National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

PP-Configuration for Mobile Device Fundamentals (MDF), Virtual Private Network (VPN) Clients, and Bluetooth

Version 1.1

15 May 2022

Report Number: CCEVS-VR-PP-0078
Dated: 28 December 2022
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
9800 Savage Road STE 6982
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory
Base and Additional Requirements
Gossamer Security Solutions, Inc.
Columbia, MD

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the PP-Configuration for Mobile Device Fundamentals (MDF), Virtual Private Network (VPN) Clients, and Bluetooth, Version 1.0 (CFG_MDF-VPNC-BT_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Protection Profile for Mobile Device Fundamentals (MDF) (PP_MDF_V3.2) Base-PP, the PP-Module for Virtual Private Network (VPN) Clients, Version 2.3 (MOD_VPNC_V2.3), and the PP-Module for Bluetooth, Version 1.0 (MOD_BT_V1.0). It presents a summary of the CFG_MDF-VPNC-BT_V1.0 and the evaluation results.

Gossamer Security Solutions, Inc., located in Columbia, Maryland, performed the evaluation of the CFG_MDF-VPNC-BT_V1.0 and the MOD_VPNC_V2.3 and MOD_BT_V1.0 contained within the PP-Configuration, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Samsung Electronics, Co., Ltd. Samsung Galaxy Devices on Android 12 – Spring (Samsung Galaxy devices).

This evaluation addressed the base security functional requirements of MOD_VPNC_V2.3 and MOD_BT_V1.0 as part of CFG_MDF-VPNC-BT_V1.0. The PP-Modules define additional requirements, some of which the Samsung Galaxy devices evaluation claimed. The Validation Report (VR) author independently performed an additional review of the PP-Configuration, Base-PP, and PP-Modules as part of the completion of this VR, to confirm they meet the claimed APE and ACE requirements.

The evaluation determined the CFG_MDF-VPNC-BT_V1.0 is both Common Criteria Part 2 Extended and Part 3 Extended. An accredited Information Technology Security Evaluation Facility (ITSEF) evaluated the PP-Configuration and PP-Modules identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Revision 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Revision 5). The Security Target (ST) includes material from the PP_MDF_V3.2, MOD_VPNC_V2.3, and MOD_BT_V1.0; completion of the ASE work units satisfied the APE work unites for this PP and ACE work units for these PP-Modules, but only for the materials defined in these PP-Modules, and only when the PP-Modules are in the defined PP-Configuration.

The evaluation laboratory conducted this evaluation in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS). The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence given.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called CCTLs. CCTLs evaluate products against Protection Profiles (PPs) and PP-Modules that have Evaluation Activities, which are interpretations of the Common Methodology for Information Technology Security Evaluation (CEM) v3.1 workunits specific to the technology described by the PP or PP-Modules. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Modules with at least one corresponding Base-PP.

To promote thoroughness and efficiency, the evaluation of the CFG_MDF-VPNC-BT_V1.0, PP_MDF_V3.2, MOD_VPNC_V2.3, and MOD_BT_V1.0, was performed concurrent with the first product evaluation to claim conformance to the PP-Configuration. In this case, the Target of Evaluation (TOE) was Samsung Galaxy Devices on Android 12 – Spring, performed by Gossamer Security Solutions, Inc. in Columbia, MD.

This evaluation addressed the base security functional requirements of PP_MDF_V3.2, MOD_VPNC_V2.3, and MOD_BT_V1.0 as part of CFG_MDF-VPNC-BT_V1.0. The PP-Module defines additional requirements, some of which the Samsung Galaxy devices evaluation claimed.

PP_MDF_V3.2, MOD_VPNC_V2.3, and MOD_BT_V1.0 contain a set of base requirements that all conformant STs must include, and additionally contain selection-based and objective requirements. Objective requirements are not currently prescribed by the Base-PP or the PP-Modules but are expected to be included in future versions of the Base-PP and PP-Modules. Vendors planning on having evaluations performed against future products are encouraged to plan for these objective requirements to be met. Selection-based requirements are those that must be included based upon the selections made in other requirements and the abilities of the TOE. The Base-PP also includes optional requirements, which may be claimed or omitted at the product vendor's discretion.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the APE_REQ workunits performed against the Base-PP and the ACE_REQ workunits performed against the PP-Modules. When an evaluation laboratory evaluates a TOE against any additional requirements not already referenced in this VR through an existing TOE evaluation, the VR may be amended to include reference to this as additional evidence that the corresponding portions of the CFG_MDF-VPNC-BT_V1.0 were evaluated.

The following identifies the Base-PP and the PP-Modules in the PP-Configuration evaluated by this VR. It also includes supporting information from the initial product evaluation performed against these PP-Modules.

PP-Configuration	PP-Configuration for Mobile Device Fundamentals (MDF), Virtual Private Network (VPN) Clients, and Bluetooth, Version 1.0, 15 May 2022
Base-PP	Protection Profile for Mobile Device Fundamentals, Version 3.2, 15 April 2021 (PP_MDF_V3.2)
Modules in PP-Configuration	PP-Module for Virtual Private Network (VPN) Clients, Version 2.3, 10 August 2021 (MOD_VPNC_V2.3) PP-Module for Bluetooth, Version 1.0, 15 April 2021 (MOD_BT_V1.0)

ST (Base)	Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 12 – Spring Security Target, Version 0.4, 20 May 2022
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	Gossamer Security Solutions, Inc. Columbia, MD

3 CFG_MDF-VPNC-BT_V1.0 Description

CFG_MDF-VPNC-BT_V1.0 is a PP-Configuration that combines the following.

