
This log demonstrates the **transition from bonding (11)** to **bonded (12)** state, complementing the second image (key generation). Together, they ensure that the pairing process is fully completed, fulfilling **LGM-1** requirements for secure pairing validation.

4. Device Management After Pairing via Fast Pair System
Use **adb logat | findstr -l "Bond"**

Log Output:

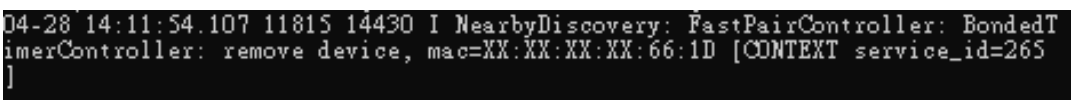


Figure 23: Fast Pair Device Management (Lifecycle Management)

Explanation:
This log shows that the FastPairController removes the device record after pairing,

	demonstrating the system's capability to track and manage paired devices. It ensures that device information is cleared when no longer required, aligning with LGM-1's requirements for post-pairing device lifecycle management and security risk mitigation. Result: **PASS**

2.6.2.[LGM-2] Persistent storage of log data

Security Flaw	Loss of event log data due to insufficient persistent storage mechanisms, resulting in the inability to track or investigate security-related events after a system reboot or power failure.	
Affected Essential Requirements	The absence of persistent storage for log data could result in data loss, making it impossible to investigate unauthorized access attempts, system errors, or potential security breaches.	
Typical Attack	Attackers might erase or manipulate log data through deliberate power cycling of the equipment or tamper with stored logs if persistent storage is not applied. Attacks exploiting the inability to retain log data after power cycles, leading to the erasure or manipulation of logs to cover unauthorized access or modifications to financial assets.	
Covered by Requirement?	EN 18031-2: 6.6.2 [LGM-2] Persistent Storage. Logging mechanisms must ensure that log data for relevant events is stored persistently on the equipment unless the log data is stored outside the equipment.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Whether the log data is stored in the equipment's persistent storage or an external system - Whether log data is accessible after power cycling or rebooting the system - Examination of log data storage locations within the equipment's persistent storage. - Verification of logging configurations supporting external storage.	
Objectively Verifiable and Reproducible?	- Reliable documentation of the logging mechanisms used	PASS
	-Complete verification that log data is retained in persistent storage after system restart	PASS
	- Functional testing of logging mechanisms	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: - Description of persistent storage locations for log data - Logs showing the events that were captured and stored - Test results verifying log retention after power cycling - Compliance with storage security protocols Documentation of logging mechanisms, including internal and external log storage, ensuring log data related to financial assets and security events is stored persistently after equipment power cycles.	

	According to the E-info-LGM-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow: **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** The log data of the DUT stores in the phone, which is outside the DUT. Therefore, LGM-2 has been assigned a result of "N/A". Result：**N/A**

2.6.3.[LGM-3] Minimum number of persistently stored event.

Security Flaw	Insufficient number of stored events, leading to incomplete logs and the inability to perform thorough security investigations. Failure to meet the minimum number of persistently stored events may result in the loss of critical event logs, making it difficult to detect and analyze security incidents, thus compromising the protection of financial assets and security assets.	
Affected Essential Requirements	A lack of sufficient log entries may hinder investigation into security incidents or system errors, resulting in incomplete audit trails. This relates to clause 3(3)d ,e,d on event logging and audit trail maintenance. The inability to store a sufficient number of events can affect the detection of unauthorized activities related to financial and security assets, potentially violating essential requirement 3(3)e.	
Typical Attack	Attackers may attempt to erase or manipulate older log data, especially if the number of events that can be stored persistently is limited, thereby covering their tracks and preventing detection. Attackers exploiting the limited number of stored events to trigger overflow and erase older, crucial logs. This may enable malicious activities to go unnoticed, such as repeated unauthorized access attempts or tampering with security assets.	
Covered by Requirement?	EN 18031-2: 6.6.3 [LGM-3] Minimum Events Storage. Logging mechanisms must store at least a minimum number of the latest events, ensuring that the most recent event is always retained.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - The ability of the equipment to store the minimum number of log events as required - Access to the stored log data and confirmation that the most recent events are recorded and retrievable - Verification of logging capacity to ensure the required minimum number of events is stored.	
Objectively Verifiable and Reproducible?	- Reliable documentation showing the number of logged events retained	PASS
	- Complete verification that the required number of events is stored persistently	PASS
	- Functional testing showing that older events are not lost	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence

Evidence includes:
- Description of the logging mechanism and the number of events that can be stored - Test results confirming the storage of the minimum required number of events
- Verification logs showing the retention of recent events

According to the E.info-LGM-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment

verdict ☑ PASS ☐ FAIL ☐ N/A

●Functional completeness assessment:

verdict ☑ PASS ☐ FAIL ☐ N/A

●Functional sufficiency assessment:

verdict ☑ PASS ☐ FAIL ☐ N/A

We use logcat to show get the log of “Music | Bower & Wilkins” APP. We find it always shows the latest logs.

```
C:\Windows\System32>adb shell ps | findstr /i "bowers"
u0_a381       16331  1067   29462812 429288 ep_poll              0 S com.bowerswilkins.splice

C:\Windows\System32>adb logcat | findstr "16331"
04-28 14:45:42.123     0     0 I [C316331] swilkins.splice: [name:mtk_swpm_dbg_v6878&]swpm_sp_routine regular update(745), total_suspend(252622842)
04-28 14:49:47.883     0     0 I [C316331] swilkins.splice: [name:mtk_swpm_dbg_v6878&]swpm_sp_routine regular update(745), total_suspend(252622842)
04-28 14:53:46.606     0     0 I [T102480] wpa_supplicant: [name:wlan_drv_gen4m_6878&][wlan][2480]mtk_cfg80211_get_station:(REQ INFO) link speed=51
04-28 14:54:20.655 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:54:23.168 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:54:23.179 16331  8950 D BluetoothLeScanner: onScannerRegistered() - status=0 scannerId=3 mScannerId=0
04-28 14:54:33.188 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:54:35.699 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:54:35.708 16331  8950 D BluetoothLeScanner: onScannerRegistered() - status=0 scannerId=3 mScannerId=0
04-28 14:54:45.717 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:54:48.230 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:54:48.238 16331  8950 D BluetoothLeScanner: onScannerRegistered() - status=0 scannerId=3 mScannerId=0
04-28 14:54:55.083     0     0 I [C316331] swilkins.splice: [name:mtk_swpm_dbg_v6878&]swpm_sp_routine regular update(745), total_suspend(252622842)
04-28 14:54:58.246 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:55:00.759 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:55:00.768 16331  8950 D BluetoothLeScanner: onScannerRegistered() - status=0 scannerId=3 mScannerId=0
04-28 14:55:06.347     0     0 I [C316331] swilkins.splice: [name:mtk_swpm_dbg_v6878&]swpm_sp_routine regular update(746), total_suspend(252622842)
04-28 14:55:10.775 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:55:13.291 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:55:13.301 16331  8950 D BluetoothLeScanner: onScannerRegistered() - status=0 scannerId=3 mScannerId=0
04-28 14:55:16.591     0     0 I [C316331] swilkins.splice: [name:mtk_swpm_dbg_v6878&]swpm_sp_routine regular update(746), total_suspend(252622842)
04-28 14:55:23.309 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:55:25.823 16331 16331 D BluetoothAdapter: isLeEnabled(): ON
04-28 14:55:25.833 16331  8950 D BluetoothLeScanner: onScannerRegistered() - status=0 scannerId=3 mScannerId=0
```

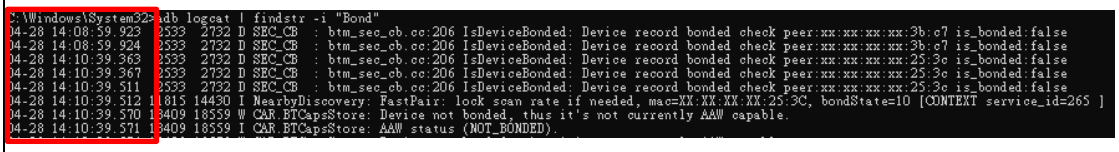
Figure 24: The log buffer of the android

Conclusion: The log always shows the newest logs. Therefore, This figure shows continuous updates in the Bluetooth scan logs, recording multiple instances of Bluetooth status (isLeEnabled()) and scanner registration (onScannerRegistered()) messages. The timestamps increase progressively, proving that the device can store multiple log events, thereby meeting the minimum event storage requirement. LGM-3 has been assigned a result of "PASS".

