TheJoin, Inc., Join-Virtual Mobile Platform 6.1.0 Security Target

Version 0.8
01/26/2024

Prepared for:

TheJoin, Inc.

3F,63, Bongeunsa-ro 30-gil
Gangnam-gu, Seoul, Republic of Korea

Prepared By:

Gossamer Laboratories

www.gossamersec.com

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the Join-Virtual Mobile Platform 6.1.0 provided by TheJoin, Inc. The TOE is being evaluated as a software application.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Objectives (Section 3)
- Extended Components Definition (Section 4)
- Security Requirements (Section 5)
- TOE Summary Specification (Section 6)

Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement. Operations performed in the Protection Profiles are not marked in the ST. The conventions below are for ST operations exclusively.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a parenthetical number placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement.
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …").
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.1 Security Target Reference

ST Title – TheJoin, Inc., Join-Virtual Mobile Platform 6.1.0 Security Target

ST Version – Version 0.8

ST Date – 01/26/2024

1.2 TOE Reference

TOE Identification – TheJoin, Inc., Join-Virtual Mobile Platform 6.1.0

TOE Developer – TheJoin, Inc.

Evaluation Sponsor – TheJoin, Inc.

1.3 TOE Overview

The Target of Evaluation (TOE) is the Join-Virtual Mobile Platform (J-VMP) 6.1.0. The TOE is the Virtual Mobile Infrastructure Client application for Android and iOS platforms. The TOE is a thin client providing access to a Virtual Mobile Infrastructure (VMI) server from a mobile device. The J-VMP and VMI are part of the J-Mobile Platform offered by TheJoin.

The TOE was tested on the following mobile devices.

Device Name	Processor	Operating System
Galaxy S22 Ultra 5G	Qualcomm Snapdragon 8 Gen 1 Mobile Platform	Android 13
Apple iPhone X	Apple A11 Bionic	Apple iOS 16

Table 1 Tested Devices

The following devices are being claimed as equivalent to the tested devices. The TOE runs on all the Samsung (VID11342, 04/26/2023 and VID11410, 10/23/2023) and Google (VID11317, 01/24/2023) devices listed below running Android 13. The TOE also runs on Apple iOS 16 (VID11349, 10/10/2023) on iPhone devices below. The same application runs on all Android devices and the same application runs on all iPhone devices.

Device Name	Operating System
Galaxy S23 Ultra 5G	Android 13
Galaxy S22 5G	Android 13
Galaxy S21 Ultra 5G	Android 13
Galaxy S20+ 5G	Android 13
Galaxy Z Flip	Android 13
Galaxy XCover Pro	Android 13
Galaxy A53 5G	Android 13
Galaxy XCover6 Pro	Android 13
Galaxy Z Flip5 5G	Android 13
Galaxy A52 5G	Android 13
Galaxy A71 5G	Android 13
Galaxy Tab Active3	Android 13
Galaxy S23 FE	Android 13
Google Devices	
Google Pixel 7 Pro	Android 13
Google Pixel 7	Android 13
Google Pixel 6 Pro	Android 13
Google Pixel 6	Android 13
Google Pixel 6a	Android 13
Google Pixel 5a-5G	Android 13
Google Pixel 5	Android 13
Google Pixel 4a-5G	Android 13
Google Pixel 4a	Android 13
Apple Devices	
iPhone 14 Plus	iOS 16
iPhone 14 Pro Max	iOS 16
iPhone 14 Pro	iOS 16
iPhone 14	iOS 16
iPhone SE (3rd gen)	iOS 16
iPhone 13 mini	iOS 16
iPhone 13 Pro Max	iOS 16
iPhone 13 Pro	iOS 16

iPhone 13	iOS 16
iPhone 12 mini	iOS 16
iPhone 12 Pro Max	iOS 16
iPhone 12 Pro	iOS 16
iPhone 12	iOS 16
iPhone SE (2nd gen)	iOS 16
iPhone 11 Pro Max	iOS 16
iPhone 11 Pro	iOS 16
iPhone 11	iOS 16
iPhone XS	iOS 16
iPhone XS Max	iOS 16
iPhone XR	iOS 16
iPhone 8 Plus	iOS 16
iPhone 8	iOS 16

Table 2 Equivalent Devices

1.4 TOE Description

A J-VMP client is a service that hosts independent workspaces for every user. A user workspace is based on the Android operating system, which is accessible via the J-VMP mobile client application installed on an Android or iOS mobile device. Using the J-VMP client application, users can access the same mobile environment that includes all their applications and data from any location, without being tied to a single mobile device. The J-VMP client presents only the interface offered by the VMI server and ensures that communication with the server utilizes secured protocols.

The TOE when executed, connects to the specified Virtual Mobile Infrastructure (VMI) server, authenticating the server's certificate received while negotiating the HTTPS or TLS session. The TOE is responsible only for protecting data-in-transit between the physical mobile device and the VMI server.

