№: RED2025-0070-N

TEST REPORT

NAME OF SAMPLE:	Touch Screen All In One Machine
CLIENT:	Guangzhou TouchWo Electronics Co., Ltd.
CLASSIFICATION OF TEST	Commission test

CVC Testing Technology Co., Ltd.

TEST REPORT

Name of product	Touch Screen All In One Machine	Trade mark	—
Type/Model	HD215	Sample status	—
Manufacturer	Guangzhou TouchWo Electronics Co.,Ltd.	Commissioned by	Guangzhou TouchWo Electronics Co., Ltd.
Manufacturer address	No.5, Environmental Protection Third Road, Xintang Town, Zengcheng District, Guangzhou City, Guangdong Province,China. 511340	Commissioner address	No.5, Environmental Protection Third Road, Xintang Town, Zengcheng District, Guangzhou City, Guangdong Province,China. 511340
Quantity of sample	4	Sampled by	—
Sample identification	1#,2#,3#,4#	Sampling at (place)	—
Means of receiving	Self delivery	Means of sampling	—
Classification of test	Commission test	Sampling date	—
Receiving date	July 16, 2025	Completing date	February 10, 2026
Tested according to	EN 18031-1-2024 Common security requirements for radio equipment - Part 1: Internet connected radio equipment EN 18031-2-2024 Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment		
Test item	ALL items		
Test conclusion	At the request of the client, testing was carried out in accordance with EN 18031-1-2024 Common security requirements for radio equipment - Part 1: Internet connected radio equipment and EN 18031-2-2024 Common security requirements for radio equipment - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment. Test conclusion: The testing items meet the standard requirements. Seal of CVC Date of issue: February 10, 2026		

Approved by: Hu Xin Reviewed by: Fang Yijie Tested by: Duan Bin

Sign: Hu Xin Sign: Fang Yijie Sign: Duan Bin

Sample Description and Instructions	Device Information: Device Name: Touch Screen All In One Machine SN: HD21520250623SZHCW04 Device Model: HD215 Hardware Version: YS-M76 Software Version: Android 14.0 Firmware Version: rk3576-14.0-20250117.145459 Tested Model: HD215 Covered Models:TD050,TD070,TD080,TD101,TD104,TD116,TD121,TD133,TD140,TD156,TD173,TD185,TD19,TD215,TD238,TD27,TD32,TD43,TD49,TD55,TD65,JD080,JD101,JD133,JD156,JD101B,JD156B,JD185B,JD215B,JD238,HD080,HD101,HD133,HD156,HD185,HD215,HD238,HD27,HD32,HD43,HD49,HD55,HD65,HD75,HD86,HD98,HD110,GD101,GD116,GD133,GD156,GD215,GD238,GD27,GD32,GD43,KD156,KD17,KD19,KD215,KD32,KD43,KD185,KD238,KD27,DM080NF,DM080WF,DM101F,DM104F,DM121F,DM133F,DM15F,DM156F,DM17F,DM185F,DM19F,DM215F,DM238F,RZ55,RZ65,RZ70,RZ75,RZ85,RZ86,RZ98,RZ100,HR32,HR43,HR49,HR55,HR65,HR75,HR85,HR98,HR100,DP101,DP104,DP121,DP133,DP15,DP156,DP17,DP185,DP19,DP215,DP238,IDP101,IDP101B,IDP121,IDP104,IDP104B,IDP121B,IDP15,IDP15B,IDP156,IDP156B,IDP17,IDP17B,IDP185,IDP185B,IDP19,IDP19B,IDP215,IDP215B,IDP238,IDP238B,WP101,WP101B,WP104,WP104B,WP121,WP121B,WP15,WP15B,WP156,WP156B,WP17,WP17B,WP185,WP185B,WP19,WP19B,WP215,WP215B,WP238,WP238B,DM080NG,DM080WG,DM101G,DM104G,DM121G,DM133G,DM15G,DM156G,DM17G,DM185G,DM19G,DM215G,DM238G,DM050,DM070,DM080,DM101,DM104,DM121,DM133,DM14,DM15,DM156,DM17,DM185,DM19,DM215,DM238,DM27,DM32,DM43,DM49,DM55,DM65. This sample is the YS-M76 smart Android motherboard, an embedded motherboard developed based on the high-performance Rockchip RK3576 chip. It comes pre-installed with the Android 14.0 system and features high computing power, multiple interfaces, and broad compatibility. It can be widely used in scenarios such as advertising screens, smart terminals, and industrial control, supporting diverse peripheral connections and dual-screen display, meeting the needs for intelligent computing and interaction in complex scenarios.
Description of sampling procedures	—

Explanation of deviations from standard methods	—
Description of testing location	—
Remark	—

Detection Tool Information

Scan Tool Information	
Tool Name	Remote Security Assessment System
Tool ID	VGDW-0058
Tool Number	NX3
System Version	V6.0R04F03SP06
System Plugin Version	V6.0R02F01.3809
Web Plugin Version	V6.0R02F01.4004
Factory Version	V6.0R03F00
Tool HASH	8BA4-EA90-4EF0-4B1A
Supplier	NSFOCUS
Vulnerability Library	
Total Number of Plugins	2562
Total number of vulnerabilities (system/application)	360975(358866/2109)
Corresponding CVE number	82598
Vulnerability Library Update Time	2025-6-3
Supplier	NSFOCUS

Network Performance Analysis System	
Device Name	Colasoft nChronos
Product Version	V7.0(Build 6.3.2.20356)
Expert Analyzer Version	15.2.0(Build 15231)
Supplier	Colasoft

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
6.1	**[ACM] Access control mechanism**		
6.1.1	**[ACM-1] Applicability of access control mechanisms** The equipment shall use access control mechanisms to manage entities' access to security assets, network assets, and privacy assets, except for access to security assets or network assets where: — public accessibility is the equipment's intended functionality; or — physical or logical measures in the equipment's targeted operational environment limit their accessibility to authorized entities; or — legal implications do not allow for access control mechanisms.	**Conceptual Assessment** There are access control mechanisms to manage entities' access to security assets: WLAN hotspot passwords, trusted CA certificates, public key certificates for creating TLS connections, Bluetooth keys, and user credentials; there are access control mechanisms to manage entities' access to network assets: WLAN configurations, paired devices, and Ethernet; there are access control mechanisms to manage entities' access to privacy assets: Google account information, Location information. **Functional Completeness Assessment** All discovered security assets are documented in [E.Info.ACM-1.SecurityAsset], all discovered network assets are documented in [E.Info.ACM-1.NetworkAsset], and all discovered privacy assets are documented in [E.Info.ACM-1.PrivacyAsset]. **Functional Sufficiency Assessment** There is no evidence that the access control mechanisms documented in [E.Info.ACM-1.SecurityAsset.ACM], [E.Info.ACM-1.NetworkAsset.ACM], or [E.Info.ACM-1.PrivacyAsset.ACM] are not implemented.	P
6.1.2	**[ACM-2] Appropriate access control mechanisms** Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets, network assets, and privacy assets.	**Conceptual Assessment** Security Assets: WLAN hotspot password: Only administrators who have successfully logged into the device can view or change the hotspot password; Trusted CA certificate: Users or guests who have successfully logged into the device can view, disable, or enable the certificate, but cannot delete it; Public key certificates used to create TLS connections: TLS key access is restricted by process labels and key file access policies, and is encapsulated and managed by the hardware security module; Bluetooth keys: The Bluetooth key is hosted by the system Bluetooth stack, and user space processes cannot access the key content, ensuring the isolation and confidentiality of the key during storage and use; User credentials: Only users or guests wh	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		o have successfully logged into the equipment can access it. Network Assets: WLAN Configuration: Administrators can view network configuration information or change the connected network through the user interface, while other users or guests can only view the name of the currently connected network; Paired devices: Only users and guests who have successfully logged into the equipment can view or change paired device information through the user interface; Ethernet: Only users and guests who have successfully logged into the equipment can view the current Ethernet connection information or turn off Ethernet through the user interface. Privacy Assets: Google account information: Only users or visitors who have successfully logged into the equipment can view or change the corresponding Google account. Location Information: Runtime permissions are assigned to executable software. **Functional Sufficiency Assessment** For each security asset documented in [E.Info.ACM-2.SecurityAsset], network asset documented in [E.Info.ACM-2.NetworkAsset], and privacy asset documented in [E.Info.ACM-2.PrivacyAsset], the validation in the relevant assessment unit for the implementation category is successful.	
6.1.3	**[ACM-3] Default Access Control for Children's Toys** If the device is a toy, for each privacy feature where a child can access external content and access by the child is governed by the access control mechanisms required by ACM-1, the access control mechanisms should, by default, ensure that external content accessed by the child through the privacy feature is limited to content from authorized entities.	The device is not a toy.	N
6.1.4	**[ACM-4] Default Access Controls for Child Privacy Assets in Toys and Childcare Devices** If the device is a toy or childcare device, any access control mechanisms for child privacy features and personal information processed by the device required by ACM-1 shall, by default, restrict access to child privacy features and personal information processed by the	This device is not a toy or a child care device.	N

