Device Certification Questionnaire v3.0 - MDSCert release

Evidence of Compliance to the ETSI TS 103 732-1/TS 103 732-2 and GSMA Requirements

Overview

The general purpose of this document is to provide a natural language translation of the Common Criteria requirements that can be more readily understood. The requirements here are a combination of Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs).

SFRs can generally be considered testable requirements on the device, though this is not always the case. In cases where it is not explicitly testable, generally evidence of meeting the requirement is provided, such as source code or pointing to another evaluation which proves the requirement is met. SFRs are always focused on the device itself, either a software or hardware component of the device which supports a security requirement.

SARs can generally be considered documentation requirements and may be focused on the device, on the production of the device (manufacturing) or in-market support. There may be some device testing done where it is possible to prove a requirement with a test (instead of documentation), but the majority of SARs will not require testing (this may change over time).

Beyond the TS 103 732 requirements, there are additional areas that require documentation to support the security evaluation of the device. These are listed after the TS 103 732 requirements.

How to complete the questionnaire:

TS 103 732 SFR, SAR or GSMA requirement	Requirement description	Supported? (Y/N)
	Evidence required for submission	
	SFR from TS 103 732 or GSMA to be filled out	***Y or N***
	OEM response goes here, depending on evidence requirement either provide a description, documentation or a reference to supporting material to be included with submission of the completed questionnaire.	

Several items will need to be submitted along with the completed questionnaire. These may include, but not limited to:

- Process, policy, procedure, architectural and design documentation
- Source code listings, samples, and repositories
- Configuration data such as kernel defconfigs, bootloader configuration, SELinux policies
- Assessment reports for items such as privileged applications, OTA update services
- Devices configured as production, as well as userdebug, and any custom tools required for loading software

When answering the questionnaire, the set of devices being considered should be limited to those released in the last 12 months or with an impending release. Where appropriate, general responses covering all devices may be provided; device-specific responses should not be needed unless requirement implementation differs significantly.

The ETSI TS 103 732-1 questionnaire sections are grouped as they are in the Protection Profile:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels

The ETSI TS 103 732-2 sections:

- Identification and Authentication

The ETSI TS 103 732-4 sections:

- Applications
- Application Risk

The ETSI TS 103 732-5 sections:

- Bootloader - User Data Protection
- Bootloader - Protection of the TSF
- Bootloader - Life Cycle
- Root of Trust - Protection of the TSF

The GSMA FS.56 sections:

- Cryptographic Support
- Identification and Authentication

- Privacy
- Protection of the TSF
- Live Cycle Requirements

Devices for Certification

The following tables are for specifying the devices that will be certified. Add rows as necessary for each separate device covered in the evaluation.

Evaluated Devices

Device	Operating System	OS Version	Kernel Version
TB711FU	Android	Android 17	6.6

Device	Model(s)	CPU Architecture	CPU
TB711FU	TB711FU	arm64-v8a	MediaTek Dimensity 9500s+

Equivalent Devices

The devices here are claimed by the developer as equivalent to an evaluated device.

Claimed Device	Evaluated Device	Differences between devices
Empty	Empty	Empty

TS 103 732-1 SFRs

Cryptographic Support

This section is focused on the cryptography that is used in the system.This includes both key lifecycles and the cryptographic algorithms that are in use.

The requirements for cryptographic algorithms are open as long as the algorithm is able to meet the requirements set by ISO for adding the algorithm to the ISO standard. Note that this does not mean that the algorithm shall be submitted to ISO for inclusion in their standards, only that it meets those requirements. This ensures that the algorithm has been publicly available and reviewed, and so is considered acceptable for use to meet the security claims of this evaluation.

FCS_RNG_EXT.1	Devices shall provide at least one random number generator (RNG) that produces uniformly-distributed, unpredictable output.	Supported? (Y/N)
	For each RNG on the device, provide a description of the type (such as physical or software) and how the amount of entropy provided has been verified. Common examples of proof would be NIST 800-90B or AIS 31 analysis.	
	FCS_RNG_EXT.1.1 The TSF shall provide a [selection: *physical, deterministic,*] random number generator. **FCS_RNG_EXT.1.2** The TSF shall provide random numbers that meet [hardware noise sources that provide at least .8bits of entropy per bit of output in the SoC and AES-CTR_DRBG in BoringSSL].	Y
	The device uses several different RNGs to provide sufficient entropy during key generation. Normal operating and startup output from the physical source has been checked using the NIST 800-90B entropy test tools to provide sufficient entropy to ensure that the output from the hardware TRNG will provide at least 1 bit of entropy for every bit requested. The DRBG uses 384 bits of input to generate the 256-bit output blocks. The AP output is provided to the system via the	

	getrandom() call in the Linux kernel. This call creates a random stream of bits that can be used as input to a DRBG. The kernel-maintained entropy pool is reseeded every 5 minutes from the SoC TRNG. In Android itself, when a request for a new random string is made, the AES TR_DRBG that is provided as part of the BoringSSL library (libcrypto) is called. This DRBG is seeded by calling the Linux kernel for 384 bits to produce a 256-bit key. Inside the TEE, when a request for a new random string is made, the AES CTR_DRBG that is provided as part of the TEE cryptographic functions is called. This DRBG is seeded by calling the TEE kernel for 384 bits to produce a 256-bit key.	

FCS_CKM.1/Asymmetric	Devices shall generate asymmetric keys properly that can meet at least the equivalent of 128-bit symmetric encryption strength.	Supported? (Y/N)
	The process for generating asymmetric keys on the device shall be explained. This will be specific to the algorithm(s) in use.	
	FCS_CKM.1.1/Asymmetric The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:RSA and ECDSA] and specified cryptographic key sizes [assignment: RSA keys of 3072, 4096, ECDSA keys of P-256, P-384, P-521] that meet the following: [assignment: FIPS 186-5].	Y
	BoringSSL and the TEE support generating RSA and ECDSA keys compliant with NIST FIPS 186-5 that are equivalent (or greater) than 128-bit symmetric strength. BoringSSL supports generating keys that are of 128-bit strength and higher for both RSA and ECDSA. In both cases the DRBG from FCS_RNG_EXT.1 is used in the process.	

FCS_CKM.1/Symmetric	Devices shall generate symmetric keys of at least 128-bit length either by generating the key using a RNG or by a derivation function.	Supported? (Y/N)
	The process for generating the keys on the device shall be explained. For example, the key is generated by calling the RNG.	
	FCS_CKM.1.1/Symmetric The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [using AES CTR_DRBG in BoringSSL] and specified cryptographic key sizes [assignment: 256-bits]	Y
	BoringSSL and the TEE support generating symmetric (AES) keys compliant with NIST FIPS 197 that are equivalent (or greater) than 128-bit symmetric strength. The DRBG from FCS_RNG_EXT.1 is used in the process.	

FCS_COP.1 Note

All the algorithms listed under FCS_COP.1 may have multiple implementations throughout the system. For example, symmetric encryption is likely to be available in low level hardware (i.e. SoC), a hardware storage encryption engine, a hardware-backed key store (if support is provided), the SEE, the kernel and within the main OS itself. Not all algorithms may be available in all components, and different configurations may provide different options.

The expectation for this section is that each instance of an algorithm type be specified if it is key to providing security services for the device (i.e. if an algorithm is available for user-installed applications or is not used by the security components of the device itself, they do not need to be listed).

FCS_COP.1/SigGen	Devices shall support an asymmetric algorithm that is used to verify the signature of update packages (both for the OS and applications). Multiple algorithms may be supported for different purposes.	Supported? (Y/N)

	Each supported algorithm shall be listed along with the key sizes supported. The listing should point to the standard used to implement the algorithm (for example FIPS 186-4 for RSA).	
	FCS_COP.1.1/SigGen The TSF shall perform [*CRYPTOGRAPHIC SIGNATURE SERVICES (GENERATION AND VERIFICATION)*] in accordance with a specified cryptographic algorithm [assignment: RSA , ECDSA using NIST] and cryptographic key sizes [RSA keys 3072-bits or greater, ECDSA using NIST curves P256, P384, P-521] that meet the following: [FIPS PUB 186-5].	Y
	BoringSSL and TEE provide FIPS 186-5 support for both RSA and ECDSA.	

FCS_COP.1/KeyEst	Devices shall support a key establishment algorithm for the encryption/decryption of user data. This shall list the algorithm used for user data encryption in transit, and algorithms used in other parts of the system.	Supported? (Y/N)
	Each supported algorithm shall be listed along with the key sizes supported. The listing should point to the standard used to implement the algorithm (for example FIPS 197 for AES).	
	FCS_COP.1.1/Symmetric The TSF shall perform [*CRYPTOGRAPHIC KEY ESTABLISHMENT*] in accordance with a specified cryptographic algorithm [[Elliptic curve-based key establishment schemes] and cryptographic key sizes [256 bits] that meet the following: [NIST Special Publication 800-56A Y Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”].	Y
	To support TLS communications, BoringSSL supports ECDH key pair generation.	

FCS_COP.1/Symmetric	Devices shall support a symmetric algorithm for the encryption/decryption of user data. This shall list the algorithm used for user data encryption, and algorithms used in other parts of the system.	Supported? (Y/N)
	Each supported algorithm shall be listed along with the key sizes supported. The listing should point to the standard used to implement the algorithm (for example FIPS 197 for AES).	
	FCS_COP.1.1/Symmetric The TSF shall perform [*SYMMETRIC ENCRYPTION AND DECRYPTION*] in accordance with a specified cryptographic algorithm [AES] and cryptographic key sizes [*256-BIT*] that meet the following: [AES as defined in FIPS PUB 197 with CBC (SP800-38A), CCM (SP800-38C), Key Wrap (SP800-38F), GCM (SP800-38D), XTS (SP800-38E) and GCM (SP800-38D) modes].	Y
	Multiple modules provide cryptographic support for symmetric encryption using AES: SOC OTP Stores cryptographic keys utilized by the boot loader and TEE. Android Keymint in TEE Android keystore in TEE to guard cryptographic key storage. File Based Encryption in Storage	

FCS_COP.1/Derivation	Devices shall support a key derivation function.	Supported? (Y/N)
	Each supported function shall be listed along with the key sizes supported. The listing should point to the standard used to implement the algorithm (for example NIST SP 800-108 for KBKDF or NIST SP 800-132 for PBKDF2).	
	FCS_COP.1.1/Derivation The TSF shall perform [*DERIVATION FUNCTION*] in accordance with a	Y

	specified cryptographic algorithm [HMAC-SHA2-256 and scrypt, CMAC-AES] and cryptographic key sizes [128 bits, 256 bits] that meet the following: [NIST SP 800-108 (CMAC-AES, HMAC-SHA2-256) and no standard (scrypt)].	
	BoringSSL and the TEE provide KDF algorithms using NIST SP 800-108.	

FCS_COP.1/Hash	Devices shall support a cryptographic hash algorithm.	Supported? (Y/N)
	Each supported algorithm shall be listed along with the key sizes supported. The listing should point to the standard used to implement the algorithm (for example FIPS 180-4 for SHA).	
	FCS_COP.1.1/Hash The TSF shall perform [*CRYPTOGRAPHIC HASHING*] in accordance with a specified cryptographic algorithm [SHA2-256, 384 and 512] and cryptographic key sizes [*NONE*] that meet the following: [FIPS 180-4].	Y
	BoringSSL and the TEE provide hash algorithms using SHA2	

FCS_COP.1/KeyedHash	Devices shall support a message authentication code algorithm.	Supported? (Y/N)
	Each supported algorithm shall be listed along with the key sizes supported. The listing should point to the standard used to implement the algorithm (for example FIPS 198-1 for HMAC).	
	FCS_COP.1.1/KeyedHash The TSF shall perform [*KEYED-HASH MESSAGE AUTHENTICATION*] in accordance with a specified cryptographic algorithm [HMAC-SHA2-256, 384, 512] and cryptographic key	Y

	sizes [256, 384 and 512 bits] that meet the following: [FIPS 198-1 and FIPS 180-4].	
	BoringSSL and the TEE provide hash algorithms using HMAC SHA2.	