Result: **PASS**

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

Security Flaw	Lack of proper timestamp or time-related information in log data, hindering the ability to determine the temporal sequence of events, which may affect security investigations. Failure to store log data with time-related information may result in the inability to trace or analyze the sequence of events, complicating the investigation of security incidents or breaches.	
Affected Essential Requirements	Incomplete or missing time information in logs can make it difficult to correlate events with other systems or establish an accurate timeline, which compromises the audit trail. This relates to clause 3(3)e,f on event logging and traceability. The lack of time-related information in logs can hinder the detection and analysis of unauthorized activities affecting financial and security assets, potentially violating essential requirement 3(3)e,f.	
Typical Attack	Attackers could manipulate the system's clock or prevent time-related information from being logged, making it harder to trace their actions or correlate events across different systems. Attackers may manipulate the time order of logged events or disrupt the sequence to hide unauthorized activities, making it difficult to detect malicious access attempts, tampering, or other security breaches.	
Covered by Requirement?	EN 18031-2: 6.6.4 [LGM-4] Time-related Information. Log data must include: - A timestamp if real time is available - Time-related information (e.g., event sequence, time since power up) if real time is unavailable.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Availability of timestamps in log data when real time information is present - Availability of time-related information when real time is not available - Verification of logging configurations regarding time-related mechanisms.	
Objectively Verifiable and Reproducible?	- Reliable documentation of how timestamps or time-related information is stored	PASS
	- Complete verification that all logged events have proper time-related data	PASS
	- Functional testing ensuring time-related data in log records	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence	Evidence includes: - Description of the timestamp or time-related information mechanism used - Logs showing time data for events, even after power cycling - Test results verifying time information availability in stored log data **According to the E.info-LGM-4，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A**  C:\Windows\System32>adb logcat	findstr -i "Bond" 04-28 14:08:59.923 2533 2732 D SEC_CB : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:3b:c7 is_bonded:false 04-28 14:08:59.924 2533 2732 D SEC_CB : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:3b:c7 is_bonded:false 04-28 14:10:39.363 2533 2732 D SEC_CB : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:25:3c is_bonded:false 04-28 14:10:39.367 2533 2732 D SEC_CB : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:25:3c is_bonded:false 04-28 14:10:39.511 2533 2732 D SEC_CB : btm_sec_cb.cc:206 IsDeviceBonded: Device record bonded check peer:xx:xx:xx:xx:25:3c is_bonded:false 04-28 14:10:39.512 11815 14430 I NearbyDiscovery: FastPair: lock scan rate if needed, mac=XX:XX:XX:XX:25:3C, bondState=10 [CONTEXT service_id=265] 04-28 14:10:39.570 13409 18559 W CAR.BTCapsStore: Device not bonded, thus it's not currently AAW capable. 04-28 14:10:39.571 13409 18559 I CAR.BTCapsStore: AAW status (NOT_BONDED). All of the logs contain the real-time timestamps Therefore Therefore, LGM-4 has been assigned a result of "PASS". Result: **PASS**

2.7. [RLM] Resilience Mechanism

Security Flaw	Denial of Service (DoS) Attacks that can disrupt or degrade network operations and network resources, impacting the availability of the equipment.	
Affected Essential Requirements	DoS attacks can compromise essential functions related to equipment availability, leading to breaches of security requirements like 3(3)d.	
Typical Attack	DoS Attacks (e.g., network flooding, service disruption), which overwhelm network interfaces or services, leading to downtime or limited network functionality.	
Covered by Requirement?	EN 18031-1: 6.6 [RLM] Resilience Mechanism Ensures that equipment has resilience mechanisms to mitigate DoS attacks, allowing the system to recover to a defined operational state after the attack.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: -Resilience mechanisms like network storm protection, rate limiting, or packet filtering can be evaluated through: - Simulated DoS attacks to test recovery. - Resilience mechanism analysis to confirm their function and configuration.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	N/A
	- Complete and structured assessment	N/A
	- Reliable assessment results requested	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence may include: - Logs of network interface activity during a simulated DoS attack. - Documentation of implemented resilience mechanisms. - Test results showing recovery to a defined state after the attack. **According to the E.info-RLM，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:**	

	verdict ☐ **PASS** ☐ **FAIL** ☑ **N/A** **●Functional sufficiency assessment:** **verdict** ☐ **PASS** ☐ **FAIL** ☑ **N/A** The device is not directly exposed to the public network, 1. If the device is connected to a network device such as an AP, the related functions to prevent DOS attacks will be introduced on the AP network device side. 2. If the device is connected to a cellular network, related functions to prevent DOS attacks will be imported into the cellular network device. Therefore, the judgment result is not applicable. Result：**N/A**

2.8.[DLM] Deletion mechanism

2.8.1.[DLM-1] Applicability of deletion mechanisms

Security Flaw	Lack of an effective deletion mechanism could lead to unintentional exposure of personal data or sensitive security parameters, especially during equipment disposal or transfer.	
Affected Essential Requirements	If a user cannot reliably delete personal or sensitive data, there is a risk of unauthorized access to sensitive information, compromising privacy and security. This relates to clause 3(3)e on data protection and privacy.	
Typical Attack	Attackers may exploit weak deletion mechanisms, potentially recovering residual personal data or sensitive information, especially if data is not fully removed from storage or encryption keys are not securely erased.	
Covered by Requirement?	EN 18031-2:6.7.1 [DLM-1] Deletion Mechanism. Equipment must enable users or authorized administrators to delete personal data and sensitive security parameters, ensuring data is unrecoverable upon equipment disposal or transfer.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Implementation of deletion mechanisms - Accessibility of deletion mechanism to authorized users - Completeness and effectiveness of the deletion process	
Objectively Verifiable and Reproducible?	- Reliable documentation of deletion methods in place	PASS
	- Complete verification that deletion covers all personal and sensitive security data	PASS
	- Functional testing ensuring unrecoverability of deleted data	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: - Description of deletion mechanisms, including user accessibility - Logs or test results showing deletion actions on personal data - Confirmation that deleted data is unrecoverable or securely erased **According to the E.info-DLM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A**	

●Functional sufficiency assessment:

verdict ☑PASS ☐ FAIL ☐ N/A

The DUT provides a factory reset function through the Bowers & Wilkins App. When the user performs a factory reset, the device displays a notification clearly stating that:

All information on the DUT will be erased.

The device will also be removed from the Bowers & Wilkins App.

This ensures that personal data and sensitive parameters related to the device are securely deleted and cannot be accessed after the reset.

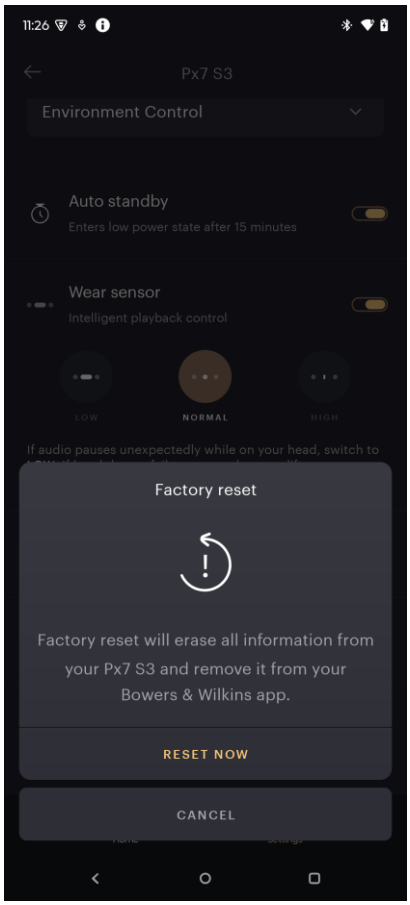


Figure 25: Factory reset notification.