- Protection Profile for Mobile Device Fundamentals, Version 3.2 (PP_MDF_V3.2)
- PP-Module for Virtual Private Network (VPN) Clients, Version 2.3 (MOD_VPNC_V2.3)
- PP-Module for Bluetooth, Version 1.0 (MOD_BT_V1.0)

This PP-Configuration is for a mobile device that includes both VPN client and Bluetooth capabilities according to the requirements of the PP-Configuration.

A VPN Client is a piece of software that allows a computer to establish a VPN with a remote peer or gateway. The VPN allows for confidentiality and integrity of the network traffic that passes over it. Specifically, MOD_VPNC_V2.3 defines IPsec as the mechanism used to implement a VPN. In the context of CFG_MDF-VPNC-BT_V1.0, the VPN client is a software component of a mobile operating system that is integrated with that operating system, with the operating system being part of a standalone mobile device.

A Bluetooth device is a communications standard for short-range wireless transmissions, which is implemented in many commercial devices. It is a logical component that executes on an end-user personal computing or mobile device. In the context of CFG_MDF-VPNC-BT_V1.0, the mobile device includes the hardware and software needed to function as a Bluetooth device.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_MDF-VPNC-BT_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_MDF_V3.2	
A.CONFIG	It is assumed that the TOE's security functions are configured correctly in a manner to ensure that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.
A.NOTIFY	It is assumed that the mobile user will immediately notify the administrator if the Mobile Device is lost or stolen.
A.PRECAUTION	It is assumed that the mobile user exercises precautions to reduce the risk of loss or theft of the Mobile Device.
A.PROPER_USER	Mobile Device users are not willfully negligent or hostile, and use the device within compliance of a reasonable Enterprise security policy.
From MOD_VPNC_V2.3	
A.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.
From MOD_BT_V1.0	
No additional assumptions defined in MOD_BT_V1.0.	

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_MDF-VPNC-BT_V1.0.

Table 2: Threats

Threat Name	Threat Definition
From PP_MDF_V3.2	
T.EAVESDROP	An attacker is 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.
T.NETWORK_ATTACK	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 update of any applications or system software on the device. These attacks also include malicious web pages or email attachments, which are usually delivered to devices over the network.
T.PHYSICAL_ACCESS	An attacker, with physical access, may attempt to access user data on the Mobile Device including credentials. These physical access threats

Threat Name	Threat Definition
	may involve attacks, which attempt to access the device through external hardware ports, impersonate the user authentication mechanisms, through its user interface, and also through direct and possibly destructive access to its storage media. Note: Defending against device re-use after physical compromise is out of scope for this Protection Profile.
T.MALICIOUS_APP	Applications loaded onto the Mobile Device may include malicious or exploitable code. This code could be included intentionally or unknowingly by the developer, perhaps as part of 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 applications 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 applications may give an attacker access to perform network-based or physical attacks that otherwise would have been prevented.
T.PERSISTENT_PRESENCE	Persistent presence on 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 on-going threat in itself. In this case, the device and its data may be controlled by an adversary as well as by its legitimate owner.
From MOD_VPNC_V2.3	
T.TSF_CONFIGURATION	Configuring VPN tunnels is a complex and time-consuming process, and prone to errors if the interface for doing so is not well-specified or well-behaved. The inability to configure certain aspects of the interface may also lead to the mis-specification of the desired communications policy or use of cryptography that may be desired or required for a particular site. This may result in unintended weak or plaintext communications while the user thinks that their data are being protected. Other aspects of configuring the TOE or using its security mechanisms (for example, the update process) may also result in a reduction in the trustworthiness of the VPN client.
T.UNAUTHORIZED_ACCESS	This PP-Module does not include requirements that can protect against an insider threat. Authorized users are not considered hostile or malicious and are trusted to follow appropriate guidance. Only authorized personnel should have access to the system or device that contains the IPsec VPN client. Therefore, the primary threat agents are the unauthorized entities that try to gain access to the protected network (in cases where tunnel mode is used) or to plaintext data that traverses the public network (regardless of whether transport mode or tunnel mode is used). The endpoint of the network communication can be both geographically and logically distant from the TOE, and can pass through a variety of other systems. These intermediate systems may be under the control of the adversary, and offer an opportunity for communications over the network to be compromised. Plaintext communication over the network may allow critical data (such as passwords, configuration settings, and user data) to be read and/or manipulated directly by intermediate systems, leading to a compromise of the TOE or to the secured environmental system(s) that