Figure 1 shows the TOE in its intended environment. The TOE runs on the mobile client and communicates securely with the VMI Server in the protected network.

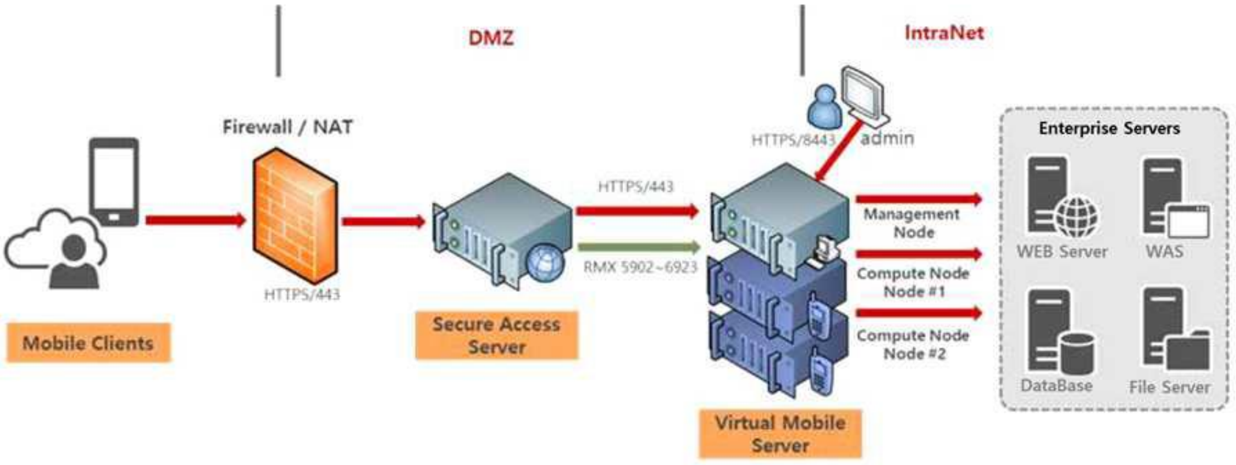

Figure 1 TOE Environment

1.4.1 TOE Architecture

The TOE is an application installed onto a physical mobile device from the Google Playstore or Apple App Store.

1.4.1.1 Physical Boundaries

The physical boundary of the TOE is the physical perimeter of the device on which the TOE resides.

1.4.1.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TSF
- Trusted path/channels

1.4.1.2.1 Cryptographic support

The J-VMP client utilizes platform APIs to provide secure network communication using the HTTPS. The client also uses its own cryptography to establish a trusted TLS channels to transmit data to the VMI Server.

1.4.1.2.2 User data protection

The J-VMP client informs a user of hardware and software resources the TOE accesses. It uses the platform's permission mechanism to get a user's approval for access. The user initiates a secure network connection to the VMI server using the TOE. In general, sensitive data resides on the VMI server and not the J-VMP Client, although the client does store encrypted credentials.

1.4.1.2.3 Identification and authentication

The J-VMP client performs certificate validation checking for TLS connections. Both Android and iOS applications support OCSP when performing validity checks.

1.4.1.2.4 Security management

The J-VMP client does not include any predefined or default credentials, and utilize the platform recommended storage process for configuration options.

1.4.1.2.5 Privacy

The J-VMP client does not collect any PII and does not transmit any PII over a network.

1.4.1.2.6 Protection of the TSF

The J-VMP client relies on the physical boundary of the evaluated platform as well as the Android and iOS operating system for the protection of the TOE's application components. All compiled J-VMP client code is designed to utilize compiler provided anti-exploitation capabilities. The J-VMP client application is available through the Google Playstore and the Apple store.

1.4.1.2.7 Trusted path/channels

The J-VMP client utilizes platform API to establish HTTPS connections to a VMI server. The client also uses its cryptographic library to establish TLS connections to a VMI server.

1.4.2 TOE Documentation

Join-Virtual Mobile Platform 6.1.0(J-VMP) USER’s Guide, version 6.1.10, 01/25/2024

2. Conformance Claims

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.
    - Part 3 Extended
- Package Claims:
    - Protection Profile for Application Software, Version 1.4, 7 October 2021 (ASPP14)
    - Functional Package for Transport Layer Security (TLS), Version 1.1, 1 March 2019 (PKGTLS11)

