Micro Focus Data Protector Premium Edition, 2020.05 (A.10.70) Security Target

Version 1.0
6 May 2020

Prepared for:

Micro Focus LLC
4555 Great America Parkway
Santa Clara, CA 95054

Prepared by:

Accredited Testing and Evaluation Labs
6841 Benjamin Franklin Drive
Columbia, MD 21046

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

This section introduces the Target of Evaluation (TOE) and describes its general functionality, and provides the Security Target (ST) and TOE identification, ST and TOE conformance claims, ST conventions, glossary and list of abbreviations.

The TOE is Micro Focus Data Protector Premium Edition, release 2020.05, software version A.10.70. (Data Protector). Data Protector is an enterprise-level software application providing backup and restore functionality.

Although Micro Focus provides both an Express and a Premium edition of the product, only the Premium edition is considered to be the TOE—the Express edition was not evaluated and no security claims are made for it.

The Security Target contains the following additional sections:

- TOE Description (Section 2)—provides an overview of the TOE and describes the physical and logical boundaries of the TOE
- Security Problem Definition (Section 3)—describes the threats and assumptions that define the security problem to be addressed by the TOE and its environment
- Security Objectives (Section 4)—describes the security objectives for the TOE and its operational environment necessary to counter the threats and satisfy the assumptions that define the security problem
- IT Security Requirements (Section 5)—specifies the security functional requirements (SFRs) and security assurance requirements (SARs) to be met by the TOE
- TOE Summary Specification (Section 6)—describes the security functions of the TOE and how they satisfy the SFRs
- Protection Profile Claims (Section 7)—provides rationale supporting the claims of conformance of this ST and the TOE to *Protection Profile for Application Software*, Version 1.3, 1 March 2019
- Rationale (Section 8)—provides mappings and rationale for the security problem definition, security objectives, security requirements, and security functions to justify their completeness, consistency, and suitability.

1.1 Security Target, TOE and CC Identification

ST Title – Micro Focus Data Protector Premium Edition, 2020.05 (A.10.70) Security Target

ST Version – Version 1.0

ST Date – 6 May 2020

TOE Identification – Data Protector Premium Edition, release 2020.05, software version A.10.70

TOE Developer – Micro Focus

Evaluation Sponsor – Micro Focus

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([PPAS])

  The following NIAP Technical Decisions issued against this PP are relevant to the TOE and have been applied in the course of the evaluation:

  - TD0416: Correction to FCS_RBG_EXT.1 Test Activity

- TD0427: Reliable Time Source
- TD0434: Windows Desktop Applications Test
- TD0437: Supported Configuration Mechanism
- TD0444: IPsec Selections
- TD0445: User Modifiable File Definition
- TD0465: Configuration Storage for .NET Apps
- TD0486: Removal of PP-Module for VPN Clients from allowed with list
- TD0495: FIA_X509_EXT.1.2 Test Clarification
- TD0498: Application Software PP Security Objectives and Requirements Rationale
- TD0505: Clarification of revocation testing under RFC6066

The following NIAP Technical Decisions issued against this PP are not relevant to the TOE:

- TD0435: Alternative to SELinux for FPT_AEX_EXT.1.3—not relevant because the TOE platform is Windows, not Linux
- TD0473: Support for Client or Server TOEs in FCS_HTTPS_EXT—not relevant because the ST does not include HTTPS SFRs.
- TD0510: Obtaining random bytes for iOS/macOS—not relevant because the platform is Windows, not iOS or MacOS.

- *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([FPTLS])

  The following NIAP Technical Decision issued against this Functional Package is relevant to the TOE and has been applied in the course of the evaluation:

  - TD0442: Updated TLS Ciphersuites for TLS Package
  - TD0469: Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1
  - TD0499: Testing with pinned certificates

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017
  - Part 2 Extended.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017
  - Part 3 Extended.

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example, FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).

- Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
- Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.4 Glossary

This ST uses a number of terms that have a specific meaning within the context of the ST and the TOE. This glossary provides a list of those terms and how they are to be understood within this ST.

cell	The Data Protector cell is the basic management unit in a deployment of Data Protector. It is a network environment consisting of a Cell Manager system, one or more Installation servers, client systems, and devices. The Cell Manager and Installation Server can be on the same system (which is the default option) or on separate systems.
Cell Manager	The main system that controls the Data Protector cell from a central point. The Cell Manager runs Session Managers that control backup and restore sessions.
Installation Server	The Installation Server is the computer where the Data Protector software repository is stored.