Threat Name	Threat Definition
	the TOE is being used to facilitate communications with. IPsec can be used to provide protection for this communication; however, there are myriad options that can be implemented for the protocol to be compliant to the protocol specification listed in the RFC. Some of these options can have negative impacts on the security of the connection. For instance, using a weak encryption algorithm (even one that is allowed by the RFC, such as DES) can allow an adversary to read and even manipulate the data on the encrypted channel, thus circumventing countermeasures in place to prevent such attacks. Further, if the protocol is implemented with little-used or non-standard options, it may be compliant with the protocol specification but will not be able to interact with other, diverse equipment that is typically found in large enterprises. Even though the communication path is protected, there is a possibility that the IPsec peer could be duped into thinking that a malicious third-party user or system is the TOE. For instance, a middleman could intercept a connection request to the TOE, and respond to the request as if it were the TOE. In a similar manner, the TOE could also be duped into thinking that it is establishing communications with a legitimate IPsec peer when in fact it is not. An attacker could also mount a malicious man-in-the-middle-type of attack, in which an intermediate system is compromised, and the traffic is proxied, examined, and modified by this system. This attack can even be mounted via encrypted communication channels if appropriate countermeasures are not applied. These attacks are, in part, enabled by a malicious attacker capturing network traffic (for instance, an authentication session) and "playing back" that traffic in order to fool an endpoint into thinking it was communicating with a legitimate remote entity.
T.USER_DATA_REUSE	Data traversing the TOE could inadvertently be sent to a different user; since these data may be sensitive, this may cause a compromise that is unacceptable. The specific threat that must be addressed concerns user data that is retained by the TOE in the course of processing network traffic that could be inadvertently re-used in sending network traffic to a user other than that intended by the sender of the original network traffic.
T.TSF_FAILURE	Security mechanisms of the TOE generally build up from a primitive set of mechanisms (e.g., memory management, privileged modes of process execution) to more complex sets of mechanisms. Failure of the primitive mechanisms could lead to a compromise in more complex mechanisms, resulting in a compromise of the TSF.
From MOD_BT_V1.0	
None defined – the PP-Module notes that the threats that apply to Bluetooth functionality are the same as those defined in the Base-PP as T.NETWORK_EAVESDROP and T.NETWORK_ATTACK because the Bluetooth capability is simply another interface over which those threats may be manifested.	

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_MDF-VPNC-BT_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From PP_MDF_V3.2	
No OSPs defined in PP_MDF_V3.2.	
From MOD_VPNC_V2.3	
No OSPs defined in MOD_VPNC_V2.3.	
From MOD_BT_V1.0	
No OSPs defined in MOD_BT_V1.0.	

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_MDF-VPNC-BT_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_MDF_V3.2	
O.PROTECTED_COMMS	To address the network eavesdropping (T.EAVESDROP) and network attack (T.NETWORK) threats described in Section 3.1 Threats, concerning wireless transmission of Enterprise and user data and configuration data between the TOE and remote network entities, conformant TOEs will use a trusted communication path. The TOE will be capable of communicating using one (or more) of these standard protocols: IPsec, DTLS, TLS, HTTPS, or Bluetooth. The protocols are specified by RFCs that offer a variety of implementation choices. Requirements have been imposed on some of these choices (particularly those for cryptographic primitives) to provide interoperability and resistance to cryptographic attack. While conformant TOEs must support all of the choices specified in the ST including any optional SFRs defined in this PP, they may support additional algorithms and protocols. If such additional mechanisms are not evaluated, guidance must be given to the administrator to make clear the fact that they were not evaluated.
O.STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of a Mobile Device (T.PHYSICAL), conformant TOEs will use data-at-rest protection. The TOE will be capable of encrypting data and keys stored on the device and will prevent unauthorized access to encrypted data.
O.CONFIG	To ensure a Mobile Device protects user and enterprise data that it may store or process, conformant TOEs will provide the capability to configure and apply security policies defined by the user and the Enterprise Administrator. If Enterprise security policies are configured these must be applied in precedence of user specified security policies.
O.AUTH	To address the issue of loss of confidentiality of user data in the event of loss of a Mobile Device (T.PHYSICAL), users are required to enter an authentication factor to the device prior to accessing protected functionality and data. Some non-sensitive functionality (e.g., emergency calling, text notification) can be accessed prior to entering the authentication factor. The device will automatically lock following

TOE Security Objective	TOE Security Objective Definition
	a configured period of inactivity in an attempt to ensure authorization will be required in the event of the device being lost or stolen. Authentication of the endpoints of a trusted communication path is required for network access to ensure attacks are unable to establish unauthorized network connections to undermine the integrity of the device. Repeated attempts by a user to authorize to the TSF will be limited or throttled to enforce a delay between unsuccessful attempts.
O.INTEGRITY	To ensure the integrity of the Mobile Device is maintained conformant TOEs will perform self-tests to ensure the integrity of critical functionality, software/firmware and data has been maintained. The user shall be notified of any failure of these self-tests. This will protect against the threat T.PERSISTENT. To address the issue of an application containing malicious or flawed code (T.FLAWAPP), the integrity of downloaded updates to software/firmware will be verified prior to installation/execution of the object on the Mobile Device. In addition, the TOE will restrict applications to only have access to the system services and data they are permitted to interact with. The TOE will further protect against malicious applications from gaining access to data they are not authorized to access by randomizing the memory layout.
O.PRIVACY	In a BYOD environment (use cases 3 and 4), a personally-owned mobile device is used for both personal activities and enterprise data. Enterprise management solutions may have the technical capability to monitor and enforce security policies on the device. However, the privacy of the personal activities and data must be ensured. In addition, since there are limited controls that the enterprise can enforce on the personal side, separation of personal and enterprise data is needed. This will protect against the T.FLAWAPP and T.PERSISTENT threats.
From MOD_VPNC_V2.3	
O.AUTHENTICATION	To address the issues associated with unauthorized disclosure of information in transit, a compliant TOE's authentication ability (IPsec) will allow the TSF to establish VPN connectivity with a remote VPN gateway or peer and ensure that any such connection attempt is both authenticated and authorized. This objective also ensures the protection of data in transit by ensuring that interfaces exist for non-TOE entities to invoke the TSF to establish an IPsec channel.
O.CRYPTOGRAPHIC_FUNCTIONS	To address the issues associated with unauthorized disclosure of information in transit, a compliant TOE will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.KNOWN_STATE	The TOE will provide sufficient measures to ensure it is operating in a known state. At minimum this includes management functionality to allow the security functionality to be configured and self-test functionality that allows it to assert its own integrity. It may also include auditing functionality that can be used to determine the operational behavior of the TOE.