Package	Technical Decision	Applied	Notes
PKG_TLS_V1.1	TD0779: Updated Session Resumption Support in TLS package V1.1	No	TLSS not claimed
PKG_TLS_V1.1	TD0770 - TLSS.2 connection with no client cert	No	TLSS not claimed
PKG_TLS_V1.1	TD0739 - PKG_TLS_V1.1 has 2 different publication dates	No	TLSS not claimed
PKG_TLS_V1.1	TD0726 - Corrections to (D)TLSS SFRs in TLS 1.1 FP	No	(D)TLSS not claimed
PKG_TLS_V1.1	TD0513 - CA Certificate loading	Yes	
PKG_TLS_V1.1	TD0499 - Testing with pinned certificates	Yes	
PKG_TLS_V1.1	TD0469 - Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	No	TLSS not claimed
PKG_TLS_V1.1	TD0442 - Updated TLS Ciphersuites for TLS Package	Yes	
PP_APP_v1.4	TD0798: Static Memory Mapping Exceptions	Yes	
PP_APP_v1.4	TD0780: FIA_X509_EXT.1 Test 4 Clarification	Yes	
PP_APP_v1.4	TD0756: Update for platform-provided full disk encryption	Yes	
PP_APP_v1.4	TD0747: Configuration Storage Option for Android	Yes	
PP_APP_v1.4	TD0743: FTP_DIT_EXT.1.1 Selection exclusivity	Yes	
PP_APP_v1.4	TD0736: Number of elements for iterations of FCS_HTTPS_EXT.1	No	Requirement not claimed
PP_APP_v1.4	TD0719 - ECD for PP APP V1.3 and 1.4	Yes	
PP_APP_v1.4	TD0717 - Format changes for PP_APP_V1.4	Yes	
PP_APP_v1.4	TD0664 - Testing activity for FPT_TUD_EXT.2.2	Yes	
PP_APP_v1.4	TD0650 - Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	No	TOE not a VPN
PP_APP_v1.4	TD0628 - Addition of Container Image to Package Format	Yes	

2.1 Conformance Rationale

The ST conforms to the ASPP14/PKGTLS11. As explained previously, the security problem definition, security objectives, and security requirements have been drawn from the PP.

3. Security Objectives

The Security Problem Definition may be found in the ASPP14/PKGTLS11 and this section reproduces only the corresponding Security Objectives for operational environment for reader convenience. The ASPP14/PKGTLS11 offers additional information about the identified security objectives, but that has not been reproduced here and the ASPP14/PKGTLS11 should be consulted if there is interest in that material.

In general, the ASPP14/PKGTLS11 has defined Security Objectives appropriate for a software application and as such are applicable to the J-VMP Client TOE.

3.1 Security Objectives for the Operational Environment

OE.PLATFORM The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.PROPER_ADMIN The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

OE.PROPER_USER The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

4. Extended Components Definition

All of the extended requirements in this ST have been drawn from the ASPP14/PKGTLS11. The ASPP14/PKGTLS11 defines the following extended requirements and since they are not redefined in this ST the ASPP14/PKGTLS11 should be consulted for more information in regard to those CC extensions.

Extended SFRs:

- ASPP14:FCS_CKM_EXT.1: Cryptographic Key Generation Services
- ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
- ASPP14:FCS_STO_EXT.1: Storage of Credentials
- PKGTLS11:FCS_TLS_EXT.1: TLS Protocol
- PKGTLS11:FCS_TLSC_EXT.1: TLS Client Protocol - per TD0442
- PKGTLS11:FCS_TLSC_EXT.4: TLS Client Support for Renegotiation
- ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
- ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
- ASPP14:FDP_NET_EXT.1: Network Communications
- ASPP14:FIA_X509_EXT.1: X.509 Certificate Validation
- ASPP14:FIA_X509_EXT.2: X.509 Certificate Authentication
- ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
- ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism
- ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
- ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
- ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
- ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
- ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries
- ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
- ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update
- ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit

Extended SARs:

- ALC_TSU_EXT.1: Timely Security Updates

5. Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the ASPP14/PKGTLS11. The refinements and operations already performed in the ASPP14/PKGTLS11 are not identified (e.g., highlighted) here, rather the requirements have been copied from the ASPP14/PKGTLS11 and any residual operations have been completed herein. Of particular note, the ASPP14/PKGTLS11 made a number of refinements and completed some of the SFR operations defined in the Common Criteria (CC) and that PP should be consulted to identify those changes if necessary.

The SARs are also drawn from the ASPP14/PKGTLS11. The ASPP14/PKGTLS11 should be consulted for the assurance activity definitions.

5.1 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by Join-Virtual Mobile Platform 6.1.0 TOE.