The device clearly informs the user that all information will be erased and the device will be removed from the associated app.

	After performing the factory reset, the DUT returns to its default state, and the previously paired device information and user data (such as settings and pairing records) are no longer accessible. Result: **PASS**

2.9. [NMM] Network Monitoring Mechanism

Security Flaw	Unusual network traffic, such as high datagram rates or malformed packets, may signal the onset of DoS attacks.	
Affected Essential Requirements	Denial of Service (DoS) attacks disrupt the availability of network services, affecting essential network functions.	
Typical Attack	Network datagrams, such as ICMP floods or malformed ARP packets, cause service degradation or total network failure.	
Covered by Requirement?	EN 18031-1 :NMM-1 Network Monitoring Mechanism ensures that network equipment includes monitoring mechanisms to detect and flag unusual network traffic, indicating potential DoS attacks.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment includes: -Simulated traffic testing using malformed or high-frequency packets. -Monitor network equipment responses for early detection and potential mitigation of attacks.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	**N/A**
	- Complete and structured assessment	**N/A**
	- Reliable assessment results requested	**N/A**
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: - Logs or alerts showing detected abnormal traffic patterns. - Documentation on implemented monitoring mechanisms. **According to the E.info-NMM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** Result: This product is not a network equipment, so it is not applicable **(N/A)**	

2.10.[TCM] Traffic control mechanism

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

Security Flaw	Lack of traffic control mechanisms to prevent malicious or anomalous data traffic.	
Affected Essential Requirements	Compromises network stability and integrity by allowing harmful or malicious traffic to traverse the network unchecked, potentially leading to misuse of resources, Denial of Service (DoS), and network outages.	
Typical Attack	An attacker may send malformed or malicious IP packets (e.g., ICMP flooding, ARP spoofing) or use unregulated traffic flows to overwhelm network resources, degrade performance, or crash network interfaces.	
Covered by Requirement?	EN 18031-1: 6.8.1 [TCM-1] Applicability of and appropriate traffic control mechanisms. Mandates that traffic control mechanisms be implemented to prevent malicious or anomalous traffic, thereby securing the flow of data and maintaining network integrity. Mechanisms such as packet filtering, traffic separation, or traffic rule implementation are required.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of traffic control mechanisms: Verifying that the network equipment can identify and filter malicious or anomalous data packets. -Functionality testing: Testing whether unauthorized or harmful traffic is detected and blocked. Combination of functional and conceptual assessments is present.	
Objectively Verifiable and Reproducible?	- Reliable documentation required	N/A
	- Complete and structured assessment	N/A
	- Reliable assessment results requested	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -Logs of traffic monitoring tools showing anomalous or malicious traffic detection and control. -Access control and filtering rules demonstrating restricted or blocked access to unauthorized IP addresses or malformed packets. -Traffic separation policies ensuring isolated and secure network domains. -Functional tests confirming that malicious traffic does not pass through network interfaces.	

	According to the E.info-RLM，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow: **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** Result: This product is not a network equipment, so it is not applicable **(N/A)**

2.11.[UNM] User notification mechanismg

2.11.1.[UNM-1] Applicability of user notification mechanisms

Security Flaw	Lack of timely or appropriate notification to the user regarding changes affecting the protection or privacy of personal information, leading to potential risks such as data misuse or unauthorized access.	
Affected Essential Requirements	Failure to notify the user about changes that affect the protection or privacy of personal data may result in uninformed decisions, exposing the user to privacy risks. This relates to clause 3(3)e on data protection and user transparency.	
Typical Attack	Attackers could exploit unnotified changes in security controls or personal data processing, potentially accessing or misusing personal information without the user's knowledge.	
Covered by Requirement?	EN 18031-2: 6.8.1 [UNM-1] User Notification Mechanism. The equipment must provide mechanisms to inform the user of changes affecting the protection or privacy of personal information.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Whether the user is notified when changes to personal information or security controls occur - Timeliness and completeness of the notification mechanism	
Objectively Verifiable and Reproducible?	- Reliable documentation on notification methods	PASS
	- Complete verification of user notifications for all applicable changes	PASS
	- Functional testing to ensure notifications are triggered and delivered	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -Description of the notification mechanism and how it informs users of changes - Logs or test results showing notifications for changes to personal information or privacy-related settings **According to the E.info-UNM-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:**	

●**Concept assessment**

verdict ☑ **PASS** ☐ **FAIL** ☐ **N/A**

●**Functional completeness assessment:**

verdict ☑ **PASS** ☐ **FAIL** ☐ **N/A**

●**Functional sufficiency assessment:**

verdict ☑ **PASS** ☐ **FAIL** ☐ **N/A**

After pairing, the device will be bound to the Google account of the phone. If someone wants to access the audio data or modify the pairing data of Noise Cancelling Wireless Headphones, they need the Google account it is bound to. If you only have the Noise Cancelling Wireless Headphones, you cannot access any personal data.

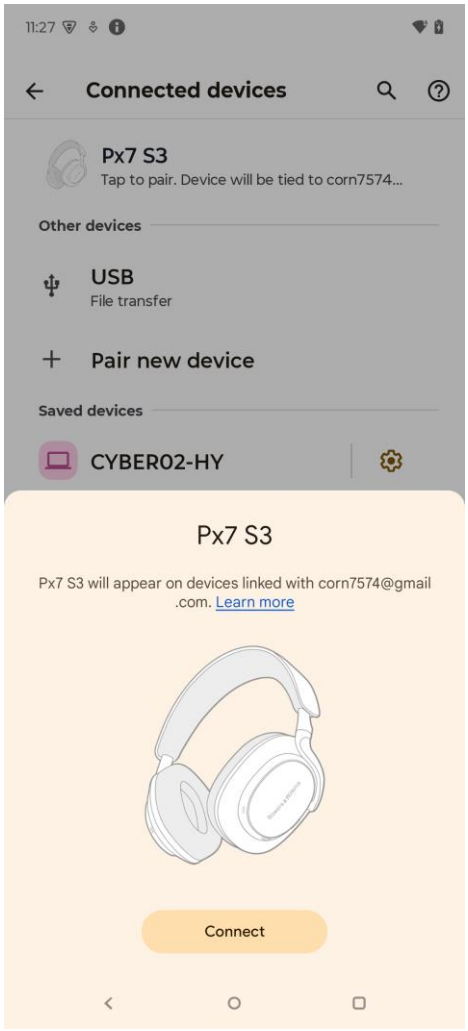


Figure 26: Noise Cancelling Wireless Headphones pairs to phone

When the user wants to **forget the device** (disconnect and remove the pairing), the device will also notify the user before completing the action.

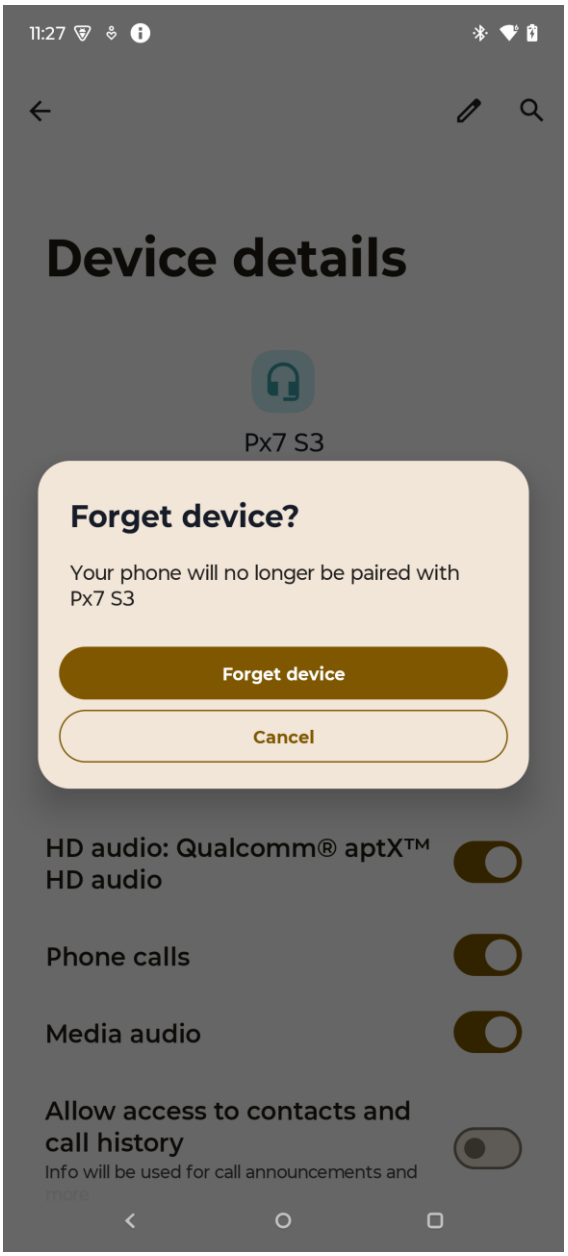


Figure 27: Remove the Noise Cancelling Wireless Headphones

	Conclusion: The device will notify the user whenever an event related to **accessing or modifying personal privacy data** is triggered. Therefore, **UNM-1** has been assigned a result of **"PASS"**. Result: PASS

