Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Protection Profile for Mobile Devices: Mobile Security Foundation

Maintained by: Information Assurance Directorate

Unique Identifier: 001

Version: 0.02

Status: Draft

Date of issue:

Approved by:

Supersedes:

Background and Purpose

This assurance standard specifies information security requirements for Mobile Devices for use in an enterprise. A Mobile Device in the context of this assurance standard is a device which is composed of a hardware platform and its system software. The device typically provides wireless connectivity and uses application software for functions like secure messaging, email, web, VPN connection, and VoIP (Voice over IP), for access to the protected enterprise network, enterprise data and applications, and for communicating to other mobile devices.

Examples of a “mobile device” that should claim compliance to this assurance standard include smartphones, tablet computers, and other mobile devices with similar capabilities.

The Mobile Device provides essential services, such as cryptographic services, data-at-rest protection, and key storage services to support the secure operation of applications on the device. Additional security features such as security policy enforcement, application mandatory access control, anti-exploitation features, user authentication, and software integrity protection are implemented in order to address threats.

This assurance standard describes these essential security services provided by the Mobile Device and serving as a foundation for a secure mobile architecture. It is expected that a typical deployment would also include either third-party or bundled components that provide:

- Data in transit protection (e.g. VPN Client, VoIP Client, Web Browser)
- Security policy management (e.g. MDM System)

If these components are bundled as part of the Mobile Device by the manufacturer, they may be separately validated against the related assurance standards. Additional applications that may come pre-installed on the Mobile Device that are not validated are considered to be potentially flawed, but not malicious. Examples include VoIP client, email client, and web browser.

Related assurance standards This assurance standard is one of a set of complementary Mobility assurance standards that can be layered together to provide a full deployment. The set of assurance standards will consist of:

1. Mobile Device: Mobile Security Foundations
2. Mobile Device Management
3. VPN Client & Gateway
4. VoIP Client & SIP Server
5. Email Client
6. Web Browser

Use Cases

A selection of use cases is elaborated below.

[USE CASE 1] Enterprise-furnished device for general-purpose enterprise use and limited personal use
An enterprise-furnished device for general-purpose business use entails a significant degree of enterprise control over configuration and, possibly, software inventory. The enterprise elects to provide users with mobile devices and additional applications (such as VPN or email clients) in order to maintain control of their sensitive data and security of their networks, while trying to balance the constraints of usability and security and considerations of personal ownership and control. Users may use Internet connectivity to browse the web or access corporate mail or run enterprise applications, but this connectivity may be under significant control of the enterprise.

[USE CASE 2]Enterprise-furnished device for specialized, high-security use An enterprise-furnished device with intentionally-limited network connectivity, tightly- controlled configuration, and limited software inventory is appropriate for specialized, high- security use cases. For example, the device may not be permitted connectivity to any external peripherals. It may only be able to communicate via its WiFi or cellular radios with the enterprise-run network, which may not even permit connectivity to the Internet. Use of the device may entail compliance with policies that would not be considered realistic in any general-purpose use case, yet may mitigate risks to highly sensitive information. As in the previous case, the enterprise will look for additional applications providing enterprise connectivity and services to have a similar level of assurance as the platform.

[USE CASE 3] Personally-furnished device for personal and enterprise useA personally-furnished device which is used for both personal activities and enterprise data is commonly called Bring Your Own Device (BYOD). Unlike in the enterprise-furnished cases, in this use case the enterprise is limited in what security policies it can enforce on the device because the user purchased the device for personal use and is unlikely to accept policies that limit the functionality of the device. However, because the enterprise allows the user full (or nearly full) access to the enterprise network, the enterprise will require certain security policies, for example a password or screenlock policy, and may require assured enterprise software, for example a VPN client, before allowing access.

[USE CASE 4] Personally-furnished device for personal and limited enterprise useA personally-furnished device may also be given access to limited enterprise services such as enterprise email. Because the user does not have full access to the enterprise or enterprise data, the enterprise may not need to enforce any security policies on the device. However, the enterprise may want secure email and web browsing with assurance that the services being provided to those clients by the mobile device are not compromised.

Resources to be protected

High-level resources to be protected are identified in the Background/Purpose.

Attacker access

Mobile devices are subject to the threats of traditional computer systems along with those entailed by their mobile nature. The requirements in this assurance standard were developed to address the threats of network eavesdropping, network attacks, physical access, and non-malicious (but potentially flawed) apps.

- Network eavesdropping involves an attack positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the Mobile Device and other endpoints.

- Network attacks encompass situations in which an attacker is positioned on a wireless communications channel or elsewhere on the network infrastructure. Attackers may initiate communications with the Mobile Device or alter communications between the Mobile Device and other endpoints in order to compromise the Mobile Device. These attacks include malicious software updates of any apps or system software on the device. These attacks include spoofing of endpoint devices, such as MDM or VPN servers. These attacks also include malicious web pages or email attachments which are usually delivered over the network to devices.

- Physical access threats involve loss or theft of the Mobile Device which may give rise to lose of confidentiality of user data including credentials. These may involve attacks which attempt to access the device through external hardware ports, through its user interface, and also through direct and possibly destructive access to its storage media. The goal of such attacks is to access data from a lost or stolen device which is not expected to return to its user. Defending against device re-use after physical compromise is out of scope for this assurance standard.

- Malicious or flawed app threats exist because apps loaded onto the Mobile Device may include malicious or exploitable code. This code could be included intentionally by its developer or unknowingly by the developer, perhaps as a software library. Malicious apps may attempt to exfiltrate data to which they have access. They may also conduct attacks against the platform's system software which will provide them with additional privileges and the ability to conduct further malicious activities. Malicious apps may be able to control the device's sensors (GPS, camera, microphone) to gather intelligence about the user's surroundings even when those activities do not involve data resident or transmitted from the device. Flawed apps may give an attack access to perform network-based or physical attacks that otherwise would have been prevented.

- Persistent access to a device by an attacker implies that the device has lost integrity and cannot regain it. The device has likely lost this integrity due to some other threat vector, yet the continued access by an attacker constitutes an ongoing threat in itself. In this case the device and its data may be controlled by an adversary at least as well as by its legitimate owner.

