IBM Corporation

IBM MaaS360 v2.91 Cloud Extender Security Target

Version 1.2.2
2018-05-24
VID: 10896

Prepared for:
IBM Corporation.
1787 SENTRY PKWY WEST,
BLDG 18: Suite 200
BLUE BELL PA 19422

www.IBM.com

Prepared by:

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759

www.atsec.com

Table of Contents

Table of Figures

Table of Tables

Revision History

Version	Date	Change
1.0	2018-01-22	Initial Version
1.2	2018-02-28	Initial version for NIAP Check-in
1.2.1	2018-04-17	Version of ST for NIAP Check-out
1.2.2	2018-05-24	Minor update in Table 12 after validators review

1 Security Target Introduction

This document is the Common Criteria Security Target (ST) for the IBM® Corporation IBM MaaS360® v2.91 Cloud Extender™ on the hardware platform listed in section 1.4, to be evaluated as Application Software in compliance with:

- U.S. Government Approved Protection Profile - Protection Profile for Application Software Version 1.2, dated 22nd April, 2016 [pp_app_v1.2]

1.1 Security Target Reference

ST Title: IBM MaaS360 v2.91 Cloud Extender Security Target

ST Version: Version 1.2.2

ST Date: 2018-05-24

TOE Developer: IBM Corp.

Evaluation Sponsor: IBM Corp.

1.2 TOE Reference

Target of Evaluation (TOE) Identification:

- IBM MaaS360 v2.91 Cloud Extender with the following modules:
  - Certificate Authority: version 2.93
  - Exchange Integration for Managing Active Sync Devices: version 2.93
  - Corporate User Visibility: version 2.93
  - Corporate Directory Authentication: version 2.93
- IBM MaaS360 Cloud Extender configuration tool version 2.93
- The TOE guidance documentation, as detailed in section 1.6

1.3 TOE Overview

The TOE consists of the IBM Cloud Extender (CE) application. It includes four modules enabling communications functionality with various customer provided services as well as the supporting documentation and a configuration tool, the IBM MaaS360 Cloud Extender configuration tool. The major security features of the TOE include cryptographic support, user data protection, Trusted Paths, and Trusted Channels.

The application is installed within a MaaS360 customer's own network in order to enable services offered by the IBM MaaS360 Enterprise Mobility Management (EMM), a cloud-based multi-tenant platform that provides a mobile device management (MDM) solution.

The Cloud Extender is a small Windows application (approx. 12MB) that is installed behind the customer firewall with network access to the appropriate internal systems.

The Cloud Extender makes an outbound connection to the MaaS360 Software as a Service (SaaS) application over port 443 (Transport Layer Security (TLS) using AES256 encryption) and uses Extensible Messaging and Presence Protocol (XMPP) protocol to maintain the connection with the MaaS360 Cloud.

The Cloud Extender is not a mobile application.

Figure 1: Trusted Communication Channels for a Cloud Extender describes the trusted communication channels which are part of this evaluation. Those communication channels represented by a broken line are not part of this TOE and are not covered by the evaluation.

The TOE is an example of [USE CASE 3] Communication described in [pp_app_v1.2] as:

"The application allows for communication interactively or non-interactively with other users or applications over a communications channel."

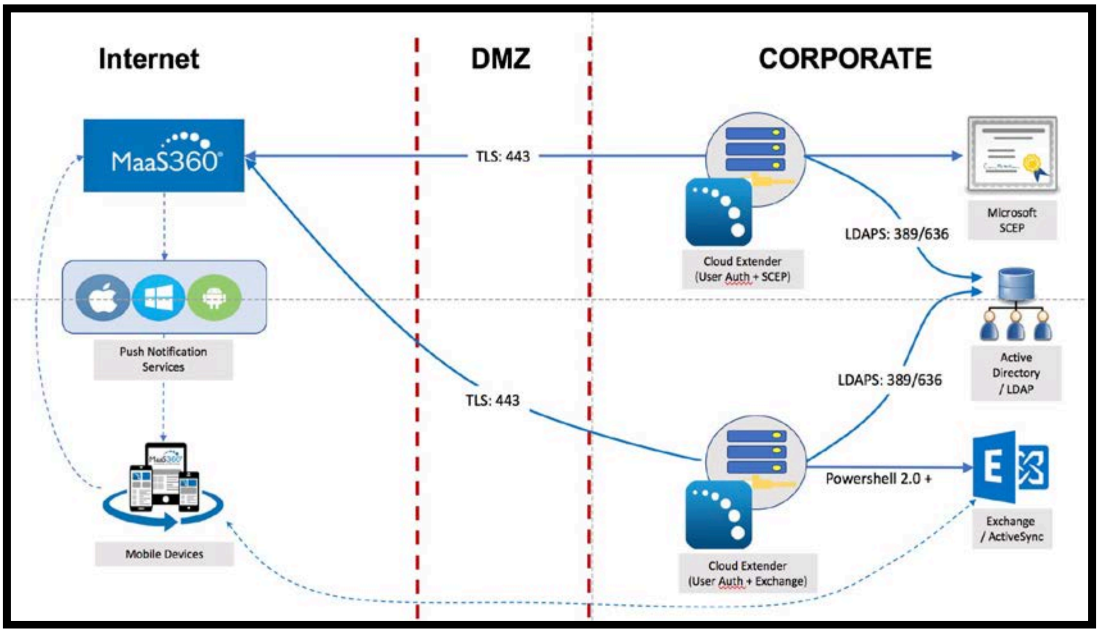


Figure 1: Trusted Communication Channels for a Cloud Extender

1.4 TOE Description

The TOE is a software application that is installed and runs as a service on a Microsoft® Windows® operating system. In this case, Microsoft Windows Server 2012 R2 (x64), which has been evaluated for conformance with the U.S. Government Protection Profile (PP) for General Purpose Operating Systems Version 4.1, and is listed on the NIAP Product Compliant List (PCL).

The TOE is used in support of the IBM MaaS360 SaaS for mobile device management. Various modules are supplied by IBM, each of which integrates with service components of the MaaS360 customer's infrastructure. For this evaluation, the four modules listed in Section 1.2 are the only modules included.

1.5 TOE Architecture

The Cloud Extender is a Windows application and service comprised of:

- Core Installer—this functions as a Windows service
- Four CE modules

The Cloud Extender consists of multiple processes running simultaneously. It uses the following cryptographic libraries:

- The Windows Cryptography API Next Generation (CNG) cryptographic library accessed via the .NET 3.5 framework.
- OpenSSL for the IBM MaaS360 Cloud Extender.

CNG is used for communication and data-at-rest purposes while Open (Secure Sockets Layer) SSL is used for HTTPS connections. OpenSSL for the IBM MaaS360 Cloud Extender is also used to encrypt configuration templates generated by the IBM MaaS360 Cloud Extender Configuration Tool should TOE administrators wish to similarly configure another Cloud Extender. As this template is stored by default in an encrypted file system (EFS) volume, the TOE platform is thusly providing the overall data-at-rest capability.

The Core Installer communicates with the MaaS360 SaaS. It uses Client for URLs (cURL) and Windows crypto for protecting the communications channel between the MaaS360 SaaS application and the Cloud Extender. The Core Installer uses TLS 1.2 and initiates all communication with the MaaS360 SaaS application. Thus, the TOE acts as a TLS client.

The TOE is packaged with several third-party libraries which are listed in FPT_LIB_EXT.1.

The IBM MaaS360 Cloud Extender configuration tool is supplied with the Cloud Extender installation package which can be used during the initial installation as well as on-demand when configuration changes are necessary.

The evaluated configuration includes four CE modules, which are packages of scripts and actions that integrate with components of the MaaS360 customer's infrastructure and provides full integration service with that component. Table 1: Description of the Cloud Extender Modules provides descriptions of each of the CE modules.

CE Module	Description
Exchange Integration for Active Sync Devices Module	The Exchange Integration module interacts with the Exchange Server to automatically discover ActiveSync-connected devices and uploads that device information to the MaaS360® Cloud. The Exchange Integration module automatically quarantines devices, allows only MaaS360 enrolled devices, carries out actions (such as Approve, Block, or Remove device from the Mailbox) sent from MaaS360, and applies ActiveSync device policies. This module supports MS Exchange 2007, 2010, 2013, 2016, Office 365, and Microsoft Business Productivity Online Suite (BPOS)-D.
Corporate Directory Authentication Modules	The User Authentication module interacts with Active Directory and LDAP directories to provide user authentication service for various MaaS360 functions, such as self-service device enrollment with corporate credentials, MaaS360 Portal login, and user management portal. The Cloud Extender supports integration with Lightweight Directory Access Protocol (LDAP) implementations, including Active Directory, Domino® LDAP, Oracle® LDAP, Novell® eDirectory LDAP, and OpenLDAP.
Corporate User Visibility Module	The User Visibility module synchs user and group information from LDAP or Active Directory directories to the MaaS360 SaaS application.
Certificate Authority Module	The Certificate Integration module facilitates the automatic provisioning, distribution, and renewal of digital identity certificates to managed mobile devices by using existing Microsoft Certificate Authority (CA), Symantec® CA, or Entrust® Admin Services and Identity Guard. The Cloud Extender interacts with the CA, and then pushes the issued certificates down to enrolled devices by using the following method: It receives certificate requests from the MaaS360 Portal for all enrolled devices that require an identity certificate. It authenticates against the CA or Registration Authority (RA) as a part of the certificate request process.

	It requests ID certificates by passing the details of the device or user and corresponding attributes as a part of the certificate request. It encrypts the received certificate by using the public key of the requesting device and pushes the encrypted payload to the MaaS360 Portal, which is then delivered to the device. It supports auto-renewals of certificates and makes sure that devices receive the new certificates before the current certificate expires.

Table 1: Description of the Cloud Extender Modules

1.5.1 Hardware

The hardware platform used during the evaluation was a Dell PowerEdge T110 II with an Intel Core i3 processor.