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
	device to any third party other than the child or their parent/guardian, except for authorized access necessary for the intended function of the device.		
6.1.5	**[ACM-5] Parent/Guardian Access Control for Children's Toys** If the device is a toy, then for each security and privacy asset accessible to a child, any access control mechanisms required by ACM-1 that govern child access should be configured by the authorized entity to restrict access to protected security and privacy assets.	The device is not a toy.	N
6.1.6	**[ACM-6] Parent/Guardian Access Control for Other Entities Accessing Managed Child Toy Privacy Assets** If the device is a toy, for each child privacy asset that is accessible to entities other than the child or their parent/guardian, and for which ACM-1 requires access by these other entities to be managed under access rights, an access control mechanism shall be configurable by authorized entities to restrict access to the managed child privacy assets by these other entities.	The device is not a toy.	N
6.2	**[AUM] Authentication mechanism**		
6.2.1	**[AUM-1] Applicability of authentication mechanisms**		
6.2.1.1	**[AUM-1-1] Requirement network interface** Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to: — read confidential network function configuration or confidential security parameters; or — modify sensitive network function configuration or sensitive security parameters; or — use network functions or security functions, except for access: — to network functions or network function configuration where the absence of authentication is required for the equipment's intended functionality; or — via networks where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorised entities.	The device does not have network interface authentication, so this is not applicable.	N

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
6.2.1.2	**[AUM-1-2] Requirement user interface** Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to: — read confidential network function configuration or confidential security parameters; or — modify sensitive network function configuration or sensitive security parameters; or — use network functions or security functions, except for access: — where physical or logical measures in the equipment's targeted operational environment limit accessibility to authorized entities; and except for read only access to network functions or network functions configuration where access without authentication is needed: — to enable the intended equipment functionality; or — because legal implications do not allow for authentication mechanisms.	**Conceptual Assessment** The device's access control mechanism uses screen unlocking, and only with the correct pattern, PIN code, or password can the device be accessed as a different user or guest. **Functional Completeness Assessment** There is no evidence that the access control mechanisms required by ACM-1 are not documented in [E.Info.AUM-1-2.ACM] for managing entities to access confidential personal information, confidential network function configuration, confidential privacy function configuration, or confidential security parameters; or to modify sensitive personal information, sensitive network function configuration, sensitive privacy function configuration,or sensitive security parameters; or to use the user interface of a network function, privacy function, or security function. **Functional Sufficiency Assessment** For each access control mechanism documented in [E.Info.AUM-1-2.ACM], each managed access to a privacy asset through the user interface documented in [E.Info.AUM-1-2.ACM.ManagedAccessPrivacyAsset], and each managed access to a security asset through the user interface documented in [E.Info.AUM-1-2.ACM.ManagedAccessSecurityAsset], access the corresponding network asset, security asset, and privacy asset and verify that an authentication mechanism is implemented.	P
6.2.2	**[AUM-2] Appropriate authentication mechanisms**		
6.2.2.1	**[AUM-2-1] Single-Factor Authentication Requirements** If the device is a toy, for each child privacy asset that is accessible to entities other than the child or their parent/guardian, and for which ACM-1 requires access by these other entities to be managed by access rights, an access control mechanism shall be configurable by the authorized entity to restrict access to the managed child privacy asset by these other entities.	**Conceptual Assessment** Users or visitors need to draw the correct pattern, or enter the correct PIN or password for authentication to access the device. **Functional Sufficiency Assessment** For each authentication mechanism required by AUM-1-1 (network interface) or AUM-1-2 (user interface) as documented in [E.Info.AuthenticationMechanism], AUM-2-1, perform au	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		thentication to confirm that the authentication mechanism is as documented.	
6.2.2.2	**[AUM-2-2] Two-factor authentication requirements** If the intended function of the primary device is to specifically process special categories of personal information, then for each access to special categories of personal information through the user interface of a network interface, the authentication mechanism should support verification of the entity's claims by evidence generated by at least two of the following elements: knowledge, possession, and innateness (two-factor authentication).	The primary intended function of the device does not involve processing special categories of personal information and is therefore not applicable.	N
6.2.3	**[AUM-3] Authenticator validation** Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use.	**Conceptual Assessment** The user draws a pattern, enters a PIN or password on the login interface. After the device collects it, it will compare it with the authenticator stored internally. Only the authenticator that is exactly the same as the one on the device can be accessed. **Functional Sufficiency Assessment** It was found that each authentication mechanism documented in [E.Info.AUM-3.AUM] was confirmed successful in the assessment unit associated with the implementation category.	P
6.2.4	**[AUM-4] Changing authenticators** Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change.	**Conceptual Assessment** Users or visitors need to draw the correct pattern or enter the correct PIN or password for authentication. Only users who have successfully logged into the device can change the authenticator. **Functional Sufficiency Assessment** There is no evidence that changing the authenticator deviates from [E.Info.AUM-4.AUM.AuthChange].	P
6.2.5	**[AUM-5] Password strength**		
6.2.5.1	**[AUM-5-1] 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.	The device does not have a factory default password set, so it does not apply.	N