1.5 Abbreviations and Acronyms

AES	Advanced Encryption Standard
API	Application Programming Interface
ASLR	Address Space Layout Randomization
CLI	Command Line Interface
DA	Disk Agent
DEP	Data Execution Prevention
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDB	Internal Database
ISO	International Organization for Standardization
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
MA	Media Agent
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology

OCSP	Online Certificate Status Protocol
OID	Object Identifier
OS	Operating System
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PP	Protection Profile
RFC	Request for Comment
SAN	Subject Alternative Name
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
UI	User Interface
URL	Uniform Resource Locator

2. TOE Description

2.1 TOE Overview

The TOE is Micro Focus Data Protector Premium Edition, release 2020.05, software version A.10.70. Data Protector provides backup and restore functionality tailored for enterprise-wide and distributed environments. Data Protector is an enterprise-level software application for Windows. It includes cryptographic modules providing NIST-validated implementations of cryptographic functionality to support secure storage of credentials and secure communications with external IT entities. Data Protector restricts network connections to those required for it to perform its intended functions. Data Protector supports the use of X.509 certificates for authentication of TLS connections. Data Protector is implemented to utilize anti-exploitation capabilities provided by its execution environment. The application installation package and application updates are digitally signed by an authorized source.

2.2 TOE Architecture

Data Protector can be used in environments ranging from a single system to thousands of systems on several sites. An installation of Data Protector is termed a "cell". Within the Data Protector cell, multiple instances of Data Protector can be installed to provide backup and restore functionality to the platforms that require it, as well as to provide access to backup media.

Depending on the deployment, an instance of Data Protector performs one or more of the following roles:

- Cell Manager—supports central management of the cell and includes the following components:
    - User Interface—provides the Data Protector GUI and part of the CLI
    - Data Protector Internal Database (IDB)
    - Installation Server—a Data Protector cell needs at least one Installation Server to support remote installations through the network and distribute Data Protector instances to the systems in the cell.

  Cell Manager runs core Data Protector software and Session Managers that start and stop backup and restore sessions and write session information to the IDB. The IDB keeps track of the backed up files as well as of the configuration of the Data Protector cell. Once the Cell Manager is installed, additional Data Protector instances can be installed on other systems in the cell.
- Disk Agent—a Data Protector instance installed on systems to be backed up (and restored if necessary). During backup, the Disk Agent reads data from a disk on the system and sends it to a Media Agent instance. During restore, the process is reversed—the Disk Agent receives data from a Media Agent and writes it to a disk on the system.
- Media Agent—a Data Protector instance installed on systems connected to backup media. During backup, the Media Agent receives data from a Disk Agent and stores it on backup media connected to the system. During restore, the process is reversed—the Media Agent retrieves data from backup media connected to the client system and sends it to a Disk Agent.

The following figure provides an overview of Data Protector in its operational environment. It shows three instances of Data Protector—one operating as the Cell Manager, one operating in the Disk Agent role, and one operating in the Media Agent role. It also shows the User Interface component installed on the Cell Manager instance, accessed via a locally connected console.