2.11.2. [UNM-2] Appropriate user notification content

Security Flaw	Lack of detailed or clear notification content could result in user confusion, preventing them from making informed decisions regarding the protection and privacy of their personal data.	
Affected Essential Requirements	Inadequate or unclear notifications may lead to users being unaware of critical changes that affect the protection and privacy of their personal information. This relates to clause 3(3)e on data protection and user transparency.	
Typical Attack	Attackers could exploit incomplete or unclear notifications to mislead users, gaining unauthorized access to personal information or taking advantage of unnotified privacy setting changes.	
Covered by Requirement?	EN 18031-2: 6.8.2 [UNM-2] Notification Content. Each notification must include: - A description of the change - An explanation of how the change affects the protection and privacy of personal information.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Whether the notification content clearly explains the nature of changes - Completeness of the notification in terms of describing the impact on data protection and privacy	
Objectively Verifiable and Reproducible?	- Reliable documentation of the notification content	PASS
	- Complete verification that all required information is included in the notification	PASS
	- Functional testing ensuring notifications are triggered with correct content	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: - Description of notification content, covering changes and their impact - Logs or test results showing notifications with complete and clear content on privacy and security impacts **According to the E.info-UNM-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A**	

As the first figure if UNM-1 shown, there is a “learn more” in pairing notification.

After we click it, we can clearly know what type of the personal data will be collected.

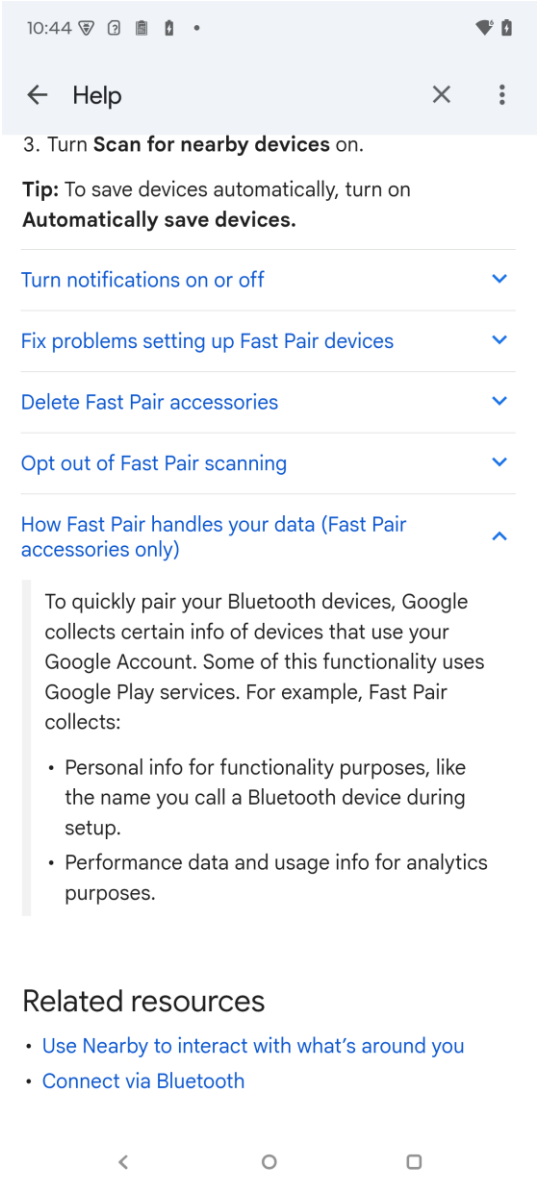


Figure 28: The “learn more” of the pairing notification

While removing the Moto tag, the notification shows how to deal with data clearly.

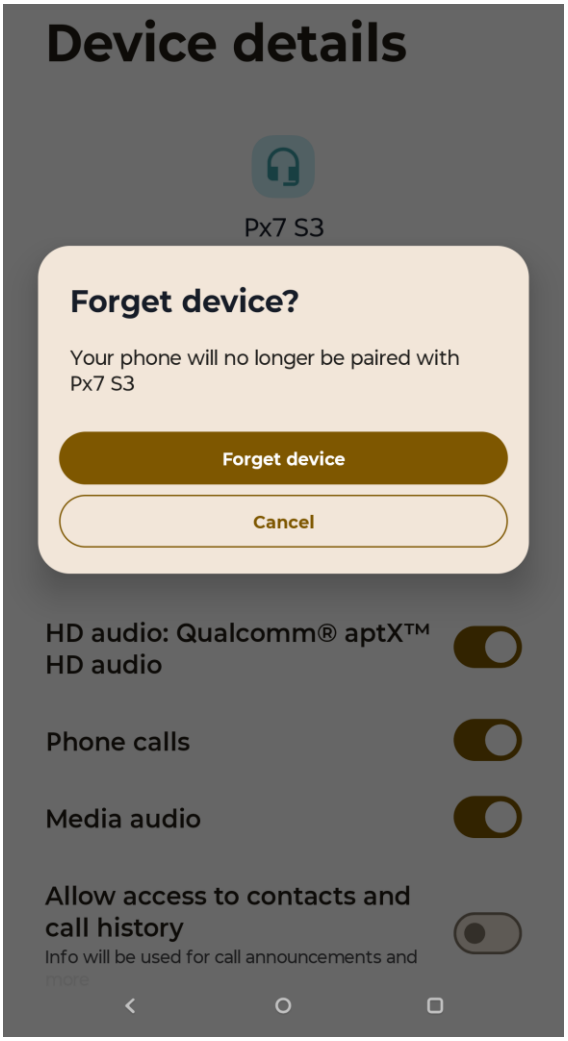


Figure 29: The notification of remove device.

Conclusion: The notifications all clearly shown how to use and deal with the personal data. Therefore, UNM-2 has been assigned a result of "PASS".

Result: **PASS**

2.12.[CCK] Confidential cryptographic keys

2.12.1.[CCK-1] Appropriate CCKs

Security Flaw	Failure to use appropriate cryptographic key strength could lead to compromised confidentiality, affecting the protection of financial assets or security assets. Attackers may exploit weaker cryptographic keys to break encryption and access sensitive data.	
Affected Essential Requirements	Failure to provide sufficient security strength for CCKs (less than 112-bits) compromises essential cryptographic functions, exposing confidential data and network resources to potential misuse or attack. Affected essential requirements include the protection of cryptographic mechanisms used to secure security assets or privacy assets in communication, storage, or during generation (refers to security strength ≥112-bits as per CCK-1).	
Typical Attack	An attacker could gain access to confidential cryptographic keys (CCKs) with weak security strength, enabling decryption of sensitive data, network resource manipulation, or unauthorized access to security assets. Attacks include brute force decryption attempts, cryptanalysis targeting weak or short cryptographic keys, key reuse exploitation, or compromise through poor entropy in key generation.	
Covered by Requirement?	EN 18031-1:6.9.1 [CCK-1] Appropriate Confidential Cryptographic Keys (CCKs) Mandates that all CCKs used in security mechanisms or cryptographic protocols must support a minimum security strength of 112-bits unless otherwise justified under ACM, AUM, SCM, SUM, or SSM sections. The requirement ensures CCKs are appropriately protected during storage and usage, and any deviation from the standard security strength must be documented and justified. EN 18031-2:6.9.1 [CCK-1] Appropriate CCKs. The cryptographic keys must support a minimum security strength of 112 bits unless a specific security mechanism justifies a deviation as outlined in ACM, AUM, SCM, SUM, or SSM sections.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of CCKs: Verifying that all preinstalled or generated CCKs meet the required minimum security strength of 112-bits. -Functionality Testing: Testing CCK implementation to ensure that the cryptographic algorithms used are appropriately secure and no CCKs deviate without justification. - Documented compliance with secure key generation, usage, and storage practices	
Objectively Verifiable and Reproducible?	- Review of cryptographic key length and strength during functional testing.	PASS
	- Examination of cryptographic algorithms and their implementation to verify compliance with the required minimum key strength.	PASS