Requirement Class	Requirement Component
FCS: Cryptographic support	ASPP14:FCS_CKM_EXT.1: Cryptographic Key Generation Services
	ASPP14:FCS_CKM.2: Cryptographic Key Establishment
	ASPP14:FCS_COP.1/Hash: Cryptographic Operation - Hashing
	ASPP14:FCS_COP.1/KeyedHash: Cryptographic Operation - Keyed-Hash Message Authentication - per TD0717
	ASPP14:FCS_COP.1/Sig: Cryptographic Operation - Signing - per TD0717
	ASPP14:FCS_COP.1/SKC: Cryptographic Operation - Encryption/Decryption
	ASPP14:FCS_RBG_EXT.1: Random Bit Generation Services
	ASPP14:FCS_STO_EXT.1: Storage of Credentials
	PKGTLS11:FCS_TLS_EXT.1: TLS Protocol
	PKGTLS11:FCS_TLSC_EXT.1: TLS Client Protocol - per TD0442
	PKGTLS11:FCS_TLSC_EXT.4: TLS Client Support for Renegotiation
FDP: User data protection	ASPP14:FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
	ASPP14:FDP_DEC_EXT.1: Access to Platform Resources
	ASPP14:FDP_NET_EXT.1: Network Communications
FIA: Identification and authentication	ASPP14:FIA_X509_EXT.1: X.509 Certificate Validation - per TD0780
	ASPP14:FIA_X509_EXT.2: X.509 Certificate Authentication
FMT: Security management	ASPP14:FMT_CFG_EXT.1: Secure by Default Configuration
	ASPP14:FMT_MEC_EXT.1: Supported Configuration Mechanism - per TD0747
	ASPP14:FMT_SMF.1: Specification of Management Functions
FPR: Privacy	ASPP14:FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable
FPT: Protection of the TSF	ASPP14:FPT_AEX_EXT.1: Anti-Exploitation Capabilities
	ASPP14:FPT_API_EXT.1: Use of Supported Services and APIs
	ASPP14:FPT_IDV_EXT.1: Software Identification and Versions
	ASPP14:FPT_LIB_EXT.1: Use of Third Party Libraries
	ASPP14:FPT_TUD_EXT.1: Integrity for Installation and Update
	ASPP14:FPT_TUD_EXT.2: Integrity for Installation and Update - per TD0664

FTP: Trusted path/channels	ASPP14:FTP_DIT_EXT.1: Protection of Data in Transit - per TD0743

Table 3 TOE Security Functional Components

5.1.1 Cryptographic support (FCS)

5.1.1.1 Cryptographic Key Generation Services – per TD0717 (ASPP14:FCS_CKM_EXT.1)

ASPP14:FCS_CKM_EXT.1.1

The application shall [***generate no asymmetric cryptographic keys***].

5.1.1.2 Cryptographic Key Establishment (ASPP14:FCS_CKM.2)

ASPP14:FCS_CKM.2.1

The application shall [***implement functionality***] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [***RSA-based key establishment schemes that meets the following: NIST Special Publication 800-56B, 'Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography'***].

5.1.1.3 Cryptographic Operation - Hashing - per TD0717 (ASPP14:FCS_COP.1/Hash)

ASPP14:FCS_COP.1.1/Hash

The application shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [***SHA-256***] and message digest sizes [***256***] bits that meet the following: FIPS Pub 180-4.

5.1.1.4 Cryptographic Operation - Keyed-Hash Message Authentication - per TD0717 (ASPP14:FCS_COP.1/KeyedHash)

ASPP14:FCS_COP.1.1/KeyedHash

The application shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm [***HMAC-SHA-256***] and [***no other algorithms***] with key sizes [**256 bits**] and message digest sizes [***256***] and [***no other size***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code' and FIPS Pub 180-4 'Secure Hash Standard'.

5.1.1.5 Cryptographic Operation - Signing - per TD0717 (ASPP14:FCS_COP.1/Sig)

ASPP14:FCS_COP.1.1/Sig

The application shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)" Section 5].

5.1.1.6 Cryptographic Operation - Encryption/Decryption - per TD0717 (ASPP14:FCS_COP.1/SKC)

ASPP14:FCS_COP.1.1/SKC

The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm [AES-CBC (as defined in NIST SP 800-38A) mode, ***AES-GCM (as defined in NIST SP 800-38D) mode***] and cryptographic key sizes [***128-bit***].

5.1.1.7 Random Bit Generation Services (ASPP14:FCS_RBG_EXT.1)

ASPP14:FCS_RBG_EXT.1.1

The application shall [***invoke platform-provided DRBG functionality***] for its cryptographic operations.

5.1.1.8 Storage of Credentials (ASPP14:FCS_STO_EXT.1)

ASPP14:FCS_STO_EXT.1.1

The application shall [***implement functionality to securely store [server account password] according to [FCS_COP.1/SKC]***] to non-volatile memory.

5.1.1.9 TLS Protocol (PKGTLS11:FCS_TLS_EXT.1)

PKGTLS11:FCS_TLS_EXT.1.1

The product shall implement [***TLS as a client***]

5.1.1.10 TLS Client Protocol - per TD0442 (PKGTLS11:FCS_TLSC_EXT.1)

PKGTLS11:FCS_TLSC_EXT.1.1

The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a client that supports the cipher suites [***TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288,***] and also supports functionality for [***session renegotiation***]. (TD0442 applied)

PKGTLS11:FCS_TLSC_EXT.1.2

The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

PKGTLS11:FCS_TLSC_EXT.1.3

The product shall not establish a trusted channel if the server certificate is invalid [***with no exceptions***]

5.1.1.11 TLS Client Support for Renegotiation (PKGTLS11:FCS_TLSC_EXT.4)

PKGTLS11:FCS_TLSC_EXT.4.1

The product shall support secure renegotiation through use of the 'renegotiation_info' TLS extension in accordance with RFC 5746.