FCS_CKH_EXT.1/Low	Devices shall provide encrypted storage that is not tied to the user credentials. This can require separate apps to explicitly implement the functionality, but it shall be available in the device.	Supported? (Y/N)
	Documentation shall provide: • Description of how DE keys are generated/derived ◦ Algorithms, key lengths used in the process • Description of how DE keys are cryptographically tied to hardware-backed keystore	
	FCS_CKH_EXT.1.1/Low The TSF shall support a key hierarchy for data encryption keys to protect [*LOW USER DATA ASSETS*]. **FCS_CKH_EXT.1.2/Low** The TSF shall ensure that all keys in the key hierarchy are derived and/or generated according to [file encryption keys are generated using AES_CTR DRBG from BoringSSL and are encrypted using a key that is derived from the DUK] ensuring that the key hierarchy uses the DUK and [NO USER CREDENTIALS] directly or indirectly in the derivation of the data encryption key(s) for [*LOW USER DATA ASSETS*]. **FCS_CKH_EXT.1.3/Low** The TSF shall ensure that all keys in the key hierarchy and all data used in deriving the keys in the hierarchy are protected according to [no other rules].	Y
	User data is encrypted at rest using File Based Encryption.	

FCS_CKH_EXT.1/MediumHigh	Devices shall provide encrypted storage that is tied to the user credentials. By default all user data shall be decrypted after the user authenticates the first time (device boot). Additionally the device shall provide the functionality to keep user data encrypted once the device has been unlocked but the user is not active (the user logged into the device at start-up and then the device has since been screen locked and requires the user to provide credentials again). This additional functionally can require separate apps to explicitly implement the functionality, but it shall be available in the device.	Supported? (Y/N)
	Documentation shall provide: • Description of how CE keys are generated/derived ◦ Algorithms, key lengths used in the process • Description of how CE keys are cryptographically tied to hardware-backed keystore • Description of how CE keys are cryptographically tangled with the user's credentials	
	FCS_CKH_EXT.1.1/MediumHigh The TSF shall support a key hierarchy for data encryption keys to protect [*MEDIUM AND HIGH USER DATA ASSETS*]. **FCS_CKH_EXT.1.2/MediumHigh** The TSF shall ensure that all keys in the key hierarchy are derived and/or generated according to [file and encryption keys are generated using AES_CTR DRBG from BoringSSL and are encrypted using a key that is derived from a combination of the user's credentials and the DUK] ensuring that the key hierarchy uses the DUK and [THE USER CREDENTIALS] directly or indirectly in the derivation of the data encryption key(s) for [*MEDIUM AND HIGH USER DATA ASSETS*]. **FCS_CKH_EXT.1.3/MediumHigh** The TSF shall ensure that all keys in the key hierarchy and all data used in deriving the keys in the hierarchy are protected according to [no other rules].	Y
	MEDIUM Android provides a key hierarchy tied to both the user's	

	password and the device root key that protects all data by default such that it is not available until after a successful authentication from the user. This is called Credentialed Encryption (CE). The CE key hierarchy binds the master encryption key to both the user's credential and the root key from the device. If an app does not do anything specific to store data, it will be stored as CE data. HIGH Android provides the ability for an app to be aware of the lock state of the device. This can be obtained through APIs: https://developer.android.com/reference/android/security/keystore/KeyGenParameterSpec.Builder#setUnlockedDeviceRequired(boolean) https://developer.android.com/reference/android/security/keystore/KeyGenParameterSpec.Builder#setUserAuthenticationRequired(boolean) When combined with the app being able to individually encrypt its own files: https://developer.android.com/topic/security/data#java An app can be developed that can maintain that its data is only able to be decrypted for use when the user is active on the device (the device is considered unlocked). This is an app-specific capability and so requires an app to be developed to utilize this capability.	

FCS_CKM.4	Devices shall clear plain-text keys when no longer needed.	Supported? (Y/N)
	Describe how keys are cleared from memory (both volatile and non-volatile). Note that some of these may not be applicable in all devices (for example there may be no non-volatile flash memory that is not wear-leveled), in which case it is sufficient to specify it is not applicable.	
	FCS_CKM.4.1 The TSF shall destroy **keys from the key hierarchy for Low, Medium, and High**	Y

	cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: • *FOR VOLATILE MEMORY, BY A SINGLE DIRECT OVERWRITE CONSISTING OF [selection: A RANDOM PATTERN, USING THE TSF'S RNG, ZEROES];* • *FOR NON-VOLATILE EEPROM, BY A SINGLE DIRECT OVERWRITE CONSISTING OF A RANDOM PATTERN, USING THE TSF'S RNG, FOLLOWED BY A READ-VERIFY;* • *FOR NON-VOLATILE FLASH MEMORY, THAT IS NOT WEAR-LEVELLED, BY [selection: A SINGLE DIRECT OVERWRITE CONSISTING OF ZEROS FOLLOWED BY A READ-VERIFY, A BLOCK ERASE THAT ERASES THE REFERENCE TO MEMORY THAT STORES DATA AS WELL AS THE DATA ITSELF];* • *FOR NON-VOLATILE FLASH MEMORY, THAT IS WEAR-LEVELLED, BY [selection: A SINGLE DIRECT OVERWRITE CONSISTING OF ZEROS, A BLOCK ERASE];* • *FOR NON-VOLATILE MEMORY OTHER THAN EEPROM AND FLASH, BY A SINGLE DIRECT OVERWRITE WITH A RANDOM PATTERN THAT IS CHANGED BEFORE EACH WRITE*]; that meets the following: [no standards].	
	The TOE clears sensitive cryptographic material (plaintext keys, authentication data, and other security parameters) from memory when no longer needed. Public keys can remain in memory when the phone is locked, but all crypto-related private keys are evicted from memory upon device lock. No plaintext cryptographic material resides in the TOE's Flash as the TOE encrypts all keys stored in Flash. When performing a full wipe of protected data, the TOE cryptographically erases the protected data by clearing the Data-At-Rest DEK. Because the Android Keystore of the TOE resides within the user data partition, the TOE effectively cryptographically erases those keys when clearing the Data-At-Rest DEK.	

User Data Protection

FDP_ACC.1/APP_Update	All applications delivered via the app store (distribution platform) shall provide a means for applications to be updated.	Supported? (Y/N)
FDP_ACF.1/APP_Update **FDP_UPF_EXT.1/APP_Update**	Document the following information about the update process: • Frequency of automatic checking with the app store • Method for verifying new updates are available (e.g. versioning such that older versions cannot be installed as an update) • Method for verifying validity of the package (i.e. signature checks)	
	FDP_ACC.1.1/APP_Update The TSF shall enforce the [*APP_UPDATE POLICY*] on [*SUBJECTS: THE TSF, OBJECTS: APP, APP_UPDATE_PACKAGE, OPERATIONS: UPDATE_APP*]. **FDP_ACF.1.1/APP_Update** The TSF shall enforce the [*APP_UPDATE POLICY*] to objects based on the following: [*SUBJECTS: THE TSF, OBJECTS[ATTRIBUTES]: APP[VERSION_ID, SIGNATURE], APP_UPDATE_PACKAGE[VERSION_ID, SIGNATURE, PACKAGE_SOURCE]*]. **FDP_ACF.1.2/APP_Update** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [• *THE TSF SHALL ALLOW THE TSF TO UPDATE_APP WITH AN APP_UPDATE_PACKAGE ONLY IF:* ◦ *THE TSF SUCCESSFULLY VERIFIES THE SIGNATURE OF THE APP_UPDATE_PACKAGE AND THE SIGNATURE IS FROM THE SAME APP OR APP DEVELOPER; AND* ◦ *[selection: THE VERSION_ID OF THE APP_UPDATE_PACKAGE IS NOT LOWER THAN THE VERSION_ID OF THE INSTALLED APP, THE UPDATE IS DOWNLOADED FROM THE APP*	Y

	DISTRIBUTION PLATFORM OF THE TOE MANUFACTURER OR OS DEVELOPER]; • *THE TSF SHALL UPDATE_APP IN AS AN ATOMIC UPDATE FUNCTION*]. **FDP_ACF.1.3/APP_Update** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *OTHER RULES ENSURING AUTHENTICITY AND INTEGRITY OF THE UPDATE PACKAGE*]. **FDP_ACF.1.4/APP_Update** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*THE TSF SHALL NOT ALLOW ANY TSF-MEDIATED ACTIONS RELATED TO THE UPDATE_APP OPERATION OR ACCESS TO THE APP DURING ITS UPDATING*]. **FDP_UPF_EXT.1.1/APP_Update** The TSF shall be able to check for a [APP] update package every [assignment: ~~*interval period*~~ ***an interval of no more than 1 day***].	
	The Play Store checks for app updates on a daily basis. Based on the user settings, the apps will be automatically updated when the device is not in use, or the user will be notified that updates are available. The user can force a check for updates (or when notified start the update immediately). When an app update is available, it will only be installed if the signature is from the same app developer as the currently installed version and that the version ID is not lower than the currently installed version of the app. When an app is being updated, if the app is currently running, the instance will be closed during the update process. If the update fails for any reason, the installation process will roll back to the version that existed at the time of the download.	

FDP_ACC.2/SSW_Update	The device shall support system software updates (i.e. OTA updates) and secure how they are downloaded and installed.	Supported? (Y/N)

FDP_ACF.1/SSW_Update **FDP_UPF_EXT.1/SSW_Update**	Document the following information about the update process: • Frequency of automatic checking with the update location • Method for verifying new updates are available (e.g. versioning such that older versions cannot be installed as an update) • Method for verifying validity of the package (i.e. signature checks) • How security is maintained during the update process (i.e. that the system cannot be circumvented during the update process) ***NOTE: The yellow highlight is a modification from GSMA FS.56.***	
	FDP_ACC.2.1/SSW_Update The TSF shall enforce the [*SSW_UPDATE POLICY*] on [*SUBJECTS: THE TSF, OBJECTS: THE SSW, SSW_UPDATE_PACKAGE, OPERATIONS: UPDATE_SSW*]. **FDP_ACC.2.2/SSW_Update** The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP. **FDP_ACF.1.1/SSW_Update** The TSF shall enforce the [*SSW_UPDATE POLICY*] to objects based on the following: [*SUBJECTS: THE TSF, OBJECTS[ATTRIBUTES]: SSW[VERSION_ID, SIGNATURE], SSW_UPDATE_PACKAGE[VERSION_ID, SIGNATURE, PACKAGE_SOURCE]*]. **FDP_ACF.1.2/SSW_Update** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [• *THE TSF IS ALLOWED TO PERFORM THE UPDATE_SSW OPERATION IF THE FOLLOWING CONDITIONS HOLD:* ◦ *[selection: THE SSW_UPDATE_PACKAGE[VERSION_ID] IS NOT LOWER THAN THE SSW[VERSION_ID], THE*	Y