TOE Security Objective	TOE Security Objective Definition
O.NONDISCLOSURE	To address the issues associated with unauthorized disclosure of information at rest, a compliant TOE will ensure that non-persistent data is purged when no longer needed. The TSF may also implement measures to protect against the disclosure of stored cryptographic keys and data through implementation of protected storage and secure erasure methods. The TOE may optionally also enforce split-tunneling prevention to ensure that data in transit cannot be disclosed inadvertently outside of the IPsec tunnel.
From MOD_BT_V1.0	
This PP-Module defines no additional TOE security objectives beyond those defined in the Base-PP. However, the SFRs defined in this PP-Module will assist in the achievement of O.PROTECTED_COMMS in the Base-PP.	

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_MDF-VPNC-BT_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_MDF_V3.2	
OE.CONFIG	TOE administrators will configure the Mobile Device security functions correctly to create the intended security policy.
OE.NOTIFY	The Mobile User will immediately notify the administrator if the Mobile Device is lost or stolen.
OE.PRECAUTION	The mobile device user exercises precautions to reduce the risk of loss or theft of the Mobile Device.
OE.DATA_PROPER_USER	Administrators take measures to ensure that mobile device users are adequately vetted against malicious intent and are made aware of the expectations for appropriate use of the device.
From MOD_VPNC_V2.3	
OE.NO_TOE_BYPASS	Information cannot flow onto the network to which the VPN client's host is connected without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
OE.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.
From MOD_BT_V1.0	
No operational environment objectives defined in MOD_BT_V1.0.	

5 Functional Requirements

As indicated above, CFG_MDF-VPNC-BT_V1.0 includes the PP_MDF_V3.2, MOD_VPNC_V2.3, and MOD_BT_V1.0.

Requirements in the PP_MDF_V3.2, MOD_VPNC_V2.3, and MOD_BT_V1.0 are comprised of the "base" requirements, additional requirements that are optional, selection-based, or objective, and, in the case of the PP-Modules, additional requirements that are dependent on the Base-PP that the PP-Modules are used with. The following table contains the "base" requirements that were validated as part of the Samsung Galaxy devices evaluation activities referenced above as well as the additional requirements that depend on the Base-PP that is claimed. In the case of the Samsung Galaxy devices evaluation, only those that apply when PP_MDF_V3.2 is the Base-PP were claimed by the TOE; those associated with other Base-PPs did not apply and have been evaluated through evaluation of the PP-Module workunits.

Table 6: Base-PP Security Functional Requirements

Requirement Class	Requirement Component	Verified By
From MOD_VPNC_V2.3		
Modified when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Module Evaluation
	FCS_CKM.2: Cryptographic Key Establishment	Module Evaluation
	FCS_COP.1(1): Cryptographic Operation (Encryption/Decryption)	Module Evaluation
Additional when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FCS: Cryptographic Support	FCS_CKM_EXT.2: Cryptographic Key Storage	Module Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.3: X.509 Certificate Authentication	Module Evaluation
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel	Module Evaluation
Modified when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM.2/UNLOCKED: Cryptographic Key Establishment	Samsung Galaxy Devices on Android 12 – Spring
	FCS_COP.1/ENCRYPT: Cryptographic Operation	Samsung Galaxy Devices on Android 12 – Spring
FDP: User Data Protection	FDP_IFC_EXT.1: Subset Information Flow Control	Samsung Galaxy Devices on Android 12 – Spring
FIA: Identification and Authentication	FIA_X509_EXT.2: X.509 Certificate Authentication	Samsung Galaxy Devices on Android 12 – Spring
FMT: Security Management	FMT_SMF_EXT.1: Specification of Management Functions	Samsung Galaxy Devices on Android 12 – Spring