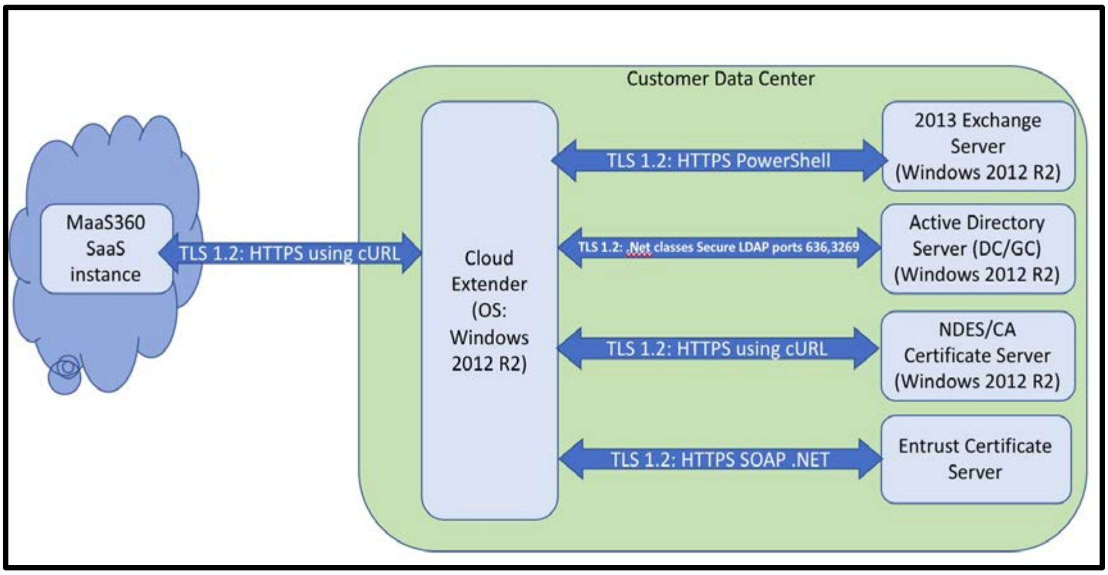
1.5.2 Operational Environment

The TOE requires the following in its operational environment.

- A configured and operational instance of the MaaS360 SaaS application
- One or more enrolled mobile devices
- A network connection to the MaaS360 SaaS application and the customer's internal network
- A Windows Server 2012 R2 platform on which it runs
- A MS Exchange Server
- An Active Directory Server
- A Network Device Enrollment Server Certificate Authority (NDES CA) server and/or An Entrust Certificate server

The TOE was tested in the environment described in Figure 2: The Operational Environment for the Cloud Extender TOE.

Figure 2: The Operational Environment for the Cloud Extender TOE


Customer Data Center
MaaS360 SaaS instance
TLS 1.2: HTTPS using cURL
Cloud Extender (OS: Windows 2012 R2)
TLS 1.2: HTTPS PowerShell
2013 Exchange Server (Windows 2012 R2)
TLS 1.2: .Net classes Secure LDAP ports 636,3269
Active Directory Server (DC/GC) (Windows 2012 R2)
TLS 1.2: HTTPS using cURL
NDES/CA Certificate Server (Windows 2012 R2)
TLS 1.2: HTTPS SOAP .NET
Entrust Certificate Server

1.5.3 Physical Boundary of the TOE

The Physical Boundary of the TOE consists of the application installer executable and guidance documents. Each of these assets is distributed digitally via the customer's portal.

1.5.4 Logical Boundary of the TOE

The figure below describes the logical boundary of the TOE which includes the TOE Security Functions (TSF) as specified in [pp_app_v1.2].

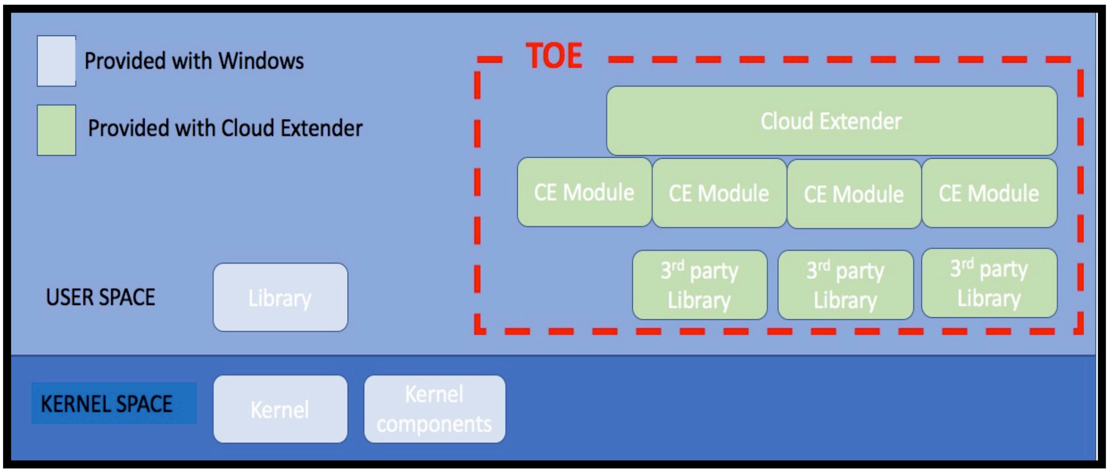


Figure 3: The Logical Boundary of the Cloud Extender TOE

1.5.5 Security Functions provided by the TOE

The TOE provides the security functionality required by [pp_app_v1.2].

1.5.5.1 Cryptographic Support (FCS)

The Cloud Extender provides cryptographic support using the Windows platform provided cryptographic services via the Cryptography API: Next Generation (CNG) for the following.

1. TLS connections—CNG is used by Secure Channel (SChannel), enabling the Cloud Extender to communicate with the Exchange Server, Domain Controller, and PKI Certificate Servers using HTTPS, limiting the protocol to TLS 1.2, and only using a subset of the TLS 1.2 ciphers.
2. Protecting data-at-rest using the Encrypted File System (EFS) to the C:\ProgramData\MaaS360\ directory that contains all configuration and log information.
3. Encrypting registry entries using the Data Protection Application Programming Interface (DAPI).
4. Generating an Exchange Server certificate during the installation process.

The inclusion of the OpenSSL for the IBM MaaS360 Cloud Extender libraries with the TOE provides cryptographic functionality for the following functions.

1. TLS connections to the MaaS360 Portal and SCEP certificate servers only. (HTTPS using cURL)
2. Encryption of configuration profiles, but as these are stored within an EFS directory above it is not the enforcing SFR.
3. Device and User Certificate generation for certificate signing requests to a SCEP server using the Device and User templates. These requests are completed by the SCEP server and certificates returned to the IBM MaaS360 Cloud Extender, as detailed in Table 2: Device and User Certificate Related Functionality.

Type	Explanation
Mobile Device	The Cloud Extender generates a certificate based on requirements and pushes that certificate to the mobile device. The Cloud Extender uses certificate templates to pass user attributes as part of the Subject Name / Alternate Name, which links the certificate to the user and is used as a device certificate. Devices treat all certificates as user certificates. Most common used certificate template type that supports Microsoft, Symantec, Entrust, and Verizon MCS. Mostly used for authentication.
User	Support for Microsoft certificates stored in AD, Entrust, and IDnomic – Mobile Guard (OpenTrust) Mostly used for S/MIME certificates to deliver signing and encryption certificates. For user certificates that are used for authentication, choose the device certificate template, and provide user attributes to pass to the CA for certificate generation.

Table 2: Device and User Certificate Related Functionality

1.5.5.2 *Entropy*

For the platform provided cryptographic functions, the entropy source is platform provided entropy.

Specifically, the entropy source for OpenSSL for the IBM MaaS360 Cloud Extender provided cryptographic functions uses a 384 bit seed for a SP800-90A DRBG implementation obtained from the platform by calling CryptGenRandom().

1.5.5.3 *User Data Protection (FDP)*

The application provides user data protection services through restricting access by the application to only those platform-based resources (sensitive data repositories, and network communications) that are needed in order to provide the needed application functionality.

Sensitive application data is encrypted using platform-provided encrypted file system (EFS) services, when stored in non-volatile memory, such as the hard disk drive(s).

1.5.5.4 *Identification and Authentication (FIA)*

The TOE supports authentication by X.509 certificates by the application and using the platform API. Certificate validation, supported properties and usage are described in section 8.3.1.

1.5.5.5 *Security Management (FMT)*

The Cloud Extender application provides the ability to set various configuration options for the TOE. These options are stored, as recommended by Microsoft, in the Windows Registry and are protected using the Data Protection application programming interface (DPAPI).

During installation, the files installed on the platform are allocated appropriate file-permissions, supporting the protection of the application, and its data from unauthorized access.

1.5.5.6 *Privacy (FPR)*

The Cloud Extender application does not specifically request Personally Identifiable Information (PII).

1.5.5.7 Protection of the TSF (FPT)

The Cloud Extender application uses only documented Windows APIs. It is packaged with third party libraries which provide supporting functionality. These are listed in section 6.6 FPT_LIB_EXT.1.

The Cloud Extender application does not write user-modifiable files to directories that contain executable files.

The Cloud Extender application is compiled using stack buffer overrun protection and uses Address Space Layout Randomization (ASLR) techniques, it does not generally request to map memory at explicit addresses. Exceptions are listed in Section 8.6.

The Cloud Extender application is packaged and delivered in the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process using the Microsoft Sign Tool.exe (v6.3). It is compiled by IBM with stack-based buffer overflow protection enabled.

1.5.5.8 Trusted Path/Channels (FTP)

The Cloud Extender application protects all transmitted data by using TLS 1.2 protected trusted channels. Protocols used within these trusted channels may include additional protection and include HTTPS, and LDAPS.

1.6 TOE Documentation

[ADMIN] The Cloud Extender Admin Guide
https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/ce_source/concepts/ce_kc_container.htm

[ARCH] The Cloud Extender Architecture
https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/ce_source/references/ce_architecture.htm

[CC-CFG] The MaaS360 Cloud Extender NIAP Protection Profile Setup and Operations Guide V1.11
https://www.niap-ccevs.org/st/st_vid10896-agd.pdf
https://www.ibm.com/support/knowledgecenter/SS8H2S/com.ibm.mc.doc/ce_source/pdfs/IBM_MaaS360_CE_NIAP_Protection_Profile_Guide.pdf?view=kc

2 Conformance Claims

2.1 CC Conformance

This [ST] is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 4, September 2012,
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 4, September 2012: Part 2 extended, and
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision 4, September 2012: Part 3 extended.

