National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

PP-Configuration for Mobile Device Fundamentals (MDF), Mobile Device Management (MDM) Agents, and Virtual Private Network (VPN) Clients, Version 1.0, 28 February 2020

Report Number: CCEVS-VR-PP-0064
Dated: 26 January 2021
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6982
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base Requirements

atsec Information Security Corporation

Austin, Texas

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, MDM Agents, and Virtual Private Network Clients Version 1.0 (CFG_MDF-MDM_AGENT-VPNC_V1.0). This PP-Configuration defines how to evaluate a TOE that claims conformance to the Mobile Device Fundamentals (PP_MD_V3.1) PP, PP-Module for MDM Agent Version 1.0 (MOD_MDM_AGENT_V1.0) and PP-Module for VPN Clients Version 2.1 (MOD_VPN_CLI_V2.1). It presents a summary of the CFG_MDF-MDM_AGENT-VPNC_V1.0 and the evaluation results.

Atsec Information Security Corporation, located in Austin, Texas performed the evaluation of the CFG_MDF-MDM_AGENT- VPNC_V1.0, concurrent with the first product evaluation against the PP-Configuration's requirements. The evaluated product was Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices.

This evaluation addressed the base security functional requirements of MOD_MDM_AGENT_V1.0 as part of CFG_MDF-MDM_AGENT-VPNC_V1.0. The Mobile Device Fundamentals (PP_MD_3.1) and the VPN Client PP-Module (MOD_VPN_CLI_V2.1) were previously validated to ensure compliance with Common Criteria requirements. The results of that evaluation were included in in Validation Report Number CCEVS-VR-PP-0050, Version 1.0, dated 11 June 2019. The Validation Report (VR) author independently performed an additional review of the PP-Configuration and PP-Modules as part of the completion of this VR, to confirm they meet the claimed ACE requirements.

The evaluation determined the CFG_MDF-MDM_AGENT- VPNC_V1.0 is both Common Criteria Part 2 Extended and Part 3 Extended. A NIAP-approved Common Criteria Testing Laboratory (CCTL) evaluated the PP-Configuration and its components identified in this VR using the Common Methodology for IT Security Evaluation (Version 3.1, Release 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Release 5). The Security Target (ST) includes material from both PP_MD_V3.1, MOD_MDM_AGENT_V1.0 and MOD_VPN_CLI_V2.1; completion of the ASE work units satisfied the ACE work units for the materials defined in the PP-Modules, and only when the PP-Modules are components of the defined PP-Configuration. The ST also claims conformance to the PP_WLAN_CLI_EP_V.10, but these materials are separate from CFG_MDF-MDM_AGENT- VPNC_V1.0 and are therefore outside the scope of this VR.

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 (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 work units specific to the technology described by the PP or PP-Module. Products may only be evaluated against PP-Modules when a PP-Configuration is defined to include the PP-Module with at least one corresponding Base-PP.

In order to promote thoroughness and efficiency, the evaluation of the CFG_MDF-MDM_AGENT- VPNC_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 Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices, performed by Atsec Information Security Corporation in Austin, Texas.

This evaluation addressed the base security functional requirements of MOD_MDM_AGENT_V1.0 as part of CFG_MDF-MDM_AGENT_V1.0. MOD_MDM_AGENT_V1.0 contains a set of base requirements that all conformant STs must include, and additionally contains objective requirements. Objective requirements specify optional functionality that the PP authors consider candidates for becoming mandatory requirements in the future.

The VR authors evaluated all discretionary requirements not claimed in the initial TOE evaluation as part of the evaluation of the ACE_REQ work units performed against the PP-Module. 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-MDM_AGENT- VPNC_V1.0 were evaluated. The following identifies the PP-Configuration, and its components, evaluated by this VR. It also includes supporting information from the initial product evaluation performed against this PP-Configuration.