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
6.2.5.2	**[AUM-5-2] 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 authorised entities; or — be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.	**Conceptual Assessment** Users or guests can only set passwords after successfully logging into the device, not through the network. **Functional Sufficiency Assessment** There is no evidence that the implementation of non-default passwords for authentication mechanisms deviates from [E.Info.AUM-5-2.AUM.Pwd Property].	P
6.2.6	**[AUM-6] Brute force protection** Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks.	**Conceptual Assessment** The device's authentication mechanism is capable of resisting brute force attacks. In the first 10 attempts, the user will be restricted to logging in for 30 seconds for every 5 incorrect attempts, and each subsequent error will be restricted to 30 seconds. **Functional Sufficiency Assessment** Each verification mechanism documented in [E.Info.AUM-6.AUM] is confirmed to be successful in the assessment unit associated with the implementation category.	P
6.3	**[SUM] Secure update mechanism**		
6.3.1	**[SUM-1] Applicability of update mechanisms** The equipment shall provide at least one update mechanism for updating software, including firmware, affecting security assets and/or network assets, except for software: — where functional safety implications do not allow updatability; or — which is immutable; or — where alternative measures protect the affected security assets and/or network assets during the entire lifecycle of the equipment.	**Conceptual Assessment** The device provides a local manual update mechanism. Update steps: 1. Connect a USB drive (containing a dedicated system package) to the device's USB port. 2. The system will detect the USB drive file and prompt you to update. 3. Confirm the update. 4. The device will automatically restart after the update is complete. **Functional Sufficiency Assessment** There is no evidence that the update mechanism documented in [E.Info.SUM-1.PartOfSoftw.SUM] cannot successfully install SW-a.	P
6.3.2	**[SUM-2] Secure updates** Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.	**Conceptual Assessment** The device has a local update mechanism, and MD5 checksum verifies its integrity. The firmware package is provided by the manufacturer and	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		can only be updated locally using a USB flash drive to ensure its authenticity. **Functional Sufficiency Assessment** The validation in the relevant assessment units for the implementation category of each update mechanism documented in [E.Info.SUM-2.SUM] was successful.	
6.3.3	**[SUM-3] Automated updates** Each update mechanism that is required per SUM-1 shall be capable of updating the software: — without human intervention at the equipment; or — via scheduling the installation of an update under human approval; or — via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment.	**Conceptual Assessment** Manual local updates do not involve network access. The device will only upgrade after the user uploads the firmware via a USB drive and confirms the update. Update steps: 1. Connect the USB drive to the device's USB port (the USB drive contains a dedicated system package). 2. The system will detect the USB drive file and prompt you to update. 3. Confirm the update. 4. The device will automatically restart after the update is complete. **Functional Sufficiency Assessment** There is no evidence that the implementation of the update mechanism deviates from the requirements of SUM-1 [E.Info.SUM-3.SUM].	P
6.4	**[SSM] Secure storage mechanism**		
6.4.1	**[SSM-1] Applicability of secure storage mechanisms** The equipment shall always use secure storage mechanisms for protecting the security assets, network assets, and privacy assets persistently stored on the equipment, except for persistently stored security assets or network assets where: — the physical or logical measures in the target environment ensures the security asset or network asset stored on the equipment accessibility is limited to authorized entities.	**Conceptual Assessment** The device uses a secure storage mechanism to protect assets stored on the device, including: Security assets: trusted CA certificates, Wi-Fi hotspot passwords, user credentials; Network assets: WLAN configuration, paired devices, Ethernet; Privacy assets: Google account information. **Functional Completeness Assessment** All discovered persistently stored security assets are recorded in [E.Info.SSM-1.SecurityAsset]. All discovered persistently stored network assets are recorded in [E.Info.SSM-1.NetworkAsset]. All discovered persistently stored privacy assets are recorded in [E.Info.SSM-1.PrivacyAsset]. **Functional Sufficiency Assessment** All persistently stored secure assets found are recorded in [E.Info.SSM-1.SecurityAsset], all persistently stor	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		ed network assets found are recorded in [E.Info.SSM1.NetworkAsset], and for each privacy asset recorded in [E.Info.SSM-1.PrivacyAsset], it is functionally confirmed that it is persistently stored only through the secure storage mechanism recorded in [E.Info.SSM-1.PrivacyAsset.SSM].	
6.4.2	**[SSM-2] Appropriate integrity protection for secure storage mechanisms** Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets, network assets, and privacy assets it stores persistently.	**Conceptual Assessment** The device uses a user credential–based encryption mechanism. The assets are encrypted during storage, and user credentials are used to verify user identity. Only after verification is passed, the system allows the use of derived keys to decrypt sensitive information that has been encrypted and protected. This protects security assets WLAN hotspot password, trusted CA certificates, WLAN Configuration, Paired devices, Ethernet, and Google account information. **Functional Sufficiency Assessment** The validation in the relevant assessment units for the implementation category of each secure storage mechanism documented in [E.Info.SSM-2.SSM] was successful.	P
6.4.3	**[SSM-3] Appropriate confidentiality protection for secure storage mechanisms** Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently.	**Conceptual Assessment** The device uses a user credential–based encryption mechanism. The security asset WLAN hotspot password is encrypted during storage, and user credentials are used to verify user identity. Only after verification is passed, the system allows the use of derived keys to decrypt sensitive information that has been encrypted and protected. **Functional Completeness Assessment** The device shall persistently store confidential security parameters,confidential personal information, or confidential privacy feature configurations as listed in [E.Info.SSM-3.SSM.Asset]. **Functional Sufficiency Assessment** For each secure storage mechanism documented in [E.Info.SSM-3.SSM] the confirmations in the implementation category dependent assessment u	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		nits are successful.	
6.5	**[SCM] Secure communication mechanism**		
6.5.1	**[SCM-1] Applicability of secure communication mechanisms** The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces, except for: — communicating security assets or network assets whose transfer is protected by physical or logical measures in the targeted environment that ensure that network assets or security assets are not exposed to unauthorised entities; or — communicating security assets or network assets whose exposure is part of establishing or managing a connection combined with additional measures to authenticate the connection or trust relation.	**Conceptual Assessment** The device uses secure communication mechanisms to ensure the secure communication of the public key and the certificate used to establish a TLS connection, Bluetooth keys, and Google account information. Data transmission between the device browser and the server can be encrypted using TLS 1.2/1.3, ensuring data protection against eavesdropping or tampering during transmission.Data transmission between the device and other paired devices is encrypted using Bluetooth 5.2 Secure Connections, using ECDH-P192 key exchange and AES-128-CCM encryption algorithms to ensure data integrity, authenticity, confidentiality, and protection against replay attacks during transmission. **Functional Completeness Assessment** All discovered communicated and stored security assets are recorded in [E.Info.SCM-1.SecurityAsset], all discovered security assets are recorded in [E.Info.SCM-1.NetworkAsset], and all discovered privacy assets are recorded in [E.Info.SCM-1.PrivacyAsset]. **Functional Sufficiency Assessment** There is no evidence that the secure communication mechanisms documented in [E.Info.SCM-1.SCM] are not implemented.	P
6.5.2	**[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms** Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and network assets communicated, except for communicating security assets or network assets where: — a deviation from best practice for integrity or authenticity protection is required for interoperability reasons.	**Conceptual Assessment** The device uses PKI-based TLS 1.2/1.3 protocols and utilizes X.509 PKI certificates to ensure data integrity and identity authenticity during transmission. Bluetooth keys are obtained through negotiation is generated through mutual authentication during the pairing process and used to derive session keys. Combined with AES-CCM encryption and message integrity verification, it protects communication data to ensure that the data is not tampered with during transmission an	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		d verifies the authenticity of the data source. **Functional Sufficiency Assessment** Each secure communication mechanism documented in [E.Info.SCM-2.SCM] is confirmed as a success in the assessment unit associated with the implementation category.	
6.5.3	**[SCM-3] Appropriate confidentiality protection for secure communication mechanisms** Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed, except for communicating security assets or network assets where: — a deviation from best practice for protecting confidentiality is required for interoperability reasons.	**Conceptual Assessment** The device uses TLS secure communication to encrypt the entire communication channel using a session key generated through ECDHE negotiation, ensuring the confidentiality of assets during transmission. In classic Bluetooth, the session key derived from the link key is used to encrypt transmitted data, ensuring that the data cannot be read by unauthorized parties during transmission, effectively protecting the confidentiality of communication content. **Functional Sufficiency Assessment** Each secure communication mechanism documented in [E.Info.SCM-3.SCM] was confirmed successful in the assessment unit associated with the implementation category.	P
6.5.4	**[SCM-4] Appropriate replay protection for secure communication mechanisms** Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the network assets communicated against replay attacks, except for communicating security assets or network assets where: — a duplicate transfer does not impose a threat of a replay attack; or — a deviation from best practice for replay protection is required for interoperability reasons.	**Conceptual Assessment** Best practices are employed to protect communication assets from replay attacks. The TLS secure communication mechanism uses implicitly incremented sequence numbers at the record layer. Each message is assigned a unique number, which participates in the AEAD encryption process. The receiver uses integrity checks to ensure that sequence numbers are not reused, thus preventing replay attacks. In classic Bluetooth, the session key derived from the negotiated link key is combined with a unique message counter and Message Integrity Code during message encryption. The receiver uses the verification counter to prevent duplicate messages, effectively preventing replay attacks. **Functional Sufficiency Assessment** Each secure communication mechanism documented in [E.Info.SCM-4.SCM] is successfully validated in the r	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		elevant assessment unit for the implementation category.	
6.6	**[RLM] Resilience mechanism**		
6.6.1	**[RLM-1] Applicability and appropriateness of resilience mechanisms** The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces and return to a defined state after the attack except for: — network interfaces that are only used in a local network that do not interoperate with other networks; or — network interfaces where other devices in the network provide sufficient protection against DoS attacks and loss of essential functions for network operations.	This device connects to the internet via Wi-Fi or Ethernet, has no open ports, and offers no server-side interface. It typically resides in a private network address space assigned by a router, making it impossible to directly connect to the device and locate and launch targeted DoS attacks. Routers have network-layer access control and traffic isolation mechanisms,which provide sufficient DoS protection, so this scenario is not applicable.	N
6.7	**[NMM] Network monitoring mechanism**		
6.7.1	**[NMM-1] Applicability and appropriateness of network monitoring mechanisms** If the equipment is a network equipment, the equipment shall provide network monitoring mechanism(s) to detect for indicators of DoS attacks in the network traffic between networks which it processes.	The device is not a network device and is not applicable.	N