	SSW_UPDATE[PACKAGE_SOURCE] IS THE TRUSTWORTHY UPDATE SOURCE DIRECTLY] ◦ *THE SSW_UPDATE_PACKAGE[SIGNATURE] IS VERIFIED BY A DIGITAL SIGNATURE FROM THE TOE MANUFACTURER STORED ON THE DEVICE* ◦ *THE SIGNATURE CHECK AND THE UPDATE_SSW ARE PERFORMED AS AN ATOMIC UPDATE FUNCTION*]. **FDP_ACF.1.3/SSW_Update** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *OTHER RULES ENSURING AUTHENTICITY AND INTEGRITY OF THE UPDATE PACKAGE*]. **FDP_ACF.1.4/SSW_Update** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*THE TSF SHALL NOT ALLOW ANY TSF-MEDIATED ACTIONS RELATED TO THE UPDATE_SSW FUNCTION DURING ITS UPDATING*]. **FDP_UPF_EXT.1.1/SSW_Update** The TSF shall be able to check for a [SYSTEM SOFTWARE] update package every [assignment: ***an interval of no more than 1 month***] and provide a notification to the user when an update is available.	
	The device automatically checks for updates every 24 hours by default. The check interval is configurable and typically occurs when the device is idle, connected to Wi-Fi, and has sufficient battery. Users can also manually trigger a check via "Settings → System → System Update". The device requests update metadata from the OTA server The update package includes a version identifier An update is considered available only if the version returned by the server is strictly higher than the current system version. Installing an older update package is prevented through	

	version comparison and signature protection. When ABOTA or Virtual A/B is used, partition status is also checked. The OTA update package is signed with the OEM's private key. The device verifies the package in Recovery or update_engine by checking: • Whether the signature matches the OEM certificate stored on the device; • Whether the signature is valid (preventing tampering); • Whether the package hash (e.g., SHA-256) matches the signed content. Android uses verity or AVB (Android Verified Boot) mechanisms to ensure the update package originates from a trusted source. If signature verification fails, the device refuses to install the update and may display an error message The update process runs in a protected execution environment: • The update_engine (userspace) downloads and verifies the package, while installation is performed in Recovery or A/B mode. • When using A/B partitioning, updates are applied to the inactive partition without affecting the currently running system. • During installation, the system does not process user input and application execution is blocked. Preventing circumvention: • The update process is controlled by init / recovery and cannot be interrupted through normal system calls. • If the update is interrupted (e.g., power loss), the device rolls back to the old version or continues the update in Recovery mode. • Executing arbitrary code or modifying system partitions during the update is not supported.	

FDP_ACC.2/Permissions **FDP_ACF.1/Permissions**	Devices shall provide access controls (permissions) to components on the system and provide the user with the opportunity to grant or block access to these components to any application or if permissions are specifically granted by the device (i.e. in the operating system the application has specific privileges already). This is divided into what the user can explicitly control and what the OS controls.	Supported? (Y/N)
	Document the following: • List of user permissions ([camera, location, the list of installed apps]) • List of OS permissions (i.e. Device ID, system permissions, sockets/IPC, files) • How permissions are granted (including for pre-installed applications where it is granted without user interaction) • How access is determined (allow/block) • SELinux is the basis for these permissions and controls	
	FDP_ACC.2.1/Permissions The TSF shall enforce the [*PERMISSIONS POLICY*] on [• *SUBJECTS: APPS, PROCESSES;* • *USER OBJECTS: [selection: CAMERA, MICROPHONE, LOCATION, CONTACTS, CALENDAR, CALL LOG, STORED PICTURES, TEXT MESSAGES, THE LIST OF INSTALLED APPS, [assignment: LIST OF OTHER SENSITIVE USER DATA ASSETS AND/OR SYSTEM SERVICES THAT CAN BE ACCESSED BY AN APP OR PROCESS];* • *MANUFACTURER OBJECTS: DEVICE ID, SYSTEM PERMISSIONS, FILES (INCLUDING INDIVIDUAL APP DATA), [selection: SECURE SOCKETS, SECURE IPC, [assignment: LIST OF OTHER SENSITIVE USER DATA ASSETS AND/OR*	Y

	*SYSTEM SERVICES THAT CAN BE ACCESSED BY AN APP OR PROCESS**];* • *OPERATIONS: READ, WRITE, EXECUTE*]. **FDP_ACC.2.2/Permissions** The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP. **FDP_ACF.1.1/Permissions** The TSF shall enforce the [*PERMISSIONS POLICY*] to objects based on the following: [• *[APPS AND PROCESSES] AND THE OPERATIONS ASSOCIATED WITH THE SUBJECT;* • *THE ACCESS CONTROL LIST ASSOCIATED WITH THE OBJECT BEING REQUESTED*]. **FDP_ACF.1.2/Permissions** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [• *THE SUBJECT, OR A GROUPING THE SUBJECT IS MAPPED TO, IS EXPLICITLY GRANTED PERMISSION BY THE USER OR TOE MANUFACTURER TO THE USER OBJECT IN THE ACCESS CONTROL LIST***].** **FDP_ACF.1.3/Permissions** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [• *THE SUBJECT IS GRANTED PERMISSION BY THE TOE MANUFACTURER TO THE MANUFACTURER OBJECT IN THE ACCESS CONTROL LIST*]. **FDP_ACF.1.4/Permissions** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [• *THE SUBJECT IS EXPLICITLY BLOCKED BY THE USER FROM ACCESSING THE USER OBJECT;* • *THERE IS NO RULE GRANTING THE SUBJECT ACCESS TO THE USER OR MANUFACTURER OBJECT IN THE ACCESS CONTROL LIST*].	
	Normal permissions (e.g., internet): automatically granted at install time, no user prompt.	

	Dangerous permissions (e.g., camera, location): granted at runtime via system permission dialog, user must explicitly allow. Pre-installed apps: • System apps (in /system/priv-app) may be granted signature/privileged permissions without user interaction. • OEM pre-installed apps are granted based on OEM policy (often automatic for basic functions or use same runtime prompt as user-installed apps). Granting methods: user taps "Allow" / "Deny"; can later change in Settings → Apps → Permissions. One-time permissions: Android can grant temporary access (e.g., "Only this time" until app process ends or device reboots). Access is determined by the Permission Controller (system service) evaluating: 1. App-level: whether the app has declared permission in its manifest. 2. Runtime grant state: user has granted or denied the permission (stored in permission manager). 3. SELinux context: kernel-level MAC rules based on domain/type. 4. UID/GID separation: each app has unique UID; system checks UID vs. permission mapping. 5. Privileged permissions: signature/role-based grants (e.g., only system apps). Decision: • Allow only if all checks pass (user granted + SELinux allows + UID valid). • Block if any check fails. • SELinux (Security-Enhanced Linux) provides mandatory access control (MAC) over all subjects (apps/processes) and objects (files, sockets, IPC, devices). • Each process runs in a domain (e.g., untrusted_app, platform_app, system_server).	

	• Each object has a type (e.g., camera_device, proc_net, system_data_file). • Access is granted only if a SELinux policy rule explicitly allows (domain, type, permission). • Even if a user grants a dangerous permission, SELinux may still block access if the policy denies it (e.g., preventing an untrusted app from directly opening /dev/mem). • Runtime permission checks and SELinux operate orthogonally: both must allow the operation for it to succeed.	

FDP_ACC.1/UserDataAsset **FDP_ACF.1/UserDataAsset**	Data stored on the device is protected with different classifications (DE/CE).	Supported? (Y/N)
	Describe how user data is protected and how it is classified on the system. DE/CE is sufficient to meet the Low/Medium differences. Explain how High can be implemented.	
	FDP_ACC.1.1/UserDataAsset The TSF shall enforce the [*USER DATA ASSET DECRYPTION POLICY*] on [• *SUBJECTS: THE TSF;* • *OBJECTS: INTERNAL STORAGE (ALL SAVED USER DATA ASSETS), [selection: REMOVABLE STORAGE (ALL SAVED USER DATA ASSETS WHEN ENCRYPTION IS ENABLED FOR REMOVABLE STORAGE), NO OTHER STORAGE];* • *OPERATIONS: DECRYPT*]. **FDP_ACF.1.1/UserDataAsset** The TSF shall enforce the [*USER DATA ASSET DECRYPTION POLICY*] to objects based on the following: [*SUBJECTS: THE TSF, OBJECTS: USER DATA ASSETS, ATTRIBUTES: SENSITIVE LEVEL OF OBJECTS, LOW, MEDIUM, HIGH*]. **FDP_ACF.1.2/UserDataAsset** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [	Y

	• *THE TSF IS ALLOWED TO DECRYPT LOW USER DATA ASSETS IF AND ONLY IF THE TOE IS SUCCESSFULLY POWERED ON; AND* • *THE TSF IS ALLOWED TO DECRYPT MEDIUM USER DATA ASSETS IF AND ONLY IF THE TOE IS SUCCESSFULLY POWERED ON AND THE USER IS SUCCESSFULLY AUTHENTICATED DURING THE FIRST AUTHENTICATION AFTER POWER ON; AND* • *THE TSF IS ALLOWED TO DECRYPT HIGH USER DATA ASSETS IF AND ONLY IF THE TOE IS SUCCESSFULLY POWERED ON, THE USER IS SUCCESSFULLY AUTHENTICATED AND THE SCREEN OF THE TOE IS NOT LOCKED*]. **FDP_ACF.1.3/UserDataAsset** The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [*NO ADDITIONAL RULES*]. **FDP_ACF.1.4/UserDataAsset** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*NO ADDITIONAL RULES*].	
	• On Android, user data is protected using: • File-Based Encryption (FBE) with different storage keys per classification level. • Direct Boot mode: allows certain data to be decrypted before user authentication (Low level). • Credential Encrypted (CE) storage: requires user authentication (Medium/High). • Device Encrypted (DE) storage: available after device power-on but before first unlock (Low). • Classification mapping on Android: • LOW: DE-protected data (e.g., alarms, notifications, accessibility services). Accessible after device boots, even if user is not yet authenticated. • MEDIUM: CE-protected data that requires user authentication after boot (e.g., contacts, call logs, SMS, user settings). Not accessible before first unlock. • HIGH: CE-protected data that additionally requires the screen to be unlocked (not just authenticated). Example: per-app encryption keys, keystore entries, or sensitive app data that is evicted when screen locks.	