5.1.2 User data protection (FDP)

5.1.2.1 Encryption Of Sensitive Application Data (ASPP14:FDP_DAR_EXT.1)

ASPP14:FDP_DAR_EXT.1.1

The application shall [***protect sensitive data in accordance with FCS_STO_EXT.1***] in non-volatile memory.

5.1.2.2 Access to Platform Resources (ASPP14:FDP_DEC_EXT.1)

ASPP14:FDP_DEC_EXT.1.1

The application shall restrict its access to [

iOS:

- ***[Camera***
- ***Location services***
- ***Microphone***
- ***Bluetooth***
- ***[Photo library***
- ***Notifications***
- ***Background operation]]***

Android:

- ***[Bluetooth***
- ***Camera***
- ***Microphone***
- ***[Access network state***
- ***Access WIFI state***
- ***Change WIFI state***
- ***Internet***
- ***Request install packages***
- ***Use fingerprint***
- ***Vibrate***
- ***Wake lock***
- ***Foreground service***
- ***Access coarse location***
- ***Access fine location]]***

].

ASPP14:FDP_DEC_EXT.1.2

The application shall restrict its access to [***no sensitive information repositories***].

5.1.2.3 Network Communications (ASPP14:FDP_NET_EXT.1)

ASPP14:FDP_NET_EXT.1.1

The application shall restrict network communication to [***user-initiated communication for [connecting to a VMI server]***].

5.1.3 Identification and authentication (FIA)

5.1.3.1 X.509 Certificate Validation - per TD0780 (ASPP14:FIA_X509_EXT.1)

ASPP14:FIA_X509_EXT.1.1

The application shall [***implement functionality***] to validate certificates in accordance with the following rules:
- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using [***OCSP as specified in RFC 6960***]
- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
o Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
o Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
o Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
o S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
o OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.

o Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kpcmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

ASPP14:FIA_X509_EXT.1.2

The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

5.1.3.2 X.509 Certificate Authentication (ASPP14:FIA_X509_EXT.2)

ASPP14:FIA_X509_EXT.2.1

The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [***HTTPS, TLS***].

ASPP14:FIA_X509_EXT.2.2

When the application cannot establish a connection to determine the validity of a certificate, the application shall [***not accept the certificate***].

5.1.4 Security management (FMT)

5.1.4.1 Secure by Default Configuration (ASPP14:FMT_CFG_EXT.1)

ASPP14:FMT_CFG_EXT.1.1

The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

ASPP14:FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect the application's binaries and data files from modification by normal unprivileged user.

5.1.4.2 Supported Configuration Mechanism - per TD0747 (ASPP14:FMT_MEC_EXT.1)

ASPP14:FMT_MEC_EXT.1.1

The application shall [***invoke the mechanisms recommended by the platform vendor for storing and setting configuration options***].

5.1.4.3 Specification of Management Functions (ASPP14:FMT_SMF.1)

ASPP14:FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [***[Specify the network address of a VMI server, Set the remember password option]***].

5.1.5 Privacy (FPR)

5.1.5.1 User Consent for Transmission of Personally Identifiable (ASPP14:FPR_ANO_EXT.1)

ASPP14:FPR_ANO_EXT.1.1

The application shall [***not transmit PII over a network***].

5.1.6 Protection of the TSF (FPT)

5.1.6.1 Anti-Exploitation Capabilities (ASPP14:FPT_AEX_EXT.1)

ASPP14:FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [**no exceptions**].

ASPP14:FPT_AEX_EXT.1.2

The application shall [***not allocate any memory region with both write and execute permissions***].

ASPP14:FPT_AEX_EXT.1.3

The application shall be compatible with security features provided by the platform vendor.

ASPP14:FPT_AEX_EXT.1.4

The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

ASPP14:FPT_AEX_EXT.1.5

The application shall be built with stack-based buffer overflow protection enabled.

5.1.6.2 Use of Supported Services and APIs (ASPP14:FPT_API_EXT.1)

ASPP14:FPT_API_EXT.1.1

The application shall use only documented platform APIs.

5.1.6.3 Software Identification and Versions (ASPP14:FPT_IDV_EXT.1)

ASPP14:FPT_IDV_EXT.1.1

The application shall be versioned with [***[a unique release number]***].

5.1.6.4 Use of Third Party Libraries (ASPP14:FPT_LIB_EXT.1)

ASPP14:FPT_LIB_EXT.1.1

The application shall be packaged with only [**See Section 6.6 for a list of libraries**].

5.1.6.5 Integrity for Installation and Update (ASPP14:FPT_TUD_EXT.1)

ASPP14:FPT_TUD_EXT.1.1

The application shall [***leverage the platform***] to check for updates and patches to the application software.

ASPP14:FPT_TUD_EXT.1.2

The application shall [***leverage the platform***] to query the current version of the application software.

ASPP14:FPT_TUD_EXT.1.3

The application shall not download, modify, replace or update its own binary code.