6.8	**[TCM] Traffic control mechanism**		
6.8.1	**[TCM-1] Applicability of and appropriate traffic control mechanisms** If the equipment is a network equipment, the equipment shall provide network traffic control mechanism(s).	The device is not a network device and is not applicable.	N
6.9	**[LGM] Logging mechanism**		
6.9.1	**[LGM-1] Applicability of Logging Mechanisms** Devices should use logging mechanisms to record internal activities related to privacy assets and their protection (hereinafter referred to as events), with the following exceptions: — Internal activities where logging is prohibited by law.	**Conceptual Assessment** The device uses system logging, stored in /data/local/yslogs/logcat/. In addition, Google provides the my activity:google.com URL to record all account activity. **Functional Sufficiency Assessment** There is no evidence that the logging mechanism documented in [E.Info.LGM-1.PrivacyAssetEvent.LGM] is not implemented.	P
6.9.2	**[LGM-2] Persistent Storage of Log Data** The logging mechanism required by LGM-1 should store log data for relevant events in persistent storage on the device, with the following exceptions: — Relevant log data is stored externally to the device.	**Conceptual Assessment** After the log stored by the log mechanism is opened, the log storage location is ./data/local/yslogs/logcat/. After clicking Export log, a copy of the log will be copied to sdcard/Download. **Functional Sufficiency Assessment** There is no evidence that the processing of log data for relevant events	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		deviates from [E.Info.LGM-2.LGM.InternalStorage].	
6.9.3	**[LGM-3] Minimum Number of Persistently Stored Events** As required by LGM-1, all log data stored in device persistent storage via the logging mechanism must always include: — A minimum number of recent events; and — The most recent event.	**Conceptual Assessment** The total size of logs stored in the device's persistent storage through the logging mechanism is 100MB. If the size exceeds 100MB, the oldest file will be cleared. A single file cannot exceed 10MBand is checked every half hour. **Functional Sufficiency Assessment** The number of logged events concurrently persistently stored on the device is no less than the quantity specified in [E.Info.LGM-3.Quantity].	P
6.9.4	**[LGM-4] Time-Related Information for Persistently Stored Log Data** As required by LGM-1, all log data stored in the device's persistent storage by the logging mechanism should include: — A timestamp if real-time information is available on the device; and — Time-related information may be used if real-time information is not available on the device.	**Conceptual Assessment** By default, the log data stored by the logging mechanism in the device's persistent storage includes a timestamp (accurate to milliseconds), log level (Verbose/Debug/Info/Warn/Error), process name,thread ID, tag, and specific content. **Functional Sufficiency Assessment** For each logging mechanism documented in [E.Info.LGM-4.LGM], confirm that the log data stored persistently on the device includes the timestamp documented in [E.Info.LGM-4.LGM.Timestamp] when real-time information is available.	P
6.10	**[DLM] Deletion mechanism**		
6.10.1	**[DLM-1] Applicability of Deletion Mechanisms** Devices should provide a deletion mechanism that allows users to delete personal data and sensitive security parameters stored on the device.	**Conceptual Assessment** The device provides a deletion mechanism that allows users to delete Google account login information, WLAN configuration and user credentials by restoring the factory settings. The device also provide a deletion mechanism that allows users to delete WLAN configuration by resetting Bluetooth & Wi-Fi. **Functional Completeness Assessment** All personal data found is recorded in [E.Info.DLM-1.PersonalData], and all sensitive security parameters found are recorded in [E.Info.DLM-1.SenSecParam]. **Functional Sufficiency Assessment**	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		For each deletion mechanism recorded in [E.Info.DLM-1.DLM], verify that the deletion mechanism is implemented on the device.	
6.11	**[UNM] User notification mechanism**		
6.11.1	**[UNM-1] Applicability of User Notification Mechanisms** Devices should provide user notification mechanisms to notify device users of changes that affect the protection or privacy of personal information, except for the following: There are other methods of notifying users that do not involve the device.	**Conceptual Assessment** The device provides user notification mechanisms. The Google privacy policies notify device users of collection and processing of personal data. Software on the device obtains explicit user authorization to access location. **Functional Completeness Assessment** All discovered personal information is recorded in [E.Info.UNM-1.PersonalInformation], and all discovered use cases are recorded in [E.Info.UNM-1.PersonalInformation.UseCase]. **Functional Sufficiency Assessment** The use case documented in [E.Info.UNM-1.PersonalInformation.UseCase] is covered by the user notification mechanism documented in [E.Info.UNM-1.PersonalInformation.UseCase.Notification].	P
6.11.2	**[UNM-2] Appropriate User Notification Content** As required by UNM-1, the notification content provided by the user notification mechanism should include at least the following: — A description of the change; and — An explanation of how the change will affect the protection and privacy of personal information.	**Conceptual Assessment** Privacy Policy: If personal data is updated, the user will be notified through the Google Privacy Statement. Location authorization information: When the software on the device obtains explicit user authorization to access location, a pop-up notification about the location permission will appear on the screen. **Functional Sufficiency Assessment** There is no evidence that the implementation of the user notification mechanism deviates from [E.Info.UNM-2.Notifications].	P
6.12	**[CCK] Confidential cryptographic keys**		
6.12.1	**[CCK-1] Appropriate CCKs** Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits, except for: — CCKs that are solely used by a specific security mechanism, where a deviation is identified and justified under the terms of sections	**Conceptual Assessment** The device uses the TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 cipher suite with a security strength of 256 bits.The Bluetooth Link Key type is the Authenticated Combination Key, P-192, whose length is 128 bits. The symmetrical eq	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
	ACM or AUM or SCM or SUM or SSM.	uivalent security strength of P-192 curve is approximately 96 bits. To maintain compatibility with earlier devices, the device continues to use P-192, so it is not applicable. The type of encryption keys in secure storage mechanism is AES-256-XTS with a 256-bit security strength. **Functional Completeness Assessment** All discovered CCKs are recorded in [E.Info.CCK-1.CCK]. **Functional Sufficiency Assessment** The length of any CCK recorded in [E.Info.CCK-1.CCK] is consistent with the documentation.	
6.12.2	**[CCK-2] CCK generation mechanisms** The generation of confidential cryptographic keys shall adhere to best practice cryptography, except for: — the generation of CCKs for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.	**Conceptual Assessment** The device's TLS_CHACHA20_POLY1305_SHA256 suite generates session keys using the ECDHE protocol, employs a temporary key exchange mechanism to ensure forward secrecy, and authenticates the server using RSA certificates. Its key negotiation relies on a secure random number source to ensure unpredictable key material. CHACHA20_POLY1305 is then used for encryption and integrity protection, and SHA-256 is used as the hash algorithm for the handshake and digital signature. This key generation and encryption scheme fully complies with current cryptographic best practices, avoiding the security risks associated with fixed key exchange methods and providing eavesdropping, tamper resistance, and high security. Therefore, there are no deviations. Bluetooth's Authenticated Combination Key (P-192) is generated through ECDH operations on the elliptic curve P-192. It relies on a random number source on both devices to generate a private key and exchange a public key. Based on identity authentication,a shared secret is generated as the Link Key, which is used to derive session keys for AES-CCM encryption and integrity protection. This scheme is applicable only to Bluetooth secure communication mechanisms and is therefore not applicable. Generation mechanism of encryption keys in secure	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		storage mechanism uses two independent keys generated from a root or protected key material through a standardized KDF. The derivation process includes structured encoding, block-level processing, and algorithmic transformations. **Conceptual completeness assessment of documentation** The device does not have a secret encryption key generation mechanism not documented in [E.Info.CCK-2. Generation].	
6.12.3	**[CCK-3] Preventing static default values for preinstalled CCKs** Preinstalled confidential cryptographic keys shall be practically unique per equipment, except for: — CCKs that are only used for establishing initial trust relationships under conditions controlled by an authorized entity; or — CCKS key are shared parameters required for the equipment's intended functionality	This device does not have pre-installed CCK and is not applicable	N
6.13	**[GEC] General equipment capabilities**		
6.13.1	**[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities** The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and network assets, except for vulnerabilities: — that cannot be exploited in the specific conditions of the equipment; or — that have been mitigated to an acceptable residual risk; or — that have been accepted on a risk basis.	The Android system protects secure and network assets through multiple layers of software mechanisms (such as runtime permissions and encrypted storage) and continuous updates (such as security patches and Play Protect). Users should remain vigilant, promptly update the system, and review application permissions. Developers should adhere to secure coding standards to mitigate vulnerabilities at the source. The discovered vulnerabilities, including the ICMP timestamp request response vulnerability and the vulnerability that allows traceroute detection, are considered low risk and acceptable.	N
6.13.2	**[GEC-2] Limit exposure of services via related network interfaces** In factory default state the equipment shall only expose — network interfaces; and — services via network interfaces affecting security assets or network assets which are necessary for equipment setup or for basic operation of the equipment.	**Conceptual Assessment** Wi-Fi, LAN, and Bluetooth are enabled by factory default. Affecting security, network, and privacy assets is necessary for device setup or basic operation. **Functional Completeness Assessment** Each discovered network interface or service (via a network interface) is exposed in [E.Info.GEC-2.Network Interface.Exposure] by factory default and is required for setup accordin	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		g to [E.Info.GEC-2.Setup] or basic device operation.	
6.13.3	**[GEC-3] Configuration of optional services and the related exposed network interfaces** Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service.	**Conceptual Assessment** Security assets, network assets, and privacy assets are affected by Wi-Fi, LAN, and Bluetooth. Authorized users are provided with the option to enable and disable network interfaces or services. **Functional Completeness Assessment** An optional network interface or optional service exposed (via a network interface) not listed in [E.Info.GEC-3.NetworkInterface.Exposure] was not discovered. **Functional Sufficiency Assessment** All optional network interfaces or optional services exposed (via a network interface) are configurable, with options to enable and disable the network interface or service, or as specified in [E.Info.GEC-3.NetworkInterface.Exposure] only authorized users can change the state of an optional network interface or optional service exposed (via a network interface) to enabled or disabled.	P
6.13.4	**[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces** The equipment's user documentation shall contain a description of — all exposed network interfaces; and — all services exposed via network interfaces, which are delivered as part of the factory default state.	According to Annex ZA of EN 18031-1:2024, clause GEC-4 is not referenced to any essential requirements of Directive 2014/53/EU Article 3 (3)(d), (e), or (f). Therefore, this clause is not applicable for RED compliance evaluation.	N
6.13.5	**[GEC-5] No unnecessary external interfaces** The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.	**Conceptual Assessment** The device's Wi-Fi antenna, LANUSB, TYPE-C, HDMI-OUT, Audio,POWER, DC are necessary for intended functions. **Functional Completeness Assessment** All discovered physical external interfaces are recorded in [E.Info.GEC-5.PhysicalExternalInterface].	P
6.13.6	**[GEC-6] Input validation** The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network as	**Conceptual Assessment** The device uses regular expressions to filter user input, and non-compliant input will be automatically reject	P