Identification and Authentication

FIA_UAU.1	When authentication is enabled, some actions may be performed before a successful login.	Supported? (Y/N)
FIA_UID.1	Document what actions are allowed before a successful login. Access to stored data shall not be allowed (i.e. access to CE data)	
	FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions NOT ACCESSING USER DATA ASSET STORED BEFORE THE ACTION IS PERFORMED UNLESS PERMITTED BY THE USER*] on behalf of the user to be performed before the user is authenticated. **FIA_UAU.1.2** The TSF shall require the user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. **FIA_UID.1.1** The TSF shall allow [assignment: *list of TSF-mediated actions NOT ACCESSING USER DATA ASSET STORED BEFORE THE ACTION IS PERFORMED UNLESS PERMITTED BY THE USER*] on behalf of the user to be performed before the user is identified. **FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	Y
	Before the user is successfully authenticated (i.e., before first unlock after boot), Android allows the following TSF-mediated actions that do not access CE (Credential Encrypted) user data, unless explicitly permitted by the user (e.g., through Direct Boot): • Power on / boot the device • Enter the first unlock credential (PIN / password / pattern / biometric) • Display the lock screen / always-on display (without accessing user data) • Make emergency calls • Receive and display incoming calls and SMS	

	notifications (but not full message content if stored in CE) • Access Device Encrypted (DE) storage (e.g., alarms, notifications, accessibility services) • Trigger and respond to system broadcasts related to ACTION_BOOT_COMPLETED for DE-aware components • Use the camera for emergency actions or 3P apps if explicitly designed for Direct Boot (with restrictions) • Connect to Wi-Fi / Bluetooth networks (credentials stored in DE) • Respond to “Find My Device” or similar trusted agent services • Display the status bar and quick settings (without exposing CE data) • Allow device admin policies that are DE-aware (e.g., remote wipe commands)	

FIA_UAU.5/Local	Multiple methods of authentication may be supported.	Supported? (Y/N)
	Describe the methods of authentication that are provided including any biometric modalities or external devices that may be supported. Describe the ordering for how multiple methods may be used at one time (for example if fingerprint is enabled, how does the device decide whether to ask for the fingerprint or PIN).	
	FIA_UAU.5.1/Local The TSF shall provide [*PASSWORD, PIN* and selection: *PATTERN, **2D FACE**, [assignment: EAF], NO OTHER MECHANISM*] to support user authentication. **FIA_UAU.5.2/Local** The TSF shall authenticate any user's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide authentication*].	Y

	Password (alphanumeric, with configurable length/complexity) PIN (numeric only, typically 4–16 digits) Pattern (3×3 grid swipe pattern) Biometric modalities (via BiometricPrompt API): When multiple authentication methods are enrolled, Android determines the order as follows: 1. Preferred strong biometric (if enabled by user and app allows biometrics): ◦ The system first attempts the strongest enrolled biometric (e.g., 3D Face > Fingerprint > 2D Face). ◦ This is controlled by device policy and BiometricPrompt preferences. 2. Fallback to primary knowledge factor (PIN/Password/Pattern): ◦ A "Use pattern/PIN/password" button is always available on the lock screen or BiometricPrompt dialog. ◦ After 5 failed biometric attempts (or 3 failed face attempts on some devices), the system requires the knowledge factor. 3. Multiple biometrics enrolled: ◦ User can set a "preferred" biometric (e.g., fingerprint first, face second). ◦ If the first biometric fails (e.g., wet finger), the system may immediately offer the next enrolled biometric or fall back to PIN. 4. External device (EAF) ordering: ◦ Typically used as a second factor after primary authentication (e.g., unlock only when smartwatch is connected AND PIN entered). ◦ Can also be a primary factor (e.g., tap YubiKey to unlock) if configured by the user. 5. System logic summary:	

	◦ The device does not ask the user to choose a method actively; it follows a priority: Strong biometric → Secondary biometric → External trusted device → Knowledge factor (PIN/Pattern/Password) ◦ Users can always bypass biometrics by explicitly selecting the knowledge factor.	

FIA_UAU.5/Peer

This is for functionality that is provided with the device from the developer and does not include apps that may be downloaded by the user after purchase.

FIA_UAU.5/Peer	When connecting to a peer device or a service, the user shall successfully authenticate before the connection is allowed.	Supported? (Y/N)
	Document the methods for connecting to: • peer-to-peer device connections ◦ Bluetooth pairing methods are handled in FTP_ITC_EXT.1/BT and not necessary here • Other services ◦ For example backup/sync services using a trusted server ◦ Screen mirroring/sharing For other services, specify what is allowed after the successful pairing	
	FIA_UAU.5.1/Peer The TSF shall provide **support to use** [selection: *EXPLICIT ACCEPTANCE OF CONNECTION, QR CODES, NFC LABELS, PINS, USING A COMMON USER ACCOUNT TO A REMOTE SERVICE ON BOTH DEVICES, [assignment: OTHER MECHANISM TO VERIFY THE PEER IDENTITY]*] **for** authentication **to peer devices before allowing any actions on behalf of the user**. **FIA_UAU.5.2/Peer** The TSF shall authenticate any	Y

	peer device's claimed identity according to the [assignment: *rules describing how the multiple authentication mechanisms provide* ***peer device*** *authentication*].	
	● Multiple authentication mechanisms are available: ● Google Home App (GHA, iOS or Android) that requires a Google Account to authenticate before performing any action via app. ● Connection to cloud endpoints that are used for configuration, upgrade, etc. These management endpoints are accessed only by authenticated and authorized users, using TLS and JWT. QR codes to initiate key exchange is also used. ● Local web service on the device used for configuration requires a valid password to perform any action.	

FIA_UAU.6	The user needs to be re-authenticated to perform specific actions (this is specifically after the initial authentication to unlock the device after a bootup/startup).	Supported? (Y/N)
	Document what actions require authentication: • Unlocking the device after it has become locked (mandatory) • Change of authentication data (any change) (mandatory) • Other conditions?	
	FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [	Y

- *ATTEMPTED CHANGE OF ANY USER AUTHENTICATION FACTOR;*
- *ATTEMPTED UNLOCKING OF A LOCKED TOE;*
- *[selection: WHEN CHANGING USER ACCOUNTS USING THE CREDENTIALS FOR THE NEW USER, USING NO CREDENTIALS FOR A GUEST USER, [assignment: OTHER CONDITIONS], NO OTHER CONDITIONS*].

Mandatory (as specified):

- **Unlocking the device after it has become locked**
  - When the screen times out, user presses the power button, or device is locked via policy, the user must re-authenticate (PIN/password/pattern/biometric) to regain access to CE-protected data and the home screen.
- **Change of authentication data (any change)**
  - Changing PIN, password, pattern, or adding/removing biometrics (fingerprint, face) requires re-authentication with the **current** credential (knowledge factor) before the change is allowed.

Other conditions (on Android):

- **Accessing certain system settings** (e.g., Developer options, factory reset, modifying lock screen settings)
- **Viewing or copying saved passwords** (e.g., in Google Password Manager or app-specific credential storage)
- **Making a payment** (e.g., Google Pay, NFC payment apps often require recent authentication)
- **Authorizing sensitive operations** (e.g., installing apps from unknown sources, granting accessibility service permissions, disabling Play Protect)
- **Accessing encrypted app data** (apps can use `setUserAuthenticationRequired(true)` on keys to force re-authentication per use)

	• **Switching user accounts** (if multiple users are configured on the device) • **Resuming from idle lock** (e.g., after 4 hours of inactivity on some OEMs, requires stronger authentication)	

FIA_UAU.7	The user should see only limited feedback during authentication is in progress	Supported? (Y/N)
	Describe what feedback is provided to the user during authentication, such as password/PIN display (how long before masking).	
	FIA_UAU.7.1 The TSF shall provide only [*BRIEF FEEDBACK ABOUT THE ENTERED CREDENTIALS*] to the user while the authentication is in progress.	Y
	## For PIN / Password / Pattern entry: • **Character display duration**: Each character (digit/letter) is shown for approximately **300–500 milliseconds** before being masked (replaced by a dot/bullet). • **Masking symbol**: A dot (•) or asterisk (*) is shown after masking. • **Pattern feedback**: Dots on the 3×3 grid light up as the finger moves; the path is displayed briefly but not stored or shown after completion. • **Error feedback**: A generic message such as "Wrong PIN" or "Try again" is shown after an incorrect attempt, without revealing which part of the credential was incorrect. • **Success feedback**: Device unlocks or proceeds to the next screen without revealing credential details. ## For Biometric authentication (fingerprint / face): • **Prompt messages**: "Touch the fingerprint sensor"	

	or "Looking for face" (generic, no detail). • **Success indicator**: Haptic feedback + checkmark icon. • **Failure indicator**: Haptic feedback + "Not recognized" or "Try again" message. • **No feedback** on how the biometric matched or where it failed.	

FIA_SOS.1	The user shall be able to set credentials of a minimum strength	Supported? (Y/N)
	Document the minimum/maximum requirements for password/PIN/pattern settings for the user and specify the character set used for a password.	
	FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [• *FOR PASSWORD AND PIN: LENGTH 4 OR MORE FROM A DEFINED CHARACTER SET;* • *FOR PATTERNS: CONSISTS OF AT LEAST 4 FROM A SET OF AT LEAST 9 AVAILABLE POINTS, WHERE EACH POINT SHALL ONLY BE USED ONCE*].	Y
	The minimum length for any password or PIN is 4 characters/numbers. Passwords consist of basic Latin characters (upper and lower case, numbers, and the following special characters: ! @ # $ % ^ & * ( ) [= + - _ ` ~ \ |] } [{ ‘ “ ; : / ? . > , < The maximum length for a password or PIN is 16 characters/numbers. For a pattern the user must trace a pattern that touches at least 4 individual points from the 9 available.	

FIA_AFL.1	When repeated authentication attempts are detected, the device should deter continued attempts. This includes all available authentication methods.	Supported? (Y/N)
	Document what actions are taken when some number of attempts have been detected (between 3-10).	
	FIA_AFL.1.1 The TSF shall detect when [*AN INTEGER BETWEEN 3 AND 10*] unsuccessful authentication attempts occur related to [*selection: PASSWORD, PIN, PATTERN, **2D FACE**, **3D FACE**, **FINGERPRINT**, EAF*]. **FIA_AFL.1.2** When the defined number of unsuccessful authentication attempts has been [MET], the TSF shall [selection: *REBOOT, PROGRESSIVELY LENGTHEN THE TIME TO ATTEMPT AN AUTHENTICATION, MAKE ALL USER DATA ASSETS UNREADABLE, [assignment: list of other actions TO REDUCE THE RISK OF ATTACKS SUCH AS BRUTE-FORCE ATTACK]*].	Y
	The device maintains in persistent storage the number of failed authentication attempts since the last login. The Gatekeeper code for calculating the delay is here (written below based on the number of attempts taken). [0, 4] -> 0 5 -> 30 [6, 10] -> 0 [11, 29] -> 30 [30, 139] -> 30 * (2^((x - 30)/10)) [140, inf) -> 1 day Every 5 consecutive failed attempts the device will force the user to wait for a period of time before further attempts (starting at 30 seconds and then doubling in time). Every 10 attempts it also requires the device to reboot to perform further attempts. Biometric authentication can be attempted up to 5 times before the biometric is disabled and the user can only use a password, PIN or pattern to authenticate. When biometrics are enabled, they can be used once the screen wakes up. Entering a password, PIN or pattern requires an additional swipe of the screen to activate the sign in dialog to enter the credential.	

Security Management

FMT_MSA.1/Permissions	The user shall be able to manage the user permissions on the available objects. The default policy if no permission is assigned should be restrictive.	Supported? (Y/N)
FMT_MSA.3/Permissions	Document what the user can do in setting permissions for access (approve/reject persistently or temporarily, etc)	
	FMT_MSA.1.1/Permissions The TSF shall enforce the [*PERMISSIONS POLICY*] to restrict the ability to [selection: *APPROVE PERSISTENTLY, APPROVE TEMPORARILY, REJECT PERSISTENTLY, REJECT TEMPORARILY, MODIFY, [assignment: other operations]*] the security attributes [*LIST OF USER OBJECTS] to [THE CURRENT USER FOR THEIR OWN PERMISSIONS]*. **FMT_MSA.3.1/Permissions** The TSF shall enforce the [*PERMISSIONS POLICY*] to provide [RESTRICTIVE] default values for security attributes that are used to enforce the SFP. **FMT_MSA.3.2/Permissions** The TSF shall allow the [*CURRENT USER FOR THEIR OWN PERMISSIONS*] to specify alternative initial values to override the default values when an object or information is created.	Y
	Users can persistently approve, temporarily approve (e.g., "only this time"), persistently reject, temporarily reject, modify, or delete/revoke permissions for user objects. Additional operations include resetting permission state and viewing permission usage. The TSF enforces restrictive default values (DENY for all dangerous permissions). Users may override these defaults by granting or denying permission per app via runtime dialogs or Settings.	