Essential Security Requirements

Random Bit Generation (RBG)

- RBG1: The MD shall perform all deterministic random bit generation services in accordance with [selection, choose one of: NIST Special Publication 80090 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 1402 Annex C: X9.31 Appendix 2.4 using AES].

- RBG2: The deterministic RBG (RBG1) shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest security strength(according to NIST SP80057) of the keys and authorization factors that it will generate. The deterministic RBG shall be seeded by an entropy source that accumulated entropy from an MD hardware-based noise source, and [selection: a software-based noise source, other independent MD-hardware-based noise source, no other noise source].

- RBG-3: The MD shall be capable of providing output of the RBG to applications running on the MD that request random bits.

- RBG-4: (Objective) The MD shall allow applications to add data to the deterministic RBG (RBG-1) using the 4
  Personalization String. The MD shall NOT count data input from an application towards the entropy required by RBG-2. Thus, the MD shall not allow the only input to the RBG seed to be from an application.

- RBG-5: (Objective) The MD shall save the state of the deterministic RBG (RBG-1) at power-off, and shall use this state in seeding the deterministic RBG at startup. The saved state shall not count towards the entropy required by RBG-2.

Keys

- KEY1: The MD shall support a hardwareprotected REK with an AES key size of 128 or 256 bits. The key shall not be able to be imported to or exported from the hardware. System software on the MD shall be able only to request encryption/decryption by the key. A REK shall be generated by a RBG in accordance with RBG1 and RBG2.

- KEY-2: All DEKs shall be randomly generated with an RBG that meets this PP. All DEKs shall have entropy corresponding to the security strength of AES key sizes of 128 or 256 bits.

- KEY-3: All KEKs, outside of those defined by standard protocols, shall be 128-bit or 256-bit keys, corresponding to the security strength of the keys encrypted by the KEK

- KEY-4: KEKs may either be generated, derived from a Password Authentication Factor, or combined from other KEKs:
  - If generated, the KEK will be randomly generated with an RBG that meets this profile
  - If derived from a password, the password/passphrase shall be conditioned with a PBKDF as described in NIST SP 800-132 with a salt generated using a RBG as specified in this PP, and an HMAC using SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512. The output of the conditioning function shall be equal in size to the size of the KEK. The SHA algorithm should use FIPS 180-4 "Secure Hash Standard." The output of the conditioning function shall be equal in size to the size of the data encryption keys.
  - If combined from other KEKs, they shall be combined in a way that preserves the effective entropy of each factor. Options include using an XOR operation, concatenating the keys and use a KDF (as described in SP800-108), or encrypting one key with another.

- KEY-5: The MD shall not store any plaintext key material in readable non-volatile memory.

- The MD shall provide secure key storage for asymmetric keys, symmetric keys, and persistent secrets (e.g. passwords).
  - Supported asymmetric algorithms shall include RSA, DSA, ECDSA

- Supported symmetric algorithms shall include AES

- KEY-7: The MD shall be capable of importing keys/secrets into the secure key storage upon request of the user or applications running on the MD.

- KEY-8: The MD shall have the capability to allow only the application that imported the key/secret the use of the key/secret without user approval. An application's use of keys/secrets imported by the user shall require user approval.

- KEY-9: The MD shall allow only the application that imported the key/secret to request that the key/secret be destroyed without user approval. The MD shall require the user to approve any application's request for the destruction of another application's key or of a user-imported key. Key destruction shall meet KEY-9.

- KEY-10: All DEKs and all software-based key storage shall be encrypted by KEKs that are either:
  1. Protected by a REK:
     a. encrypted by a REK; or
     b. encrypted by a KEK chaining to a REK

     OR
  2. Protected by a REK and the password:
     a. encrypted by a REK and the password-derived KEK; or
     b. encrypted by a KEK chaining to a REK and the password-derived KEK.

     A REK and the password-derived KEK may be combined to form a combined KEK (as described in KEY-4) in order to meet this requirement.

  Sensitive data (DAR-5) shall be protected according to 2, The software-based key storage shall either all be protected according to 2 or shall allow users and applications to mark the key as sensitive (protected according to 2).

- KEY-11: The integrity of any encrypted key, including software-based key storage, shall be protected from corruption by at least one of:
  - a AEAD or Key Wrap cipher mode (Key Wrap, Key Wrap with Padding, GCM, or CCM) for encryption according to KEY-10;
  - a hash (ALG-4) of the stored key that is encrypted by a key protected by KEY-10;
  - a keyed hash (ALG-6) using a key protected by a key protected by KEY-10;
  - a digital signature of the stored key using an asymmetric key protected according to KEY-10.

  The hash/digital signature shall be verified before use of the stored key.

- KEY-12: The MD shall clear cryptographic keys contained within the MD either by clearing the KEK encrypting the target key or in accordance with the following rules:
  - For non-volatile memory other than EEPROM and flash, the destruction shall be executed by overwriting three or more times using a different alternating data pattern each time.
  - For volatile memory and non-volatile EEPROM, the destruction shall be executed by a single direct overwrite consisting of a pseudo random pattern based on the RBG specified in this PP, followed a read-verify.
  - For volatile memory and non-volatile flash memory, the destruction shall be executed by a single direct overwrite consisting of zeros followed by a read-verify or by a block erase followed by a read-verify.

- KEY-13: Plaintext DEKs, and KEKs shall not be exportable by the user or administrator.

- KEY-14: Whenever a KEK is used for encryption, it must have a unique IV for every key that it encrypts when applicable for the encryption mode (reference the NIST SP 800-38 series).

- KEY-15: All salts shall be generated using a RBG as specified in this paper.

- KEY-16: No plain text key material (intermediate keys, passwords, etc.) shall be transmitted from the process which makes use of it.

- KEY-17: All code for the product shall clear all plaintext keying material (authentication data, secret/private symmetric keys, etc.) in volatile memory according to KEY-12 when entering the powered off state.

Cryptographic Algorithm Services

- ALG-1: The MD shall generate asymmetric cryptographic keys used for key establishment in accordance with at least one of:
    - NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for finite field-based key establishment schemes;
    - NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” for elliptic curve-based key establishment schemes and implementing “NIST curves” P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, “Digital Signature Standard”)
    - [selection: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for RSA-based key establishment schemes, no other]

  are specified cryptographic key sizes equivalent to, or greater than, a symmetric key stength of 112 bits.