Requirement Class	Requirement Component	Verified By
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Trusted Channel Communication	Samsung Galaxy Devices on Android 12 – Spring
Additional when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
There are no additional SFRs when the MDF PP is the Base-PP.		
Modified when the Protection Profile for Application Software is the Base-PP		
FCS: Cryptographic Support	FCS_CKM.1(1): Cryptographic Asymmetric Key Generation	Module Evaluation
	FCS_CKM.2: Cryptographic Key Establishment	Module Evaluation
	FCS_CKM_EXT.1: Cryptographic Key Generation Services	Module Evaluation
	FCS_COP.1(1): Cryptographic Operation – Encryption/Decryption	Module Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.2: X.509 Certificate Authentication	Module Evaluation
FTP: Trusted Path/Channels	FTP_DIT_EXT.1: Protection of Data in Transit	Module Evaluation
Additional when the Protection Profile for Application Software is the Base-PP		
FCS: Cryptographic Support	FCS_CKM_EXT.2: Cryptographic Key Storage	Module Evaluation
	FCS_CKM_EXT.4: Cryptographic Key Destruction	Module Evaluation
Modified when the Protection Profile for Mobile Device Management is the Base-PP		
FCS: Cryptographic Support	FCS_CKM_EXT.1: Cryptographic Key Generation	Module Evaluation
	FCS_CKM_EXT.2: Cryptographic Key Establishment	Module Evaluation
	FCS_COP.1(1): Cryptographic Operation (Confidentiality Algorithms)	Module Evaluation
FIA: Identification and Authentication	FIA_X509_EXT.2: X.509 Certificate Authentication	Module Evaluation
FPT: Protection of the TSF	FPT_ITT.1(1): Basic Internal TSF Data Transfer Protection	Module Evaluation
FTP: Trusted Path/Channels	FTP_ITC.1(1): Inter-TSF Trusted Channel (Authorized IT Entities)	Module Evaluation
	FTP_TRP.1(1): Trusted Path (for Remote Administration)	Module Evaluation
Additional when the Protection Profile for Mobile Device Management is the Base-PP		
There are no additional SFRs when the MDM PP is the Base-PP.		
From MOD_BT_V1.0		
Modified when the Protection Profile for Mobile Device Fundamentals is the Base-PP		

Requirement Class	Requirement Component	Verified By
FMT: Security Management	FMT_SMF_EXT.1: Specification of Management Functions	Samsung Galaxy Devices on Android 12 – Spring
Additional when the Protection Profile for Mobile Device Fundamentals is the Base-PP		
FMT: Security Management	FMT_SMF_EXT.1/BT: Specification of Management Functions	Samsung Galaxy Devices on Android 12 – Spring
Modified when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior	Module Evaluation
	FMT_SMF_EXT.1: Specification of Management Functions	Module Evaluation
Additional when the Protection Profile for General Purpose Operating Systems is the Base-PP		
FMT: Security Management	FMT_MOF_EXT.1/BT: Management of Security Functions Behavior	Module Evaluation
	FMT_SMF_EXT.1/BT: Specification of Management Functions	Module Evaluation

The following table contains the “base” requirements specific to the TOE.

Table 7: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
From PP_MDF_V3.2		
FAU: Security Audit	FAU_GEN.1: Audit Data Generation	Samsung Galaxy Devices on Android 12 – Spring
	FAU_STG.1: Audit Storage Protection	Samsung Galaxy Devices on Android 12 – Spring
	FAU_STG.4: Prevention of Audit Data Loss	Samsung Galaxy Devices on Android 12 – Spring
FCS: Cryptographic Support	FCS_CKM.1: Cryptographic Key Generation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM.2/UNLOCKED: Cryptographic Key Establishment	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM.2/LOCKED: Cryptographic Key Establishment	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM_EXT.1: Cryptographic Key Support	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM_EXT.2: Cryptographic Key Random Generation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM_EXT.3: Cryptographic Key Generation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM_EXT.4: Key Destruction	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM_EXT.5: TSF Wipe	Samsung Galaxy Devices on Android 12 – Spring
	FCS_CKM_EXT.6: Salt Generation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_COP.1/ENCRYPT: Cryptographic Operation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_COP.1/HASH: Cryptographic Operation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_COP.1/SIGN: Cryptographic Operation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_COP.1/KEYHMAC: Cryptographic Operation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_HTTPS_EXT.1: HTTPS Protocol	Samsung Galaxy Devices on Android 12 – Spring
	FCS_IV_EXT.1: Initialization Vector Generation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_RBG_EXT.1: Random Bit Generation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_SRV_EXT.1: Cryptographic Algorithm Services	Samsung Galaxy Devices on Android 12 – Spring

	FCS_STG_EXT.2: Encrypted Cryptographic Key Storage	Samsung Galaxy Devices on Android 12 – Spring
	FCS_STG_EXT.3: Integrity of Encrypted Key Storage	Samsung Galaxy Devices on Android 12 – Spring
FDP: User Data Protection	FDP_ACF_EXT.1: Access Control for System Services	Samsung Galaxy Devices on Android 12 – Spring
	FDP_DAR_EXT.1: Protected Data Encryption	Samsung Galaxy Devices on Android 12 – Spring
	FDP_DAR_EXT.2: Sensitive Data Encryption	Samsung Galaxy Devices on Android 12 – Spring
	FDP_IFC_EXT.1: Subset Information Flow Control	Samsung Galaxy Devices on Android 12 – Spring
	FDP_STG_EXT.1: Subset Information Flow Control	Samsung Galaxy Devices on Android 12 – Spring
	FDP_UPC_EXT.1/APPS: Inter-TSF User Data Transfer Protection (Applications)	Samsung Galaxy Devices on Android 12 – Spring
FIA: Identification and Authentication	FIA_AFL_EXT.1: Authentication Failure Handling	Samsung Galaxy Devices on Android 12 – Spring
	FIA_PMG_EXT.1: Password Management	Samsung Galaxy Devices on Android 12 – Spring
	FIA_TRT_EXT.1: Authentication Throttling	Samsung Galaxy Devices on Android 12 – Spring
	FIA_UAU.5: Multiple Authentication Mechanisms	Samsung Galaxy Devices on Android 12 – Spring
	FIA_UAU.6: Re-Authentication	Samsung Galaxy Devices on Android 12 – Spring
	FIA_UAU.7: Protected Authentication Feedback	Samsung Galaxy Devices on Android 12 – Spring
	FIA_UAU_EXT.1: Authentication for Cryptographic Operation	Samsung Galaxy Devices on Android 12 – Spring
	FIA_UAU_EXT.2: Timing of Authentication	Samsung Galaxy Devices on Android 12 – Spring
	FIA_X509_EXT.1: X.509 Validation of Certificates	Samsung Galaxy Devices on Android 12 – Spring
	FIA_X509_EXT.2: X.509 Certificate Authentication	Samsung Galaxy Devices on Android 12 – Spring
	FIA_X509_EXT.3: Request Validation of Certificates	Samsung Galaxy Devices on Android 12 – Spring
FMT: Security Management	FMT_MOF_EXT.1: Management of Security Functions Behavior	Samsung Galaxy Devices on Android 12 – Spring
	FMT_SMF_EXT.1: Specification of Management Functions	Samsung Galaxy Devices on Android 12 – Spring