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
	sets.	ed. Using a self-developed keyboard fuzzing script, random characters and abnormal sequences were injected into the input interface for verification. The system maintained normal responses throughout the process without any abnormal behavior. Using a self-developed Wi-Fi fuzzing script, malformed 802.11 frames and randomized protocol fields were continuously injected into the target device for verification. Throughout the fuzzing process, the target device maintained normal operation without crashes, resets, or functional abnormalities. Based on the consistency of the protocol, the LAN interface verifies the length and validity of the packet. During the testing process, it was found that the device initiates a security pairing procedure when establishing a classic Bluetooth (BR/EDR) connection, requiring both parties to compare and confirm a visual pairing code. Without completing this manual confirmation step, the Bluetooth link cannot transition to a paired or encrypted state, and the controller will directly reject subsequent RFCOMM/L2CAP connection requests. As a result, under unpaired conditions, external devices cannot establish an effective data channel with the target device. All fuzzing-generated input packets fail to reach the upper protocol stack or application layer, rendering test actions unable to effectively engage the device's processing logic. **Functional Completeness Assessment** All discovered external interfaces are documented in [E.Info.GEC-6ExternallInterface]. **Functional Sufficiency Assessment** There is no evidence that any input validation test successfully compromises, extracts, or misuses any security asset described in [E.Info.GEC-6.SecurityAsset], any network asset described in [E.Info.GEC-6.NetworkAsset], or any privacy asset describe	