- ALG-2: The MD shall perform encryption/decryption of data for transport using AES operating in CBC (as defined in NIST SP 800-38A), GCM (as defined in NIST SP 800-38D), or CCM (as defined in NIST SP 800-38C) with 128-bit or 256-bit key sizes.

- ALG-3: The MD shall perform encryption/decryption of keys for storage using Key Wrap (KW) (as defined in NIST SP 800-38F), or Key Wrap with Padding (KWP) (as defined in NIST SP 800-38F), or GCM (as defined in NIST SP 800-38D), or CCM (as defined in NIST SP 800-38C), or CBC (as defined in NIST SP 800-38A) mode with 128-bit or 256-bit key sizes.

- ALG-4: The MD shall perform encryption/decryption of data for storage using AES operating in CBC (as defined in NIST SP 800-38A), or XTS (as defined in NIST SP 800-38E) with 128-bit or 256-bit key sizes.

- ALG-5: The MD shall perform cryptographic hashing using SHA-1, SHA-256, SHA-384, SHA-512 algorithms (FIPS Pub 180-4).

- ALG-6: The MD shall perform cryptographic signature services (generation and verification) using: RSA with a key size (modulus) of 2048 bits or greater (FIPS Pub 186-3) or ECDSA with a key size of 256 bits or greater using NIST curves P-256, P-384, P-521 (FIPS Pub 186-3).

- ALG-7: The MD shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-[selection: SHA-1, SHA-256, SHA-384, SHA-512], key sizes [assignment: key size (in bits) used in HMAC], and message digest sizes [selection: 160, 256, 384, 512] bits that meet the following: FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-4, “Secure Hash Standard.”

- ALG-8: The MD shall generate asymmetric cryptographic keys used for authentication in accordance with a [selection, choose at least one of:
    - FIPS PUB 186-3, “Digital Signature Standard (DSS)”, Appendix B.3 for RSA schemes;
    - FIPS PUB 186-3, “Digital Signature Standard (DSS)”, Appendix B.4 for ECDSA schemes and implementing “NIST curves” P-256, P-384 and [selection: P-521, no other curves];
    - ANSI X9.31-1998, Appendix A.2.4 Using AES for RSA schemes]

  and specified cryptographic key sizes equivalent to, or greater than, a symmetric key strength of 112 bits.

- ALG-9: The MD shall run a suite of self-tests during initial start-up (on power-up) to demonstrate the correct operation of all cryptographic functionality. This can be performed via known-answer tests.

- ALG-10: The MD shall provide a mechanism for applications to request the MD to perform cryptographic algorithm services.

Certificates

- CER-1: The MD shall store a list of trusted root Certificate Authority (CA) certificates, called the Trust Anchor Database.

- CER-2: The MD shall be capable of importing certificates into the Trust Anchor Database upon request of the user, applications, or the administrator. The MD shall require user approval before importing certificates from applications.

- CER-3: The MD shall allow users, applications, and the administrator to remove and modify certificates from the Trust Anchor Database. The MD shall require user approval before removing or modifying a certificate upon an application's request.

- CER-4: The MD shall validate certificates using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 2560, a Certificate Revocation List (CRL) as specified in RFC 5759] and in accordance with RFC 5280 certificate validation and certificate path validation. To be valid, the path must terminate with a certificate in the Trust Anchor Database. The MD shall validate a certificate path by ensuring the presence of the basicConstraints extension is present and the cA flag is set to TRUE for all CA certificates.

- CER-5: The MD shall not treat a certificate as a CA certificate if the basicConstraints extension is not present or the CA flag is not set to TRUE.

- CER-6: The MD shall allow applications to request certificate validation, shall perform the validation in accordance with CER-4, and shall respond to the application with a value indicating the result of that validation.

Data-At-Rest Protection

- General DAR
  - DAR-
    1: Before decryption of sensitive data, the product shall require user authentication in the form of a password.

  - DAR-
    2: Aside from configuring the product and providing the authorization credential, the user should not have any interaction with the DAR protection. Encryption shall cover all non-system data and shall not require the user to mark specific files as sensitive.

- DAR for Screen Lock
  - DAR-
    3: The product shall include a key scheme to encrypt data received while the product is locked. The key scheme shall involve an asymmetric public/private key pair, shall prevent the received (stored) data (at rest) from being decrypted in the locked state, and shall require authentication factors to be entered to unlock the device before the data can be decrypted.

  - DAR-
    4: Sensitive data received while the product is in a locked state shall be encrypted and protected by a key scheme satisfying the requirements specified in DAR-3 and ALG-1 of this profile.

  - DAR-5 The MD shall provide a mechanism for applications to mark data and keys as sensitive, and, therefore inaccessible in the locked state.

- DAR-6: Attempts to decrypt keys and files that have not been marked as sensitive shall fail in locked states and be able to succeed only during unlocked states.

- DAR-7: When locked state is initiated, the product shall clear sensitive decryption keys and all sensitive plaintext keying material (authentication data, secret/private symmetric keys, etc.) in volatile memory according to KEY-12 for all data not designated/marked to be available at screen lock. (Note that this requirement corresponds to AUTH-5 and AUTH-6.)

- Data Wipe
  - DAR-8: The wipe command shall either
    1. Cryptographically erase the encrypted DEKs and/or the KEKs in non-volatile memory by following the requirements in KEY-12; or
    2. Overwrite the entire memory and drive space using non-sensitive data such as a pseudorandom data pattern or a fixed data value. The following requirements will be followed, based on the memory type.
       - For non-volatile memory other than EEPROM and flash, the wipe shall be executed by overwriting three or more times using a different alternating data pattern each time.
       - For volatile memory and non-volatile EEPROM, the wipe shall be executed by a single direct overwrite consisting of a pseudo random pattern based on the RBG specified in this PP, followed a read-verify.
       - For volatile memory and non-volatile flash memory, the wipe shall be executed by a single direct overwrite consisting of zeros followed by a read-verify, or by a block erase followed by a read-verify.