ASPP14:FPT_TUD_EXT.1.4

Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

ASPP14:FPT_TUD_EXT.1.5

The application is distributed [***as an additional software package to the platform OS***].

5.1.6.6 Integrity for Installation and Update - per TD0664/0628 (ASPP14:FPT_TUD_EXT.2)

ASPP14:FPT_TUD_EXT.2.1

The application shall be distributed using ***[the format of the platform-supported package manager]***.

ASPP14:FPT_TUD_EXT.2.2

The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

ASPP14:FPT_TUD_EXT.2.3

The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

5.1.7 Trusted path/channels (FTP)

5.1.7.1 Protection of Data in Transit - per TD0743 (ASPP14:FTP_DIT_EXT.1)

ASPP14:FTP_DIT_EXT.1.1

The application shall [

- ***encrypt all transmitted [sensitive data] with [TLS as a client as defined in the Functional Package for TLS for [passing data]]***
- ***invoke platform-provided functionality to encrypt all transmitted data with [HTTPS] for [authenticating to the server]***

]] between itself and another trusted IT product.

5.2 TOE Security Assurance Requirements

The SARs for the TOE are the components as specified in Part 3 of the Common Criteria. Note that the SARs have effectively been refined with the assurance activities explicitly defined in association with both the SFRs and SARs.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1: Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labelling of the TOE
	ALC_CMS.1: TOE CM Coverage
	ALC_TSU_EXT.1: Timely Security Updates
ATE: Tests	ATE_IND.1: Independent Testing - Conformance
AVA: Vulnerability assessment	AVA_VAN.1: Vulnerability Survey

Table 4 Assurance Components

5.2.1 Development (ADV)

5.2.1.1 Basic Functional Specification (ADV_FSP.1)

ADV_FSP.1.1d

The developer shall provide a functional specification.

ADV_FSP.1.2d

The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1c

The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2c

The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3c

The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4c

The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2e

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.2.2 Guidance documents (AGD)

5.2.2.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1d

The developer shall provide operational user guidance.

AGD_OPE.1.1c

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

AGD_OPE.1.2c

The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3c

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

AGD_OPE.1.4c

The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5c

The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences, and implications for maintaining secure operation.

AGD_OPE.1.6c

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

AGD_OPE.1.7c

The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.2.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1d

The developer shall provide the TOE, including its preparative procedures.

AGD_PRE.1.1c

The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c

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

AGD_PRE.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2e

The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.2.3 Life-cycle support (ALC)

5.2.3.1 Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1d

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

ALC_CMC.1.1c

The application shall be labelled with a unique reference.

ALC_CMC.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1d

The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1c

The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2c

The configuration list shall uniquely identify the configuration items.

ALC_CMS.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.3.3 Timely Security Updates (ALC_TSU_EXT.1)

ALC_TSU_EXT.1.1d

The developer shall provide a description in the TSS of how timely security updates are made to the TOE. Note: Application developers must support updates to their products for purposes of fixing security vulnerabilities.

ALC_TSU_EXT.1.2d

The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.

ALC_TSU_EXT.1.1c

The description shall include the process for creating and deploying security updates for the TOE software.

ALC_TSU_EXT.1.2c

The description shall express the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE.

ALC_TSU_EXT.1.3c

The description shall include the mechanisms publicly available for reporting security issues pertaining to the TOE.

Note: The reporting mechanism could include web sites, email addresses, as well as a means to protect the sensitive nature of the report (e.g., public keys that could be used to encrypt the details of a proof-of-concept exploit).

ALC_TSU_EXT.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.2.4 Tests (ATE)

5.2.4.1 Independent Testing - Conformance (ATE_IND.1)

ATE_IND.1.1d

The developer shall provide the TOE for testing.

ATE_IND.1.1c

The TOE shall be suitable for testing.

ATE_IND.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.1.2e

The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.2.5 Vulnerability assessment (AVA)

5.2.5.1 Vulnerability Survey (AVA_VAN.1)

AVA_VAN.1.1d

The developer shall provide the TOE for testing.

AVA_VAN.1.1c

The TOE shall be suitable for testing.

AVA_VAN.1.1e

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.1.2e

The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3e

The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Privacy
- Protection of the TSF
- Trusted path/channels

6.1 Cryptographic support

ASPP14:FCS_CKM_EXT.1

The TOE does not generate asymmetric cryptographic keys. The TOE does use RSA keys as part of RSA key establishment when making TLS connections. Key generation is not required as the ASPP14 notes that if the TOE acts as a receiver in the RSA key establishment scheme, the TOE does not need to implement RSA key generation.

ASPP14:FCS_CKM.2

The TOE supports RSA key establishment (key size 2048) as part of HTTPS/TLS. The TOE acts as a client for TLS or HTTPS (RSA) when communicating with the VMI Server. The TOE's RSA key exchange mechanism is used in the TLS handshake process and during product development, the TOE's implementation undergoes testing to ensure TLS compatibility.