PP-Configuration	PP-Configuration for Mobile Device Fundamentals (MDF), Mobile Device Management (MDM) Agents, and Virtual Private Network (VPN) Clients Version 1.0
Base-PP	Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 June 2017
PP-Module(s) in PP-Configuration	PP-Module for MDM Agents, Version 1.0, 25 April 2019 PP-Module for VPN Clients, Version 2.1, 05 October 2017
ST (Base)	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices Security Target (ST), Version 1.7, dated 2020-11-10
Assurance Activity	Assurance Activity Report for Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices Assurance Activity Report, Version 1.4, 10 November 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5
Conformance Result	CC Part 2 Extended, CC Part 3 Extended
CCTL	atsec information security corporation

3 CFG_MDF-MDM_AGENT- VPNC_V1.0 Description

This PP-Configuration includes the following components:

- Base-PP: Protection Profile for Mobile Device Fundamentals, Version 3.1 (PP_MD_V3.1)
- PP-Module: PP-Module for MDM Agents, Version 1.0 (MOD_MDM_AGENT_V1.0)
- PP-Module: PP-Module for Virtual Private Network (VPN) Clients, Version 2.1 (MOD_VPN_CLI_V2.1)

This PP-Configuration is for a mobile device that is bundled with a VPN Client and has a Mobile Device Management Agent running on it according to the requirements of the PP-Configuration.

4 Security Problem Description and Objectives

4.1 Assumptions

Table 1 shows the assumptions defined in the individual components of CFG_MDF-MDM_AGENT- VPNC_V1.0.

Table 1: Assumptions

Assumption Name	Assumption Definition
From PP_MD_V3.1	
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.
From MOD_MDM_AGENT_V1.0	
A.CONNECTIVITY	The TOE relies on network connectivity to carry out its management activities. The TOE will robustly handle instances when connectivity is unavailable or unreliable.
A.MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon mobile platform and hardware evaluated against the MDF PP and assured to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM Agent.
A.PROPER_ADMIN	One or more competent, trusted personnel who are not careless, willfully negligent, or hostile, are assigned and authorized as the TOE Administrators, and do so using and abiding by guidance documentation.
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_VPN_CLI_V2.1	
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.

4.2 Threats

Table 2 shows the threats defined in the individual components of CFG_MDF-MDM_AGENT-VPNC_V1.0.

Table 2: Threats

Threat Name **From PP_MD_V3.1**	**Threat Definition**
T.EAVESDROP Network Eavesdropping	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 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 Physical Access	An attacker, with physical access, may attempt to access user data on the Mobile Device including credentials. These physical access threats 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.FLAWAPP Malicious or Flawed Application	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 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_MDM_AGENT_V1.0	
T.BACKUP	An attacker may try to target backups of data or credentials and exfiltrate data. Since the backup is stored on either a personal computer or end user's backup repository, it's not likely the enterprise would detect compromise.
From MOD_VPN_CLI_V2.1	
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 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 13 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.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_UPDATE	Since the most common attack vector used involves attacking unpatched versions of software containing well-known flaws, updating the VPN client is necessary to ensure that changes to threat environment are addressed. Timely application of patches ensures that the client is a "hard target", thus increasing the likelihood that product will be able to maintain and enforce its security policy. However, the updates to be applied to the product must be trustable in some manner; otherwise, an attacker can write their own "update" that instead contains malicious code of their choosing, such as a rootkit, bot, or other malware. Once this "update" is installed, the attacker then has control of the system and all of its data. Methods of countering this threat typically involve hashes of the updates, and potentially cryptographic operations (e.g., digital signatures) on those hashes as well. However, the validity of these methods introduces additional threats. For instance, a weak hash function could result in the attacker being able to modify the legitimate update in such a way that the hash remained unchanged. For cryptographic signature schemes, there are dependencies on 1) the strength of the cryptographic algorithm used to provide the signature, and 2) the ability of the end user to verify the signature (which typically involves checking a hierarchy of digital signatures back to a root of trust (a certificate authority)) If a cryptographic signature scheme is weak, then it may be compromised by an attacker and the end user will install a malicious update, thinking that it is legitimate. Similarly, if the root of trust can be compromised, then a strong digital signature algorithm will not stop the malicious update from being installed (the attacker will just create their own signature on the update using the compromised root of trust, and the malicious update will then be installed without detection).
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.

4.3 Organizational Security Policies

Table 3 shows the organizational security policies defined in the individual components of CFG_MDF-MDM_AGENT- VPNC_V1.0.