Management

- MGMT-1: The MD shall provide its user and the administrator the ability to query the current version of the MD operating system and all firmware that can be updated separately. [MOS PP FPT_TUD_EXT.1.1(1)]

- MGMT-2: The MD shall provide its user and the administrator the ability to query the hardware model of the device. This hardware model identifier must be sufficient to indicate, in tandem with manufacturer documentation, the hardware which comprises the device.

- MGMT-3: The MD shall provide its user and the administrator the ability to query the current version of all installed mobile applications. [MOS PP FPT_TUD_EXT.1.1(2)]

- MGMT-4: (Objective) The MD shall cryptographically sign all responses to device identifier queries in MGMT-1, MGMT-2, and MGMT-3. The key used to perform this signature shall be protected by the secure key storage (KEY-6).

- MGMT-5: The MD shall provide the user the following management functions [MDPP FMT_SMF.1.1]
  - management of session locking; [MDM PP 2.1.1 Screen Lock]
    - screen-lock enabled/disabled
    - screen lock timeout (AUTH-5)
    - number of authentication failures (AUTH-1)
  - management of the enable/disable state the VPN protection; [MDM PP 2.5.1 VPN Enable/Disable]
  - (High-security) management of enable/disable state of data transfer capabilities over [assignment: list of externally accessible hardware ports (e.g. USB, SD card, HDMI)];[MDM PP 2.7.1 Peripherals Enable/Disable]
  - (High-security) management of enable/disable state of [assignment: list of radios (e.g. Wi-Fi, GPS, cellular, NFC, Bluetooth)]; [MDM PP 2.7.1 Peripherals Enable/Disable]
  - (High-security) management of enable/disable state of [assignment: list of audio or visual collection devices (e.g. camera, microphone)]; [MDM PP 2.7.1 Peripherals Enable/Disable]
  - if developer modes are supported, management of enable/disable state of developer modes [MDM PP 2.2.1 Debug Mode]
  - management of enable state of data-at-rest protection (section 1.5) if not natively enabled [MDM PP 2.6.1 DAR Protection Enable]

        - if removable storage is supported, management functions should include enable of removable media's data-at-rest protection
        - if the MD offers the option to locally bypass authentication while in the locked state using features such as "Forgot password", management functions shall include enable/disable of this feature.
    - [selection: (High-security) management of the Access Point Name and proxy used for communications between the cellular network and other networks, [assignment: list of other management functions to be provided by the MD], no other management functions].

- MGMT-6: The MD shall provide the administrator the following management functions [MDPP FMT_SMF.1.1]
    - password policy management (AUTH-4); [MDM PP 2.1.3 Password Reset]
        - minimum password length (AUTH-9)
        - minimum password complexity (AUTH-9)
        - maximum password lifetime
    - management of session locking policy; [MDM PP 2.1.1 Screen Lock]
        - screen-lock enabled/disabled
        - screen lock timeout (AUTH-5)
        - number of authentication failures (AUTH-1)
    - management of the enable/disable state the VPN protection [MDM PP 2.5.1 VPN Enable/Disable]
    - (High-security) management of enable/disable state of data transfer capabilities over [assignment: list of externally accessible hardware ports (e.g. USB, SD card, HDMI)];[MDM PP 2.7.1 Peripherals Enable/Disable]
    - (High-security) management of enable/disable state of [assignment: list of radios (e.g. Wi-Fi, GPS, cellular, NFC, Bluetooth)]; [MDM PP 2.7.1 Peripherals Enable/Disable]
    - (High-security) management of enable/disable state of [assignment: list of audio or visual collection devices (e.g. camera, microphone)]; [MDM PP 2.7.1 Peripherals Enable/Disable]
    - if developer modes are supported, management of enable/disable state of developer modes [MDM PP 2.2.1 Debug Mode]
    - management of enable state of data-at-rest protection (section 1.5) if not natively enabled [MDM PP 2.6.1 DAR Protection Enable]
        - if removable storage is supported, management functions should include enable of removable media's data-at-rest protection
        - if the MD offers the option to locally bypass authentication while in the locked state using features such as "Forgot password", management functions shall include enable/disable of this feature. Any offered remote authentication bypass (such as remote password reset) requires an authorized administrator (MGMT-8).
    - management of application installation policies: either specifying authorized application repository(s) or specifying a set of allowed applications and versions (an application whitelist)
    - [selection: (High-security) management of the Access Point Name and proxy used for communications between the cellular network and other networks, [assignment: list of other management functions to be provided by the MD], no other management functions].

- MGMT-7: The MD shall be capable of performing management of the WLAN trusted channel to specify wireless networks (SSID) that are acceptable for the MD to connect (WLAN-11) and the following management functions for each network:
    - Specify the CA(s) from which the MD will accept WLAN authentication server certificate(s) or specify the FQDN(s) of acceptable WLAN authentication server certificate(s), (WLAN-8, WLAN-10)
    - ability to specify security type (e.g. WPA2-PSK, WPA2 Enterprise)
    - ability to specify authentication protocol (WLAN-5) (e.g. EAP-TLS)
    - specify the client credentials to be used for authentication
    - [assignment: any additional WLAN management functions].

- MGMT-8: While in the unenrolled state, the MD shall restrict the ability to perform the functions to manage the MD security functions and execute administrative commands to the user. While in the enrolled state, the MD shall restrict the ability to perform [selection: all management functions, [assignment:list of management functions]] to the administrator. If the administrator does not have a policy set for a management function, the user retains the right to perform the management function. [MDPP FMT_MOF.1.1(1)]

- MGMT-9: The MD shall provide remediation actions to users and administrators including:
  - alerting the user or administrator
  - transitioning to the locked state
  - full wipe of all data according to DAR-8
  - [selection: wipe of sensitive data, removal of installed applications, [assignment: list of other remediation actions], no other remediation actions].

- MGMT-10: The MD shall perform remediation actions in MGMT-9 on command of the administrator or on administrator-configured triggers including at least authentication failures (AUTH-2) and unenrollment.

- MGMT-11: The MD shall allow administrators to set policies regarding the management function in MGMT-6 and MGMT-7, shall enforce those policies, and shall be capable of reporting that the policy is currently in effect.