	- Verification of cryptographic mechanisms during assessment.	PASS
	- Testing for secure key storage and appropriate key lifetime	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	-Logs showing the bit length and security strength of CCKs used in cryptographic algorithms. -Justification for any deviation from the minimum security strength due to interoperability, password key derivation, or other protocol-related reasons. NOT Applicable -Records showing CCK generation processes and secure deletion practices for unused keys. **According to the E.info-CCK-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** Qualification Workspace Qualified Product Details The details below should reflect how the Products are advertised, packaged, and distributed commercially. Product List Product Name / Product Description / Model Number Noise Cancelling Wireless Headphones / Noise Cancelling Wireless Headphones / Px7 S3 Noise Cancelling Wireless Headphones / Noise Cancelling Wireless Headphones / Px8 S2 2 Product(s) found Note: Only Products that have completed the Bluetooth Qualification Process will appear in the Qualified Product database search results on the specified Product Publication Date Member Details Member Company B&W Group Ltd Figure 30:This DUT has been certified by Bluetooth SIG to meet the requirements of CCK-1 The Device Under Test (DUT), a Bluetooth headset equipped with Qualcomm QCC3084, utilizes AES-128 encryption and ECDH-based key exchange, both of which provide >112-bit security strength, fulfilling the EN 18031 CCK-1 requirement for confidential cryptographic keys (CCKs).	

	Result：**PASS**

2.12.2.[CCK-2] CCK generation mechanisms

Security Flaw	**Inadequate generation of confidential cryptographic keys (CCKs) due to poor choices in random sources, RNG, or key derivation methods, resulting in weak or predictable keys.**
Affected Essential Requirements	Weak cryptographic key generation undermines security mechanisms, compromising network or security assets, leading to potential misuse of sensitive resources. Confidential cryptographic keys must be generated following best practices to protect the security assets and privacy assets they secure. The requirement is focused on the secure generation of CCKs. Weak CCK generation could violate essential security requirements, particularly those related to ensuring confidentiality and integrity of financial and security assets .
Typical Attack	Attacks can include guessing, brute-forcing, or reconstructing CCKs based on patterns or known weaknesses in the random number generation process or key derivation algorithms. Typical attacks include: - Guessing or brute-forcing cryptographic keys - Compromising CCKs through poor entropy sources or predictable key derivation mechanisms - Attacks on weak or reused keys.
Covered by Requirement?	EN 18031-1:6.9.2 [CCK-2] Confidential Cryptographic Key Generation Mechanisms Mandates that CCK generation mechanisms must adhere to best cryptographic practices, ensuring strong keys for securing network or security assets. Deviations must be justified under ACM, AUM, SCM, SUM, or SSM. EN 18031-2:6.9.2 [CCK-2] CCK generation mechanisms must adhere to cryptographic best practices. This includes using recognized standards such as NIST SP800-90A, ISO/IEC 18031, and other best practices for key generation.
The security flaw is directly addressed by the requirement	
Detectable in Assessment?	The assessment process includes: -Review of CCK Generation: Verifying that CCKs generated adhere to best cryptographic practices. -Functionality Testing: Testing the robustness of CCK generation, ensuring the RNG and key derivation processes generate secure and unpredictable keys. Assessment includes: - Verification of adherence to recognized best practices - Confirmation of the random number generation (RNG) mechanisms used - Evaluation of key generation and derivation algorithms. - Review of CCK generation mechanisms to ensure compliance with best practices for random number generation and key derivation.

	- Functional examination of RNGs and key generation mechanisms. - Evaluation of entropy sources and randomness quality.	
Objectively Verifiable and Reproducible?	- RNG configuration	PASS
	- Random number source initialization	PASS
	- Key length and strength checks	PASS
	- Evidence of compliance with security standards for cryptographic key generation	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -Documentation of the random number generation process and key derivation algorithms used for CCK generation. -Logs demonstrating adherence to best practices for RNGs (e.g., NIST SP800-90A/B/C, BSI AIS31, ISO/IEC 18031). -Functional tests confirming that generated CCKs have sufficient security strength and are resistant to attacks. -Verification of compliance with recognized cryptographic standards and certification schemes for key generation mechanisms. **According to the E.info-CCK-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** According to test results in CCK-1, all confidential cryptographic keys (CCKs) are generated via appropriate mechanisms, without deviation, and meet the required key strength. The generation processes follow cryptographic best practices, thus complying with the requirements of CCK-2. Result: **PASS**	

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

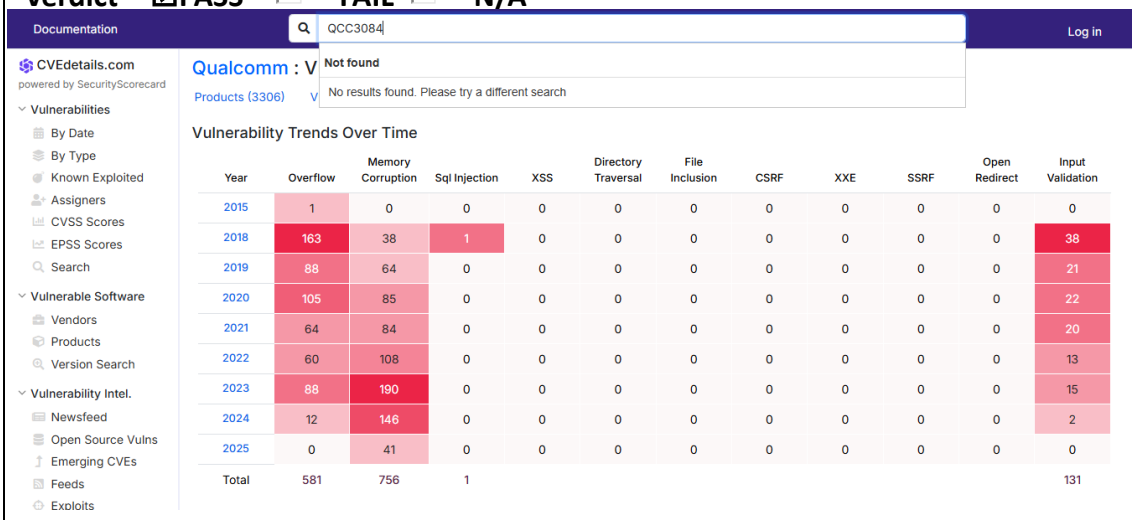
Security Flaw	Use of static default values for preinstalled CCKs, which can be guessed, shared, or reused across multiple equipment instances, resulting in compromised security. Confidential cryptographic keys (CCKs) that are preinstalled with static default values across multiple devices may lead to exposure of security assets and privacy assets, allowing attackers to compromise these assets. Static or shared preinstalled CCKs could expose the system to widespread attacks due to non-unique or easily derived keys across equipment units.
Affected Essential Requirements	Compromises security mechanisms reliant on cryptography, increasing the risk of unauthorized access to network assets or security assets. CCKs must be practically unique per equipment to prevent the use of easily predictable keys across multiple devices, mitigating the risk of successful brute force attacks and unauthorized access. Non-unique preinstalled CCKs can violate essential security requirements related to confidentiality and integrity of financial and security assets .
Typical Attack	Attackers exploit static preinstalled keys by brute-forcing or deriving CCKs from predictable values like MAC addresses, model numbers, or manufacturer information, enabling access to secure resources. Typical attacks include: - Brute force attacks targeting identical or easily derived keys - Exploiting static preinstalled keys across multiple devices to access security or privacy assets. Attackers target shared or static CCKs to perform unauthorized access to multiple devices, creating a broad attack surface due to reused or predictable keys across similar equipment.
Covered by Requirement?	EN 18031-1:6.9.3 [CCK-3] Preventing Static Default Values for Preinstalled Confidential Cryptographic Keys (CCKs) Mandates that preinstalled CCKs must be practically unique per equipment instance unless they are used to establish initial trust under controlled conditions or are essential for shared functionality. EN 18031-2:6.9.3 [CCK-3] mandates that preinstalled CCKs be practically unique for each equipment unless they are used in controlled initial trust relationships or as shared parameters for necessary functionality.
The security flaw is directly addressed by the requirement	
Detectable in Assessment?	The assessment process includes: -Review of Preinstalled CCKs: Verifying that preinstalled CCKs are unique and resist brute-force attacks.