	FMT_SMF_EXT.2: Specification of Remediation Actions	Samsung Galaxy Devices on Android 12 – Spring
FPT: Protection of the TSF	FPT_AEX_EXT.1: Application Address Space Layout Randomization	Samsung Galaxy Devices on Android 12 – Spring
	FPT_AEX_EXT.2: Memory Page Permissions	Samsung Galaxy Devices on Android 12 – Spring
	FPT_AEX_EXT.3: Stack Overflow Protection	Samsung Galaxy Devices on Android 12 – Spring
	FPT_AEX_EXT.4: Domain Isolation	Samsung Galaxy Devices on Android 12 – Spring
	FPT_JTA_EXT.1: JTAG Disablement	Samsung Galaxy Devices on Android 12 – Spring
	FPT_KST_EXT.1: Key Storage	Samsung Galaxy Devices on Android 12 – Spring
	FPT_KST_EXT.2: No Key Transmission	Samsung Galaxy Devices on Android 12 – Spring
	FPT_NOT_EXT.1: Self-Test Notification	Samsung Galaxy Devices on Android 12 – Spring
	FPT_STM.1: Reliable Time Stamps	Samsung Galaxy Devices on Android 12 – Spring
	FPT_TST_EXT.1: TSF Cryptographic Functionality Testing	Samsung Galaxy Devices on Android 12 – Spring
	FPT_TST_EXT.2/PREKERNEL: TSF Integrity Checking (Pre-Kernel)	Samsung Galaxy Devices on Android 12 – Spring
	FPT_TUD_EXT.1: Trusted Update: TSF Version Query	Samsung Galaxy Devices on Android 12 – Spring
	FPT_TUD_EXT.2: TSF Update Verification	Samsung Galaxy Devices on Android 12 – Spring
	FPT_TUD_EXT.3: Application Signing	Samsung Galaxy Devices on Android 12 – Spring
FTA: TOE Access	FTA_SSL_EXT.1: TSF- and User-Initiated Locked State	Samsung Galaxy Devices on Android 12 – Spring
FTP: Trusted Path/Channels	FTP_ITC_EXT.1: Trusted Channel Communication	Samsung Galaxy Devices on Android 12 – Spring
From MOD_VPNC_V2.3		
FCS: Cryptographic Support	FCS_CKM.1/VPN: Cryptographic Key Generation (IKE)	Samsung Galaxy Devices on Android 12 – Spring
	FCS_IPSEC_EXT.1: IPsec	Samsung Galaxy Devices on Android 12 – Spring
FDP: User Data Protection	FDP_RIP.2: Full Residual Information Protection	Samsung Galaxy Devices on Android 12 – Spring

FMT: Security Management	FMT_SMF.1/VPN: Specification of Management Functions (VPN)	Samsung Galaxy Devices on Android 12 – Spring
FPT: Protection of the TSF	FPT_TST_EXT.1/VPN: TSF Self-Test (VPN Client)	Samsung Galaxy Devices on Android 12 – Spring
From MOD_BT_V1.0		
FAU: Security Audit	FAU_GEN.1/BT: Audit Data Generation (Bluetooth)	Samsung Galaxy Devices on Android 12 – Spring
FCS: Cryptographic Support	FCS_CKM_EXT.8: Bluetooth Key Generation	Samsung Galaxy Devices on Android 12 – Spring
FIA: Identification and Authentication	FIA_BLT_EXT.1: Bluetooth User Authorization	Samsung Galaxy Devices on Android 12 – Spring
	FIA_BLT_EXT.2: Bluetooth Mutual Authentication	Samsung Galaxy Devices on Android 12 – Spring
	FIA_BLT_EXT.3: Rejection of Duplicate Bluetooth Connections	Samsung Galaxy Devices on Android 12 – Spring
	FIA_BLT_EXT.4: Secure Simple Pairing	Samsung Galaxy Devices on Android 12 – Spring
	FIA_BLT_EXT.6: Trusted Bluetooth Device User Authorization	Samsung Galaxy Devices on Android 12 – Spring
	FIA_BLT_EXT.7: Untrusted Bluetooth Device User Authorization	Samsung Galaxy Devices on Android 12 – Spring
FTP: Trusted Path/Channels	FTP_BLT_EXT.1: Bluetooth Encryption	Samsung Galaxy Devices on Android 12 – Spring
	FTP_BLT_EXT.2: Persistence of Bluetooth Encryption	Samsung Galaxy Devices on Android 12 – Spring
	FTP_BLT_EXT.3/BR: Bluetooth Encryption Parameters (BR/EDR)	Samsung Galaxy Devices on Android 12 – Spring