EN 18031-1-2024、EN 18031-2-2024			
No	Test items and requirements	Test results	Judgment
		d in [E.Info.GEC-6.PrivacyAsset].	
6.13.7	**[GEC-7] Documenting External Sensing Capabilities** All external sensing capabilities in a device that are relevant to the user or subscriber's privacy should be documented for the user.	According to Annex ZA of EN 18031-1:2024, clause GEC-7 is not referenced to any essential requirements of Directive 2014/53/EU Article 3(3)(d), (e), or (f). Therefore, this clause is not applicable for RED compliance evaluation.	N
6.14	**[CRY] Cryptography**		
6.14.1	**[CRY-1] Best practice cryptography** The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets, except for: — cryptography used for a specific security mechanism, where a deviation is identified and justified under the terms of sections ACM or AUM or SCM or SUM or SSM.	**Conceptual Assessment** The device uses best cryptographic practices to protect secure or privacy assets. Cipher suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 The Bluetooth Authenticate Combination Key (P-192) is used only for Bluetooth secure communication mechanisms and is not applicable. The Bluetooth encryption algorithm to ensure the integrity, authenticity, and confidentiality of Bluetooth communication data during transmission is AES-128-CCM. The MD5 is only used to perform a consistency check against the manufacturer-provided checksum to confirm the firmware used for updating has not been corrupted or modified during copying or storage, and the integrity and authenticity of the firmware are fundamentally ensured by the manufacturer distribution process, while. Therefore, it is not applicable. **Functional Completeness Assessment** The cryptographic techniques used on the device are all documented in [E.Info.CRY-1.Assets.Cryptography]. **Functional Sufficiency Assessment** For each cryptographic protection documented in [E.Info.CRY-1.Assets.Cryptography], the implementation does not deviate from the relevant documentation.	P

Sample Photos

Figure 1 Equipment appearance

Figure 2 Equipment nameplate

Sample Photos

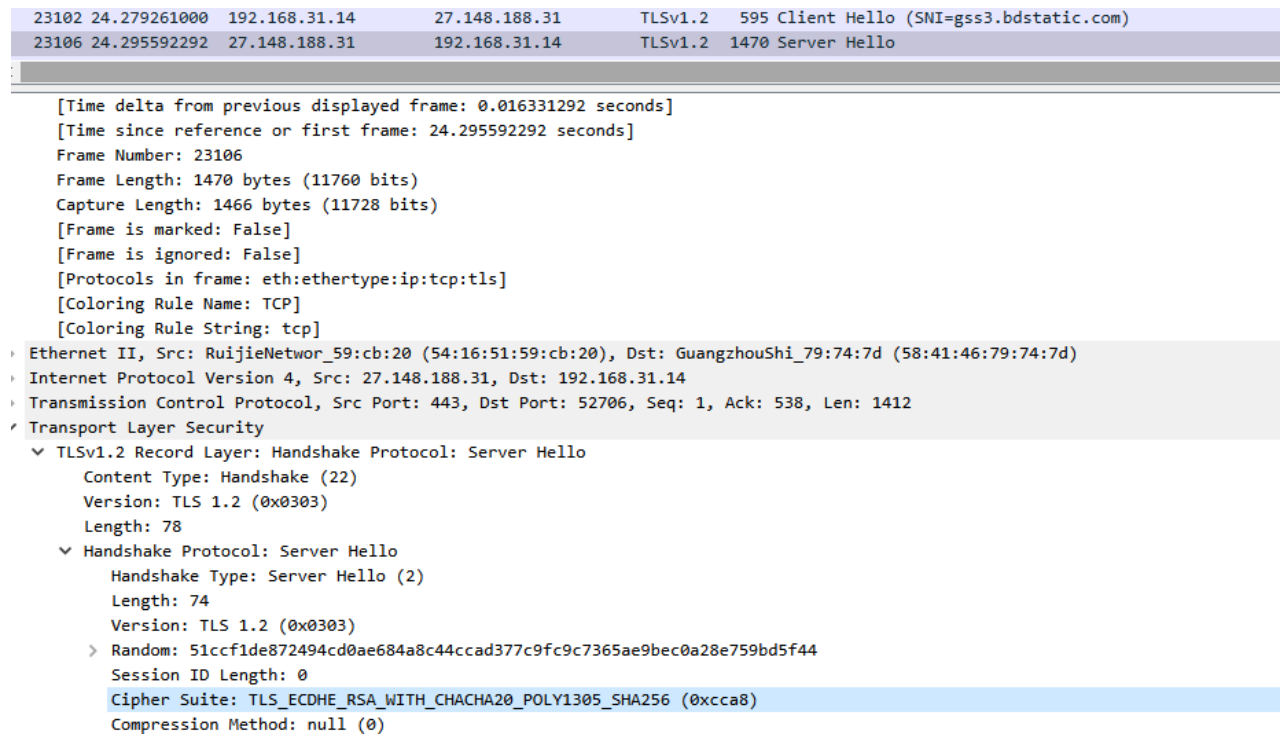

Figure 3 TLS communication encryption suite

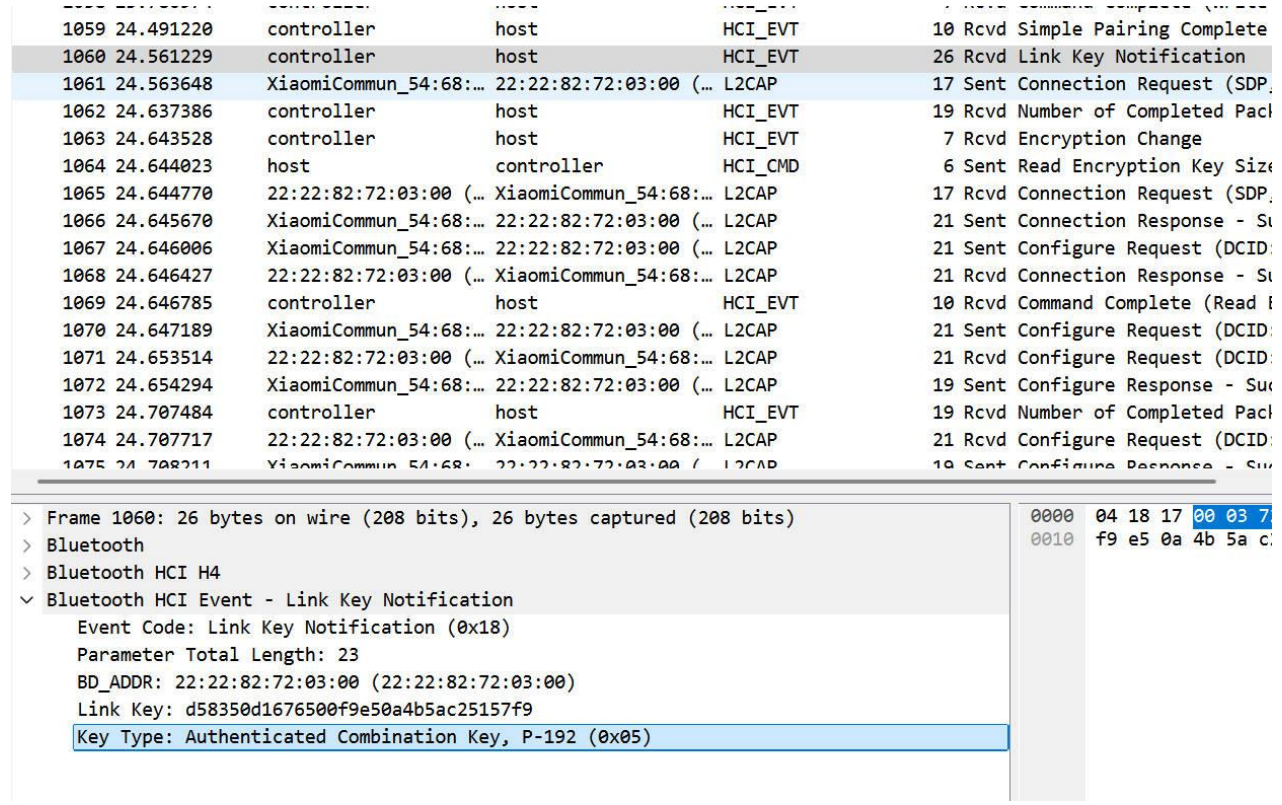

Figure 4 Bluetooth communication link key

Sample Photos

4 Vulnerability Information

Vulnerability Distribution

No	Vulnerability Name	Affects the number of hosts	Percentage of affected hosts	Frequency of occurrence
1	ICMP timestamp request response vulnerability	1/1	100%	1
2	Allow Traceroute detection	1/1	100%	1
Total				**2**