	-Functionality Testing: Testing to ensure that preinstalled CCKs are not derived from predictable values and cannot be reused across devices.	
Objectively Verifiable and Reproducible?	-Verification that CCKs are unique per equipment	PASS
	-Compliance with cryptographic strength and randomness	PASS
	-Documentation and comparison of CCKs across devices for uniqueness	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -Documentation of CCK generation processes ensuring randomness and uniqueness per device. -Logs verifying that preinstalled CCKs resist brute-force attacks and are not derived from predictable values. -Testing of two or more devices to ensure CCK uniqueness and that CCKs cannot be derived from other devices. -Security documentation showing that shared CCKs are necessary and justified for specific equipment functionality. **According to the E.info-CCK-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **Verdict: ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **Verdict: ☑ PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **Verdict: ☑ PASS ☐ FAIL ☐ N/A** According to the test results of CCK-1, all confidential cryptographic keys comply with the requirements of CCK-2. Result：**PASS**	

2.13.[GEC] General equipment capabilities

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

Security Flaw	Inclusion of publicly known exploitable vulnerabilities that could compromise security assets and network assets. Publicly known exploitable vulnerabilities in software or hardware that, if exploited, compromise security or privacy assets. Publicly known vulnerabilities in the equipment's software or hardware that, if exploited, could compromise security or financial assets.	
Affected Essential Requirements	Equipment containing unpatched vulnerabilities can lead to unauthorized access to or exploitation of security and network assets, affecting the confidentiality, integrity, and availability of these assets**.**	
Typical Attack	Attackers exploit publicly known vulnerabilities in outdated software or hardware, leading to unauthorized access, data leaks, and malicious actions on the equipment and network**.**	
Covered by Requirement?	EN 18031-1: 6.10.1 [GEC-1] Up-to-Date Software and Hardware with No Publicly Known Exploitable Vulnerabilities. Mandates that equipment must not include any publicly known exploitable vulnerabilities unless they are mitigated or accepted based on risk analysis. EN 18031-2: 6.10.1 [GEC-1] requires that the equipment should not have publicly known exploitable vulnerabilities affecting security or privacy, unless: - The vulnerability cannot be exploited in the specific equipment condition; - Mitigations have been applied to reduce residual risk; - The vulnerability has been accepted based on risk assessment.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of Vulnerabilities: Identifying all publicly known vulnerabilities in the hardware and software used by the equipment. -Functionality Testing: Testing the equipment to verify that no vulnerabilities are exploitable or have been mitigated.	
Objectively Verifiable and Reproducible?	- Comprehensive documentation of all known vulnerabilities	PASS
	- Verification through vulnerability scanning tools	PASS
	- Functional assessment of implemented mitigations	PASS

The security flaw is traceable in an objectively verifiable manner	
Evidence	Evidence includes: -Documentation of hardware and software versions, identifying any vulnerabilities and the measures taken to mitigate them. -Access to public vulnerability databases, such as NIST National Vulnerabilities Database (NVD). -Security logs and records showing remediation or risk acceptance for known vulnerabilities. -Penetration test results demonstrating that vulnerabilities are not exploitable or have been mitigated effectively. **According to the E.info-GEC-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A**  Year | Overflow | Memory Corruption | Sql Injection | XSS | Directory Traversal | File Inclusion | CSRF | XXE | SSRF | Open Redirect | Input Validation 2015 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 2018 | 163 | 38 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 38 2019 | 88 | 64 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 21 2020 | 105 | 85 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 22 2021 | 64 | 84 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 20 2022 | 60 | 108 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 13 2023 | 88 | 190 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 15 2024 | 12 | 146 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 2025 | 0 | 41 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 Total | 581 | 756 | 1 | | | | | | | | 131 According to the search result from the CVE Details vulnerability database (https://www.cvedetails.com/), there are no publicly known exploitable vulnerabilities associated with the Qualcomm QCC3084 Bluetooth chipset. Therefore, the DUT complies with EN 18031 [GEC-1] requirements, as no exploitable CVEs are present for the hardware in use.

	Result: PASS

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

Security Flaw	Exposure of unnecessary network interfaces and services, which may compromise security or network assets.	
Affected Essential Requirements	Exposing unnecessary services or network interfaces in the factory default state can increase the attack surface and lead to security vulnerabilities.	
Typical Attack	Attackers exploit exposed network interfaces or services to gain unauthorized access, manipulate network traffic, or compromise sensitive information.	
Covered by Requirement?	EN 18031-1: 6.10.2 [GEC-2] Limit Exposure of Services via Related Network Interfaces. Mandates that, in the factory default state, only the essential network interfaces and services required for setup or basic operation should be exposed. EN 18031-2:6.10.2 [GEC-2] requires that in the factory default state: - Only essential network interfaces are exposed; - Only services via network interfaces that are necessary for setup or basic operation are exposed.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of Exposed Services: Verifying whether the exposed network interfaces or services are necessary for the equipment's setup or basic operation. -Functionality Testing: Testing whether any unnecessary services or interfaces are exposed in the factory default state. - If exposed network interfaces and services affect security or privacy assets.	
Objectively Verifiable and Reproducible?	- Reliable documentation required for all exposed network interfaces.	PASS
	- Verification using network scanning tools and equipment setup procedures.	PASS
	- Consistent discovery of unnecessary interfaces through automated tools	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence	Evidence includes: -Documentation of network interfaces and services exposed by the equipment in the factory default state. -Technical details on whether the exposed services are essential for setup or basic operation. -Network scans or penetration testing results verifying the absence of unnecessary network services or interfaces. **According to the E.info-GEC-2，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑ PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** The DUT is a Bluetooth-only headset with no IP-based or wireless broadband network interfaces (e.g., Wi-Fi, LTE, NFC). As no unnecessary network interfaces or services are exposed in the factory default state, the DUT complies with EN 18031 [GEC-2]. Result:**PASS**

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

Security Flaw	Exposed optional services and network interfaces that cannot be controlled by authorized users, potentially increasing the attack surface.	
Affected Essential Requirements	Allowing uncontrolled exposure of optional services and network interfaces increases the attack surface and risk of exploitation.	
Typical Attack	An attacker may exploit optional network interfaces or services exposed in the factory default state, gaining unauthorized access or performing malicious activities.	
Covered by Requirement?	EN 18031-1: 6.10.3 [GEC-3] Configuration of Optional Services and Network Interfaces Mandates that all optional network interfaces and services exposed in the factory default state must have the option for authorized users to enable or disable them. EN 18031-2:6.10.3 [GEC-3] requires that optional network interfaces and services, in factory default state, should be configurable by authorized users, allowing them to enable or disable services as necessary.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of Optional Interfaces/Services: Verifying the ability of an authorized user to enable or disable optional network interfaces or services. -Functionality Testing: Testing whether the configuration option is available for all optional services and interfaces in the factory default state.	
Objectively Verifiable and Reproducible?	- Documentation of optional network interfaces and services	PASS
	- Functional testing of the enable/disable configuration for optional services	PASS
	- Verifiable through user authorization and access control mechanisms	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -Documentation of optional network interfaces and services exposed in the factory default state. -Configuration settings showing that authorized users can enable or disable these interfaces or services. -Logs or records of authorized user actions taken to modify network configurations. - Compliance evidence that optional network interfaces and services are configurable according to the requirements of GEC-3. **According to the E.info-GEC-3，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:**	