- (Objective) The MD shall provide read access to audit logs kept by the MD (in accordance with INT-12) to the administrator.

- MGMT-13: (BYOD)
  (Objective) The MD, if it supports policies from multiple management sources, will resolve any differences by enforcing the most restrictive. If there is no clear policy hierarchy, the MD shall panic and make a car-alarm sound. Or notify the user and the administrators.

- MGMT-14: (BYOD) The MD shall require user approval to enroll in management. This user approval notice shall include the policies to be applied by the agent.

- MGMT-15: (BYOD)(Objective) The MD shall notify the user of any change made by the administrator to the enforced policies.

- MGMT-16: (High-security)(Objective) The MD shall provide management functions to the user and administrator to restrict
  - cellular voice functionality, including the ability to disable voice calls completely (except emergency dialing).
  - device messaging capabilities (e.g. SMS, MMS, and voicemail) including the ability to disable device messaging completely.
  - the cellular protocols used to connect to cellular network base stations
  - voice command control of device functions

Access Control & Separation

- Access Control
  - ACC-1: The OS shall enforce a mandatory access control policy that prevents processes from modifying the OS, device drivers, system and security configuration files, and key material with the exception of those processes dedicated to performing updates of those elements.

  - ACC-2: (objective) The OS shall be configurable to enforce a mandatory access control policy that prevents application processes from accessing data stored by other applications unless such sharing is explicitly authorized by the user, or the applications originate from a common publisher.

  - ACC-3: (objective) The OS shall be configurable to enforce a mandatory access control policy that prevents applications from writing files to locations on local device storage that can be read by other applications. An exception is to facilitate sharing, which must be explicitly authorized by the user or performed by applications which originate from a common publisher.

- ACC-
  4: (objective) The OS shall be configurable to enforce a mandatory access control policy that prohibits all IPC mechanisms between apps except for that which is explicitly permitted.

- ACC-
  5: The OS shall enforce a mandatory access control policy that restricts the system services to which an application may communicate via IPC mechanisms.

- ACC-
  6: The OS shall enforce a mandatory access control policy that prohibits an application from having both write and execute permission to a file on the device.

- ACC-7: The OS shall enforce a mandatory access control policy that requires application processes to obtain authorization in order to access sensitive data.

- Anti-Exploitation Services
  - AEX-
    1: The OS shall provide address space layout randomization (ASLR) to applications. The OS shall randomly position all memory mappings of an application process at selection: [its load time, the load time of its parent process]. The base address of any userspace memory mapping will consist of at least 8 random bits provided by the MD RBG services.

  - AEX-2: The mobile operating system and its memory management unit shall be capable of enforcing a policy which prevents any range of addresses (page, segment, region) of a process from being simultaneously writable and executable, except for memory used for just in time (JIT) compilation.

  - AEX-
    3: (Objective) The bootloader shall provide address space layout randomization (ASLR) for the OS kernel. The bootloader shall randomly position the kernel image at load time. The base address of the kernel memory mapping will consist of at least 4 bits which cannot be inferred by an adversary without an information leak.

  - AEX-
    4: (Objective) The mobile operating system and its memory management unit shall enforce a policy which prevents any range of addresses (page, segment, region) of the kernel from being simultaneously writable and executable. The memory management unit shall enforce these memory protections and transition the system to a non-operational state if any violation is detected.

- Baseband Separation
  - BBD-1: (High-security)
    (Objective) Code executing on any baseband processor (BP) shall not be able to access application processor (AP) resources except when mediated by the AP.
    These resources include:
    - Volatile and non-volatile memory
    - Control of and data from integrated and non-integrated peripherals (e.g. USB controllers, touch screen controllers, LCD controller, codecs)
    - Control of and data from integrated and non-integrated I/O sensors (e.g. camera, light, mic, GPS, accelerometers, geomagnetic field sensors)

Trusted Channel

- Information Flow Control
  - IFC-1: (High-security) The MD shall have the ability to route all IP traffic (other than IP traffic required to establish the VPN connection) through a VPN client. The MD shall either provide this routing configuration or shall allow the VPN client to specify this routing.

- IFC-
  2: The MD shall enforce the [assignment: Enterprise Information Flow Control SFP] on [assignment: all communication to and from the mobile device enterprise perimeter]. [MDPP FDP_IFC.1.1]

- IFC-3: The MD shall enforce the [assignment: Enterprise Information Flow Control SFP] based on the following types of subject and information security attributes: [assignment: list of subjects and information controlled under the indicated SFP, and for each, the security]. [MDPP FDP_IFF.1.1(1)]

- IFC-
  4: The MD shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: for each operation, the security attribute-based
  relationship that must hold between subject and information security attributes]. [MDPP FDP_IFF.1.2(1)]

- IFC-5: The MD shall enforce the [assignment: additional information flow control SFP rules]. [MDPP FDP_IFF.1.3(1)]

- IFC-
  6: The MD shall explicitly authorise an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly authorise information flows]. [MDPP FDP_IFF.1.4(1)]

- IFC-
  7: The MD shall explicitly deny an information flow based on the following rules: [assignment: rules, based on security attributes, that explicitly deny information flows]. [MDPP FDP_IFF.1.5(1)]

- IFC-
  8: The MD shall enforce that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to, deallocation of the resource from] all objects.

- WLAN Trusted Channel
  - WLAN-1: The MD shall be capable of communicating over a trusted channel using Wi-Fi.