2.2 Protection Profile (PP) Conformance

This [ST] is conformant to:

- U.S. Government Approved Protection Profile for Application Software, Version 1.2, dated 22 April, 2016 [pp_app_v1.2]
  https://www.niap-ccevs.org/Profile/Info.cfm?PPID=394&id=394

2.3 Conformance Rationale

This [ST] provides exact conformance with version 1.2 of the U.S. Government Approved Protection Profile for Application Software [pp_app_v1.2]. The security problem definition, security objectives and security requirements in this [ST] are all taken from the PP performing only operations defined there.

The requirements in the PP are assumed to represent a complete set of requirements that serve to address any interdependencies. Given that all of the appropriate functional requirements given in the PPs have been copied into this ST, the dependency analysis for the requirements is assumed to be already performed by the PP authors and is not reproduced in this document.

2.4 Technical Decisions

The following technical decisions were found to be applicable to the TOE at the time of the evaluation.

[TD0304] Update to FCS_TLSC_EXT.1.2
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=310

[TD0300] Sensitive Data in FDP_DAR_EXT.1
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=306

[TD0296] Update to FCS_HTTPS_EXT.1.3
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=302

[TD0295] Update to FPT_AEX_EXT.1.3 Assurance Activity
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=301

[TD0293] Update to FCS_CKM.1(1)
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=299

[TD0283] Cipher Suites for TLS in SWApp v1.2
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=289

[TD0268] FMT_MEC_EXT.1 Clarification
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=274

[TD0244] FCS_TLSC_EXT – TLS Client Curves Allowed
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=250

[TD0238] User-modifiable files FPT_AEX_EXT.1.4
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=244

[TD0221] FMT_SMF.1.1 – Assignments moved to Selections
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=226

[TD0217]: Compliance to RFC5759 and RFC5280 for using CRLs
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=222

[TD0215] Update to FCS_HTTPS_EXT.1.2
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=220

[TD0192] Update to FCS_STO_EXT.1 Application Note
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=196

[TD0174] Optional Ciphersuites for TLS
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=178

[TD0172] Additional APIs added to FCS_RBG_EXT.1.1
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=176

[TD0163] Update to FCS_TLSC_EXT.1.1 Test 5.4 and FCS_TLSS_EXT.1.1 Test
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=167

[TD0121] FMT_MEC_EXT.1.1 Configuration Options
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=124

[TD0119] FCS_STO_EXT.1.1 in PP_APP_v1.2
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=122

[TD0107] FCS_CKM - ANSI X9.31-1998, Section 4.1.for Cryptographic Key Generation
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=110

The following technical decisions have been released but were found to be not applicable to the TOE at the time of the evaluation since they address SFRs or assurance activities not selected/applicable in this ST:

[TD0305] Handling of TLS connections with and without mutual authentication
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=311

[TD0267] TLSS testing - Empty Certificate Authorities list
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=273

[TD0241] Removal of Test 4.1 in FCS_TLSS_EXT.1.1
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=247

[TD0178] Integrity for installation tests in AppSW PP
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=182

[TD0177] FCS_TLSS_EXT.1 Application Note Update
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=181

[TD0131] Update to FCS_TLSS_EXT.1.1 Test 4.5
https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=134

3 Security Problem Definition

The security problem definition has been taken from [pp_app_v1.2]. It is reproduced here for the convenience of the reader.

3.1 Threats

T.NETWORK_ATTACK

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.

T.NETWORK_EAVESDROP

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

T.LOCAL_ATTACK

An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.

T.PHYSICAL_ACCESS

An attacker may try to access sensitive data-at-rest.

3.2 Assumptions

A.PLATFORM

The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

A.PROPER_USER

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

A.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.

3.3 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of rules, practices, and procedures imposed by an organization to address its security needs.

There are no Organizational Security Policies for the application.

4 Security Objectives

The security objectives have been taken from [pp_app_v1.2]. They are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

O.INTEGRITY

Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom if ever shipped without errors, and the ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.

Addressed by: FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1

O.QUALITY

To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.

Addressed by: FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1

O.MANAGEMENT

To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.

Addressed by: FMT_SMF.1, FPT_TUD_EXT.1.5, FPR_ANO_EXT.1

O.PROTECTED_STORAGE

To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.

Addressed by: FDP_DAR_EXT.1, FDP_DAR_EXT.1, FCS_STO_EXT.1, FCS_RBG_EXT.1

O.PROTECTED_COMMS

To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

Addressed by: FTP_DIT_EXT.1, FCS_TLSC_EXT.1, FCS_RBG_EXT.1

4.2 Security Objectives for the TOE Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the 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_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.

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.

5 Extended Components Definition

The Security Target draws upon the extended components implicitly defined in the [pp_app_v1.2].

6 Security Functional Requirements

This chapter describes the Security Functional Requirements (SFRs) for the TOE. The SFRs have been taken from [pp_app_v1.2] with selections and assignments being applied.

Selections and assignment operations performed as required by [pp_app_v1.2] are marked in **bold**.

Note that this ST does not identify selections, assignments or refinements already applied in [pp_app_v1.2].

The requirements in the PP are assumed to represent a complete set of requirements that serve to address any interdependencies. Given that all of the appropriate functional requirements given in the PPs have been copied into this ST, the dependency analysis for the requirements is assumed to be already performed by the PP authors and is not reproduced in this document.

6.1 Cryptographic Support (FCS)

FCS_CKM_EXT.1(TOE Application) Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall **implement asymmetric key generation**.

FCS_CKM.1(TOE Application) Cryptographic Asymmetric Key Generation [1]

FCS_CKM.1.1(TOE Application))

The application shall **implement functionality** to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm

RSA schemes using cryptographic key sizes of 2048 bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3.

ECC schemes using "NIST curves" P-256, and P-384 that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS), Appendix B.4

FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1.

FCS_CKM.1(TOE Platform) Cryptographic Asymmetric Key Generation [2]

FCS_CKM.1.1(TOE Platform)

The application shall **implement functionality** to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm

RSA schemes using cryptographic key sizes of 2048 bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3.

ECC schemes using "NIST curves" P-256, and P-384 that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS), Appendix B.4

FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1.

FCS_CKM.2(TOE Application) Cryptographic Key Establishment

FCS_CKM.2.1

The application shall **implement functionality** to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

[1] TD0107 and TD0293 is applicable to this SFR.

[2] TD0107 and TD0293 is applicable to this SFR.

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” and:

Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”,

Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”.

FCS_COP.1(1)(TOE Application) Cryptographic Operation - Encryption/Decryption

FCS_COP.1.1(1)

The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm.

- AES-CBC (as defined in NIST SP 800-38A) mode;

and **AES-GCM (as defined in NIST SP 800-38D)**

and cryptographic key sizes 256-bit and **128 bit**.

FCS_COP.1(2)(TOE Application) Cryptographic Operation - Hashing

FCS_COP.1.1(2)

The application shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm:

SHA-1,

SHA-256,

SHA-384.

and message digest sizes:

160,

256,

384.

bits that meet the following: FIPS Pub 180-4.

FCS_COP.1(3)(TOE Application) Cryptographic Operation - Signing

FCS_COP.1.1(3)

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 4,

ECDSA schemes using “NIST curves” P-256, P-384 and no other curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.

FCS_COP.1(4)(TOE Application) Cryptographic Operation - Keyed-Hash Message Authentication

FCS_COP.1.1(4)

The application shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm

- HMAC-SHA-256

and

SHA-1,

SHA-384

with key sizes **160**, **256 and 384 bits** and message digest sizes 256 and 160 and ***348*** bits that meet the following: FIPS Pub 198-1 *The Keyed-Hash Message Authentication Code* and FIPS Pub 180-4 *Secure Hash Standard*.

FCS_HTTPS_EXT.1(1)(TOE Platform)

FCS_HTTPS_EXT.1.1

The application shall implement the HTTPS protocol that complies with RFC 2818

FCS_HTTPS_EXT.1.2[3]

The application shall implement HTTPS using TLS in accordance with **FCS_TLSC_EXT.1**

FCS_HTTPS_EXT.1.3[4]

The application shall **notify the user and not establish the connection** if the peer certificate is deemed invalid.

FCS_HTTPS_EXT.1(2)(TOE Application)

FCS_HTTPS_EXT.1.1

The application shall implement the HTTPS protocol that complies with RFC 2818

FCS_HTTPS_EXT.1.2[2]

The application shall implement HTTPS using TLS in accordance with **FCS_TLSC_EXT.1**

FCS_HTTPS_EXT.1.3[5]

The application shall **notify the user and not establish the connection** if the peer certificate is deemed invalid.

FCS_RBG_EXT.1(1)(TOE Platform) Random Bit Generation Services

FCS_RBG_EXT.1.1[6]

[3] TD0215 is applicable to this element
[4] TD0296 is applicable to this element
[5] TD0296 is applicable to this element
[6] TD0172 is applicable to this element

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

FCS_RBG_EXT.1(2)(TOE Application)Random Bit Generation Services

FCS_RBG_EXT.1.1[7]

The application shall **implement DRBG functionality** for its cryptographic operations.

FCS_RBG_EXT.2(TOE Application) Random Bit Generation from Application

FCS_RBG_EXT.2.1

The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using **CTR_DRBG (AES)**.

FCS_RBG_EXT.2.2

The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and **no other noise source** with a minimum of **128 bits** of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_STO_EXT.1(TOE Platform) Storage of Credentials[8]

FCS_STO_EXT.1.1[9]

The application shall, **invoke the functionality provided by the platform to securely store certificates for MaaS360 SaaS application, Customer's instantiation of Microsoft SCEP, Customer's instantiation of Active Directory and/or LDAP server, Customer's instantiation of Microsoft Exchange and/or Active Sync to non-volatile memory.**

FCS_TLSC_EXT.1(1)(TOE Platform) TLS Client Protocol

FCS_TLSC_EXT.1.1[10]

The application shall **invoke platform-provided TLS 1.2** supporting the following cipher suites:
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246.

FCS_TLSC_EXT.1.2

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

FCS_TLSC_EXT.1.3

[7] TD0172 is applicable to this element
[8] TD0192 is applicable to this component
[9] TD0119 is applicable to this element
[10] TD0174, TD0163 and TD0283 are applicable to this element

The application shall establish a trusted channel only if the peer certificate is valid.