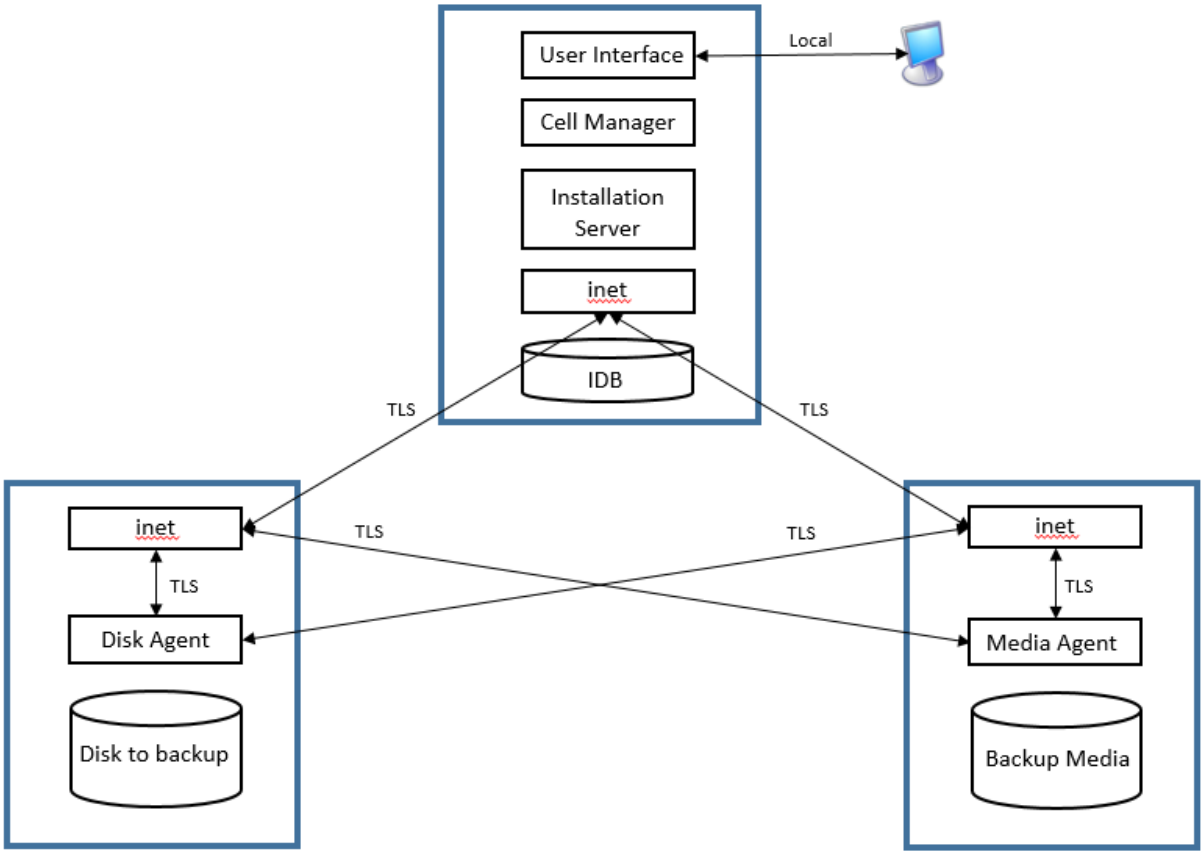

Figure 1 Example TOE Deployment

Data Protector runs several Windows services that enable it to run backup and restore sessions. It provides the necessary communication paths, activates backup and restore sessions, starts Disk Agents and Media Agents, and stores information about what was backed up. The following are the primary services involved in Data Protector operations:

- Cell Request Server (CRS)—runs on the Cell Manager. It starts and controls backup and restore sessions. The service is started when Data Protector is installed on the Cell Manager system and is restarted each time the system is restarted.
- Backup Session Manager (BSM)—runs on the Cell Manager and controls the backup session. This process reads the backup specification for information on what to back up, and which options, media, and devices to use for the backup.
- Restore Session Manager (RSM)—runs on the Cell Manager and controls the restore session.
- Media Management Daemon (MMD)—runs on the Cell Manager. It is started by the CRS and controls media management and device operations.
- Inet—runs on each Windows system in the Data Protector cell. It is responsible for communication between systems in the cell and starts other processes needed for backups and restores. The Data Protector Inet service is started when Data Protector is installed on a system.
- Key Management Server (KMS)—runs on the Cell Manager and provides key management for the Data Protector encryption functionality. The service is started when Data Protector is installed on the Cell Manager.

- Internal Database Service (**hpdp-idb**)—the service under which the IDB runs. It is accessed locally on the Cell Manager by processes that need information from the IDB. This service is accessed remotely only for media management information about transfer from the IDB on the Cell Manager to the IDB on the Manager-of-Manager (not in the evaluated configuration).
- Internal Database Connection Pool (**hpdp-idb-cp**)—offers a pool of open connections to the **hpdb-idb** that can be used on request, instead of opening a new connection for every request, thus ensuring **hpdp-idb** connection scalability. The service runs on the Cell Manager and is accessed only by local processes.

The Cell Manager also includes its own web server (Application Server) which allows for a remote instance of the User Interface to connect to the IDB through a HTTPS connection. However, remote User Interface connections are not supported in the evaluated configuration, so the Application Server has no role to play in the evaluated configuration.

2.2.1 Physical Boundaries

The TOE comprises the Data Protector software described in Section 2.2 above, installed in a non-clustered environment. A Data Protector instance configured to provide the Cell Manager, Installation Server, and User Interface is installed on one server, Data Protector instances configured to provide the Disk Agent are installed on systems that are to be backed up, and Data Protector instances configured to provide the Media Agent are installed on systems connected to backup media.

The TOE in its evaluated configuration has the following system requirements for its host platforms:

- Data Protector as Cell Manager (including Installation Server and User Interface):
  - Windows Server 2016 (64 bit) (x64)
  - Minimum hardware: 16 GB RAM; 5 GB of free disk space + approximately 100 bytes for each backed up file (for use by the IDB)
- Data Protector as Disk Agent:
  - Windows Server 2016 (64 bit) (x64)
  - Minimum hardware: 64 MB RAM (128 MB recommended); 20 MB of disk space
- Data Protector as Media Agent:
  - Windows Server 2016 (64 bit) (x64)
  - Minimum hardware: 64 MB RAM (128 MB recommended); 20 MB of disk space.