  - WLAN-
    2: The MD shall derive symmetric cryptographic keys in accordance with a specified cryptographic key derivation algorithm (PRF-
    384) with specified cryptographic key size (128 bits) using a Random Bit
    Generator as specified in RBG-1 and with an administratively-
    configured cryptoperiod with a granularity no greater than an hour that meet the following: 802.11-2012. [WLAN FCS_CKM.1]

  - WLAN-
    3: The MD shall distribute Group Temporal Key (GTK) in accordance with a specified cryptographic key distribution method: AES Key Wrap in an EAPOL-
    Key frame that meets the following: [RFC 3394 for AES Key Wrap, 802.11-2012 for the packet format and timing considerations] and does not expose the cryptographic keys. [WLAN FCS_CKM.2]

  - WLAN-
    4: The MD shall perform encryption and decryption in accordance with the specified cryptographic algorithm AES CCMP and cryptographic key size of 128 bits that meet the following: FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2012. [WLAN FCS_COP.1(5)]

  - WLAN-5: The MD shall implement the EAP-
    TLS protocol as specified in RFC 5216 supporting the following ciphersuites: [WLAN FCS_EAP-TLS_EXT.1.1] Mandatory Ciphersuites in accordance with RFC 3268:
    - TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_AES_256_CBC_SHA

Optional Ciphersuites:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 524
- TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 524
- 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_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5430
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5430

- WLAN-6: The MD shall generate random values used in the EAP-TLS exchange using the RBG specified in RBG-1. [WLAN FCS_EAP-TLS_EXT.1.2]

- WLAN-7: The MD shall verify that the server certificate presented for EAL-TLS includes the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extended KeyUsage field. [WLAN FCS_EAP-TLS_EXT.1.4]

- WLAN-
  8: The MD shall allow configuration of the acceptable authentication server certificates (MGMT-5). The MD shall verify that the server certificate presented for EAP-
  TLS either chains to one of the specified
  CAs or contains the specified FQDN of the acceptable authentication server certificate. [WLAN FCS_EAP-TLS_EXT.1.5]

- WLAN-
  9: The MD shall conform to IEEE Standard 802.1X for a Port Access Entity (PAE) in the “Supplicant” role. [WLAN FIA_8021X_EXT.1.1]

- WLAN-
  10: The MD shall use X.509v3 certificates as defined by RFC 5280 to support authentication for EAP-TLS exchanges. The MD shall use certificate validation as specified in CER-4. The MD shall not establish a trusted WLAN communication channel if the authentication server certificate is deemed invalid. The key for the client’s X.509v3 certificate shall be stored in the secure key storage (KEY-6). [WLAN FIA_X509_EXT.1.1]

- WLAN-
  11: The MD shall only attempt connections to wireless networks specified as acceptable networks based on [assignment: attribute(s) used to identify the list of acceptable networks] as configured by the administrator MGMT-7. [WLAN FTA_WSE_EXT.1.1]

- WLAN-12: The MD shall use 802.11-2012, 802.1X, and EAP-TLS to provide a trusted communication channel between itself and a wireless access point that is logically distinct from other communication channels and provides assured identification of its endpoints and protection of the channel data from disclosure and detection of modification of the channel data. [WLAN FTP_ITC.1.1]

- WLAN-
  13: The MD shall permit the MD to initiate communication via the WLAN trusted channel. [WLAN FTP_ITC.1.2]

- WLAN-14: The MD shall clear according to KEY-
  12 all plaintext secret and private cryptographic keys and
  CSPs related to WLAN when no longer required.

- Additional Trusted Channels
  - TC-
    1: The MD shall be capable of communicating over a trusted channel implementing the IPsec, TLS, DTLS, or SSH protocol.

  - TC-2: The MD shall clear according to KEY-
    12 all plaintext secret and private cryptographic keys and CSPs related to the trusted channel when no longer required.

  - IPsec
    - FCS_IPSEC_EXT.1.1 The MD shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-
      256 (both specified by RFC 3602), [selection: no other algorithms, AES-GCM-128, AES-GCM-
      256 as specified in RFC 4106], and using [selection, choose at least
      one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 fo
      hash functions]].

    - FCS_IPSEC_EXT.1.2 The MD shall ensure that either
      - IKEv2 SA lifetimes can be configured by an [selection: an Administrator, VPN Gateway] based on number of packets/number of bytes or length of time, where the time values can be limited to: 24 hours for IKE SAs and 8 hours for IPsec SAs; or
      - IKEv1 SA lifetimes can be configured by an [selection: an Administrator, VPN Gateway] based on number of packets/number of bytes or length of time, where the time values can be limited to: 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

    - FCS_IPSEC_EXT.1.5 The MD shall ensure that all IKE protocols implement DH Groups 14 (2048-
      bit MODP), and [selection: 24 (2048-bit MODP with 256-bit POS), 19 (256-
      bit Random ECP), 20 (384-bit
      Random ECP), [assignment: other DH groups that are implemented by the MD], no other DH groups].

    - FCS_IPSEC_EXT.1.6 The MD shall ensure that all IKE protocols implement Peer Authentication using the [selection: RSA, ECDSA] algorithm.

    - FCS_IPSEC_EXT.1.7 (optional) The MD shall support the use of pre-
      shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

    - FCS_IPSEC_EXT.1.8 (optional) The MD shall support the following:
      1. Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, *assignment: other characters;

      2. Pre-
         shared keys of 22 characters and [selection: [assignment: other supported lengths], no other lengths].

  - TLS FCS_TLS_EXT.1 Explicit: TLS
    - FCS_TLS_EXT.1.1 The MD shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:
      Mandatory Ciphersuites:
      - TLS_RSA_WITH_AES_128_CBC_SHA
      - TLS_RSA_WITH_AES_256_CBC_SHA

      Optional Ciphersuites:
      - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
      - TLS_DHE_RSA_WITH_AES_256_CBC_SHA

        - TLS_RSA_WITH_AES_128_CBC_SHA256
        - TLS_RSA_WITH_AES_256_CBC_SHA256
        - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
        - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA25
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

    - TLS-2: The MD shall verify that the server certificate presented for EAL-TLS includes the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.

    - TLS-3: The MD shall generate random values used in the TLS exchange using the RBG specified in RBG-1.

    - TLS-4: The MD shall be capable of using X.509v3 certificates as defined by RFC 5280 to support authentication for TLS exchanges. The MD shall use certificate validation as specified in CER-4. The key for the X.509v3 certificate shall be stored in the secure key storage (KEY-6).

- DTLS FCS_DTLS_EXT.1 Extended: Datagram Transport Level Security
    - FCS_DTLS_EXT.1.1 The MD shall implement the DTLS protocol in accordance with one or more of [selection: DTLS 1.0 (RFC 4347), DTLS 1.2 (RFC 6347)].