The following table contains the "**Optional**" requirements contained in Appendix A.1 and A.3 of the Base-PP and PP-Modules, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given optional requirement, the VR author has evaluated it through the completion of the relevant APE and ACE work units and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 7: Optional Requirements

Requirement Class	Requirement Component	Verified By
From PP_MDF_V3.2		
FDP: User Data Protection	FDP_UPC_EXT.1/BLUETOOTH: Inter-TSF User Data Transfer Protection (Bluetooth)	Samsung Galaxy Devices on Android 12 – Spring
FIA: Identification and Authentication	FIA_UAU_EXT.4: Secondary User Authentication	Samsung Galaxy Devices on Android 12 – Spring
From MOD_VPNC_V2.3		
FDP: User Data Protection	FDP_IFC_EXT.1/VPN: Subset Information Flow Control (VPN)	Samsung Galaxy Devices on Android 12 – Spring
From MOD_BT_V1.0		
The MOD_BT_V1.0 does not define any additional optional requirements.		

The following table contains the "**Selection-Based**" requirements contained in Appendix B of the Base-PP and PP-Modules, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given selection-based requirement, the VR author has evaluated it through the completion of the relevant APE and ACE work units and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 8: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
From PP_MDF_V3.2		
FCS: Cryptographic Support	FCS_CKM_EXT.7: Cryptographic Key Support (REK)	PP Evaluation
FDP: User Data Protection	FDP_ACF_EXT.2: Access Control for System Resources	Samsung Galaxy Devices on Android 12 – Spring
FIA: Identification and Authentication	FIA_BMG_EXT.1: Accuracy of Biometric Authentication	Samsung Galaxy Devices on Android 12 – Spring
FPT: Protection of the TSF	FPT_TST_EXT.3: TSF Integrity Testing	PP Evaluation
	FPT_TUD_EXT.4: Trusted Update Verification	PP Evaluation
From MOD_VPNC_V2.3		
FIA: Identification and Authentication	FIA_PSK_EXT.1: Pre-Shared Key Composition	Samsung Galaxy Devices on Android 12 – Spring

Requirement Class	Requirement Component	Verified By
From PP_MDF_V3.2		
FCS: Cryptographic Support	FCS_CKM_EXT.7: Cryptographic Key Support (REK)	PP Evaluation
FDP: User Data Protection	FDP_ACF_EXT.2: Access Control for System Resources	Samsung Galaxy Devices on Android 12 – Spring
FIA: Identification and Authentication	FIA_BMG_EXT.1: Accuracy of Biometric Authentication	Samsung Galaxy Devices on Android 12 – Spring
FPT: Protection of the TSF	FPT_TST_EXT.3: TSF Integrity Testing	PP Evaluation
	FPT_TUD_EXT.4: Trusted Update Verification	PP Evaluation
From MOD_VPNC_V2.3		
From MOD_BT_V1.0		
FTP: Trusted Path/Channels	FTP_BLT_EXT.3/LE: Bluetooth Encryption Parameters (LE)	Samsung Galaxy Devices on Android 12 – Spring

The following table contains the "**Objective**" requirements contained in Appendix A.2 of the Base-PP and PP-Modules, and an indication of how those requirements were evaluated (from the list in the *Identification* section above). If no completed evaluations have claimed a given objective requirement, the VR author has evaluated it through the completion of the relevant APE and ACE work units and has indicated its verification through "PP Evaluation" or "Module Evaluation."