FCS_TLSC_EXT.1(2)(TOE Application) TLS Client Protocol

FCS_TLSC_EXT.1.1[11]

The application shall **implement TLS1.2 (RFC 5246)** supporting the following cipher suites:
TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246,
TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246.

FCS_TLSC_EXT.1.2[12]

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

FCS_TLSC_EXT.1.3

The application shall establish a trusted channel only if the peer certificate is valid.

FCS_TLSC_EXT.4(1)(TOE Platform) TLS Client Protocol

FCS_TLSC_EXT.4.1[13]

The application shall present the supported Elliptic Curves Extension in the Client Hello with the following NIST curves: **secp256r1, secp384r1**.

FCS_TLSC_EXT.4(2)(TOE Application) TLS Client Protocol

FCS_TLSC_EXT.4.1[14]

The application shall present the supported Elliptic Curves Extension in the Client Hello with the following NIST curves: **secp256r1, secp384r1**.

6.2 User Data Protection (FDP)

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1

The application shall restrict its access to **network connectivity** and **no additional hardware resources.**

FDP_DEC_EXT.1.2

[11] TD0174, TD0163 and TD0283 are applicable to this element

[12] TD0304 is applicable to this element

[13] TD0244 is applicable to this element

[14] TD0244 is applicable to this element

The application shall restrict its access to **the Windows Credential Store as well as system logs and Windows Event logs-application with the following folders and sub-folders:**

- **C:\Program Files (x86)\MaaS360\Cloud Extender**
- **C:\ProgramData\MaaS360\Cloud Extender**
- **C:\Program Files (x86)\Common Files\MaaS360\Visibility_2.91.002.**

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to
respond to no remotely initiated communication,
MaaS360 SaaS application,
customer's instantiation of Microsoft NDES CA,
customer's instantiation of Entrust CA,
customer's instantiation of Active Directory and/or LDAP server,
customer's instantiation of Microsoft Exchange and/or Active Sync.

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1 [15]

The application shall **leverage platform-provided functionality to encrypt sensitive data** in non-volatile memory.

6.3 Identification and Authentication (FIA)

FIA_X509_EXT.1(1)(TOE Platform) X.509 Certificate Validation

FIA_X509_EXT.1.1 [16]

The application shall **invoke platform-provided 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 and that the CA flag is set to TRUE for all CA certificates.
- The application shall validate the revocation status of the certificate using **a Certificate Revocation List (CRL) as specified in RFC 5759.**
- The application shall validate the extendedKeyUsage field according to the following rules:
  - 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.
  - 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 extendedKeyUsage field.

[15] TD0300 is applicable to this element
[16] TD 0217 is applicable to this element

  - 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 extendedKeyUsage field.
  - 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 extendedKeyUsage field.
  - 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 extendedKeyUsage field.
  - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp- cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.

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.

FIA_X509_EXT.1(2)(TOE Application) X.509 Certificate Validation

FIA_X509_EXT.1.1 [17]

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 and that the CA flag is set to TRUE for all CA certificates.
- The application shall validate the revocation status of the certificate using **a Certificate Revocation List (CRL) as specified in RFC 5759.**
- The application shall validate the extendedKeyUsage field according to the following rules:
  - 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.
  - 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 extendedKeyUsage field.
  - 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 extendedKeyUsage field.
  - 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 extendedKeyUsage field.
  - 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 extendedKeyUsage field.
  - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp- cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.

[17] TD 0217 is applicable to this element

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.

FIA_X509_EXT.2(1)(TOE Platform) X.509 Certificate Authentication

FIA_X509_EXT.2.1

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

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.**

FIA_X509_EXT.2(2)(TOE Application) X.509 Certificate Authentication

FIA_X509_EXT.2.1

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

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.**

6.4 Security Management (FMT)

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1

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

FMT_CFG_EXT.1.2

The application shall be configured by default with file permissions which protect it and its data from unauthorized access.

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1[18]

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

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1[19]

The TSF shall be capable of performing the following management functions: **configure cryptographic functionality**.

[18] TD0121 and TD0268 are applicable to this element

[19] TD0221 is applicable to this element

6.5 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1

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

6.6 Protection of the TSF (FPT)

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

- The application shall not request to map memory at an explicit address except for the **OpenSSL for the IBM MaaS360 Cloud Extender and FIPS Object Modules.**

FPT_AEX_EXT.1.2

The application shall **allocate memory regions with write and execute permissions for only EntrustCerts.exe, EntrustCertsConfig.exe, LDAPAuth.exe, LDAPConfig.exe, LDAPUsersInfo.exe and LDAPConfig.exe**.

FPT_AEX_EXT.1.3[20]

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

FPT_AEX_EXT.1.4[21]

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

FPT_AEX_EXT.1.5

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

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1

The application shall **provide the ability** to check for updates and patches to the application software.

FPT_TUD_EXT.1.2

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

FPT_TUD_EXT.1.3

[20] TD0295 is applicable to this element

[21] TD0238 is applicable to this element

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.

FPT_TUD_EXT.1.4

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

FPT_TUD_EXT.1.5

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

FPT_TUD_EXT.1.6

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

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1

The application shall be packaged with only

SQLite, 3.15.0
OpenSSL, 1.0.2o with OpenSSL FIPS Module, 2.0.13[22]
libcURL, 7.58.1
Zlib vc, 1.1.4
Protobuf, 2.6.1
Boost, 1.5.9
Bitwise Operation Library 2008
Lua, 5.1
Lua cURL, 1.6
luasql, 2.1
DotNetZip, 1.9.1.8
NSIS, 2.46
CMarkUp, 11.2
Gloox Library, 1.0.1
Microsoft Framework, 8.0
InstallShield, 2015 + SP1 Professional

6.7 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1(1)(TOE Platform) Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall **encrypt all transmitted sensitive data with HTTPS, TLS** between itself and another trusted IT product.

FTP_DIT_EXT.1(2)(TOE Application) Protection of Data in Transit

FTP_DIT_EXT.1.1

[22] This library implements OpenSSL for the IBM MaaS360 Cloud Extender.

The application shall **encrypt all transmitted sensitive data with HTTPS** between itself and another trusted IT product.

7 Security Assurance Requirements

The Security Assurance Requirements for the TOE are defined in [pp_app_v1.2].

The assurance components included in [pp_app_v1.2] are:

- ASE_CCL.1
- ASE_ECD.1
- ASE_INT.1
- ASE_OBJ.1
- ASE_REQ.1
- ASE_SPD.1
- ASE_TSS.1
- ADV_FSP.1
- AGD_OPE.1
- AGD_PRE.1
- ALC_CMC.1
- ALC_CMS.1
- ALC_TSU_EXT.1
- ATE_IND.1
- AVA_VAN.1

7.1 Security Target Evaluation

7.1.1 Conformance Claims (ASE_CCL.1)

ASE_CCL.1.1D

The developer shall provide a conformance claim.

ASE_CCL.1.2D

The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C

The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C

The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C

The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C

The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C

The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C

The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C

The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C

The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C

The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C

The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

ASE_CCL.1.1E

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

7.1.2 Extended Components Definition (ASE_ECD.1)

ASE_ECD.1.1D

The developer shall provide a statement of security requirements.

ASE_ECD.1.2D

The developer shall provide an extended components definition.

ASE_ECD.1.1C

The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C

The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C

The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C

The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C

The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

ASE_ECD.1.1E

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

ASE_ECD.1.2E

The evaluator shall confirm that no extended component can be clearly expressed using existing components.

7.1.3 ST Introduction (ASE_INT.1)

ASE_INT.1.1D

The developer shall provide an ST introduction.

ASE_INT.1.1C

The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C

The ST reference shall uniquely identify the ST.

ASE_INT.1.3C

The TOE reference shall identify the TOE.

ASE_INT.1.4C

The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C

The TOE overview shall identify the TOE type.

ASE_INT.1.6C

The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C

The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C

The TOE description shall describe the logical scope of the TOE.

ASE_INT.1.1E

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

ASE_INT.1.2E

The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

7.1.4 Security Objectives for the Operational Environment (ASE_OBJ.1)

ASE_OBJ.1.1D

The developer shall provide a statement of security objectives.

ASE_OBJ.1.1C

The statement of security objectives shall describe the security objectives for the operational environment.

ASE_OBJ.1.1E

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

7.1.5 Stated Security Requirements (ASE_REQ.1)

ASE_REQ.1.1D

The developer shall provide a statement of security requirements.

ASE_REQ.1.2D

The developer shall provide a security requirements rationale.

ASE_REQ.1.1C

The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C

All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C

The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C

All operations shall be performed correctly.

ASE_REQ.1.5C

Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.1.6C

The statement of security requirements shall be internally consistent.

ASE_REQ.1.1E

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

7.1.6 Security Problem Definition (ASE_SPD.1)

ASE_SPD.1.1D

The developer shall provide a security problem definition.

ASE_SPD.1.1C

The security problem definition shall describe the threats.

ASE_SPD.1.2C

All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C

The security problem definition shall describe the OSPs.

ASE_SPD.1.4C

The security problem definition shall describe the assumptions about the operational environment of the TOE.

ASE_SPD.1.1E

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

7.1.7 TOE Summary Specification (ASE_TSS.1)

ASE_TSS.1.1D

The developer shall provide a TOE summary specification.

ASE_TSS.1.1C

The TOE summary specification shall describe how the TOE meets each SFR.

ASE_TSS.1.1E

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

ASE_TSS.1.2E

The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

7.2 Development (ADV)

7.2.1 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.

Application Note: As indicated in the introduction to this section, the functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation. The developer may reference a website accessible to application developers and the evaluator. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.

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 categorisation 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.

7.3 Guidance Documents (AGD)

7.3.1 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1.1D

The developer shall provide operational user guidance.

Application Note: The operation user guidance does not have to be contained in a single document. Guidance to users, administrators and application developers can be spread among documents or web pages. Where appropriate, the guidance documentation is expressed in the eXtensible Configuration Checklist Description Format (XCCDF) to support security automation. Rather than repeat information here, the developer should review the assurance activities for this component to ascertain the specifics of the guidance that the evaluator will be checking for. This will provide the necessary information for the preparation of acceptable 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.

Application Note: User and administrator are to be considered in the definition of user role.

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 fulfil 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.

7.3.2 Preparative Procedures (AGD_PRE.1)

AGD_PRE.1.1D

The developer shall provide the TOE including its preparative procedures.