ASPP14:FCS_COP.1/Hash, ASPP14:FCS_COP.1/KeyedHash, ASPP14:FCS_COP.1/Sig & ASPP14:FCS_COP.1/SKC

The TOE provides cryptographic functions using its internal J-VMP Security Module version 6.1 (built on the OpenSSL library). The AES operations are used in HTTPS/TLS as well as password storage. The hash function is used as part of HTTPS/TLS cipher negotiation.

The TOE has the following Cryptographic Algorithm Validation Program (CAVP) certificates.

Functions	Requirement	Cert #
Encryption/Decryption		
AES CBC (128 bits) AES GCM (128 bits)	ASPP14:FCS_COP.1/SKC	A3593
Cryptographic hashing		
SHA-256	ASPP14:FCS_COP.1/Hash	A3593
Keyed Hash		
HMAC-SHA256	ASPP14:FCS_COP.1/KeyedHash	A3593
Digital Signature		
RSA Sign/Verify 2048 bits	ASPP14:FCS_COP.1/Sig	A3593

Table 5 CAVP Certificates

ASPP14:FCS_RBG_EXT.1

The TOE uses random data as part of its HTTPS/TLS connection and this random data is obtained from an approved DRBG provided by the platform. The TOE uses the javax.crypto.KeyGenerator class, /dev/random and /dev/urandom on Android and /dev/random and SecRandomCopyBytes on iOS when invoking the DRBG.

ASPP14:FCS_STO_EXT.1

The client implements functionality to securely store server and account information in a local database. For the VMI server, the TOE stores the server address, port, username and password. The stored password is encrypted with AES128 CBC mode according to FCS_COP.1/SKC

PKGTLS11:FCS_TLS_EXT.1/PKGTLS11:FCS_TLSC_EXT.1/PKGTLS11:FCS_TLSC_EXT.4

The TOE communicates with the VMI Server using HTTPS/TLS. The HTTPS portion of the connection is implemented by the platform. The HTTPS portion is used for user authentication and getting the access token. The TOE then supports a protected communication channel using TLS v1.2 (RFC 5246) secure communication protocol to transfer data. The TOE supports use of the following ciphersuite: TLS_RSA_WITH_AES_128_GCM_SHA256.

The following reference identifiers are supported – optional Subject Alternate Name (SAN) (i.e., DNS, IP Address, or URI) and required Common Name (CN). The TOE supports wildcard reference identifiers in both the SAN and CN. If present, the TOE will check the correctness of the SAN extension, otherwise the TOE will check the CN field against the established reference identifier supplied by the user. Certificate pinning is not supported. If the server certificate is invalid, then a connection is not made.

6.2 User data protection

ASPP14:FDP_DAR_EXT.1

The only sensitive data in the TOE is the server password and that is protected as described in ASPP14:FCS_STO_EXT.1.

ASPP14:FDP_DEC_EXT.1

The TOE can access the physical resources on the mobile device. For an Android device, the TOE can access Location services, Camera, Phone, Wake lock, Microphone, Bluetooth, Network Access, Audio Settings, and Vibration. For an iOS device, the TOE can access location services, camera, photos, microphone, notifications, Bluetooth, and background operations. However, the TOE cannot access any of the logical data repositories.

ASPP14:FDP_NET_EXT.1

The TOE allows network communication to be initiated by a user in order to connect to a VMI server. The J-VMP client use VMI Server-initiated network communications to check for notifications and display to user (on iOS).

6.3 Identification and authentication

ASPP14:FIA_X509_EXT.1/ASPP14:FIA_X509_EXT.2

The TOE performs certificate validation checking for TLS connections. The TOE comes pre-loaded with a certificate. The following fields are verified as appropriate: SAN checks, key usages, chain validation, and lastly expiration status. Wildcards are not allowed in certificates. Both Android and iOS applications support OCSP when performing validity checks. Both applications do not accept certificates as valid when revocation status cannot be determined.

6.4 Security management

ASPP14:FMT_CFG_EXT.1

The J-VMP client does not include any predefined or default credentials.

ASPP14:FMT_MEC_EXT.1

The evaluated Android platform on which the TOE executes automatically uses /data/data/package/shared_prefs/ to store configuration options and settings. For an iOS platform, all settings are stored in the iOS user defaults system.

ASPP14:FMT_SMF.1

The TOE provides the ability to specify the network address of a VMI server. The J-VMP Client can enable the Remember Password setting for each account. The J-VMP Client Remember Password setting can also be disabled by policies received from the server.

6.5 Privacy

ASPP14:FPR_ANO_EXT.1

The J-VMP client does not collect any PII and does not intentionally transmit any PII over a network. Users may choose to transmit any data over an established connection to the VMI server, but it is not specifically identifiable as PII.

6.6 Protection of the TSF

ASPP14:FPT_AEX_EXT.1

Memory mapping and permissions on memory regions are not functions applicable to a Java script application. However, some 3rd party libraries are written in a language other than Java and thus are subject to the requirement for Anti-Exploitation Capabilities. However, none of the 3rd party libraries used by the TOE request memory mapping at explicit addresses, and none allocate memory for both write and execute permission.