Figure 5 Vulnerability Scanning

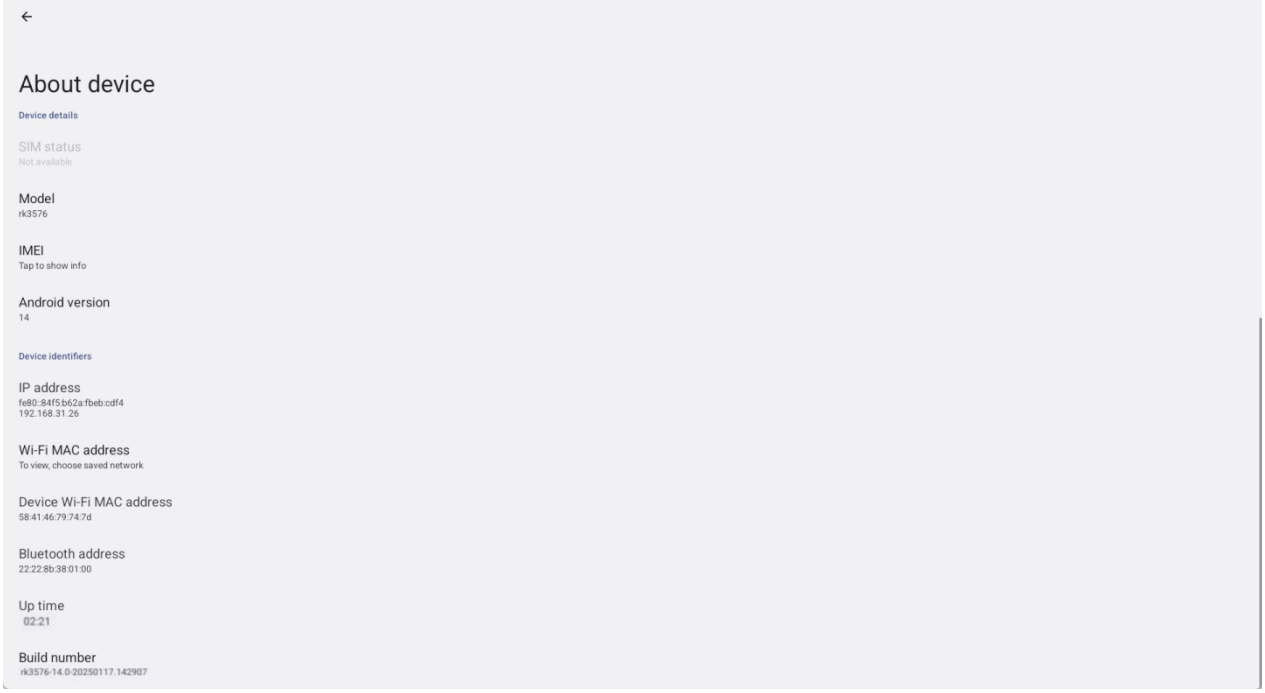

Figure 6 Firmware version before update

Sample Photos

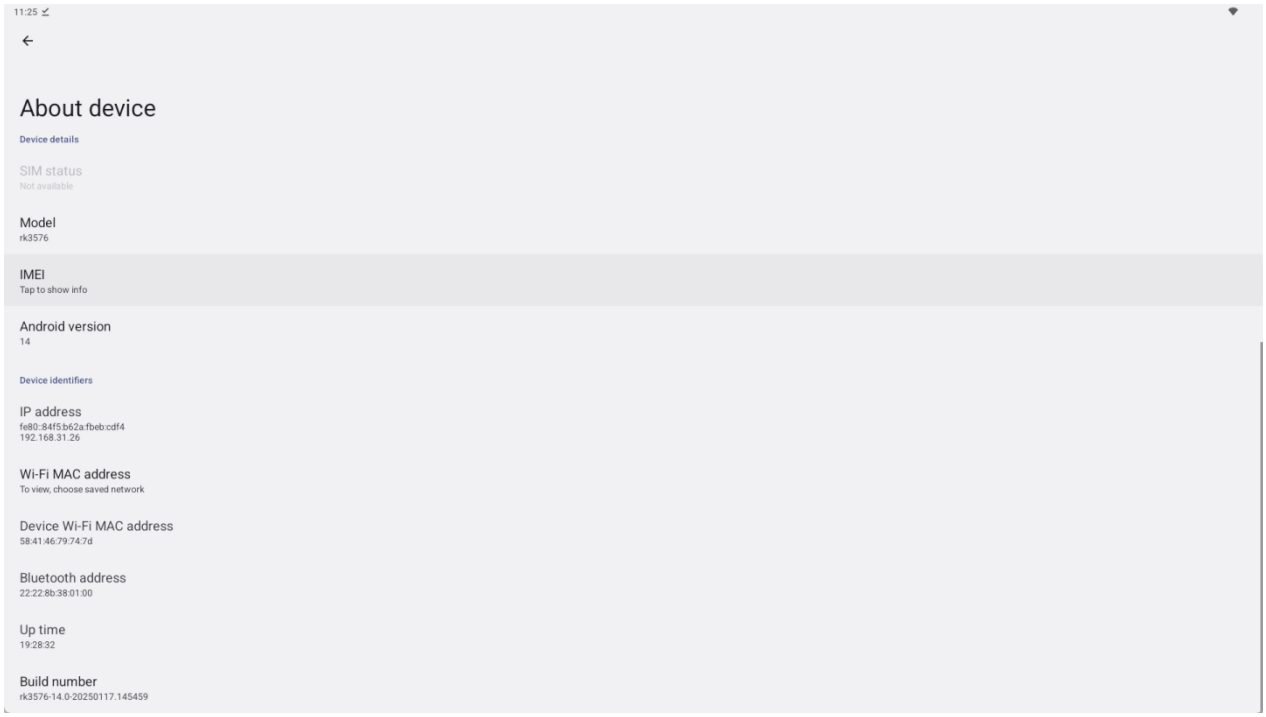

Figure 7 Firmware updated version

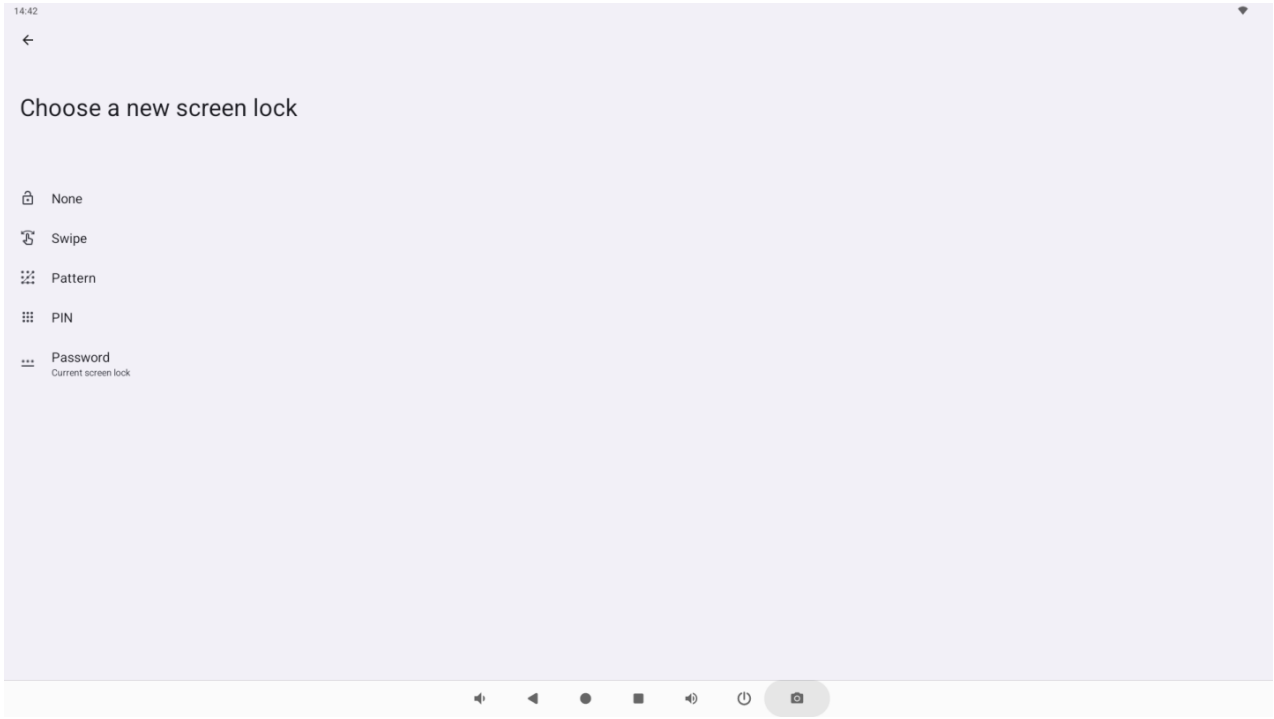

Figure 8 Changing the authenticator

Sample Photos

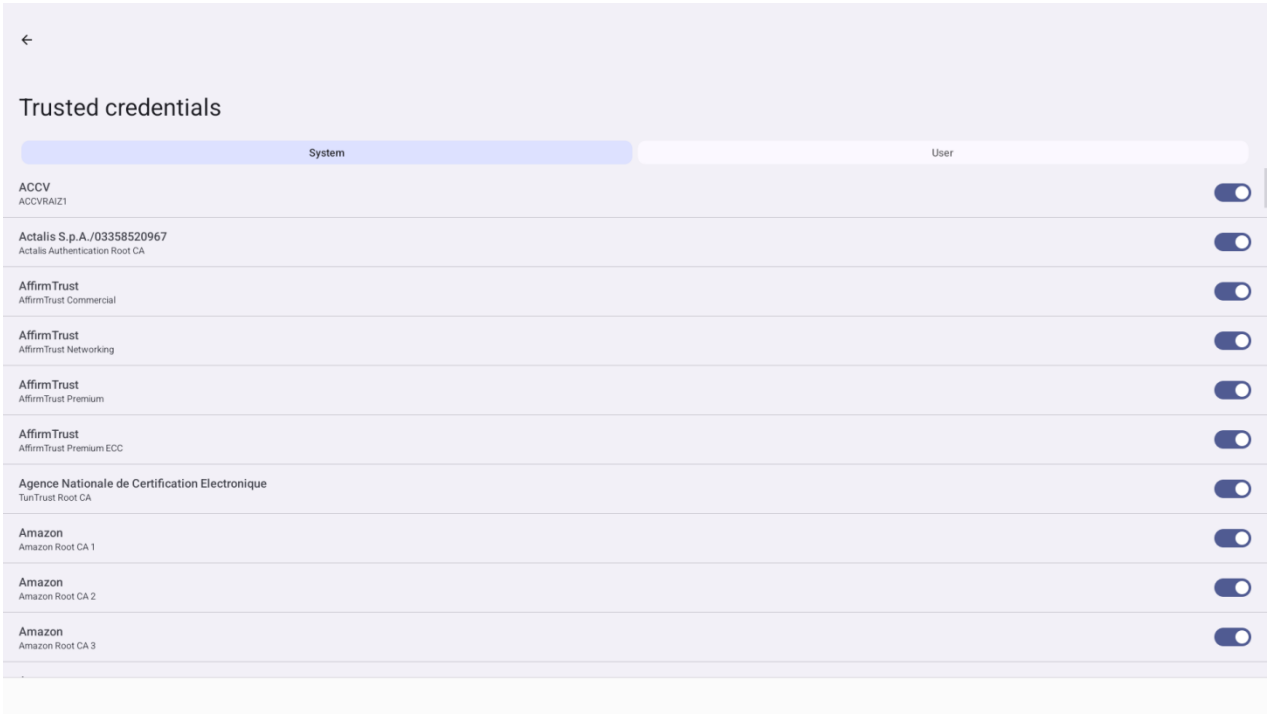

Figure 9 Trusted CA certificate viewing

Figure 10. WLAN hotspot password viewing

Sample Photos

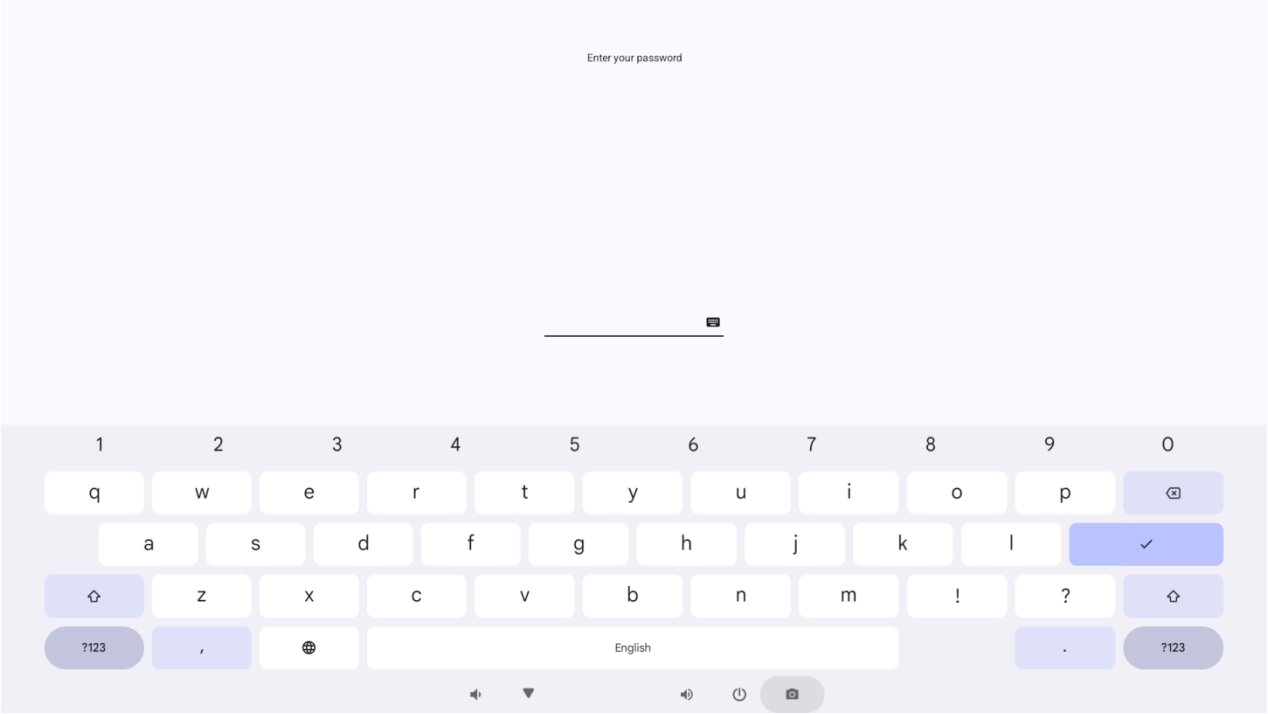

Figure 11 Password authentication

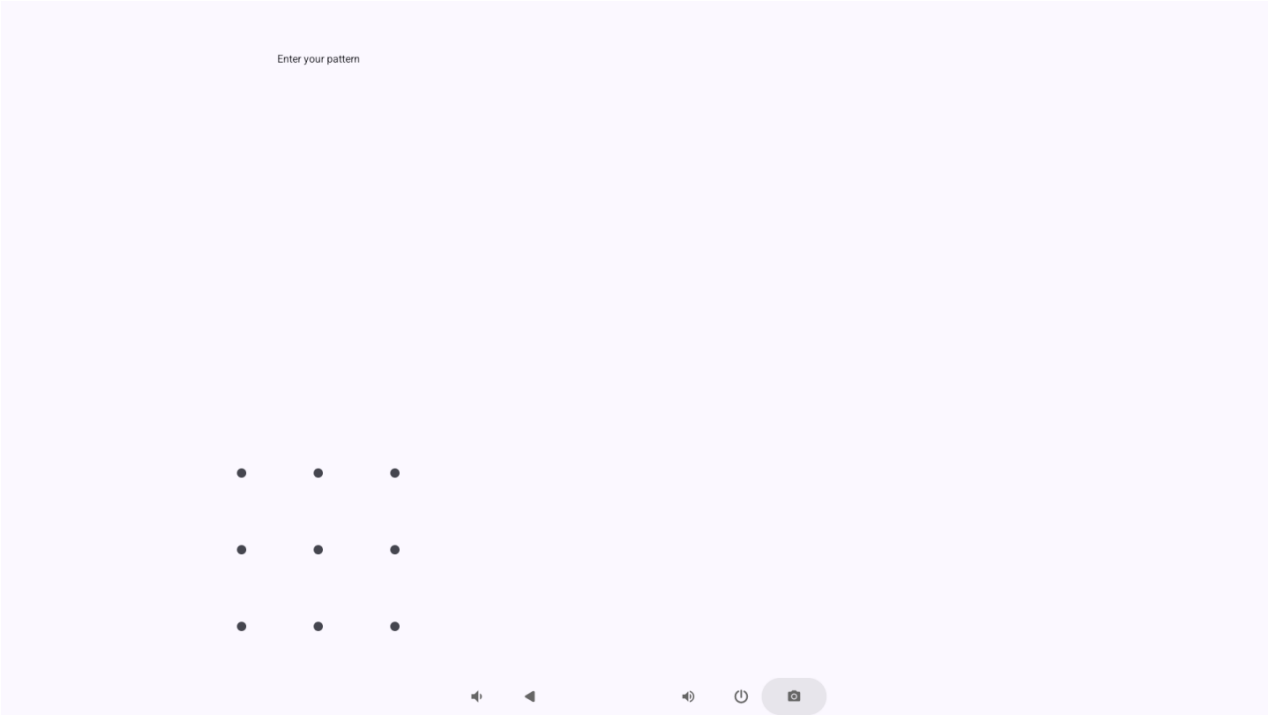

Figure 12 Pattern authentication

Sample Photos

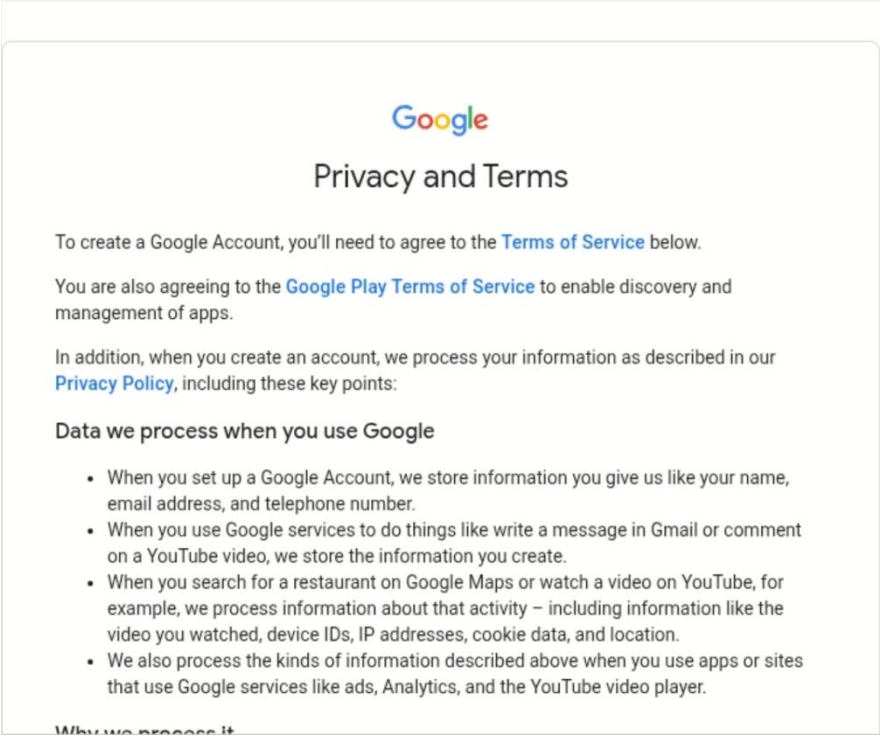

Figure 13 User Notification Mechanism

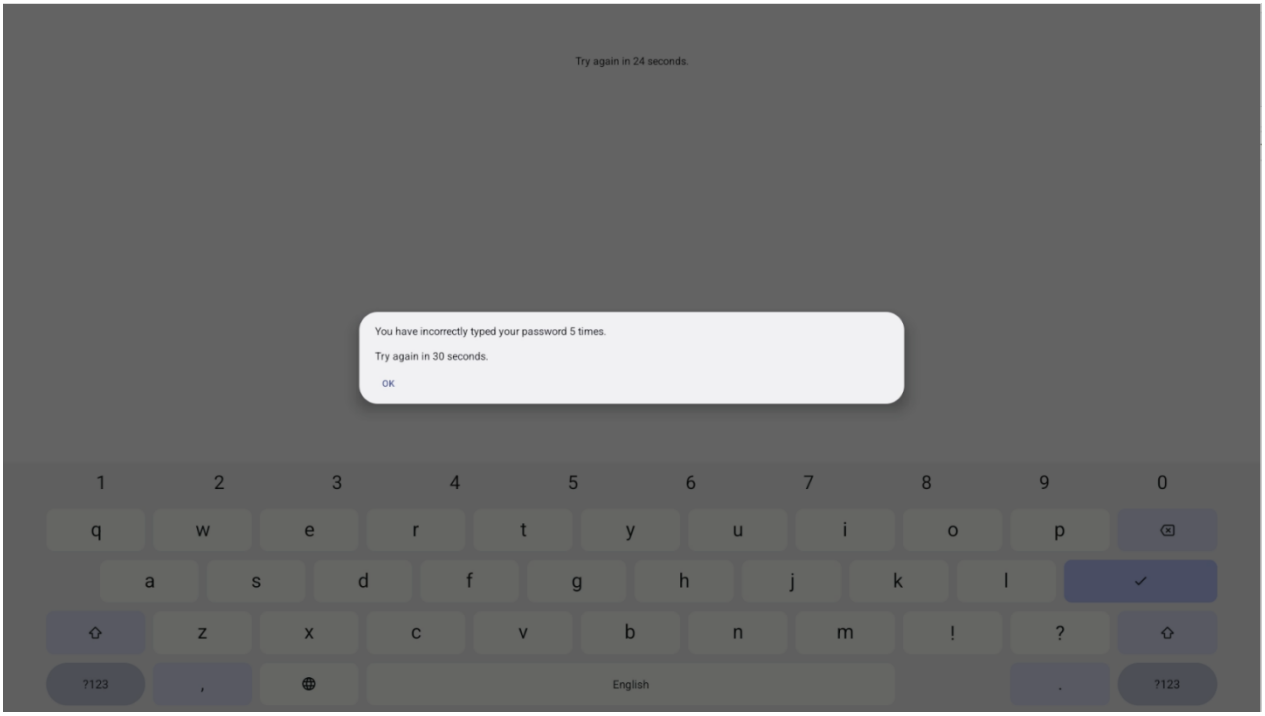

Figure 14 Anti brute force cracking mechanism

Sample Photos

```
11-10 16:16:04.896  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:175 - ### Keystore Watchdog report - END ###
11-10 16:16:04.927  303   303 E keystore2: system/security/keystore2/src/error.rs:180 - system/security/keystore2/src/security_level.rs:622
11-10 16:16:04.927  303   303 E keystore2:
11-10 16:16:04.927  303   303 E keystore2: Caused by:
11-10 16:16:04.927  303   303 E keystore2:     0: system/security/keystore2/src/security_level.rs:620: While generating Key without explicit attestation key.
11-10 16:16:04.927  303   303 E keystore2:     1: Error::Km(r#UNKNOWN_ERROR)
11-10 16:16:06.726  267   267 I servicemanager: Found android.hardware.security.keymint.IRemotelyProvisionedComponent/default in device VINTF manifest.
11-10 16:16:05.431  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:114 - ### Keystore Watchdog report - BEGIN ###
11-10 16:16:05.431  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:123 - When extracting from a bug report, please include this header
11-10 16:16:05.431  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:124 - and all 1 records below.
11-10 16:16:05.432  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:164 - ThreadId(1) Calling get_rkpd_attestation_key() Pending: 501.141666ms Overdue 1.144292ms
11-10 16:16:05.432  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:175 - ### Keystore Watchdog report - END ###
11-10 16:16:06.432  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:114 - ### Keystore Watchdog report - BEGIN ###
11-10 16:16:06.432  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:123 - When extracting from a bug report, please include this header