    - FCS_DTLS_EXT.1.2 The MD shall implement the requirements in FCS_TLS_EXT.1 for the DTLS implementation, except where variations are allowed according to RFC 4347 or RFC 6347.

- SSH FCS_SSH_EXT.1 Explicit: SSH
    - FCS_SSH_EXT.1.1 The MD shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

    - FCS_SSH_EXT.1.2 The MD shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

    - FCS_SSH_EXT.1.3 The MD shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes] bytes in an SSH transport connection are dropped.

    - FCS_SSH_EXT.1.4 The MD shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms].

    - FCS_SSH_EXT.1.5 The MD shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms,] as its public key algorithm(s).

    - FCS_SSH_EXT.1.6 The MD shall ensure that data integrity algorithms used in SSH transport connection is [selection: hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96].

    - FCS_SSH_EXT.1.7 The MD shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

- HTTPS FCS_HTTPS_EXT.1 Explicit: HTTPS
  - FCS_HTTPS_EXT.1.1 The MD shall implement the HTTPS protocol that complies with RFC 2818.
  - FCS_HTTPS_EXT.1.2 The MD shall implement HTTPS using TLS as specified in section 4.3.2.
- Baseband Trusted Channel
  - CNAU-1: (High-security) (Objective) The MD shall authenticate all base stations of the cellular network to which it connects unless the cellular protocol does not support authentication.
  - CNAU-2: (High-security) (Objective) The MD shall visually indicate to the user the cellular protocol it is using and the network to which it currently is connected.
  - CNAU-3: (High-security) (Objective) The MD shall be configurable to connect to cellular network base stations using only the cellular protocols configured by the user or MDM agent.

- Identification & Authentication
  - AUTH-1: The MD shall detect when an administrator-configured positive integer (MGMT-5 and MGMT-6) within [assignment: range of acceptable values] unsuccessful authentication attempts by a user on the MD occur related to unsuccessful authentication attempts since the last successful authentication by that user. [MDPP FIA_AFL.1.1 and MDM PP 2.1.1 Screen Lock]
  - AUTH-2: When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the MD shall perform a remediation action set by the administrator MGMT-10. [MDPP FIA_AFL.1.2 and MDM PP 2.1.2 Authentication Failures]
  - AUTH-3: The MD shall enforce a delay between incorrect authentication attempts. The minimum delay shall be such that no more than 10 attempts can be attempted per 500 milliseconds.
  - AUTH-4: The MD shall provide a mechanism to verify that the Password Authorization Factors comply with the password policy set by the administrator in MGMT-6. [MDPP FIA_SOS.1]
  - AUTH-5: The MD shall transition to the locked state after a time interval of inactivity set by the user within a range specified by the administrator according to MGMT-5 or MGMT-6 by: [MDPP FTA_SSL.1 and MDM PP 2.1.1 Screen Lock]
    a. clearing or oveerwriting display devices, making the current contents unreadable;
    b. disabling any activity of the user's data access/display devices other than unlocking the session or those allowed in AUTH-8
    c. clearing all sensitive data/keys and all plaintext keying material (authentication data, secret/private symmetric keys, etc.) for sensitive data/keys in volatile memory according to KEY-12 (DAR-5)
  - AUTH-6: The MD shall allow user-initiated locking of the user's own interactive session, by: [MDDP FTA_SSL.2]
    a. clearing or overwriting display devices, making the current contents unreadable;
    b. disabling any activity of the user's data access/display devices other than unlocking the session or those allowed in AUTH-8
    c. clearing all sensitive data/keys and all plaintext keying material (authentication data, secret/private symmetric keys, etc.) for sensitive data/keys in volatile memory according to KEY-

12 (DAR-5)

- AUTH-7: The MD shall require the user to enter the correct Password Authorization Factor when the user changes their Password Authorization Factor, following MD-initiated locking (AUTH-5) in order to transition to the unlocked state, following user-initiated locking (AUTH-6) in order to transition to the unlocked state, [selection: [assignment: other conditions], no other conditions].

- AUTH-8: The MD shall allow the user to limit information that may be automatically displayed to unauthenticated users in the locked state. [MDPP FIA_UAU.1.1]

- AUTH-9: The MD shall support the following for the Password Authorization Factor:
  a. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, *assignment: other characters;
  b. Passwords of up to 14 characters.

- AUTH-10: The Password Authorization Factor shall be used to derive a KEK as specified in KEY-4.

- AUTH-11: If the product supports additional forms of authentication, such as a raw key stored on an external token or biometrics, and if the product uses these factors to derive KEKs, these additional authentication factors shall be conditioned to have size equal to the size of the KEK derived by the Password Authentication Factor and shall be used in conjunction with the KEK derived from the Password Authentication Factor.

- Integrity

  - INT-1: The MD shall run a suite of tests, at least during initial start-up, to demonstrate the correct operation of the MD. At a minimum, the MD is expected to perform tests to confirm correct operations of crypto-related hardware functionality. [MDPP FPT_TST.1.1]

  - INT-2: The MD shall notify the user and, if configured, the administrator when the following types of failures occur:
    - failures resulting from self-tests performed per during self-testing under INT-1
    - MD software integrity verification failures under INT-4
    - [assignment: other failures].

  - INT-3: The MD shall take the following actions for failures specified in INT-2:
    - log failures in the audit record
    - preserve a secure state and transition to non-operational mode,
    - [assignment: other actions taken].

  - INT-4: The MD shall verify the integrity of the bootloader software either by a digital signature using an hardware-protected asymmetric key or by a hardware-protected hash before loading additional software. The software integrity of both the firmware/software on the AP and the firmware/software on the BP shall be verified. The asymmetric key or hash shall be either protected by a REK or stored in a hardware module. The key or hash shall only be updated by verified and authenticated software.

  - INT-5: (Objective) Each software piece (starting with the bootloader) thereafter shall verify the integrity of any software it loads using a digital signature or hash. The software integrity of both the firmware/software on the AP and the firmware/software on the BP shall be verified.

- INT-6: (BYOD) The MD shall provide users the ability to initiate updates to MD system software. The MD may also provide the administrator the ability to initiate updates.