Application Note: As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to 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.

7.4 Life-cycle Support (ALC)

7.4.1 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 TOE shall be labelled with its unique reference.

Application Note: Unique reference information includes:

- *Application Name*
- *Application Version*
- *Application Description*

- *Platform on which Application Runs*
- *Software Identification (SWID) tags, if available*

ALC_CMC.1.1E

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

7.4.2 TOE CM Coverage (ALC_CMS.1)

ALC_CMS.2.1D

The developer shall provide a configuration list for the TOE.

ALC_CMS.2.1C

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

ALC_CMS.2.2C

The configuration list shall uniquely identify the configuration items.

ALC_CMS.2.1E

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

7.4.3 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.1.1C

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

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.

7.5 Tests (ATE)

7.5.1 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.

Application Note: The evaluator shall test the application on the most current fully patched version of the platform.

7.6 Vulnerability Assessment (AVA)

7.6.1 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.

Application Note: Suitability for testing means not being obfuscated or packaged in such a way as to disrupt either static or dynamic analysis by the evaluator.

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.

Application Note: Public domain sources include the Common Vulnerabilities and Exposures (CVE) dictionary for publicly known vulnerabilities. Public domain sources also include sites which provide free checking of files for viruses.

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.

8 TOE Summary Specification (TSS)

This chapter describes the relevant aspects of how the security functional requirements are implemented in the security functionality provided by the TOE. This chapter is structured in accordance with the structuring of the security functional requirements in chapter 6 of this document, which in turn has been taken from the structure of the description of the security functional requirements in [pp_app_v1.2].

8.1 Cryptographic Support (FCS)

8.1.1 Asymmetric keys (FCS_CKM.1(TOE Application) and FCS_CKM.1(TOE Platform))

Section 6 indicates in FCS_CKM.1.1(TOE Application) and FCS_CKM.1.1(TOE Platform) that the following schemes are used.

Scheme	Scheme usage	Key sizes
RSA schemes using cryptographic key sizes of 2048 bit or greater that meet FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	HTTPS/TLS communications	2048 bits or greater
ECC schemes using "NIST curves" P-256 and P-384 that meet FIPS PUB 186-4, "Digital Signature Standard (DSS), Appendix B.4	HTTPS/TLS communications	P-256 and P-384
FFC schemes using cryptographic key sizes of 2048 bit or greater that meet FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1	HTTPS/TLS communications	2048 bits or greater

Table 3: Asymmetric Key Sizes Used by the TOE

The application invokes platform-provided functionality for asymmetric key generation. The key generation functionality is invoked through calls to the relevant crypto API in Windows.

The application also implements asymmetric key generation through the OpenSSL for the IBM MaaS360 Cloud Extender cryptographic module for HTTPS /TLS communication purposes.

8.1.2 Cryptographic Key Establishment (FCS_CKM.2(TOE Application))

Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC) and Finite Field Cryptography (FFC) key establishment schemes are supported by the TOE for the establishment of TLS/HTTPS communications in which the TOE may act as a sender or recipient.

All decryption errors are generically captured by the Endpoint Management System (EMS) agent log located in the platform provided EFS. Additionally, if the decryption error occurs while the IBM MaaS360 Cloud Extender Configuration Tool is being used, the user will receive a pop-up error stating that the connection has failed.

8.1.3 Encryption/Decryption (FCS_COP.1(1)(TOE Application))

The TOE implements Encryption and Decryption operations in support of TLS/HTTPS communications. The supported algorithms can be found in FCS_COP.1(1)(TOE Application). These operations are implemented via the TOE's OpenSSL for the IBM

MaaS360 Cloud Extender cryptographic module. All algorithms have been certified by the Cryptographic Algorithm Validation Program (CAVP). See Table 12: SFR to CAVS Cert Number for more information.

8.1.4 Hashing (FCS_COP.1(2)(TOE Application))

Cryptographic hashing operations are performed in support of TLS/HTTPS connections. The supported hashes can be found in FCS_COP.1(2)(TOE Application). Hashing functionality is handled via the TOE's OpenSSL for the IBM MaaS360 Cloud Extender cryptographic module and has been certified by the Cryptographic Algorithm Validation Program (CAVP). See Table 12: SFR to CAVS Cert Number for more information.

8.1.5 Signing (FCS_COP.1(3)(TOE Application))

Digital signature services provided by the TOE support X.509 authentication for RSA schemes implemented by the OpenSSL for the IBM MaaS360 Cloud Extender module as well as the Elliptic Curve Digital Signature Algorithm (ECDSA). All algorithms have been certified by the Cryptographic Algorithm Validation Program (CAVP). See Table 12: SFR to CAVS Cert Number for more information.

8.1.6 Keyed-Hash Message Authentication (FCS_COP.1(4) (TOE Application))

The TOE implements keyed-hash message authentication operations in support of TLS/HTTPS communications. The supported algorithms can be found in FCS_COP.1(4)(TOE Application). These operations are implemented via the TOE's OpenSSL for the IBM MaaS360 Cloud Extender cryptographic provider. All algorithms have been certified by the Cryptographic Algorithm Validation Program (CAVP). See Table 12: SFR to CAVS Cert Number for more information.

8.1.7 Random Bit Generation Services (FCS_RBG_EXT.1(1)(TOE Platform),FCS_RBG_EXT.1(2)(TOE Application), FCS_RBG_EXT.2(TOE Application))

The TOE implements its own deterministic random bit generator (DRBG) functionality but collects entropy from the underlying platform as a seed. The TOE includes an OpenSSL for the IBM MaaS360 Cloud Extender implementation of the CTR_DRBG (AES) which is invoked by the TOE for random bit generation services by default. There is no ability to specify the use of an alternative DRBG. The TOE's DRBG is seeded with entropy data that is collected from the underlying platform using the BCryptGenRandom API. The amount of entropy that is collected is greater than or equal to the security strength of the data that is being output (e.g. a 256-bit AES key generation operation will collect at least 128 bits of entropy before the DRBG is invoked). The entropy source is described in greater detail in the proprietary Entropy Assessment Report.

TOE function	Platform (Windows) API
TLSC	BCryptGenRandom
HTTPS	BCryptGenRandom

Table 4: Functions Obtaining Random Numbers from Windows

All algorithms have been certified by the Cryptographic Algorithm Validation Program (CAVP). See Table 12: SFR to CAVS Cert Number for more information.

8.1.8 Credentials used by the Cloud Extender (FCS_STO_EXT.1(TOE Platform))

Credentials necessary for the operation of the TOE can be found in Table 5: Credential List, below. It should be noted, however, that credentials for the TOE modules (e.g. Entrust or NDES Certificate, LDAP Bindings, etc) are passed through the TOE via encrypted channels defined in section 1.5.3.3.

Persistent credential	Purpose	Storage
Private PKI keys	EFS encryption	Windows certificate store
Private keys	Backup/transfer of Cloud Extender configuration file	EFS protected directory
	Registration request encryption	EFS protected directory
	License key	EFS protected directory

Table 5: Credential List

8.1.9 TLS Client Protocol FTP_DIT_EXT.1(1)(TOE Platform), FCS_TLSC_EXT.1(1)(TOE Platform), FCS_TLSC_EXT.4(1)(TOE Platform), FCS_HTTPS_EXT.1(1)(TOE Platform)

The Cloud Extender (the TOE) implements TLS 1.2 in support of HTTPS and TLS over LDAPS secure communications. The TLS Client protocol is provided from the Windows platform for LDAPS and HTTPS.

The [CC-CFG] instructs the administrator to configure the TOE Platform so that the following ciphersuites, and where specified, elliptic curve extensions are enabled.

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246.

The Cloud Extender (the TOE) validates the peer certificate used for the connection.

When negotiating a TLS 1.2 elliptic curve cipher suite, Windows will include automatically as part of the Client Hello message both its supported elliptic curves extension, i.e., secp256r1, secp384r1, and secp512r as well as signature algorithm, i.e., SHA, SHA256, SHA384, and SHA512 based on the ciphersuites selected by the administrator. By default, the curve secp512r1 is disabled. This curve can be enabled adding its name in the ECC Curve Order file. In addition, the curve priority can be edited in this file.

On the other hand, by default the signature algorithms in the Client Hello message are: SHA1, SHA256, and SHA384. The signature algorithm extension is configurable by editing a registry key to meet with the FCS_TLSC_EXT.1(1)(TOE Platform) requirements. Each Windows component that uses TLS checks that the identifying information in the certificate matches what is expected, the component should reject the connection, these checks include checking the expected Distinguished Name (DN), Subject Name (SN), or Subject Alternative Name (SAN) attributes along with any applicable extended key usage identifiers. The DN, and any SAN, in the certificate is checked against the identity of the remote computer's DNS entry or IP address to ensure that it matches as described at http://technet.microsoft.com/en-us/library/cc783349(v=WS.10).aspx, and in particular the "Server Certificate Message" section.

A certificate that uses a wildcard in the leftmost portion of the resource identifier (i.e., *.contoso.com) can be accepted for authentication, otherwise the certificate will be deemed invalid.

Windows does not provide a general-purpose capability to "pin" TLS certificates.

Windows implements HTTPS as described in RFC 2818 so that system applications executing on the TOE can securely connect to external servers using HTTPS.

8.1.10 TLS Client Protocol FTP_DIT_EXT.1(2)(TOE Application), ,FCS_TLSC_EXT.1(2)(TOE Application), FCS_TLSC_EXT.4(2)(TOE Application), FCS_HTTPS_EXT.1(2)(TOE Application)

A TLS Client protocol is provided from the TOE Application via the cURL library for HTTPS connection to the MaaS360 Cloud and to Certificate Enrollment servers using Simple Certificate Enrollment Protocol (SCEP).

The [CC-CFG] instructs the administrator to configure the TOE Application so that the following ciphersuites are enabled.

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246.

The Cloud Extender (the TOE) validates the peer certificate used for the connection.

When negotiating a TLS 1.2 elliptic curve cipher suite, the TOE Application will include automatically as part of the Client Hello message both its supported elliptic curves extension, i.e., secp256r1 and secp384r1 as well as signature algorithm, i.e., SHA, SHA256 and SHA384 based on the ciphersuites selected by the administrator of the endpoint. Only the secp256r1 and secp384r1 curves are supported by default and no additional configuration is available.