Table 3: Organizational Security Policies

OSP Name	OSP Definition
From PP_MD_V3.1	
N/A	N/A
From MOD_MDM_AGENT_V1.0	
P.ACCOUNTABILITY	Personnel operating the TOE shall be accountable for their actions within the TOE.
P.ADMIN	The configuration of the mobile device security functions must adhere to the Enterprise security policy.
P.DEVICE_ENROLL	A mobile device must be enrolled for a specific user by the administrator of the MDM prior to being used in the Enterprise network by the user.
P.NOTIFY	The mobile user must immediately notify the administrator if a mobile device is lost or stolen so that the administrator may apply remediation actions via the MDM system.

4.4 Security Objectives

Table 4 shows the security objectives for the TOE defined in the individual components of CFG_MDF-MDM_AGENT- VPNC_V1.0.

Table 4: Security Objectives for the TOE

TOE Security Objective	TOE Security Objective Definition
From PP_MD_V3.1	
O.COMMS Protected Communications	To address the network eavesdropping (T.EAVESDROP) and network attack (T.NETWORK) threats described in Section 3.1, 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. Addressed by: FCS_CKM.1, FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM_EXT.8(OPTIONAL), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_DTLS_EXT.1(OPTIONAL), FCS_HTTPS_EXT.1, FCS_RBG_EXT.1, FCS_RBG_EXT.2(OPTIONAL), FCS_RBG_EXT.3(OPTIONAL), FCS_SRV_EXT.1, FCS_SRV_EXT.2(OPTIONAL), FCS_TLSC_EXT.1, FCS_TLSC_EXT.2(OPTIONAL), FCS_TLSC_EXT.3(OPTIONAL), FDP_BLT_EXT.1(OPTIONAL), FDP_IFC_EXT.1, FDP_STG_EXT.1, FDP_UPC_EXT.1, FIA_BLT_EXT.1, FIA_BLT_EXT.2, FIA_BLT_EXT.3, FIA_BLT_EXT.4, FIA_BLT_EXT.5(OPTIONAL), FIA_BLT_EXT.6(OPTIONAL), FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3, FIA_X509_EXT.4(OPTIONAL), FIA_X509_EXT.5(OPTIONAL), FPT_BLT_EXT.1(OPTIONAL), FTP_BLT_EXT.1(OPTIONAL), FTP_BLT_EXT.2(OPTIONAL), FTP_ITC_EXT.1
O.STORAGE Protected 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. Addressed by: FCS_CKM_EXT.1, FCS_CKM_EXT.2, FCS_CKM_EXT.3, FCS_CKM_EXT.4, FCS_CKM_EXT.5, FCS_CKM_EXT.6, FCS_CKM_EXT.7(OPTIONAL), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_COP.1(5), FCS_IV_EXT.1, FCS_RBG_EXT.1, FCS_RBG_EXT.2(OPTIONAL), FCS_RBG_EXT.3(OPTIONAL), FCS_STG_EXT.1, FCS_STG_EXT.2, FCS_STG_EXT.3, FDP_ACF_EXT.2(OPTIONAL), FDP_ACF_EXT.3(OPTIONAL), FDP_DAR_EXT.1, FDP_DAR_EXT.2, FIA_UAU_EXT.1, FPT_KST_EXT.1, FPT_KST_EXT.2, FPT_KST_EXT.3, FPT_JTA_EXT.1
O.CONFIG Mobile Device Configuration	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. Addressed by: FMT_MOF_EXT.1, FMT_SMF_EXT.1, FMT_SMF_EXT.2, FTA_TAB.1(OPTIONAL)
O.AUTH Authorization and Authentication	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 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. Addressed by: FCS_CKM.2(1), FDP_PBA_EXT.1(OPTIONAL), FIA_AFL_EXT.1, FIA_BLT_EXT.1, FIA_BLT_EXT.2, FIA_BLT_EXT.3, FIA_BMG_EXT.1(OPTIONAL), FIA_BMG_EXT.2(OPTIONAL), FIA_BMG_EXT.3(OPTIONAL), FIA_BMG_EXT.4(OPTIONAL), FIA_BMG_EXT.5(OPTIONAL), FIA_BMG_EXT.6(OPTIONAL), FIA_PMG_EXT.1, FIA_TRT_EXT.1, FIA_UAU_EXT.1, FIA_UAU_EXT.2, FIA_UAU_EXT.4(OPTIONAL), FIA_UAU.5, FIA_UAU.6, FIA_UAU.7, FIA_X509_EXT.2, FIA_X509_EXT.4(OPTIONAL), FIA_X509_EXT.5(OPTIONAL), FTA_SSL_EXT.1
O.INTEGRITY Mobile Device 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. Addressed by: FAU_GEN.1, FAU_SAR.1(OPTIONAL), FAU_SEL.1(OPTIONAL), FAU_STG.1, FAU_STG.4, FCS_COP.1(2), FCS_COP.1(3), FDP_ACF_EXT.1, FDP_ACF_EXT.3(OPTIONAL), FPT_AEX_EXT.1, FPT_AEX_EXT.2, FPT_AEX_EXT.3, FPT_AEX_EXT.4, FPT_AEX_EXT.5(OPTIONAL), FPT_AEX_EXT.6(OPTIONAL), FPT_AEX_EXT.7(OPTIONAL), FPT_BBD_EXT.1(OPTIONAL), FPT_NOT_EXT.1, FPT_NOT_EXT.2(OPTIONAL), FPT_STM.1, FPT_TST_EXT.1, FPT_TST_EXT.2(1), FPT_TST_EXT.2(2)(OPTIONAL), FPT_TST_EXT.3(OPTIONAL), FPT_TUD_EXT.1, FPT_TUD_EXT.2, FPT_TUD_EXT.T(OPTIONAL), FPT_TUD_EXT.4(OPTIONAL)
O.PRIVACY End User Privacy and Device Functionality	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. Addressed by: FDP_ACF_EXT.1,