FMT_SMF.1/Authentication	The user shall be able to specify and later change their authentication credentials	Supported? (Y/N)
	Document how the user can set and change the password/PIN/pattern/biometric	

	FMT_SMF.1.1/Authentication The TSF shall be capable of performing the following management functions: [selection: • *ENTERING AN INITIAL OR CHANGING (INCLUDING REMOVAL OF) THE KAF,* • *REGISTRATION OR CHANGING (INCLUDING REMOVAL OF) THE EAF,* • *SHOW THE LENGTH OF THE CREDENTIAL THE USER IS REQUESTED TO ENTER DURING AUTHENTICATION*].	Y
	The user can set or change their password, PIN, pattern, and biometric credentials (fingerprint, face) via **Settings → Security → Screen lock** or **Biometric Preferences**. For KAF (knowledge factor), the user enters an initial credential during device setup and can later change (including removal) by providing the current credential. For EAF (external factor, e.g., smartwatch or FIDO2 key), registration and removal are managed via **Settings → Connected devices** or **Security → External credential**. During authentication, the system shows the **minimum required credential length** (e.g., "PIN must be at least 4 digits") when the user is setting or entering a credential.	

FMT_SMF.1/Permissions	The user shall be able to manage the permissions provided to apps and some system services	Supported? (Y/N)
	• Document how the user can view, grant and revoke permissions for any app	
	FMT_SMF.1.1/Permissions The TSF shall be capable of performing the following management functions: [• *VIEW PERMISSIONS GRANTED TO AN APP; AND* • *GRANT/REVOKE PERMISSION TO/FROM AN APP OR PROCESS TO HAVE READ AND/OR WRITE ACCESS TO A USER OBJECT*].	Y
	Users can view, grant, and revoke permissions for any	

	app via **Settings** → **Apps** → **[App]** → **Permissions** or **Settings** → **Privacy** → **Permission manager**. The user can see which permissions are already granted, change a permission from "Allow" to "Deny" (revoke) or from "Deny" to "Allow" (grant). This applies to read and/or write access to user objects such as camera, microphone, location, contacts, storage, and calendar. The TSF supports the management functions of **VIEW_PERMISSIONS_GRANTED** and **GRANT/REVOKE** permission for read/write access to user objects.	

FMT_SMF.1/UserControls	The user shall be able to manage various settings on the device	Supported? (Y/N)
	• Document the settings for accessibility service, notifications • Document how the user can set the default USB mode when connecting to a computer • Removable media encryption	
	FMT_SMF.1.1/UserControls The TSF shall be capable of performing the following management functions: [• *GRANT/REVOKE PERMISSION TO/FROM AN APP OR PROCESS TO HAVE ACCESS TO ACCESSIBILITY SERVICE; AND* • *GRANT/REVOKE PERMISSION TO/FROM AN APP OR PROCESS TO HAVE ACCESS TO DEVICE NOTIFICATION; AND* • *[selection: CHARGE ONLY MODE BY DEFAULT, FILE TRANSFER MODE, [assignment: OTHER WIRED CHARGING MODE]] WHEN THE TOE IS CONNECTED VIA THE WIRED CHARGING INTERFACE TO ANOTHER DEVICE; AND* • *[selection: ENABLE/DISABLE REMOVABLE MEDIA ENCRYPTION, NO SUPPORT FOR REMOVABLE MEDIA]; and* • *[assignment: list of management functions to be*	Y

	provided by the TSF].	
	The user can manage apps that can access accessibility service through: Settings -> Accessibility The user can manage the notifications (which apps can provide notifications, access to read notifications, whether they can be seen on the lock screen) through: Settings -> More connections The user can manage USB connectivity to another device (such as a PC) through the USB preferences. By default, the selection is to not transfer data over the connection. This option becomes available when the device is connected to another device, at which point these settings can be adjusted for the connection. The device does not support removable media	

FMT_SMF.1/Privacy	The user shall be able to change the alias used as an identifier for ads and developers	Supported? (Y/N)
	Document how the user can change the alias (or disable it).	
	FMT_SMF.1.1/Privacy The TSF shall be capable of performing the following management functions: [selection: • *CHANGE OR RESET THE PRIVACY ALIASES;* • *BLOCK THE CREATION/USE OF A UNIQUE ID FOR ADVERTISING (NO PERSONALIZED TRACKING)*].	Y
	The user can access the advertising controls in: Settings -> Security & privacy -> Privacy controls ->Ads Here the user can reset the advertising ID or delete it completely. If the ID is deleted then personalized	

	tracking can be disabled. The user generally does not have access to identifiers that have been requested by an app. Some apps may provide this information internally, but this is a developer choice. If the user wants to reset the identifier (or delete it), they can delete the app (or clear all storage for the app, which would remove all associated app data). This will delete the local identifier such that the user would be able to have a new identifier created the next time the app is run.	

FMT_SMF.1/APP_Update	The user shall be able to manage applications on the device (update/uninstall)	Supported? (Y/N)
	Describe how application updates can be initiated and how apps (including pre-installed) can be uninstalled.	
	FMT_SMF.1.1/APP_Update The TSF shall be capable of performing the following management functions: [• *SPECIFY TO [selection: NOTIFY THE USER WITHOUT DOWNLOADING, NOTIFY THE USER AFTER DOWNLOADING, AUTOMATICALLY INSTALL] WHEN AN AUTOMATIC CHECK TO THE ADP HAS FOUND AN UPDATE; AND* • *INITIATE AN IMMEDIATE CHECK FOR UPDATE; AND* • *INITIATE AN UPDATE OF THE APP (IF AVAILABLE); AND* • *DISPLAY THE VERSION NUMBER OF THE APP; AND* • *UNINSTALL DOWNLOADED APPS (INCLUDING APPS DOWNLOADED AS PART OF THE SETUP PROCESS)*].	Y
	Through the Play Store the user can manage the apps they download to the device. The Play Store allows the user to install apps, check for updates, and uninstall apps. The Play Store	

	checks for updates to the installed apps roughly once per day to see if there are new versions to be installed. In general the apps	

FMT_SMF.1/SSW_Update	The user shall be able to check for system software updates	Supported? (Y/N)
	Describe how the user can check for new system software updates and how they can be installed.	
	FMT_SMF.1.1/SSW_Update The TSF shall be capable of performing the following management functions: [• • *SPECIFY TO [selection: NOTIFY THE USER WITHOUT DOWNLOADING, NOTIFY THE USER AFTER DOWNLOADING, AUTOMATICALLY INSTALL] WHEN AN AUTOMATIC CHECK TO THE TRUSTWORTHY UPDATE SOURCE HAS FOUND AN UPDATE; AND* • *INITIATE AN IMMEDIATE CHECK FOR UPDATE; AND* • *INITIATE AN UPDATE OF THE SYSTEM SOFTWARE (IF AVAILABLE); AND* • *PROVIDE THE STATUS OF THE UPDATE PROCESS AND THE RESULTS OF THE UPDATE; AND* • *[selection: DELAY TEMPORARILY, BLOCK PERSISTENTLY] AUTOMATIC INSTALLATION OF SYSTEM SOFTWARE UPDATES; AND* • *DISPLAY THE VERSION NUMBER OF THE SYSTEM SOFTWARE*].	Y
	The user can check for new updates by going to: Settings -> About tablet -> System Update This location also shows the installation status/progress of the update (until the reboot to switch to the updated version).	

Privacy

FPR_PSE.1	Advertisers and app developers shall be provided a unique device identifier that can be modified by the user.	Supported? (Y/N)
	Describe how the unique identifier is provided and how this can be changed by the user.	
	FPR_PSE.1.1/Advertisers The TSF shall ensure that [*AD NETWORKS*] are unable to **access Device ID** bound to [*THE TOE (HARDWARE PLATFORM)*] **according to the Permissions Policy**. **FPR_PSE.1.2/Advertisers** The TSF shall be able to provide [*AT LEAST ONE UNIQUE*] alias**(**es**)** of the **Device ID** to [*AD NETWORKS*]. **FPR_PSE.1.3/Advertisers** The TSF shall [DETERMINE AN ALIAS FOR A DEVICE ID]. **FPR_PSE.1.1/APP_Dev** The TSF shall ensure that [*APP DEVELOPERS*] are unable to **Device ID** bound to [*THE TOE (HARDWARE PLATFORM)*] **according to the Permissions Policy**. **FPR_PSE.1.2/APP_Dev** The TSF shall be able to provide [*AT LEAST ONE UNIQUE*] alias**(**es**)** of the **Device ID** to [*EACH APP DEVELOPER*]. **FPR_PSE.1.3/APP_Dev** The TSF shall [PROVIDE AN ALIAS FOR A DEVICE ID]- **upon request by the App developer**.	Y
	The device provides a single identifier for advertisers to use. This identifier is not tied to the hardware (it is not derived from any hardware identifiers) and is randomly generated. Advertisers are not able to access unique hardware identifiers through the access control permissions on access to them (such as the IMEI). The advertiser identifier string can be seen by the user in: Settings -> Security & privacy -> Privacy controls ->

Ads

App developers can have unique identifiers generated for them by the system to enable identification of the | |

	device tied to the user within their services. The unique identifier for the app is randomly generated and not tied to the hardware unique identifiers in any way. Each app developer can request an identifier (a developer with multiple apps may utilize the same identifier across all apps, that is a developer choice). An app developer can use the API randomUUID to request a random identifier.	

Protection of the TSF

FPT_PHP.3	OEMs and ODMs shall provide a hardware-backed key store implemented within a SEE, Secure Element or equivalent solution. Plaintext private key material shall not exist outside of the hardware-backed key store.	Supported? (Y/N)
	Provide documentation on the hardware-backed credential storage capabilities of the device, as well as the specific configurations.	
	FPT_PHP.3.1 The TSF shall resist [*to:* • *READ OR MODIFY THE DUK; AND* • *READ OR MODIFY [assignment: no keys (keys are not stored unencrypted]; AND* • *MODIFY [assignment: HASHES OF KEY(S)] USED TO VERIFY THE INTEGRITY OF THE TSF IN FPT_TST.1; AND* • *MODIFY [assignment: HASHES OF KEY(S)] USED TO VERIFY THE INTEGRITY AND AUTHENTICITY OF UPDATES TO THE TSF IN FCS_COP.1/ASYMMETRIC; AND* • *READ OR MODIFY [assignment: list of other data and/or keys]*]; to the **[***HARDWARE BASED SECURE ENVIRONMENT OF THE TSF***]** by responding automatically such that **it is impossible to read or modify this data and/or key(s)**.	Y

	The device provides multiple hardware-based storage locations for keys to maintain confidentiality and integrity. The DUK is stored in one-time fuses in the AP itself. These are never read directly by anything outside a security subsystem included in the AP. The device also provides support for the StrongBox Keystore. Apps and processes can use this to store keys instead of just placing them into the TEE Keystore. No Strongbox, but the TEE provides hardware-level protection.	