- INT-7: The MD shall verify software updates to the MD using a digital signature mechanism implemented according to ALG-5 prior to installing those updates. The update mechanism itself shall have been verified by INT-4 and INT-5.

- INT-8: The MD shall by default only accept operating system and firmware software updates cryptographically signed by the vendor or a party authorized by the vendor. The signing key shall be validated to a hardware-protected public key (either stored in a hardware module or in the Trust Anchor Database) or shall match a hardware-protected public key. If the signing public key is part of a certificate, this certificate shall be verified to have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field and shall be validated according to CER-4. The MD shall not install software updates to the MD if the code signing certificate is deemed invalid.

- INT-9: (BYOD) The MD shall provide users the ability to initiate updates to mobile applications. The MD should also provide the administrator the ability to initiate application updates.

- INT-10: The MD shall verify software updates to mobile applications using a digital signature mechanism prior to installing those updates. The MD shall validate the code signing certificate used to sign the application in accordance with CER-4. This certificate shall be verified to have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. The MD shall not run or install applications or updates to applications if the code signing certificate is deemed invalid.

- INT-11: (Objective) The MD shall require applications to be signed by either a vendor-assigned public key(s) or by a user/administrator configured public key(s).

- INT-12: The MD shall be able to generate an audit record of the following auditable events:
  a. Start-up and shutdown of the audit functions;
  b. All auditable events for the any level of audit; and
  c. All administrative actions;
  d. Authentication failures (AUTH-1, AUTH-2, AUTH-7);
  e. Failures of security functions (INT-1);
  f. Integrity verification failures (INT-4);
  g. Software upgrades (INT-6, INT-7, INT-8)

- INT-13: The MD shall record within each audit record at least the following information:
  a. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
  b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, auditable events to be derived from the requirements in this profile.

- INT-14: (Objective) The audit record shall be cryptographically protected from modification using a digital signature mechanism implemented according to ALG-5. The key used to perform this signature shall be protected by the secure key storage (KEY-6). The key should be unique per mobile device and should be capable of being signed by an external Certificate Authority.

- INT-15: The MD shall be able to provide reliable time stamps.

- INT-16: The MD shall overwrite the oldest stored audit records if the audit trail is full.

- Documentation
  - Guidance Documentation
    The guidance documents will be provided with the ST. Guidance must include a description of how the user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by the user.

    Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes
    - Instructions to successfully install the MD in that environment; and
    - Instructions to manage the security of the MD as a product and as a component of the larger operational environment.

    Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the assurance activities specified with each requirement.

    Operational User Guidance
    The developer shall provide operational user guidance. It shall be expressed in the eXtensible Configuration Checklist Description Format (XCCDF) to support security automation.

    The operational user guidance shall describe the user- accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

    The user guidance should focus on the management of the MD by the administrator in addition to local management by the local mobile user.

    The operational user guidance shall describe how to use the available interfaces provided by the MD in a secure manner.

    [Appendix for US only] The operational user guidance shall express each configuration guidance item that could be used in a compliance checking regime as an XCCDF Rule element, and provide references to the NIST 800-53 controls which the item satisfies.

    The operational user guidance shall describe the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

    The operational user guidance shall clearly present each type of security-
    relevant event that require user
    approval resulting from applications under the control of the MD changing security characteristics of the MD.

    The operational user guidance shall identify all possible modes of operation of the MD, their consequences and implications for maintaining secure operation.

    The operational user guidance shall describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

    The operational user guidance shall be clear and reasonable.

    Setup Guide The developer shall provide the MD including its preparative/setup procedures.

    As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative/setup procedures.

    The preparative/installation procedures shall describe all the steps necessary for secure setup of the MD and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

    Life Cycle Support Life-cycle support is limited to end- user-visible aspects of the life-
    cycle, rather than an examination of the
    MD vendor’s development and configuration management process. This is not meant to diminish the critical role that a developer’s practices play in contributing to the overall trustworthiness of a product; rather, it’s a reflection on the information to be made available for evaluation.

    Labeling of the MD
    This component is targeted at identifying the MD such that it can be distinguished from other products or from other versions of the software and hardware from the same vendor and can be easily specified when being procured by an end user.

The developer shall provide the MD and a reference for the MD.

The MD shall be labeled with its unique reference.

Identification of Security Measures The developer shall produce and provide development security documentation

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 MD design and implementation in its development and manufacture environment.

Application Programming Interface (API)
The developer shall provide documentation of the API available to application developers for the MD. The developer may reference a website accessible to application developers and the evaluator.

The API documentation shall include those interfaces required in this profile.

The API documentation shall clearly indicate to which products and versions each available function applies.
7.2.4 Timely Security Updates
The vendor, in conjunction with any other parties necessary to facilitate update of end-user devices, shall
provide documentation which describes the process for creating and deploying security updates for the mobile device software/firmware. The software to be described includes the operating systems of the application processor and the baseband processor, as well as any firmware.

Timely Security Updates
The vendor, in conjunction with any other parties necessary to facilitate update of end-user devices, shall
provide documentation which describes the process for creating and deploying security updates for the mobile device software/firmware. The software to be described includes the operating systems of the application processor and the baseband processor, as well as any firmware.

The vendor shall identify the maximum time window that may remain open for this process. This time window is defined as the length of time between public disclosure of a vulnerability and the widespread availability of security updates to mobile devices.

Assumptions

1. The Mobile Device will be provisioned for a specific mobile user in the enterprise environment by the administrator prior to use by the mobile user.

2. The administrator will configure the Mobile Device security functions correctly to create the intended security policy.

3. The Mobile User will immediately notify the administrator if the Mobile Device is lost or stolen.

4. The Mobile User is not malicious, and exercises precautions to reduce the risk of loss or theft of the Mobile Device.

Optional Extensions

Optional Extensions are Identified within the Security Requirements.

Outside the TOE's Scope

The Mobile Device is also vulnerable due to the access of service providers who, in their role, can easily eavesdrop on mobile communications or inject malicious or flawed code into the mobile device. At this time, this assurance standard provides few mitigations to the access available to service providers, or adversaries posing as service providers; however, several future requirements addressing this threat are identified, with the expectation that industry will feedback as to the feasibility of such requirements.