	FDP_BCK_EXT.1(OPTIONAL), FMT_SMF_EXT.1, FMT_SMF_EXT.3(OPTIONAL)
From MOD_MDM_AGENT_V1.0	
O.ACCOUNTABILITY	The TOE must provide logging facilities, which record management actions undertaken by its administrators.
O.APPLY_POLICY	The TOE must facilitate configuration and enforcement of enterprise security policies on mobile devices via interaction with the mobile OS and the MDM Server. This will include the initial enrollment of the device into management, through its entire lifecycle, including policy updates and its possible unenrollment from management services.
O.DATA_PROTECTION_TRANSIT	Data exchanged between the MDM Server and the MDM Agent must be protected from being monitored, accessed, or altered.
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 platform provide key storage. The TOE is expected to protect its persistent secrets and private keys.

Table 5 shows the security objectives for the Operational Environment defined in the individual components of CFG_MDF-MDM_AGENT- VPNC_V1.0.

Table 5: Security Objectives for the Operational Environment

Environmental Security Objective	Environmental Security Objective Definition
From PP_MD_V3.1	
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 User exercises precautions to reduce the risk of loss or theft of the Mobile Device.
From MOD_MDM_AGENT_V1.0	
OE.DATA_PROPER_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
OE.DATA_PROPER_USER	Users of the mobile device are trained to securely use the mobile device and apply all guidance in a trusted manner.

OE.IT_ENTERPRISE	The Enterprise IT infrastructure provides security for a network that is available to the TOE and mobile devices that prevents unauthorized access.
OE-MOBILE_DEVICE_PLATFORM	The MDM Agent relies upon the trustworthy mobile platform and hardware to provide policy enforcement as well as cryptographic services and data protection. The mobile platform provides trusted updates and software integrity verification of the MDM Agent.
OE.WIRELESS_NETWORK	A wireless network will be available to the mobile devices.
From MOD_VPN_CLI_V2.1	
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.

5 Functional Requirements

As indicated above, CFG_MDF-MDM_AGENT- VPNC_V1.0 includes PP_MD_V3.1, MOD_MDM_AGENT_V1.0 and MOD_VPN_CLI_V2.1. The functional requirements from PP_MD_V3.1 and MOD_VPN_CLI_V2.1 were evaluated separately so this section applies only to requirements of MOD_MDM_AGENT_V1.0.