	●Conceptual assessment **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** The DUT is a Bluetooth-only headset with no additional IP-based interfaces (e.g., Wi-Fi, USB, NFC, VPN). In the factory default state, Bluetooth is the only network interface exposed. The user is allowed to **enable or disable Bluetooth functionality** via the paired mobile app or physical buttons on the headset. Optional Bluetooth services, such as pairing mode, are **not persistently active** and must be explicitly triggered by the user (e.g., long press to enter pairing mode). Therefore, the only exposed optional interface (Bluetooth) is **fully user-controllable**, and the DUT complies with EN 18031 [GEC-3]. Result： **PASS**

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

Security Flaw	Lack of documentation for exposed network interfaces and services, leading to potential security vulnerabilities by increasing the attack surface.	
Affected Essential Requirements	Lack of documentation compromises the ability of users to configure the equipment securely, increasing the risk of unauthorized access.	
Typical Attack	An attacker could exploit undocumented network interfaces or services, bypassing security measures and gaining unauthorized access to equipment or network assets.	
Covered by Requirement?	EN 18031-1 :6.10.4 [GEC-4] Documentation of Exposed Network Interfaces and Services. Mandates that user documentation must include a description of all exposed network interfaces and services delivered in the factory default state, to ensure proper configuration and security. EN 18031-2 :6.10.4 [GEC-4] Documentation of Exposed Network Interfaces and Services. Mandates that user documentation must include a description of all exposed network interfaces and services delivered in the factory default state, to ensure proper configuration and security.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of User Documentation: Ensuring that all network interfaces and services exposed in the factory default state are clearly documented. -Functionality Testing: Using network and service scanning tools to verify that no exposed services or interfaces are missing from the documentation. - Completeness of user documentation regarding exposed network interfaces and services	
Objectively Verifiable and Reproducible?	- Documentation of all network interfaces and services in the factory default state	N/A
	- Functional assessment using network scanning tools to confirm documentation	N/A
	- Verifiable through service scanning tools	N/A
The security flaw is traceable in an objectively verifiable manner		

Evidence

Evidence includes:
-User documentation listing all exposed network interfaces and services in the factory default state.
-Network and service scanning tool results confirming that no interfaces or services are undocumented.
-Logs or reports from functionality testing confirming that the documentation is complete and accurate.

According to regulations EN 18031-1, EN 18031-2, GEC-4 is not classified as a mandatory test item under RED 3.3 (d), (e), and is therefore determined as N/A

EN 18031-1

Annex ZA
(informative)

Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2022) 5637 and its amendment C(2023) 5624 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3).

In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail.

Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153]

Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
3.3.(d)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11	

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

EN 18031-2

Annex ZA
(informative)

Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2022) 5637 and its amendment C(2023) 5624 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3).

In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail.

Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153]

Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
3.3.(e)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11	

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

Result:**N/A**

2.13.5.[GEC-5] No unnecessary external interfaces

Security Flaw	Exposing unnecessary physical external interfaces increases the equipment's potential attack surface and poses a security risk.	
Affected Essential Requirements	Physical external interfaces not required for the intended functionality of the equipment may expose the equipment to potential threats, affecting the security of assets. This relates to the minimization of attack vectors under the equipment's security framework.	
Typical Attack	Attackers may exploit exposed and unnecessary physical external interfaces to bypass security controls. Common examples include accessing external ports (e.g., USB, network ports) to inject malicious code or extract sensitive data.	
Covered by Requirement?	EN 18031-1: 6.10.5 [GEC-5] No Unnecessary External Interfaces Requires that the equipment only expose physical external interfaces necessary for its intended functionality, reducing unnecessary exposure. EN 18031-2: 6.10.5 [GEC-5] ensures that only necessary physical external interfaces for the equipment's intended functionality are exposed. Unnecessary interfaces are to be disabled or blocked to reduce the attack surface.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Documentation review: Verifying that each physical external interface is documented with a clear purpose. -Examination of the device: Identifying all present physical external interfaces, such as USB ports, buttons, and slots for extensions, to confirm they are documented and justified.	
Objectively Verifiable and Reproducible?	- Documentation of physical external interfaces, including their purpose	PASS
	- Verification through functional assessment of exposed and blocked interfaces	PASS
	- Use of testing tools to confirm presence or absence of unnecessary interfaces	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -User manuals and technical documentation listing all physical external interfaces and their purposes. -Physical inspection logs identifying all external interfaces present on the equipment. -Design documentation indicating the necessity of each interface for the equipment's intended functionality.	

According to the E.info-GEC-5，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:

●Conceptual assessment
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional completeness assessment:
verdict ☑ PASS ☐ FAIL ☐ N/A
●Functional sufficiency assessment:
verdict ☐ PASS ☐ FAIL ☑ N/A

The DUT is a Bluetooth audio headset designed for wireless audio streaming and hands-free communication.
Physical inspection confirms that the only external interface available is the Type-C charging port, which is necessary for normal device operation.
No unnecessary physical interfaces, such as debug UART, JTAG, memory card slot, or OTG USB, are present or accessible to end users.
The enclosure is sealed, and no test points or unutilized physical connectors are externally exposed.
Therefore, the DUT complies with EN 18031 [GEC-5] requirement.

Figure 31:Typc*1

Result: **PASS**

2.13.6.[GEC-6] Input validation

Security Flaw	Improper input validation for external interfaces can lead to successful attacks, such as data corruption, unauthorized data extraction, and compromising security or network assets.
Affected Essential Requirements	Improper input validation can compromise the integrity, confidentiality, and availability of security and privacy assets. This relates to the safeguarding of data under the equipment's security policies and standards, impacting both personal information and critical system functions.
Typical Attack	Exploiting unvalidated input through network interfaces to inject malicious code, compromise security, or extract confidential data. Attackers may inject malicious input to exploit weak validation mechanisms, such as SQL injections, buffer overflows, or path traversal. Common attack vectors include network interfaces that fail to properly check input syntax and semantics, resulting in unauthorized data access or corruption. Attackers may attempt to inject malicious code (e.g., SQL, OS command) or input invalid data (e.g., buffer overflows, path traversal) to exploit input validation weaknesses.
Covered by Requirement?	EN 18031-1: 6.10.6 [GEC-6] Input Validation Requires input validation to ensure proper syntax and semantics, mitigating risks from untrusted or malicious sources. EN 18031-2:6.10.6 [GEC-6] Input validation ensures that inputs received via external interfaces are validated, including checks for: - Syntax (e.g., format, length) - Semantics (e.g., range of values, special characters) - Inclusive listing to only accept predefined input patterns.
The security flaw is directly addressed by the requirement	
Detectable in Assessment?	The assessment process includes: -Review of external interfaces: Ensuring that each input via external interfaces has proper validation mechanisms (syntax and semantics). -Functionality testing: Testing the system's ability to reject improper inputs and prevent attacks targeting security or network assets. The assessment verifies: - Input validation mechanisms on external interfaces - Syntax and semantic checks for inputs affecting security and privacy assets - Resilience of input mechanisms against attacks like injection or buffer overflow - Examination of external interfaces for appropriate input validation mechanisms (e.g., input length, data type, content checks). - Functional assessment of input methods using network analysis and fuzzing tools.

Objectively Verifiable and Reproducible?	- Reliable documentation required on input validation techniques. - Verifiable through traffic analysis and equipment examination.	PASS
	- Verifiable through traffic analysis and equipment examination.	PASS
	- Consistent results necessary across repeated tests.	PASS
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: -Detailed logs showing validation checks on input data (e.g., length, format, content). -Testing results of various inputs for vulnerabilities like SQL injection, path traversal, and buffer overflows. -Design documentation and functional assessments that confirm input validation methods. **According to the E.info-GEC-6，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** The DUT is a Bluetooth wireless headset using the Qualcomm QCC3084 chipset. It supports Bluetooth Classic (A2DP, HFP) and Bluetooth LE for OTA firmware updates and mobile app interaction. The DUT includes two external interfaces capable of receiving input: TYPE-C: Used for charging and basic audio interface; not involved in data processing that affects security assets. Bluetooth: Supports OTA firmware updates, which involve receiving signed update packages over Bluetooth LE. Since the Bluetooth interface is capable of receiving input that directly affects security assets (e.g., firmware images), input validation is applicable under [GEC-6]. Input validation measures include: OTA updates must be digitally signed and validated before application.	