11-10 16:16:06.432  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:124 - and all 1 records below.
11-10 16:16:06.433  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:164 - ThreadId(1) Calling get_rkpd_attestation_key() Pending: 1.501719042s Overdue 1.001720209s
11-10 16:16:06.433  303  3624 W keystore2: system/security/keystore2/src/watchdog.rs:175 - ### Keystore Watchdog report - END ###
11-10 16:16:06.531  723  2020 D CompatibilityChangeReporter: Compat change id reported: 161252188; UID 1000; state: DISABLED
11-10 16:16:06.531  723  2020 D hxs     : check_packageName = com.android.settings  originalIntent = Intent { act=android.intent.action.MAIN cat=[android.intent.category.LAUNCHER]
flg=0x10200000 cmp=com.android.settings/.Settings bnds=[390,977][770,1039] }  mRequest.callingPackage = com.android.launcher3
11-10 16:16:06.536  723   771 I DropBoxManagerService: add tag=system_app_strictmode isTagEnabled=true flags=0x2
11-10 16:16:06.543  723  2020 I Camera  : callprocess:com.android.settings
```

Figure 15 Event Log

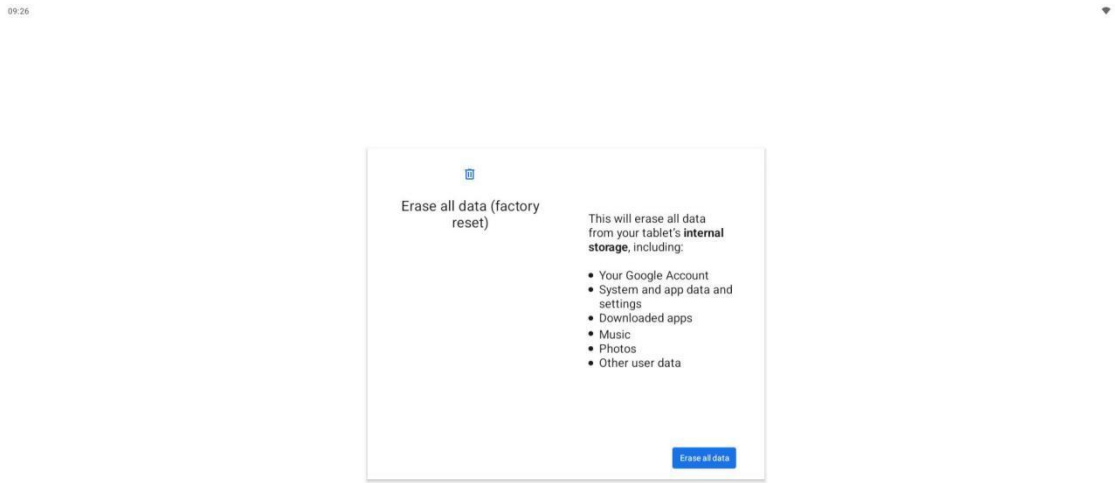

Figure 16 Deletion mechanism - restore the factory settings

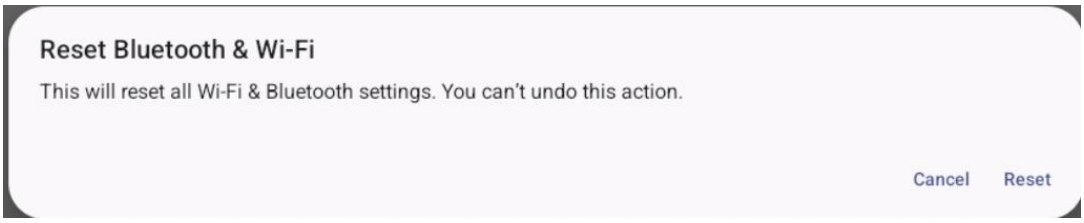

Figure 17 Deletion mechanism - reset Bluetooth & Wi-Fi

Figure 18 Firmware integrity and authenticity checksum

Important

1. The test report is invalid without the official stamp of CVC;
2. Any photocopies or part photocopies of the test report are forbidden without the written permission from CVC;
3. The test report is invalid without the signatures of tester, reviewer and approval;
4. The test report is invalid if altered;
5. Objections to the test report must be submitted to CVC within 15 days;
6. Generally, commission test is responsible for the tested samples only;The sample information is provided by the customer and the laboratory is not responsible for its authenticity;
7. As for the test result, “—”or “N” means “not applicable”, “ / ”means “not test” “P” means “pass” and “F” means “fail”.

The test data and test results given in this test report should only be used for purposes of scientific research, teaching and internal quality control when the CMA symbol is not presented.

Lab Name: CVC Testing Technology Co.,Ltd.
Lab Address: No.3,Tiantaiyi Road, Kaitai Avenue, Science City, Guangzhou, China
Tel：020 32293888
Fax：020 32293889
Post Code：510663
E-mail：office@cvc.org.cn
http://www.cvc.org.cn