On the other hand, by default the signature algorithms in the Client Hello message are: SHA1, SHA256, and SHA384. The signature algorithm extension is configurable by editing a registry key to meet with the FCS_TLSC_EXT.1(2)(TOE Application) requirements. The TOE Application uses TLS checks that the identifying information in the certificate matches what is expected, the component should reject the connection, these checks include checking the expected Distinguished Name (DN), Subject Name (SN), or Subject Alternative Name (SAN) attributes along with any applicable extended key usage identifiers. The DN, and any SAN, in the certificate is checked against the identity of the remote computer's DNS entry or IP address to ensure that it matches.

A certificate that uses a wildcard in the leftmost portion of the resource identifier (i.e., *.contoso.com) can be accepted for authentication, otherwise the certificate will be deemed invalid. The TOE Application does not provide a general-purpose capability to "pin" TLS certificates.

The TOE Application implements HTTPS as described in RFC 2818 so that system applications executing on the TOE can securely connect to external servers using HTTPS.

By default, the CN and SAN reference identifiers are verified. The CN and SAN are the only supported reference identifiers that can be forced as part of the certificate validation and this behavior is not configurable.

8.2 User Data Protection (FDP)

8.2.1 Encryption of Sensitive Application Data (FDP_DAR_EXT.1)

The Cloud Extender utilizes platform-provided functionality to encrypt sensitive data in non-volatile memory. In particular, it uses the Windows EFS to store sensitive data. Users are instructed to ensure that EFS is enabled for the folders identified in FDP_DAR_EXT.1.

The following sensitive information is stored:

- The C:\ProgramData\MaaS360\ directory that contains all configuration and log information.
- Registry entries using the Data Protection Application Programming Interface (DAPI).
- Private PKI keys
- Private keys
- User Modifiable Files

8.2.2 Access to Platform Resources (FDP_DEC_EXT.1)

With the exception of network connectivity, the TOE application does not restrict any access to platform hardware resources or peripherals. Additionally, the following sensitive information repositories are applicable to the TOE:

- Windows Credential Store (Protected by Platform DAC)
- TOE Windows Registry assets (Protected by DPAPI)

Restriction of access to the directories and files identified in FDP_DEC_EXT.1.2 is provided by the TOE platform's discretionary access controls.

8.2.3 Network Communications (FDP_NET_EXT.1)

Network communications are established between the Cloud Extender and the customer's internal services as described in Figure 2: The Operational Environment for the Cloud Extender TOE.

The Cloud Extender (the TOE) acts as a bridge between the customer's servers and the SaaS based cloud portal. The customer will configure which servers will be integrated into the solution and since exact DNS or URLs cannot be provided, example URLs and port addresses are given in the below table.

Network Communication Type	Information	Example Port
MS Exchange	https://[Exchange]/powershell https://mail01f35.forest35.fiberlinkqa.local/powershell	
User Auth/ Vis Secure LDAP	domaincontroller forest35.fiberlinkqa.local	636

Network Communication Type	Information	Example Port
Entrust	https://Entrust Server] :Port/mdmws/services/AdminServiceV9 https://asmobileenrolldemo.entrust.com:19443/mdmws/services/AdminServiceV9	
NDES	https://[NDES Server]/certsrv/mscep/mscep.dll https://ca01f35.forest35.fiberlinkqa.local/certsrv/mscep/mscep.dll https://[NDES Server]/certsrv/mscep_admin https://ca01f35.forest35.fiberlinkqa.local/certsrv/mscep_admin	

Table 6: Cloud Extender Connections to Customer's Services

The Cloud Extender makes an outbound connection to the MaaS360 SaaS application. The following table outlines the outbound connection requirements for each instance of MaaS360 Cloud. Every customer will be assigned to a single MaaS360 SaaS application instance.

Network Communication Type	Information	Port
MaaS360 SaaS application	maas-central.maas360.com 208.76.130.120	443
	maas-central-##.maas360.com (where ## is an instance number) 208.76.128.150	443
M1 (portal.fiberlink.com)	services.fiberlink.com 208.76.128.153 208.76.130.181	443
	mpns.maas360.com 208.76.128.168 208.76.131.110	443
	internettest.fiberlink.com 208.76.128.58 208.76.130.58	80
	upload.fiberlink.com: 72.21.0.0/16	443
	dl.maas360.com (no IP range)	-
M2 (m2.maas360.com)	services.m2.maas360.com:443 88.205.104.145 217.112.145.234	443
	mpns.m2.maas360.com:443 88.205.104.154 217.112.145.235	443
	internettest.fiberlink.com:80 208.76.128.58 208.76.130.58	80
	upload.fiberlink.com:443 72.21.0.0/16	443
	dl.m2.maas360.com (no IP range)	-
M3 (m3.maas360.com)	services.m3.maas360.com 208.76.133.30 50.204.34.212	443

Network Communication Type	Information	Port
	mpns.m3.maas360.com 208.76.133.28 50.204.34.211	443
	internettest.fiberlink.com 208.76.128.58 208.76.130.58	80
	upload.fiberlink.com 72.21.0.0/16	443
	dl.m3.maas360.com (no IP range)	-
M4 (m4.maas360.com)	services.m4.maas360.com:443 119.81.110.141 119.81.173.174	443
	mpns.m4.maas360.com:443 119.81.110.140 119.81.173.173	443
	internettest.fiberlink.com:80 208.76.128.58 208.76.130.58	80
	upload.fiberlink.com:443 72.21.0.0/16	443
	dl.m4.maas360.com (no IP range)	-

Table 7: Cloud Extender Connections to MaaS360 SaaS Application

8.3 Identification and Authentication (FIA)

8.3.1 X.509 Certificate Validation (FIA_X509_EXT.1(1)(TOE Platform),FIA_X509_EXT.1(2)(TOE Application), FIA_X509_EXT.2(1)(TOE Platform, FIA_X509_EXT.2(2)(TOE Application))

The TOE conducts certificate validation by performing the following:

- Certificate validation and certificate path validation conforms to RFC 5280.
- The certificate path must terminate with a trusted CA certificate.
- All CA certificates must have the basicConstraints extension present and the CA flag set to TRUE.
- The certificate must not be revoked. This is established by a certificate revocation list (CRL) that is referenced by the TOE.
- The extendedKeyUsage field must be valid based on the following rules:
  - Certificates used for trusted updates and executable code integrity verification must have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS must have the Server Authentication purpose (id-kp with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS must have the Client Authentication purpose (id-kp2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.

    - Server certificates presented for EST must have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.
- The SAN/CN checks follow all other certificate checks (e.g. signature validation, expiry, certificate purpose etc.)
    - If SAN is defined in the configuration file:
        - If the SAN defined in presented certificate exactly matches the SAN defined in the configuration file the certificate is accepted.
        - Otherwise certificate is rejected.
    - If CN is defined and SAN is not present:
        - CN in presented certificate must match CN defined in the configuration file.
        - If there are no CNs listed in the configuration file, the certificate is accepted.

The TOE uses X.509 in support of TLS authentication. The use of certificates is enabled by default. TOE administrators may also specify the path to a certificate revocation list so that revocation status can be checked during authentication. The actual certificates and keys to be used by the TOE can be specified through the use of the Windows Credential Store for the platform provided TLS. The TOE implementation of OpenSSL, OpenSSL for the IBM MaaS360 Cloud Extender, does not support the addition or configuration of additional TLS certificates. While the HTTPS implementation will automatically reject a certificate if it is found to be invalid, a certificate with unknown revocation status (because the TSF is unable to read or obtain the CRL) is rejected. In this case, an error message is generated and logged for TOE administrator.

8.4 Security Management (FMT)

8.4.1 Secure By Default Configuration (FMT_CFG_EXT.1)

The Cloud Extender does not require any credentials for access control to the application. A license key must be obtained from IBM in order to install the application.

Default credentials installed as a result of the Cloud Extender installation include those detailed in Table 8: Default Credentials.

Credential Name
ComodoCA.pem
DigiCert_High_Assurance_EV_Root_CA.pem
entrustsecureserver.pem
GTECyberTrustGlobalRoot.pem
VerisignCAG2.pem
VerisignCAG3.pem
VerisignCAG5.pem
Certificate for accessing the MaaS360 SaaS application

Table 8: Default Credentials.

8.4.2 Supported Configuration Mechanism (FMT_MEC_EXT.1, FMT_SMF.1)

The Cloud Extender is supplied along with the IBM MaaS360 Cloud Extender configuration tool. The configuration data for the Cloud Extender application is stored in the platform’s Windows Registry and may optionally be exported to an encrypted file that is stored in an EFS protected folder on the platform. The following table details settings that pertain to SFR functionality:

Configuration Options	How Configured
TLS 1.2 System default	Manually (see [CC-CFG])
Limit HTTPS to TLS 1.2	Manually (see [CC-CFG])
Configure and enable the EFS Service	Manually (see [CC-CFG])
Use Proxy Authentication	CE configuration tool
Mode	CE configuration tool
Exchange ActiveSync Manager	CE configuration tool
User Authentication	CE configuration tool
User Visibility	CE configuration tool
Certificates Integration	CE configuration tool
Configure Service Account	CE configuration tool
Configure Certificate Templates	CE configuration tool
Configure Cloud Extender Configuration	CE configuration tool

Table 9: Cloud Extender Configuration Options

Additionally, the application relies on platform provided access control mechanisms (user permissions) for securing access to TOE components outside of the EFS such as the installation directory where TOE binaries are located. The configuration of these elements are defined in the [CC-CFG]

No other TOE management functions are applicable to the Cloud Extender.

8.5 Privacy (FPR)

8.5.1 User Consent for Transmission of PII (FPR_ANO_EXT.1)

The application does not contain any functionality that relates to Personally Identifiable Information (PII).

8.6 Protection of the TSF (FPT)

8.6.1 Anti-exploitation Capabilities (FPT_AEX_EXT.1)

The following compiler flags and linker options are used to enable ASLR when the application is compiled.

/DYNAMICBASE (Use address space layout randomization)
This linker option modifies the header of an executable to indicate whether the application should be randomly rebased at load time.

An explanation of the linker option can be found in the Microsoft Developer Network (MSDN) library at:

https://msdn.microsoft.com/en-us/library/bb384887.aspx

All the Dynamic Linked Libraries (DLLs) are compiled with the /DYNAMICBASE linger setting, which enables ASLR.