FPT_FLS.1	A failure in the system software update shall not expose user data.	Supported? (Y/N)
	Describe how a failure of the update process is managed. For example, an automatic rollback, or some other process which would allow the user to restore the system but which would not expose any encrypted user data.	
	FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [*FAILURE OF THE UPDATE_THE_TOE_SOFTWARE OPERATION IN FDP_ACF.1/SSW_UPDATE*].	Y
	If system update is failed, the device will boot with current bootable data (as device supported A/B bank update mechanism)	

FPT_TST.1	During the device start-up process, the integrity of the system software shall be verified.	Supported? (Y/N)
	Different tests are allowed for different types of checks. For example: • Cryptographic algorithms can run self-tests (RBG	

	can verify output) • Bootloader and other system checks using hash trees, signatures (or hashes)	
	FPT_TST.1.1 The TSF shall run a suite of self-tests **and integrity verification** [DURING INITIAL START-UP] to demonstrate the correct operation of [[selection: *[assignment: parts of TSF], the TSF*] BY SELF TESTS AND THE BOOTLOADER, MAIN OS KERNEL [selection: SEE, *[assignment: PARTS OF TSF]*] BY INTEGRITY, WHERE INTEGRITY IS VERIFIED BY [selection: *A DIGITAL SIGNATURE USING AN IMMUTABLE HARDWARE ASYMMETRIC KEY, AN IMMUTABLE HARDWARE HASH OF AN ASYMMETRIC KEY, AN IMMUTABLE HARDWARE HASH, A DIGITAL SIGNATURE USING A HARDWARE-PROTECTED ASYMMETRIC KEY*]]. **FPT_TST.1.2** The TSF shall provide authorised users with the capability to verify the integrity [*NO DATA*]. **FPT_TST.1.3** The TSF shall provide authorised users with the capability to verify the integrity of [*NONE*].	Y
	The device verifies the integrity using hardware-backed cryptographic solution TEE. The NIST SP 800-90B entropy health tests are started when the device powers on and are then run continuously thereafter. The device verifies the integrity of the following components during the start-up: ● Bootloader ● OS kernel ● TEE ● Executable code stored in /system and /vendor partitions All these are verified by checking the signature using the hash of an asymmetric key that is fused into the SoC during manufacturing. The code stored in the /system and /vendor partitions is checked using dm-verity, where the tree is verified to the hash. Dm-verity can correct some errors automatically (depends on the size of the error). Other than errors that can be corrected	

	automatically, any failure of a match will cause the device to halt the boot process.	

FPT_RCV.2	The device shall support a maintenance mode to enable recovery from malicious/persistent software.	Supported? (Y/N)
	Describe the process by which malicious software may be removed automatically (where possible), and if this isn't possible, how the user may do so (for example, safe boot, manually re-installing the system software or a factory reset)	
	FPT_RCV.2.1 When automated recovery from [*DETECTION OF A MALEVOLENT PERSISTENT PRESENCE BY FPT_TST.1 OR AN UPDATE FAILURE BY FDP_ACF.1/SSW_UPDATE*] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided. **FPT_RCV.2.2** For [*DETECTION OF A MALEVOLENT PERSISTENT PRESENCE BY FPT_TST.1 OR AN UPDATE FAILURE BY FDP_ACF.1/SSW_UPDATE*], the TSF shall ensure the return of the TOE to a secure state using automated procedures.	Y
	For detection of issues in the /system and /vendor partitions (such as an attempt to write malicious code or make other malicious changes to code stored there), most errors will be automatically corrected by the dm-verity check during the startup (the error will be detected and corrected automatically).	

Trusted Path/Channels

FTP_ITC_EXT.1/BT	The device shall support at least Bluetooth Core Specification v4.1	Supported? (Y/N)

	Document the Bluetooth support on the device Describe the process for regenerating ECDH key pairs with paired devices	
	FTP_ITC_EXT.1.1/BT The TSF shall use [*BLUETOOTH® CORE SPECIFICATION THAT CONFORMS TO [selection: v4.1 [11], v4.2 [12], v5.0 [13], v5.1 [14], v5.2 [15], [assignment: A VERSION HIGHER THAN V5.2]]*] to provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC_EXT.1.2/BT** The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel. **FTP_ITC_EXT.1.3/BT** The TSF shall initiate communication via the trusted channel for [*CONNECTIONS TO BLUETOOTH DEVICES*]. **FTP_ITC_EXT.1.4/BT** The protocol used by the communications channel shall support the following requirements: [• *REQUIRE EXPLICIT USER AUTHORISATION BEFORE PAIRING; AND* • *USE SECURE SIMPLE PAIRING AND SECURE CONNECTIONS FOR PAIRING; AND* • *NOT ALLOW MORE THAN ONE BLUETOOTH CONNECTION TO THE SAME BLUETOOTH DEVICE ADDRESS; AND* • *GENERATE NEW ECDH PUBLIC/PRIVATE KEY PAIRS EVERY [selection: 24 HOURS, THREE FAILED AUTHENTICATION ATTEMPTS FROM ANY BLUETOOTH DEVICE ADDRESS, TEN SUCCESSFUL PAIRINGS FROM ANY BLUETOOTH DEVICE ADDRESS, [assignment: OTHER FREQUENCY AND/OR CRITERIA FOR NEW KEY PAIR GENERATION]]*].	Y
	The device has been qualified according to the	

	Bluetooth 5.2 specification. Pairing is not allowed without explicit authorization from the user (this cannot be programmatically entered but must be input directly from the user). If the device is already paired with a peer, a second peer attempting to connect with the same BD_ADDR will be rejected (so a device that has been made to look like the first peer will be blocked from connecting while the original device is already connected). Each time the device is connected to a peer over Bluetooth a new ECDH key pair will be created for the connection.	

FTP_ITC_EXT.1/HTTPS **FTP_ITC_EXT.1/TLS**	The device shall support TLS 1.2 or higher	Supported? (Y/N)
	Document the following: • versions of TLS that are supported (1.2 & 1.3 expected) • IETF RFC 5280 support for certificate revocation checking • What happens if a certificate is determined to be invalid • What TLS ciphersuites are supported (for apps/websites to use)	
	FTP_ITC_EXT.1.1/HTTPS The TSF shall use [*HTTPS THAT CONFORMS TO IETF RFC 2818 [5]*] to provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC_EXT.1.2/HTTPS** The TSF shall permit [THE TSF] to initiate communication via the trusted channel. **FTP_ITC_EXT.1.3/HTTPS** The TSF shall initiate communication via the trusted channel for [*COMMUNICATION WITH A TRUSTED IT PRODUCT*]. **FTP_ITC_EXT.1.4/HTTPS** The protocol used by the	Y

communications channel shall support the following requirements: [*USE TLS AS SPECIFIED IN FTP_ITC_EXT.1/TLS TO IMPLEMENT HTTPS*].

FTP_ITC_EXT.1.1/TLS The TSF shall use [*TLS THAT CONFORMS TO [selection: TLS V1.2 [6], TLS V1.3 [10], [assignment: A VERSION OF TLS HIGHER THAN V1.2 [6]]]*] to provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC_EXT.1.2/TLS The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC_EXT.1.3/TLS The TSF shall initiate communication via the trusted channel for [*COMMUNICATION WITH A TRUSTED IT PRODUCT*].

FTP_ITC_EXT.1.4/TLS The protocol used by the communications channel shall support the following requirements: [

- *SUPPORT X.509V3 CERTIFICATES FOR MUTUAL AUTHENTICATION; AND*
- *DETERMINE VALIDITY OF THE PEER CERTIFICATE BY CERTIFICATE PATH, EXPIRATION DATE AND REVOCATION STATUS ACCORDING TO IETF RFC 5280 [7]; AND*
- *NOTIFY THE TSF AND [selection: NOT ESTABLISH THE CONNECTION, REQUEST APPLICATION AUTHORIZATION TO ESTABLISH THE CONNECTION, NO OTHER ACTION] IF THE PEER CERTIFICATE IS DEEMED INVALID; AND*
- *SUPPORTS THE FOLLOWING CIPHER SUITES [selection:*
    - *TLS_RSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5288 [8]),*
    - *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5288 [8]),*
    - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (IETF RFC 5289 [9]),*

	◦ *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5289 [9]),* ◦ *[assignment: OTHER PUBLISHED TLS CIPHER SUITE]*].	
	The device supports TLS v1.2 and TLS v1.3 (TLS v1.3 is the default). TLS is available directly via Android APIs (such as for an app to communicate to a server) or through HTTPS connections (such as when using a web browser. The device supports mutual authentication using certificates and can check the validity of the peer certificate according to RFC 5280. Android supports the ability for an app to check the certificate revocation status using OCSP. The app must implement the APIs to enable the check and determine the action to take if the certificate is found to be revoked (Android does not perform any action based on the information itself other than notify the app requesting the check of the state). The device does not act as a server so TLS connections must be initiated by the device (a request from a server to switch to a TLS connection will cause the device to start one) as opposed to accepting incoming connections that are not responses to a request originating from the device. The following cipher suites are supported: ● TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, ● TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, ● TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, ●TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, ●TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA38	

	4 as defined in RFC 5289 ● TLS_AES_128_GCM_SHA256 as defined in RFC 8446 ● TLS_AES_256_GCM_SHA384 as defined in RFC 8446 ● TLS_CHACHA20_POLY1305_SHA256 as defined in RFC 8446	

FTP_ITC_EXT.1/WLAN	The device shall support IEEE 802.11-2012, 802.1X & EAP-TLS connectivity	Supported? (Y/N)
	Document the Wi-Fi support on the device including • Key lengths supported • TLS 1.2 or higher support • IETF RFC 5280 support for certificate revocation checking • What happens if a certificate is determined to be invalid • What TLS ciphersuites are supported • MAC address randomization process (frequency)	
	FTP_ITC_EXT.1.1/WLAN The TSF shall use [*WLAN THAT CONFORMS TO 802.11-2012 [16]*] to provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **FTP_ITC_EXT.1.2/WLAN** The TSF shall permit [selection: *the TSF, another trusted IT product*] to initiate communication via the trusted channel. **FTP_ITC_EXT.1.3/WLAN** The TSF shall initiate communication via the trusted channel for [*COMMUNICATION WITH THE TRUSTED IT PRODUCT THROUGH WLAN CHANNEL*]. **FTP_ITC_EXT.1.4/WLAN** The protocol used by the communications channel shall support the following	Y

	requirements: [• *GENERATE SYMMETRIC KEYS ACCORDING TO [selection: PRF-384 WITH KEY LENGTH 128 BIT, PRF-704 WITH KEY LENGTH 256 BIT]; AND* • *USES [selection: TLS V1.2 [6], TLS V1.3 [10], [assignment: A VERSION OF TLS HIGHER THAN V1.2 [6]]]; AND* • *SUPPORTS THE FOLLOWING CIPHER SUITES [selection:* ◦ *TLS_RSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5288 [8]),* ◦ *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5288 [8]),* ◦ *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (IETF RFC 5289 [9]),* ◦ *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (IETF RFC 5289 [9])]* • *RANDOMLY GENERATE A NEW MAC ADDRESS EACH TIME IT CONNECTS TO A DIFFERENT ACCESS POINT*].	
	The device has been certified to meet the requirements for the Wi-Fi Alliance. The device supports PRF-384 and PRF-704 key generation and TLS v1.2. The following cipher suites are supported:	

	● TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, ●TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, ●TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, ● TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, ● TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289	

TS 103 732-2 SFRs

Identification and Authentication

FIA_MBE_EXT.1	The user must be able to enroll their biometric sample to create an authentication template.	Supported? (Y/N)
	Document the process for enrolling the user's biometric.	
	FIA_MBE_EXT.1.1 The TSF shall provide a mechanism to enrol an authenticated user to the biometric system.	Y
	The device supports 2D face. User could enroll the 2D face by taking the face picture. Setting -> Security&Privacy -> Device lock -> Face	

FIA_MBV_EXT.1	Biometric authentication sensors shall meet minimum requirements for use.	Supported? (Y/N)
	Document the FAR/FRR information for each biometric modality available.	
	FIA_MBV_EXT.1.1 The TSF shall provide a biometric verification mechanism using [*2D FACE*]. **FIA_MBV_EXT.1.2** The TSF shall provide a biometric verification mechanism with the [FAR] not exceeding	Y

	[selection: *1:50 000 FOR 2D FACE* and [FRR] not exceeding [selection: *1:20 FOR 2D FACE,*	
	This test is included in the BCR certification; the certification ID returned by Google is: Process [BCR7.0] Face 2D : Class 1 (formerly Convenience) : Lenovo/TB711FU_PRC/TB711FU:16/BP2A.250605.031.A3/ZUXOS_2.0.02.0998_26 Fixed 3/496396296 Self-Assessment Report: **[Android Biometrics Test Report (Android 16 Protocols- Face) 2026-03-20_for_Beryl_byArc.xlsx]**	

Management

FMT_SMF.1/BAF	The user must be able to manage their biometric templates.	Supported? (Y/N)
	Document what the user can do in terms of managing enrolled biometrics.	
	FMT_SMF.1.1/BAF The TSF shall be capable of performing the following management functions: [• *ENROL THE INITIAL [2D FACE]; AND* • *RE-ENROL OR CHANGE THE [2D FACE]*.	Y
	User could delete, disable their enrolled fingerprint or 2D face. And add their fingerprint.	