	Bluetooth communication is secured using LE Secure Connections (AES-128), ensuring input integrity and authentication. There is no general-purpose operating system or command-line interface, reducing risk of injection attacks (e.g., SQL or command injection). Result: PASS

2.13.7. [GEC-7] Documentation of external sensing capabilities

Security Flaw	The presence of undocumented external sensing capabilities (e.g., microphones, cameras) could lead to privacy breaches, unauthorized surveillance, and misuse of sensitive personal information.	
Affected Essential Requirements	The lack of proper documentation on external sensing capabilities can impact users' awareness of potential privacy risks. This is crucial for data protection under privacy and security regulations.	
Typical Attack	Attackers could exploit undocumented or poorly documented external sensing capabilities (e.g., access to camera or microphone) to gather sensitive user data, potentially leading to privacy violations or data breaches.	
Covered by Requirement?	EN 18031-2: 6.10.7 [GEC-7] Documentation of external sensing capabilities. The equipment's user documentation must describe: - All external sensing interfaces (e.g., microphone, camera) - Potential impact on users' privacy.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment verifies: - Presence of documented external sensing interfaces - Functionality of sensors such as cameras or microphones and whether their use is disclosed to users in the equipment's documentation.	
Objectively Verifiable and Reproducible?	- Proper documentation of external sensing interfaces	N/A
	- Full verification of documentation to match actual device capabilities	N/A
	- Clear transparency for users regarding privacy risks	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	Evidence includes: - User documentation that describes all external sensing interfaces (e.g., microphones, cameras) - Assessment results confirming that all sensing capabilities are documented and match device functionality. .	

EN 18031-1

Annex ZA
(informative)

Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2022) 5637 and its amendment C(2023) 5624 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3).

In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail.

Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153]

Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
3.3.(d)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11	

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

EN 18031-2

Annex ZA
(informative)

Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2022) 5637 and its amendment C(2023) 5624 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3).

In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail.

Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153]

Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
3.3.(e)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10.1, 6.10.2, 6.10.3, 6.10.5, 6.10.6, 6.11	

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

EN 18031-3

Annex ZA
(informative)

Relationship between this European Standard and the Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d) (e) and (f), of that Directive aimed to be covered

This European Standard has been prepared under a Commission's standardization request C(2022) 5637 and its amendment C(2023) 5624 final to provide one voluntary means of conforming to essential requirements of Directive 2014/53/EU [OJ L 153] of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3).

In case of differences between terms defined in this European standard and terms defined in that Regulation, the terms defined in the Regulation shall prevail.

Once this standard is cited in the Official Journal of the European Union under that Delegated Regulation (EU) 2022/30, compliance with the normative clauses of this standard given in Table ZA.1 confers, within the limits of the scope of this standard, a presumption of conformity with the corresponding essential requirements of Directive 2014/53/EU and associated EFTA regulations.

Table ZA.1 — Correspondence between this European Standard and Directive 2014/53/EU [OJ L 153]

Essential Requirements of Directive 2014/53/EU	Clause(s)/sub-clause(s) of this EN	Remarks/Notes
3.3.(f)	Clauses 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8.1, 6.8.2, 6.8.3, 6.8.5, 6.8.6, 6.8.8, 6.9	

WARNING 1 — Presumption of conformity stays valid only as long as a reference to this European Standard is maintained in the list published in the Official Journal of the European Union. Users of this standard should consult frequently the latest list published in the Official Journal of the European Union.

WARNING 2 — Other Union legislation may be applicable to the product(s) falling within the scope of this standard.

According to regulations EN 18031-1, EN 18031-2, and EN 18031-3 Annex-ZA, GEC-7 is not classified as a mandatory test item under RED 3.3 (d), (e), or (f) and is therefore determined as N/A.

Result: **N/A**

2.13.8. [GEC-8] Equipment Integrity

Security Flaw	Lack of cryptographic verification of the boot process integrity and authenticity, which could lead to unauthorized modification or tampering with software, impacting financial and security assets.	
Affected Essential Requirements	Insufficient boot integrity validation, violating essential requirements 5(a) and 6(c), which could compromise the root of trust and affect asset security and integrity.	
Typical Attack	Attackers could insert malicious software in an unverified boot process, tampering with software or monitoring the boot process to access or modify financial and security assets.	
Covered by Requirement?	EN 18031-3: 6.8.8 [GEC-8]: All software must undergo integrity and authenticity checks during the boot process, using an immutable root of trust or cryptographically authenticated authorization.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	- Review cryptographic integrity validation mechanisms for the boot process, such as chain of trust and root of trust. - Verify if all software processing security and financial assets undergo boot verification.	
Objectively Verifiable and Reproducible?	- Check for consistent documentation of the root of trust and chain of trust configuration.	N/A
	- Repeat tests should show the same validation results, confirming cryptographic consistency in the boot process.	N/A
The security flaw is traceable in an objectively verifiable manner		
Evidence	- Documentation from the manufacturer or subcontractor on boot integrity, including root of trust, chain of trust, and cryptographic methods. - Evidence should show how each software component meets boot process integrity and verification requirements. **According to the E.info-GEC-8，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional completeness assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A** **●Functional sufficiency assessment:** **verdict ☐ PASS ☐ FAIL ☑ N/A**	

	The DUT does not need to test EN 18031-3,so the GEC-8 is not applicable. Result: **N/A**

2.14. [CRY] Cryptography

2.14.1. [CRY-1] Best practice cryptography

Security Flaw	Use of cryptography that does not adhere to best practices, making the security and network assets vulnerable to attacks. Use of non-best practice or deprecated cryptography could lead to the compromise of security assets or privacy assets, rendering protection insufficient against potential attacks.	
Affected Essential Requirements	Weak or outdated cryptography can compromise security assets and network assets, leading to unauthorized access or data breaches. Inadequate cryptographic practices can lead to vulnerabilities in protecting data integrity, confidentiality, and authenticity. This is critical for protecting security and privacy assets per clause 3(3) on cryptographic protection.	
Typical Attack	An attacker exploits weaknesses in cryptographic algorithms, leading to the compromise of secure communications, storage, or key generation. Attackers may exploit weaknesses in cryptographic algorithms (e.g., deprecated or compromised algorithms), leading to unauthorized access, data decryption, or manipulation of protected assets.	
Covered by Requirement?	EN 18031-1: 6.11.1 [CRY-1] Best Practice Cryptography Requires that all cryptographic mechanisms used to protect security or network assets must follow best practices unless a deviation is identified and justified. EN 18031-2: 6.11.1 [CRY-1] Best Practice Cryptography: The equipment must use best practice cryptography for protecting security and privacy assets. Exceptions are allowed under ACM, AUM, SCM, SUM, or SSM if justified.	
The security flaw is directly addressed by the requirement		
Detectable in Assessment?	The assessment process includes: -Review of Cryptographic Methods: Verifying that cryptography used for protection adheres to established best practices. -Functionality Testing: Ensuring the cryptography implementation matches the documentation and resists attacks.	
Objectively Verifiable and Reproducible?	- Verified use of best practice cryptographic methods	PASS
	- Complete and accurate documentation of cryptographic implementations	PASS
	- No unjustified deviations from best practices	PASS
The security flaw is traceable in an objectively verifiable manner		

Evidence	Evidence includes: -Cryptographic catalogs such as SOGIS or NIST to confirm the best practices are followed. -Documentation of all cryptographic protections for assets. -Security analysis of the cryptographic algorithms to ensure they are robust and suitable for their intended use. -Crypto agility documentation confirming that cryptography can be updated if new vulnerabilities are found. **According to the E.info-CRY-1，the results of Conceptual assessment 、funtional completeness assessment and functional sufficiency assessment describe as follow:** **●Conceptual assessment** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional completeness assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** **●Functional sufficiency assessment:** **verdict ☑PASS ☐ FAIL ☐ N/A** According to the test results of CCK-1, The equipment use best practice for cryptography that is used for the protection of the security assets comply with the requirements of CRY-1. Result：**PASS**

———THE END———