Android's application management requires application updates to be signed with an Android key, thus allowing the secure updates of its applications. The Android OS Linux kernel is capable of ASLR (address space layout randomization), ensuring that no application uses the same address layout on two different devices.

The TOE libraries are also compiled with the '-fstack-protector-all –fno-exceptions' flags in order to enable ASLR and stack-based buffer over flow protections. On iOS the ASLR feature (-pie) is not set by a compiler flag, because it is on by default on the C-language compiler and this setting is required by the Apple App store.

The TOE produces such pieces of executable code in runtime and are available in-memory only for the running instance of the application. No piece of user-initiated JIT executable code is ever stored on disk. Also, after the Javascript engine has finished producing this JIT code it is turned into read-only executable memory, limiting the exposure of write-and-execute memory areas.

ASPP14:FPT_API_EXT.1

The TOE uses the platform provided APIs for random number operations and HTTPS connections. Refer to the Section 7 for a full list of APIs used by the TOE.

ASPP14:FPT_IDV_EXT.1

The platform user interface provides a method to query the current version of many components, including the TOE software. The TOE software version can be accessed on the Settings display in both devices. It is showed in format of "6.0.xxxx", the "6.0" is the major version, the xxxx is the build number.

ASPP14:FPT_LIB_EXT.1

The TOE uses the following third-party libraries:

iOS:

Library	Usage
FirebaseMessaging	Used for FCM Push notification

Swift	Default
GoogleDataTransport	FirebaseMessaging support
GoogleUtilities	FirebaseMessaging support
nanopb	FirebaseMessaging support
open SSL	Toolkit for TLS protocol
AFNetworking	Used for HTTPS request
ASIHTTPRequest	Used for HTTPS request
Libegal	Render remote user interface
Libjpeg	Image processing
LibOpenGLRender	Render remote user interface
FMDB	sqlite support
G726	decode audio stream
EGOImageLoading	Image caching
MBProgressHUD	Client user interface
SFHFKeychainUtils	System keychain support
Reachability	Network detection
SBJson	deserialization and serialization
SPLockScreen	Client user interface
TheSidebarController	Client user interface
JSBadgeView	Client user interface

Android:

Library	**Usage**
Skia	Render remote user interface
open SSL	Toolkit for TLS protocol
google.conscrypt	Cryptographic Support
x264-152	To encode video streams
ffmpeg	To decode video and audio streams
com.google.code.gson	Deserialization and serialization
org.samba.jcifs	For cryptography support
fr.avianey.com.viewpagerindicator	Client user interface
com.guanaj.easyswipemenulibrary.EasySwipeMenuLayout	Client user interface

ASPP14:FPT_TUD_EXT.1/2

The TOE (J-VMP client) application is available through the Google Playstore and the Apple store. The platform will be providing all required capabilities for trusted updates for store version. TheJoin will notify customer of updates using each customer's preferred communication mechanism. Bug reporting is available to users as described in ASPP14:ALC_TSU_EXT.1.

ASPP14:ALC_TSU_EXT.1

TheJoin accepts bug reports (including reports for security vulnerabilities) through email (bugs@thejoin.co.kr) and web (http://www.thejoin.co.kr) support channels. TheJoin reviews all bug reports when making product changes to resolve issues associated with the TOE. TheJoin makes updates and code patches to resolve issues as quickly as possible, and makes updates available to customers. TOE updates are distributed through the Apple App Store and Google Play. For maximum compatibility, TheJoin recommends customers use the iOS and Android update mechanisms to keep the J-VMP client up-to-date.

6.7 Trusted path/channels

ASPP14:FTP_DIT_EXT.1

The TOE utilizes the platform API to establish HTTPS connections to a VMI server. The TOE utilizes its internal cryptographic library to establish TLS1.2 connections to a VMI server.

7. Security Related Platform APIs Invoked by TOE

This section identifies the Platform APIs that are invoked by the TOE which utilize security functions provided by the platform.

7.1 Android Java APIs

android.net.http.X509TrustManagerExtensions

android.security.KeyChain

java.security.KeyStore

java.security.KeyStoreException

java.security.MessageDigest

java.security.NoSuchAlgorithmException

java.security.cert.Certificate

java.security.cert.CertificateException

java.security.cert.CertificateExpiredException

java.security.cert.CertificateNotYetValidException

java.security.cert.X509Certificate

javax.net.ssl.TrustManager

javax.net.ssl.TrustManagerFactory

javax.net.ssl.X509TrustManager

javax.crypto.Cipher;

javax.crypto.spec.IvParameterSpec

javax.crypto.spec.SecretKeySpec

7.2 iOS Obj-C APIs

NSURLProtocol

NSURLRequest

NSURLConnection

[NSURLConnection willSendRequestForAuthenticationChallenge]

[NSURLConnection willSendRequest]

[NSURLConnection didFailWithError]

CCCrypt