Table 9: Objective Requirements

Requirement Class	Requirement Component	Verified By
From PP_MDF_V3.2		
FAU: Security Audit	FAU_SAR.1: Audit Review	Samsung Galaxy Devices on Android 12 – Spring
	FAU_SEL.1: Selective Audit	PP Evaluation
FCS: Cryptographic Support	FCS_RBG_EXT.2: Random Bit Generator State Preservation	Samsung Galaxy Devices on Android 12 – Spring
	FCS_RBG_EXT.3: Support for Personalization String	PP Evaluation
	FCS_SRV_EXT.2: Cryptographic Algorithm Services	Samsung Galaxy Devices on Android 12 – Spring
FDP: User Data Protection	FDP_ACF_EXT.3: Security Attribute Based Access Control	Samsung Galaxy Devices on Android 12 – Spring
	FDP_BCK_EXT.1: Application Backup	PP Evaluation
	FDP_BLT_EXT.1: Limitation of Bluetooth Device Access	PP Evaluation
FIA: Identification and Authentication	FIA_BMG_EXT.2: Biometric Enrollment	PP Evaluation
	FIA_BMG_EXT.3: Biometric Verification	PP Evaluation
	FIA_BMG_EXT.4: Biometric Templates	PP Evaluation
	FIA_BMG_EXT.5: Handling Unusual Biometric Templates	PP Evaluation
	FIA_BMG_EXT.6: Spoof Detections for Biometrics	PP Evaluation
	FIA_X509_EXT.4: X.509 Certificate Enrollment	PP Evaluation
	FIA_X509_EXT.5: X.509 Certificate Requests	PP Evaluation
FMT: Security Management	FMT_SMF_EXT.3: Current Administrator	Samsung Galaxy Devices on Android 12 – Spring
FPT: Protection of the TSF	FPT_AEX_EXT.5: Kernel Address Space Layout Randomization	Samsung Galaxy Devices on Android 12 – Spring
	FPT_AEX_EXT.6: Write or Execute Memory Page Permissions	Samsung Galaxy Devices on Android 12 – Spring
	FPT_AEX_EXT.7: Heap Overflow Protection	PP Evaluation
	FPT_BBD_EXT.1: Application Processor Mediation	Samsung Galaxy Devices on Android 12 – Spring
	FPT_BLT_EXT.1: Limitation of Bluetooth Profile Support	PP Evaluation
	FPT_NOT_EXT.2: Self-Test Notification	PP Evaluation
	FPT_TST_EXT.2/POSTKERNEL: TSF Integrity Checking (Post-Kernel)	Samsung Galaxy Devices on Android 12 – Spring
	FPT_TUD_EXT.5: Application Verification	PP Evaluation

	FPT_TUD_EXT.6: Trusted Update Verification	Samsung Galaxy Devices on Android 12 – Spring
FTA: TOE Access	FTA_TAB.1: Default TOE Access Banners	Samsung Galaxy Devices on Android 12 – Spring
From MOD_VPNC_V2.3		
FAU: Security Audit	FAU_GEN.1/VPN: Audit Data Generation (VPN Client)	Module Evaluation
	FAU_SEL.1/VPN: Selective Audit (VPN Client)	Module Evaluation
From MOD_BT_V1.0		
FIA: Identification and Authentication	FIA_BLT_EXT.5: Bluetooth Secure Connections	Module Evaluation

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_MDF_V3.2. The SARs defined in that PP are applicable to MOD_VPNC_V2.3 and MOD_BT_V1.0, as well as CFG_MDF-VPNC-BT_V1.0 as a whole.

7 Results of the Evaluation

Note that for APE and ACE elements and workunits identical to ASE elements and workunits, the lab performed the ACE workunits concurrent to the ASE workunits.

Table 10: Evaluation Results: PP_MDF_V3.2

APE Requirement	Evaluation Verdict	Verified By
APE_INT.1	Pass	PP Evaluation
APE_CCL.1	Pass	PP Evaluation
APE_SPD.1	Pass	PP Evaluation
APE_OBJ.1	Pass	PP Evaluation
APE_ECD.1	Pass	PP Evaluation
APE_REQ.1	Pass	PP Evaluation

Table 10: Evaluation Results: MOD_VPNC_V2.3

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module Evaluation
ACE_CCL.1	Pass	Module Evaluation
ACE_SPD.1	Pass	Module Evaluation
ACE_OBJ.1	Pass	Module Evaluation
ACE_ECD.1	Pass	Module Evaluation
ACE_REQ.1	Pass	Module Evaluation

Table 10: Evaluation Results: MOD_BT_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	Module Evaluation
ACE_CCL.1	Pass	Module Evaluation
ACE_SPD.1	Pass	Module Evaluation
ACE_OBJ.1	Pass	Module Evaluation
ACE_ECD.1	Pass	Module Evaluation
ACE_REQ.1	Pass	Module Evaluation

Table 10: Evaluation Results: CFG_MDF-VPNC-BT_V1.0

ACE Requirement	Evaluation Verdict	Verified By
ACE_MCO.1	Pass	PP-Config Evaluation
ACE_CCO.1	Pass	PP-Config Evaluation

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate unambiguously that a given implementation is correct with respect to the formal model.
- **Evaluation**. An IT product's assessment against the Common Criteria using the Common Criteria Evaluation Methodology as the supplemental guidance, interprets it in the MOD_VPNC_V2.3 and MOD_BT_V1.0 Evaluation Activities to determine whether the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process the CCEVS Validation Body uses that leads to the issuance of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 5, dated: April 2017.

[2] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 5, dated: April 2017.

[3] Common Criteria Project Sponsoring Organizations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 5, dated: April 2017.

[4] Common Criteria Project Sponsoring Organizations. *Common Evaluation Methodology for Information Technology Security*, Version 3.1, Revision 5, dated: April 2017.

[5] CC and CEM addenda – Exact Conformance, Selection-Based SFRs, Optional SFRs, Version 0.5, dated: May 2017.

[6] Protection Profile for Mobile Device Fundamentals, Version 3.2, 15 April 2021.

[7] PP-Module for Virtual Private Network (VPN) Clients, Version 2.3, 10 August 2021.

[8] PP-Module for Bluetooth, Version 1.0, 15 April 2021.

[9] PP-Configuration for Mobile Device Fundamentals (MDF), Virtual Private Network (VPN) Clients, and Bluetooth, Version 1.0, 15 May 2022.

[10] Samsung Electronics Co., Ltd. Samsung Galaxy Devices on Android 12 – Spring Security Target, Version 0.4, 20 May 2022.