All compilations are made with the /GS flag set. This is the default option for that compiler flag.

Two Cloud Extender components (luaCrypto and luaPKIExtender) contain support for enabling Federal Information Processing Standard (FIPS) 140-2 conformance via the OpenSSL for the IBM MaaS360 Cloud Extender FIPS Object Module. Please note that this implementation of the OpenSSL FIPS Object Module, OpenSSL for the IBM MaaS360

Cloud Extender, was not submitted for CMVP validation and such status is not being claimed. Both these modules statically link the OpenSSL for the IBM MaaS360 Cloud Extender library. It is a requirement of OpenSSL for the IBM MaaS360 Cloud Extender that the statically linked libraries specify a base address. The actual address is specified in the linker options. There is no specific address required, just that the address chosen is specified during the FIPS link step. IBM uses the following addresses:

- luaCrypto: /BASE:0xFD00000
- luaPKIExtender: /BASE:0x1A000000

Additionally, all executable files are located in the Cloud Extender installation directory while all user-modifiable files are written to a separate location within the EFS volume described in the [CC-CFG].

8.6.2 Use of Supported Services and APIs (FPT_API_EXT.1)

Category	Windows APIs
Microsoft Certificate Store APIs	CertAddCertificateContextToStore
	CertCloseStore
	CertComparePublicKeyInfo
	CertEnumCertificatesInStore
	CertEnumCRLsInStore
	CertFindCertificateInStore
	CertNameToStr
	CertOpenStore
	CertOpenSystemStore
	CertSetCertificateContextProperty
	PFXExportCertStore
RBG	BCryptGenRandom
Hash and Encryption APIs	CryptAcquireContext
	CryptBinaryToString
	CryptCreateHash MD5
	CryptDecryptMessage
	CryptDeriveKey RC4, 128-bit Key used in CryptEncrypt
	CryptDestroyHash
	CryptDestroyKey
	CryptEncrypt
	CryptExportPublicKeyInfo
	CryptGetUserKey
	CryptHashData
	CryptImportKey
	CryptMsgOpenToDecode
	CryptMsgUpdate
	CryptMsgGetParam
	CryptReleaseContext

Table 10: List of Windows APIs Used by the Cloud Extender

The table above lists the TOE Platform APIs which are specific to certain cryptographic and certificate operations. A full listing of all TOE Platform APIs used by the TOE Application is provided in Appendix A of this ST.

The Cloud Extender installation package is signed by IBM using a Symantec certificate issued to IBM. Instructions for viewing the certificate are found in the [CC-CFG].

The Cloud Extender is not subject to updates.

The version of the core installer can be determined via the Control Panel»Program and Features facility in Windows.

The version of the modules can be inspected through the Windows File Manager. Right-click on the emsagent.exe file and select Properties.

The module versions are displayed on one of the final IBM MaaS360 Cloud Extender Configuration Tool screens.

8.6.3 Use of Third Party Libraries (FPT_LIB_EXT.1)

Table 11: 3rd Party Libraries details the use of third party libraries that are employed by the TOE.

Library:	URL:
SQLite, 3.15.0	https://sqlite.org/
OpenSSL, 1.0.2o with OpenSSL FIPS Module, 2.0.13	https://www.openssl.org/
libcURL, 7.58.1	https://curl.haxx.se
Zlib vc, 1.1.4	https://zlibc.linux.lu
Protobuf, 2.6.1	https://code.google.com/p/protobuf/
Boost, 1.5.9	http://www.boost.org
Bitwise Operation library 2008	https://github.com/mcschroeder/lua-5.2.0-special/blob/master/src/lbitlib.c
Lua, 5.1	http://www.lua.org
Lua cURL, 1.6	https://github.com/Lua-cURL/
luasql, 2.1	https://keplerproject.github.io/luasql/
DotNetZip, 1.9.1.8	https://dotnetzip.codeplex.com/
NSIS, 2.46	http://nsis.sourceforge.net/Download
CMarkUp, 11.2	http://www.firstobject.com/
Gloox Library, 1.0.1	https://camaya.net/gloox/
Microsoft Framework, 8.0	https://www.microsoft.com/net/
InstallShield, 2015 + SP1 Professional	https://www.flexerasoftware.com

Table 11: 3rd Party Libraries

8.7 Timely Security Updates (FPT_TUD_EXT.1, ALC_TSU_EXT.1)

8.7.1 Security Update Process for the Cloud Extender

Note that the TOE is not subject to updates. If security updates are identified a new version of the TOE must be installed. Installers for the TOE are signed by IBM in accordance with the Microsoft Authenticode process using a Class 3 SHA256 provided by Symantec. This signature is the only authorized source for the TOE.

The TOE provides capabilities for checking the current version and if updates are available through the IBM MaaS360 Cloud Extender Configuration Tool as documented in the [CC-CFG]. If an update is available, the new installer must be obtained from the customer portal which requires authentication. Automatic updates are not available and the TOE has no capacity to download, modify, or replace its own binary code. Additionally, uninstall procedures provided in the [CC-CFG] will result in the complete removal of the TOE from the TOE platform including all log and configuration data.

8.7.1.1 Reporting security vulnerabilities

A publicly available mechanism for reporting security issues pertaining to the TOE (web site, email address) is available at: https://www-03.ibm.com/security/secure-engineering/report.html

During the analysis of the vulnerability, IBM identifies which part of the TOE or third-party libraries are involved. Any necessary updates to third party components are included and distributed with the updated CE application. Hence no third-party processes need to be considered by users.

Users are notified when updates change security properties or configuration of the product.

IBM request that sensitive information is encrypted and supply a Pretty Good Privacy (PGP) public key for the purpose.

8.7.1.2 IBM's process for handling security vulnerabilities

The IBM Product Security Incident Response Team (PSIRT) process is described at:
https://www.ibm.com/security/secure-engineering/process.html

The process for creating and deploying security updates is as follows.

1. Internal or external testing or a 3rd party report discovers a vulnerability.
2. The IBM X-Force team provides CVSS scoring.
3. Development teams investigate and remediate the issue.
4. A fix is tested and validated in QA and Staging.
5. The fix is deployed via the appropriate distribution channels (SaaS continuous integration / continuous deployment (CI/CD) release window or publishing apps to the relevant app stores).

The length of time in days between public disclosure of a vulnerability and the public availability of the security update for the TOE can vary based on their severity as follows.

Time frames are set by IBM PSIRT based on CVSS scoring as follows:

- **CVSS Effective Score 7-10** - Resolve as soon as possible, not to exceed 90 days, less than 30 days preferred
- **CVSS Effective Score 0-6.9** - Resolve as soon as possible, not to exceed 180 days

The PSIRT team may also flag vulnerabilities to be expedited regardless of CVSS Effective Score of a finding if circumstances warrant a faster resolution.

8.7.1.3 Notification of updates and security related fixes

Customers can use any or all of the following notification mechanisms.

1. The Cloud Extender heartbeats into the MaaS360 platform every 5 minutes. If updates are available there will be an event written to the Windows System Event log. The log can be viewed by an administrator. Additionally, administrators may manually check for updates using the procedure described in the [CC-CFG].
2. All release communication is found on the IBM Developer Release Wiki :
https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/W0dcb4f3d0760_48cd_9026_a90843b9da06/page/2017%20MaaS360%20Release%20Announcements.
Subscribed users will get an email notification when the Wiki is updated.
3. Whenever IBM elevates new code to the portal, the Wiki is updated and customers are notified to review these updates.

Information about how and where security bulletins are published is found at:
https://www-03.ibm.com/security/secure-engineering/bulletins.html

8.8 CAVS Certificates

8.8.1 Mapping of CAVS Certificates to SFRs

The following table lists the CAVS certificates of the TOE Application to the respective security functional requirements:

SFR	Cryptographic function	Algorithm	Modes/Options	CAVS# OpenSSL for the IBM MaaS360 Cloud Extender

FCS_CKM_EXT.1(TOE Application)
FCS_CKM.1(TOE Application)
	Asymmetric Key Generation	RSA
		(FIPS 186-4)
			RSA:
			186-4:
			Key Generation:
			Public Key Exponent: Fixed (10001)
			Probable Primes with Conditions:
			Mod lengths: 2048, 3072 (bits)
			Primality Tests: C.2
			Prerequisite: DRBG #2078
				RSA #2872

		ECDSA (FIPS 186-4)	ECDSA: 186-4: Key Pair Generation: Curves: P-256, P-384 Generation Methods: Testing Candidates Public Key Validation: Curves: P-256, P-384 Prerequisite: DRBG #2078	ECDSA #1416

		DSA
		(FIPS 186-4)
			DSA:
			186-4:
			PQGGen:
			L = 2048, N = 224 SHA: SHA-256, SHA-384
			L = 2048, N = 256 SHA: SHA-256, SHA-384
			L = 3072, N = 256 SHA: SHA-256, SHA-384
			KeyPair:
			L = 2048, N = 224
			L = 2048, N = 256
				DSA #1387

FCS_CKM.2(TOE Application)	Key establishment	RSA (SP 800-56B)	(SP 800-56B)	Vendor Affirmed. See FIPS 140-2 I.G. D.4: Vendor Affirmation.