TS 103 732-4 SFRs

Applications

FAP_LFC.1	The developer shall describe how preloaded apps included in the system image are updated.	Supported? (Y/N)
	The developer can provide a list of the apps along with how they are updated.	
	FAP_LFC.1.1 The TSF shall ensure that preloaded applications are updated by [selection: *using an ADP and system software updates (to the version maintained in firmware), only by system software updates*].	Y
	Some preloaded applications are only updated as part of the system software updates but most are provided as apps in the Play Store and can be updated as any application update.	

FAP_LFC.2	The developer shall specify what happens when a preloaded app is uninstalled and the app reverts back to the one included in the current system image.	Supported? (Y/N)
	The developer shall explain the actions that are taken automatically and what the user may be able to do with the app once it has been uninstalled.	
	FAP_LFC.2.1 When a preloaded app update is uninstalled, the TSF shall warn the user the preloaded app will revert to the version in the system image and allow the following actions: [selection: *disable the app, warn the user on the next use, none*].	Y
	Some preloaded apps may be able to be disabled (along with uninstalling any app updates). This depends on the app (some are critical to the device and so cannot be disabled). When the app is not able to be disabled the user is warned about uninstalling the updates and then continuing to use the app from that point.	

FAP_LFC.3	The developer shall specify the ADP(s) where preinstalled apps are linked to for updates.	Supported? (Y/N)

	The developer should provide information about the ADP(s) where preinstalled apps will download updates from (updates should not be downloaded from a location that is not an ADP)..	
	FAP_LFC.3.1 The TSF shall ensure that preinstalled applications are only updated from the ADP(s) of the TOE manufacturer and/or OS developer.	Y
	All preinstalled apps are installed through the Play Store and so use the Play Store for all updates.	

FAP_LFC.4	The developer shall specify the ADP(s) where preinstalled apps are downloaded from during the installation process.	Supported? (Y/N)
	The developer should provide information about the allowed ADP(s) where apps may be downloaded from. The apps do not have to be specified.	
	FAP_LFC.4.1 The TSF shall ensure that preinstalled applications are only downloaded from the ADP(s) of the TOE manufacturer and/or OS developer.	Y
	All preinstalled apps are installed from the Play Store.	

FAP_PRM.1	The developer shall specify the permissions that are restricted to only preloaded and vendor-owned preinstalled apps.	Supported? (Y/N)
	The developer provides a list of system permissions that are restricted to only these apps so that any other app cannot successfully request access to the specified permission.	
	FAP_PRM.1.1 The TSF shall restrict the ability of applications to request [assignment: *permissions defined as system permission by the TOE developer*] to only preloaded applications and preinstalled applications created by the TOE developer.	Y

	Permissions that are categorized at a Protection level of “signature” can only be assigned to apps that are signed by the Google platform signing key. These permissions are not accessible by any apps that are not signed with this key and so cannot be requested. More information about the specific permissions available (and what permissions are categorized as signature) can be found at: https://developer.android.com/reference/android/Manifest.permission	

Application Risk

FPA_RSK.1	No sensitive data should be stored outside of the app container or system credential storage facilities.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.1.1 The applications on the TOE shall only store data within their own storage context. **FPA_RSK.1.2** The applications on the TOE shall only store keys using the TSF-provided key storage.	Y
	Tested as part of the Preloaded App Scripts	

FPA_RSK.2	The app does not rely on symmetric cryptography with hardcoded keys as a sole method of encryption.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.2.1 The applications on the TOE shall use appropriate cryptographic primitives to support the	Y

	algorithms in use. **FPA_RSK.2.2** The applications on the TOE shall not use deprecated cryptographic modes or algorithms.	
	Tested as part of the Preloaded App Scripts	

FPA_RSK.3	The app uses cryptographic primitives that are appropriate for the particular use-case, configured with parameters that adhere to industry best practices.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.3.1 The applications on the TOE shall not have hardcoded symmetric keys as the method of internal data protection.	Y
	Tested as part of the Preloaded App Scripts	

FPA_RSK.4	Data is encrypted on the network using TLS. The secure channel is used consistently throughout the app.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.4.1 The applications on the TOE shall not have hardcoded unencrypted URLs for network communications.	Y
	Tested as part of the Preloaded App Scripts	

FPA_RSK.5	The TLS settings are in line with current best practices, or as close as possible if the mobile operating system does not support the recommended standards.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.5.1 The applications on the TOE shall use the trusted channels provided by FTP_ITC_EXT.1/HTTPS or FTP_ITC_EXT.1/TLS.	Y
	Tested as part of the Preloaded App Scripts	

FPA_RSK.6	The app verifies the X.509 certificate of the remote endpoint when the secure channel is established.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.6.1 The applications on the TOE shall validate the X.509 server certificate according to the following rules: • The certificate path must terminate with a certificate in the TOE trust anchor; • The TOE shall use the main OS-provided method to verify the certificate.	Y
	Tested as part of the Preloaded App Scripts	

FPA_RSK.7	All inputs from external sources and the user are validated and if necessary sanitized. This includes data received via the UI, IPC mechanisms such as intents, custom URLs, and network sources.	Supported? (Y/N)

	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.7.1 The applications on the TOE shall sanitize all input from external sources via any available interface.	Y
	Tested as part of the Preloaded App Scripts	

FPA_RSK.8	The app does not export sensitive functionality via custom URL schemes, unless these mechanisms are properly protected. Apps by a common app developer may be acceptable in some circumstances.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.8.1 The applications on the TOE shall not support unauthorized direct access to data from external apps.	Y
	Tested as part of the Preloaded App Scripts	

FPA_RSK.9	The app is signed and provisioned with a valid certificate for the platform.	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.9.1 The applications on the TOE shall be signed with certificates with a signature format valid for	Y

	the platform.	
	Tested as part of the Preloaded App Scripts	

FPA_RSK.10	The app has been built in release mode, with settings appropriate for a release build (e.g. non-debuggable).	Supported? (Y/N)
	Output from a script that checks for proper usage and a report on any apps that could not provide a clear answer from the evaluator.	
	FPA_RSK.10.1 The applications on the TOE shall not have any debug functionality enabled.	Y
	Tested as part of the Preloaded App Scripts	

APA_LST.1	Enumerating the preloaded and preinstalled applications with system permissions is necessary to ensure how apps are separate from the OS.	Supported? (Y/N)
	The developer shall list the preloaded apps and any preinstalled apps (ones that are downloaded during the install) that are assigned system permissions.	
	APA_LST.1.1D The developer shall provide a list of all preloaded and preinstalled applications with system permissions included on the consumer mobile device at the completion of the initial CMD setup. **APA_LST.1.1C** The list of preloaded applications shall include all applications contained within the system software. **APA_LST.1.2C** The list of preinstalled applications shall include all applications installed on the consumer mobile device at the completion of the initial CMD setup that have been assigned system permissions.	Y

	APA_LST.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	
	Google does not specifically distinguish between preloaded and preinstalled apps, all are considered preloaded by internal Google definitions as any application that would have system permissions but is updated through the Google Play Store is considered preloaded (Google does not make any distinction between Preloaded and Preinstalled in the manner specified in the requirements).	

TS 103 732-5 SFRs

Bootloader - User data protection

FDP_ULK.1	If the bootloader is able to be unlocked, user data shall be protected (though wipe).	Supported? (Y/N)
	Describe whether the bootloader can be unlocked, and if so, how the device is wiped when the bootloader state changes. (Locking does not require a wipe, only unlocking)	
	FDP_ULK.1.1 The TSF shall ensure that [*changing the bootloader to an unlocked state will wipe all user data*].	Y
	When the bootloader is unlocked the device will be wiped of all user data.	

FDP_BBY.1	Any boot modes must continue to enforce user data security (no bypass)	Supported? (Y/N)
	Describe protections that ensure that alternative boot modes don’t bypass the security functions.	

	Note this normally would focus on how the data encryption can not be bypassed (i.e. the device booted to user data without any authentication).	
	FPT_BBY.1.1 The TSF shall be enforced in any alternative boot modes.	Y
	There are no boot modes that can bypass the data security.	

Bootloader - Protection of the TSF

FPT_BLP.1	The bootloader must run in the least privileged mode (ARM EL1 for example) possible.	Supported? (Y/N)
	Provide documentation about the boot process and the modes the bootloader runs in, with particular focus on the last stage. If the bootloader is completely removed from memory after loading the OS, then that is sufficient to meet this.	
	FPT_BLP.1.1 The bootloader shall be configured to run in the least privileged mode of the processor.	Y
	The bootloader initially loads at EL3 (the first stage of the bootloader), but once it has completed the loading process moves to EL1 to proceed with the boot process.	

FPT_PRT.1	The partition configuration protection shall be specified to ensure that the system is properly defined.	Supported? (Y/N)
	Provide information about how the integrity of the partition configuration is ensured.	
	FPT_PRT.1.1 The TSF shall protect the integrity of the partition configuration to prevent changes outside of the system image update process.	Y

	The integrity of the partition table is maintained using dm-verity.	

FPT_PRT.2	Bootable partitions must be documented, including all settings used on bootable partitions.	Supported? (Y/N)
	Document the partitions of the device. Include both fstab (or equivalent partition table from the device) for all mounted partitions and any additional information for partitions that may not be mounted by the OS but are used for special operations.	
	FPT_PRT.2.1 The TOE has the following partitions marked as bootable: the main OS and [selection: *recovery*, [assignment: *other bootable partitions*], *no other partitions*]. **FPT_PRT.2.2** The TSF enforces restrictions on writing data, code execution and system permissions through the use of partition flags during the mounting of partitions for use by the TOE.	Y
	fstab file for the device Android partition table descriptions	

FPT_ROL.1	Bootloaders must enforce rollback protection for firmware on the device. Tamper-evident storage must support the rollback implementation.	Supported? (Y/N)
	Provide documentation about how rollback protection is implemented and which components support it (and any conditions under which rollback may be bypassed and an earlier version installed).	
	FPT_ROL.1.1 The TSF shall permit rollback of the system software and [selection: *tamper-evident storage firmware*, [assignment: *other software/firmware*], *no other software/firmware*] under [selection: *all, no, [assignment:*	Y

	other conditions]] conditions.	
	System software can only be rolled back when the bootloader has been unlocked (which requires a device wipe first). In the unlocked state any system image may be installed. Followed Android AVB rollback protection mechanism	

Bootloader - Functional Specification

ADV_FSP.2	Boot arguments/commands that may be passed to the kernel from the boot process shall be documented.	Supported? (Y/N)
	The focus here is on commands that can be provided outside of the normal programmed commands, so commands from the user that may be passed. This is a modification to the ADV_FSP.2 documentation that is already required as part of the evaluation.	
	As part of the functional specification, the interface between the bootloader and the kernel shall be considered as a TSFI. Boot arguments or commands that may be passed from the bootloader to the kernel outside those that are provided as part of the TOE configuration (such as arguments that may be passed by the user through an external connection to the device) shall be documented and reviewed.	Y
	Lenovo adds a few internal fastboot oem arguments specific to the device beyond the normal ones found in AOSP. The commands available do not bypass any security functionality on the device such as enabling a bypass of the authentication process to unlock user data.	