As indicated above, requirements in the MOD_MDM_AGENT_V1.0 are comprised of the "base" requirements and additional requirements that are objective. The following table contains the "base" requirements that were validated as part of the atsec Information Security Corporation evaluation activities referenced above.

Table 6: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_ALT_EXT.2: Agent Alerts	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices
	FAU_GEN.1(2): Audit Data Generation	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices
	FAU_SEL.1(2): Security Audit Event Selection	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices
FIA: Identification and Authentication	FIA_ENR_EXT.2: Agent Enrollment of Mobile Device into Management	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices
FMT: Security Management	FMT_POL_EXT.2: Agent Trusted Policy Update	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices

	FMT_SMF_EXT.4: Specification of Management Functions	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices
	FMT_UNR_EXT.1: User Unenrollment Prevention	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices

The following table contains requirements that only apply when the PP-Module is paired with the MDF PP. If no completed evaluations have claimed a given requirement, the VR author has evaluated it through the completion of the relevant ACE work units and has indicated its verification through "PP-Module Evaluation."

Table 7: TOE Security Functional Requirements

Requirement Class	Requirement Component	Verified By
FCS: Cryptographic Support	FCS_STG_EXT.4: Cryptographic Key Storage	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices
FTP: Trusted Path/Channels	FTP_ITC_EXT.1(2): Trusted Channel Communication	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices
	FTP_TRP.1(2): Trusted Path (for Enrollment)	Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices

The following table contains the "**Optional**" requirements contained in Appendix A, 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 ACE work units and has indicated its verification through "PP-Module Evaluation."

Table 8: Optional Requirements

Requirement Class	Requirement Component	Verified By
The MOD_MDM_AGENT_V1.0 does not define any additional optional requirements.		

The following table contains the "**Selection-Based**" requirements contained in Appendix B, and an indication of what evaluation those requirements were verified in (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 ACE work units and has indicated its verification through "PP-Module Evaluation."

Table 9: Selection-Based Requirements

Requirement Class	Requirement Component	Verified By
The MOD_MDM_AGENT_V1.0 does not define any additional selection-based requirements.		

The following table contains the "**Objective**" requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (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 ACE work units and has indicated its verification through "PP-Module Evaluation."

Table 10: Objective Requirements

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_STG_EXT.3: Security Audit Event Storage	PP-Module Evaluation
FPT: Protection of the TSF	FPT_NET_EXT.1: Network Reachability	PP-Module Evaluation

6 Assurance Requirements

The PP-Configuration defines its security assurance requirements as those required by PP_MD_V3.1. The SARs defined in that PP are applicable to MOD_MDM_AGENT_V1.0 as well as CFG_MDF-MDM_AGENT- VPNC_V1.0 as a whole.

7 Results of the Evaluation

Note that for ACE elements and work units identical to ASE elements and work units, the lab performed the ACE work units concurrent to the ASE work units.

Table 11: Evaluation Results

ACE Requirement	Evaluation Verdict	Verified By
ACE_INT.1	Pass	PP-Module evaluation
ACE_CCL.1	Pass	PP-Module evaluation
ACE_SPD.1	Pass	PP-Module evaluation
ACE_OBJ.1	Pass	PP-Module evaluation
ACE_ECD.1	Pass	PP-Module evaluation
ACE_REQ.1	Pass	PP-Module evaluation
ACE_MCO.1	Pass	PP-Module evaluation
ACE_CCO.1	Pass	PP-Module 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_MDM_AGENT_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] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 3.0, May 2014.

[6] Protection Profile for Mobile Device Fundamentals, Version 3.1, 16 July 2017.

[7] PP-Module for MDM Agents, Version 1.0, 25 April 2019.

[8] PP-Module for Virtual Private Network (VPN) Clients, Version 2.1, 05 October 2017.

[9] Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devces Security Target, Version 1.7, 10 November 2020.

[10] Apple iOS 13 on iPhone and Apple iPadOS 13 on iPad Mobile Devices Assurance Activity Report, Version 1.4, 10 November 2020.