SFR	Cryptographic function	Algorithm	Modes/Options	CAVS# OpenSSL for the IBM MaaS360 Cloud Extender
		800-56A KDF (KAS)	KAS ECC: Functions: Partial Public Key Validation Schemes: Ephemeral Unified: Key Agreement Roles: Initiator, Responder Parameter Sets: EC: Curve: P-256 SHA: SHA-256 ED: Curve: P-384 SHA: SHA-384 Prerequisite: SHS #4311, ECDSA #1416, DRBG #2078 KAS FFC: Functions: Partial Public Key Validation Schemes: dhEphem: Key Agreement Roles: Initiator, Responder Parameter Sets: FC: SHA: SHA-256 Prerequisite: DSA #1387, DRBG #2078	CVL #1836
		AES-CBC 128, 256 AES-GCM 128, 256 (FIPS 197, SP 800-38A, SP 800-38D)	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128, 256 (bits) AES-GCM: Modes: Decrypt, Encrypt IV Generation: Internal (using Section 8.2.1) Key Lengths: 128, 256 (bits) Tag Lengths: 32, 64, 96, 104, 112, 120, 128 (bits) Plain Text Lengths: 128, 136, 256, 264 (bits) AAD Lengths: 0, 128, 136, 256, 264 (bits) 96 bit IV supported	AES #5369
		SHA-1 SHA-256 SHA-384 (FIPS 180-4)	SHA-1: SHA-256: SHA-384:	SHS #4311

SFR	Cryptographic function	Algorithm	Modes/Options	CAVS# OpenSSL for the IBM MaaS360 Cloud Extender
FCS_COP.1(1)(TOE Application)	Encryption/ Decryption	AES-CBC 128, 256 AES-GCM 128, 256 (FIPS 197, SP 800-38A, SP 800-38D)	AES-CBC: Modes: Decrypt, Encrypt Key Lengths: 128, 256 (bits) AES-GCM: Modes: Decrypt, Encrypt IV Generation: Internal (using Section 8.2.1) Key Lengths: 128, 256 (bits) Tag Lengths: 32, 64, 96, 104, 112, 120, 128 (bits) Plain Text Lengths: 128, 136, 256, 264 (bits) AAD Lengths: 0, 128, 136, 256, 264 (bits) 96 bit IV supported	AES #5369
FCS_COP.1(2)(TOE Application)	Hashing	SHA-1 SHA-256 SHA-386 (FIPS 180-4)	SHA-1: SHA-256: SHA-384:	SHS #4311
FCS_COP.1.1(3)(TOE Application)	Signing	RSA (FIPS 186-4)	RSA: 186-4: Signature Generation PKCS1.5: Mod 2048 SHA: SHA-1, SHA-256, SHA-384 Mod 3072 SHA: SHA-1, SHA-256, SHA-384 Signature Verification PKCS1.5: Mod 2048 SHA: SHA-1, SHA-256, SHA-384 Mod 3072 SHA: SHA-1, SHA-256, SHA-384 Prerequisite: SHS #4311	RSA #2872
		ECDSA P-256, P-384 (FIPS 186-4)	ECDSA: 186-4: Signature Generation: P-256 SHA: SHA-1, SHA-256, SHA-384 P-384 SHA: SHA-1, SHA-256, SHA-384 Signature Verification: P-256 SHA: SHA-1, SHA-256, SHA-384 P-384 SHA: SHA-1, SHA-256, SHA-384 Prerequisite: SHS #4311	ECDSA #1416

SFR	Cryptographic function	Algorithm	Modes/Options	CAVS# OpenSSL for the IBM MaaS360 Cloud Extender
FCS_COP.1(4)(TOE Application)	Keyed-Hash Message Authentication	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 (FIPS 198-1)	HMAC-SHA-1: Key Sizes < Block Size Prerequisite: SHS #4311 HMAC-SHA2-256: Key Sizes < Block Size Prerequisite: SHS #4311 HMAC-SHA2-384: Key Sizes < Block Size Prerequisite: SHS #4311	HMAC #3557
		SHA-1 SHA-256 SHA-384 (FIPS 180-4)	SHA-1: SHA-256: SHA-384:	SHS #4311

FCS_RBG_EXT.1(2)(TOE Application)
FCS_RBG_EXT.2(TOE Application)
	Random Bit Generation	CTR_DRBG (AES)
		(SP 800-90A)
			Counter:
			Modes: AES-128, AES-256
			Derivation Function States: Derivation Function not used, Derivation Function used
			Prediction Resistance Modes: Enabled, Not Enabled
			Prerequisite: AES #5369
				DRBG #2078

Table 12: SFR to CAVS Cert Number (Application)

Per NIAP's interim guidance on the evaluation of Platform-Dependent Products the following table lists the CAVS certificates for the platform dependent CAVS certificates. For more information please see Table 10 in the ST for the platform.

SFR	Algorithm	CAVS#
Note: The following certificate is related to the RBG used in support of OpenSSL for the IBM MaaS360 Cloud Extender (within the TOE boundary).		
FCS_RBG_EXT.1(1)(TOE Platform) Random Bit Generation Services	CTR_DRBG (AES) NIST SP 800-90A	DRBG #489
	Prerequisite: AES	AES #2832
Note: The following certs are related to protocol SFRs claimed by the ST but which use platform provided services (Outside the TOE boundary).		
FCS_CKM.1.1(TOE Platform) FCS_TLSC_EXT.1(1)(TOE Platform) TLS Client Protocol FCS_TLSC_EXT.4(1)(TOE Platform) TLS Client Protocol FIA_X509_EXT.1(1)(TOE Platform) X.509 Certificate Validation FIA_X509_EXT.2(1)(TOE Platform) X.509 Certificate Authentication FTP_DIT_EXT.1(1)(TOE Platform) Protection of Data in Transit	FIPS 197 AES NIST, For CBC, CCM, and GCM modes	AES #2848, #2832, #2853, #3903
	FIPS 186-4 DSA	DSA #855
	FIPS 186-4 RSA	RSA #1487, #1493, #1494, #1519
	FIPS 186-4 ECDSA	ECDSA #505
	FIPS 180-4 SHA-1, SHA-256, SHA-384, and SHA-512	SHS #2373, #2396
	NIST SP 800-56A EC DH NIST SP 800-56B RSA	KAS #47 Tested by the CCRA Laboratory that performed the platform evaluation
	FIPS 198-1 HMAC	HMAC #1773
	NIST SP 800-90A CTR_DRBG(AES)	DRBG #489
	SP 800-108 KDF	KDF #30
	SP 800-135 KDF	CVL #323

Table 13: SFR to CAVS Cert Number (Platform)

8.9 Mapping of SFRs to the Security Functional Requirements

The following table provides a mapping of the SFRs defined in chapter 6 of this [ST] to the functions implemented by the TOE, referring to the previous sections of this TSS where additional information is required.

SFR	TSS Section	Cryptographic protection	User Data Protection	Security Management	Privacy Protection	TSF Protection	Trusted Channel
FCS_CKM_EXT.1(TOE Application)	8.1.1	X					
FCS_CKM.1(TOE Application)	8.1.1	X					
FCS_CKM.1(TOE Platform)	8.1.1	X					
FCS_CKM.2 (TOE Application)	8.1.2	X					
FCS_COP.1(1)(TOE Application)	8.1.3	X					
FCS_COP.1(2)(TOE Application)	8.1.4	X					
FCS_COP.1(3)(TOE Application)	8.1.5	X					

SFR	TSS Section	Cryptographic protection	User Data Protection	Security Management	Privacy Protection	TSF Protection	Trusted Channel
FCS_COP.1(4)(TOE Application)	8.1.6	X					

FCS_HTTPS_EXT.1(1)(TOE Platform)
FCS_HTTPS_EXT.1(2)(TOE Application)
	8.1.9	X					

FCS_RBG_EXT.1(1)(TOE Platform)
FCS_RBG_EXT.1(2)(TOE Application)
	8.1.7	X					

FCS_RBG_EXT.2(TOE Application)	8.1.7	X					
FCS_STO_EXT.1(TOE Platform)	8.1.8	X					

FCS_TLSC_EXT.1(1)(TOE Platform)
FCS_TLSC_EXT.1(2)(TOE Application)
	8.1.9,
	8.1.10
		X					

FCS_TLSC_EXT.4(1)(TOE Platform)
FCS_TLSC_EXT.4(2)(TOE Application)
	8.1.9,
	8.1.10
		X					

FDP_DEC_EXT.1	8.2.2		X				
FDP_NET_EXT.1	8.2.3		X				
FDP_DAR_EXT.1	8.2.1		X				

FIA_X509_EXT.1(1)(TOE Platform)
FIA_X509_EXT.1(2)(TOE Application)
	8.3.1		X				

FIA_X509_EXT.2(1)(TOE Platform)
FIA_X509_EXT.2(2)(TOE Application)
	8.3.1		X				

FMT_CFG_EXT.1	8.4.1			X			
FMT_MEC_EXT.1	8.4.2			X			
FMT_SMF.1	8.4.2			X			
FPR_ANO_EXT.1	8.5.1				X		
FPT_API_EXT.1.1	8.6.2					X	
FPT_AEX_EXT.1	8.6.1					X	
FPT_TUD_EXT.1	8.7					X	
FPT_LIB_EXT.1	8.6.3					X	
FTP_DIT_EXT.1(1)(TOE Platform)	8.1.9						X
FTP_DIT_EXT.1(2)(TOE Application)	8.1.10						X

Table 14: Mapping of SFRs to TSS and Security Functionality

9 Abbreviations and Acronyms

Abbreviation	Term
AES	Advanced Encryption System
API	Application Program Interface
ASLR	Address Space Layout Randomization
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CAVS	Cryptographic Algorithm Validation System
CBC	Cypher Block Chaining
CC	Common Criteria
CE	Cloud Extender
CCM	Counter with CBC-MAC
CI/CD	Continuous Integration / Continuous Deployment
CNG	Cryptography API: Next Generation
CRL	Certificate Revocation List
cURL	Client for URLs
CVL	Component Validation List
CVSS	Common Vulnerability Scoring System
DLL	Dynamic Link Library
DMZ	De-militarized Zone
DN	Distinguished Name
DPAPI	Data Protection Application Programming Interface
DRBG	Deterministic Random Bit Generator
EAR	Entropy Analysis Report
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EFS	Encrypted File System
EMM	Enterprise Mobility Management
EMS	Endpoint Management System
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
HMAC	Keyed-hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol over TLS
IBM	International Business Machines
LDAP	Lightweight Directory Access Protocol
LDAPS	Secure LDAP
MSDN	Microsoft Developers Network
NDES	Network Device Enrollment Service
NIAP	National Information Assurance Partnership
OSP	Organizational Security Policies
PCL	Product Compliant List
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PP	Protection Profile
PSIRT	Product Security Incident Response Team
RBG	Random Bit Generator
RSA	Rivest-Shamir-Adleman
SaaS	Software as a Service
SAN	Subject Alternative Name
SCEP	Simple Certificate Enrollment Protocol
SN	Subject Name
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
SWID	Software ID
TLS	Transport Layer Security

Abbreviation	Term
TSF	**TOE Security Function**
TSFI	**TOE Security Function Interfaces**
TSS	**TOE Security Summary**
VPN	**Virtual Private Network**
XMPP	**Extensible Messaging and Presence Protocol**