Root of Trust - Protection of the TSF

FPT_INI.1	The device provides a method for verifying the integrity of the device during the boot process (a Root of Trust).	Supported? (Y/N)

	Document what the Root of Trust is, how it provides support for the initialization and what happens when an error is detected.	
	FPT_INI.1.1 The TOE shall provide an initialization function which is self-protected for integrity and authenticity. **FPT_INI.1.2** The TOE initialization function shall ensure that certain properties hold on certain elements immediately before establishing the TSF in a secure initial state, as specified in FPT_INI.1.2 Table. ID1 [*INTEGRITY*] [*ROOT OF TRUST*] ID2 [*PREVENTION OF DOWNGRADE TO PREVIOUS VERSIONS*] [*ELEMENTS AS SPECIFIED IN FPT_ROL.1.1*] **FPT_INI.1.3** The TOE initialization function shall detect and respond to errors and failures during initialization such that the TOE [selection: is halted]. **FPT_INI.1.4** The TOE initialization function shall only interact with the TSF in [assignment: *defined methods*] during initialization.	Y
	A public key on the device used to verify the initial bootloader is considered the Root of Trust on the device. This key is fused into the SoC into special OTP eFuses which cannot be changed once they have been set maintaining the integrity of the key. The device utilizes Android Verified Boot 2.0 to ensure the integrity of the system as it loads on the device. The trust of the boot sequence is derived from the public signature key hash which is set into One-Time Programmable (OTP) eFuses in the SoC. This hash is used to verify that the signature provided as part of the vmbeta partition is valid (and hence that the partition can be trusted).	

FPT_RDI.1	The integrity of the stored Root of Trust data is monitored.	Supported? (Y/N)
	Explain how the data used by the Root of Trust is monitored for integrity.	
	FPT_RDI.1.1 The TSF shall monitor Root of Trust data stored in containers controlled by the TSF for integrity errors.	Y
	A public key on the device used to verify the initial bootloader is considered the Root of Trust on the device. The RoT key is not specifically monitored by a program but is stored into a set of OTP eFuses which cannot be changed once set. Integrity is implied when the bootloader image is successfully verified using the programmed key. If that fails, it will be a problem with the image	

GSMA Requirements (FS.56)

Cryptographic Support

FCS_STG_EXT.1	Developers must provide a keystore that is tied to the hardware outside the main OS.	Supported? (Y/N)
	Provide documentation of how the keys are protected in a key store outside the main OS and how this is tied specifically to the hardware.	
	FCS_STG_EXT.1.1 The TSF shall provide [hardware based] secure cryptographic key storage.	Y

	NOTE: Hardware-based => TEE or similar Hardware isolated => eSE, SPU or similar **FCS_STG_EXT.1.2** The TSF shall utilize the provided secure cryptographic key storage for protecting the key hierarchy.	
	The Android keystore (KeyMint) uses a TEE to protect keys from the main OS.	

Identification and Authentication

FIA_SAR.1	Biometric authentication shall meet minimum requirements to detect spoof attempts.	Supported? (Y/N)
	Document the SAR (or IAPMR) information for each biometric modality available.	
	FIA_SAR.1.1 The TSF shall provide a biometric verification mechanism with the SAR no exceeding [selection: • *BELOW 7%*].	Y
	"Based on the SAR-Face test results, the Overall SAR (IAPMR) for the 2D Face biometric system is 5.795% (with Level A SAR at 0.330%, Level B SAR at 18.547%, and the maximum per-species SAR at 29.231%)."	

Privacy

FPR_ANO.2	The OTA client shall not access user data that is not necessary to perform an update.	Supported? (Y/N)
	Document what data is needed by the OTA client (such as IMEI or email to be authorized to access the update) and how the permissions on the device protect the client from user data. Since the client will have high permissions, showing how the user data is protected	

	from the OTA client (or the client is prevented from accessing the data) is to be shown.	
	FPR_ANO.2.1 The TSF shall ensure that [THE SYSTEM SOFTWARE OTA CLIENT] is unable to determine the real user data bound to [the TOE (HARDWARE PLATFORM)]. **FPR_ANO.2.2** The TSF shall provide [SYSTEM SOFTWARE UPDATES] to [THE USER] without soliciting any reference to the real user data.	Y
	The OTA client is part of AOSP (https://cs.android.com/android/_/android/platform/system/updat e_engine) and maintained as part of that project. OTA client undergoes a privacy review with every release. The review ensures that the client does not export personal dentification information of the user. Additionally, the client is not provided privileges which would provide it access to user/app data.	

Protection of the TSF

FPT_EAT_ EXT.1	Access to telephony commands (such as AT commands or other terminal listeners) via USB or other external interfaces must be disabled at ship time. This is intended to cover commands such as those entered via the dialer to provide various device information and not access to the modem itself (such as programmatic access).	Supporte d? (Y/N)
	Document how telephony commands can be accessed (both locally through the interfaces and remotely, if possible, from external devices).	
	FPT_EAT_EXT.1.1 The TSF shall only allow access to AT modem commands from [*the user interface*]. **FPT_EAT_EXT.1.2** The TSF shall prompt for approval of AT modem commands sent to the device from outside	NA

	the user interface [selection: is not applicable].	
	Wifi only	

FPT_LNW_EXT.1	Root or system owned processes do not expose any listening network sockets externally or on loopback interfaces. Disabling a listening socket must not require an OTA.	Supported? (Y/N)
	Document the network sockets that are available after the boot has completed from the device. Both loopback and external open ports must be documented.	
	FPT_LNW_EXT.1.1 The TSF shall ensure that no listening network sockets to the external or loopback IP networks are associated with processes with system permissions on the device. **FPT_LNW_EXT.1.2** The TSF shall ensure that [assignment: No Network sockets and associated processes] exposed to the external or loopback IP networks have no system permission on the device.	Y
	No network sockets or processes that are exposed to the network have system permissions.	

Life Cycle Requirements

The highlighted text are changes from what is included in the TS 103 732-1 SARs.

ALC_CMC.2	Any third party code shall be added to the developer's CM system.	
	The process for importing third party code and then maintaining that code shall be described.	
	ALC_CMC.2.4D The developer shall provide guidance for importing and updating external software components into the CM system.	Y

	ALC_CMC.2.4C The CM documentation shall describe the method used to identify external software components and how those components are updated.	
	All external code is brought into the internal git repository. Google code is brought in based on the version of Android being targeted.	

ALC_CMS.2	Any third party software components shall be documented where applicable.	
	For external software components, the original maintainer of the software shall be specified.	
	ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE including any external software components. **ALC_CMS.2.2E** The evaluator shall confirm that for external software components, the developer shall include the source and original maintainer of the component.	Y
	All external components that are included in the device are tracked in the CM system and included as part of the SBOM for the device. The source of all external components is maintained as part of that inclusion into the internal CM system. Information about how this code is tracked is in the document for ALC_CMC.2.	

ALC_DVS_EXT.1	The developer shall describe the process for generating the signing keys and unique identifiers on the device (ones that are fixed).	Supported? (Y/N)
	The developer needs to provide documentation about how the identifiers are generated and put on the device. This includes how these are secured while in the factory and cleared when not needed.	

	The developer must also describe how signing keys are generated, stored and protected. This includes how they are used (procedures for ensuring rogue builds cannot be created). Here the term keybox is used to identify the location on the device where the unique keys for the device will be stored. This can be in various hardware layers below the OS (the SEE). ***Note that the highlighted sections are where these are changes from the PP. Other sections without changes are not included.***	
	ALC_DVS_EXT.1.1D The developer shall produce and provide development security documentation on the generation, ~~and~~ protection and use of signing keys. **ALC_DVS_EXT.1.2D** The developer shall produce and provide development security documentation on the acquisition or generation of device unique identifiers. **ALC_DVS_EXT.1.3D** The developer shall produce and provide development security documentation on the provisioning of data or keys that may be used by a Root of Trust. **ALC_DVS_EXT.1.1C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the keys used to sign the publicly released system software and its updates. **ALC_DVS_EXT.1.2C** The development security documentation shall describe the procedures for selecting the proper signing keys used for a device and to ensure the use of the proper keys in the build process. **ALC_DVS_EXT.1.3C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the unique, non-modifiable identifiers (such as IMEI,	Y

	attestation keys or Device Unique Keys) and how they are properly acquired/created and provisioned for each device. **ALC_DVS_EXT.1.4C** The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the data and keys provisioned to the device for a Root of Trust for the device.	
	All signing keys are securely generated, stored and protected.	

ALC_FLR.3	The developer shall have a process for receiving information about flaws and then provide patches for those flaws to the impacted devices. In addition this includes a defined period and frequency of updates to the device (including both OS updates and regular security patches).	Supported? (Y/N)
	The developer needs to provide documentation about the flaw remediation/patching process. This can include public sites/information along with the support information for the device under evaluation. ***Note that the highlighted sections are where these are changes from the PP.***	
	ALC_FLR.3.1D The developer shall document and provide flaw remediation procedures addressed to TOE manufacturers. **ALC_FLR.3.2D** The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws. **ALC_FLR.3.3D** The developer shall provide flaw remediation guidance addressed to TOE users.	Y

	ALC_FLR.3.4D The developer shall provide public guidance related to the duration period, frequency and type of updates that will be released to support the TOE. **ALC_FLR.3.5D** The developer shall provide a public vulnerability disclosure program to provide security bulletins about the flaws that have been remediated. **ALC_FLR.3.6D** The developer shall establish procedures for ensuring that no known security vulnerabilities rated as High and Critical (e.g. as classified in public databases) are included in the TOE at public release. **ALC_FLR.3.1C** The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE. **ALC_FLR.3.2C** The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw. **ALC_FLR.3.3C** The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws. **ALC_FLR.3.4C** The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users. **ALC_FLR.3.5C** The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE. **ALC_FLR.3.6C** The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.	

	ALC_FLR.3.7C The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users. **ALC_FLR.3.8C** The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws. **ALC_FLR.3.9C** The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE. **ALC_FLR.3.10C** The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections. **ALC_FLR.3.11C** The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE. **ALC_FLR.3.12C** The flaw remediation procedures documentation shall define the planned minimum duration after release of the TOE that these methods will be used to maintain the TOE. **ALC_FLR.3.13C** The flaw remediation procedures documentation shall define the types of updates (such as security/maintenance or operating system) and the frequency of these updates being provided for the TOE. **ALC_FLR.3.14C** The flaw remediation procedures documentation shall describe the process for publicly releasing security flaw remediation information, including the location(s) where this will be publicly available. **ALC_FLR.3.15C** The flaw remediation procedures documentation shall describe the process for verifying known security flaws are not propagated into a new (not yet released) TOE.	

	ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.	
	Lenovo has a well-managed process to response on privacy issues and vulnerabilities as described in evidence documents. Besides, Users can receive security flaw reports and corrections by accessing to the security patch maintenance webpage: https://support.lenovo.com/gb/en/product_security/home A vulnerability disclosure policy webpage: https://support.lenovo.com/us/en/product_security/vulnerability-disclosure-policy	