Note, Windows Server 2016 can be running directly on a hardware platform or can be deployed in a VMware ESXi virtual environment. Evaluation testing of the TOE took place on Windows Server 2016 Standard deployed on VMware ESXi 6.5, running on an Intel Xeon Gold 6140 processor (Skylake microarchitecture).

The following network port must be open for the TOE to function:

- 5565 – port required for new installation in Data Protector.

The TOE supports a FIPS-mode of operation, which must be enabled in the evaluated configuration.

2.2.2 Logical Boundaries

This section summarizes the security functions provided by Data Protector:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels.

2.2.2.1 Cryptographic Support

Data Protector incorporates OpenSSL to provide its cryptographic functionality.

Data Protector provides cryptographic mechanisms for symmetric encryption and decryption, cryptographic signature services, cryptographic hashing services, keyed-hash message authentication services, deterministic random bit generation seeded from a suitable entropy source, key establishment, and secure credential storage. The cryptographic mechanisms support TLS used for secure communication, both as client and server.

2.2.2.2 User Data Protection

Data Protector leverages the BitLocker functionality of its Windows platform to protect backed-up data written to disk on a Media Agent instance.

Data Protector does not access sensitive information repositories as defined and intended by [PPAS].

Data Protector restricts network communications to application-initiated network communication for scheduled backup and restore operations.

2.2.2.3 Identification and Authentication

The TOE supports the use of X.509 certificates for authentication of TLS connections.

The TOE will not accept a certificate if it is unable to determine the revocation status of the certificate.

2.2.2.4 Security Management

Data Protector does not create credentials by default. The user logged into the underlying Windows system with admin privileges performs the installation and the TOE subsequently ensures only that user is able to run the TOE.

2.2.2.5 Privacy

Data Protector does not collect Personally Identifiable Information (PII) from administrators or users.

2.2.2.6 Protection of the TSF

Data Protector uses only documented platform APIs.

Data Protector does not perform memory mapping to explicit addresses.

Data Protector does not make any memory mapping requests with both write and execute permissions.

Data Protector runs successfully with process exploit mitigations enabled on the underlying Windows Server platform

Data Protector documentation describes the procedure for users to check for the availability of updates. Data Protector is packaged in the standard Windows Installer (.MSI) format and signed by a code-signing certificate.

Data Protector provides the ability to query the current version of the application software.

2.2.2.7 Trusted Path/Channels

All data transmitted by Data Protector is assumed to be sensitive data.

A Data Protector instance uses TLS to protect all data it transmits to other Data Protector instances.

2.3 Unevaluated and Excluded Functionality

The backup and restore functions provided by Data Protector Premium Edition, release 2020.05, software version A.10.70 are not covered by any security functional requirements and so were not addressed by the evaluation. The evaluation covered the ability of the TOE to protect data transmitted between separate TOE instances using TLS, but did not cover the actual backup and restore functions of the TOE.

The following capabilities of the product are excluded in the evaluated configuration:

- Remote administration—in the evaluated configuration, the User Interface component must be installed only on the same platform as the TOE instance in the Cell Manager role, thus providing local administration for

the Cell Manager. The User Interface is not to be installed on other platforms in the network (e.g., administrator workstations) and remote administration is not supported.

- Remote authentication—the product supports remote authentication using LDAP, but this capability was not tested, nor was the ability of the product to protect communications with the external LDAP server using TLS.
- REST API—the product provides a REST API to access management functionality, but this interface is excluded from use in the evaluated configuration.

2.4 TOE Documentation

Micro Focus provides the following guidance documentation necessary to install, configure, and operate the TOE in its evaluated configuration:

- Data Protector, Version: 2020.05.

  Note: The guidance documentation is also available in an online format at: https://docs.microfocus.com/itom/Data_Protector:2020.05/Home. A PDF of the entire online documentation is also available for download by clicking on the "Export to PDF" option in the right top quadrant of the web page and selecting "All the pages" in the dropdown.

3. Security Problem Definition

The Security Problem Definition (composed of threat statements and assumptions) has been drawn verbatim from the *Protection Profile for Application Software*, Version 1.3, 1 March 2019. This PP offers additional information about the identified threats, but that has not been reproduced here and the PP should be consulted if there is interest in that material.

In general, the PP has presented a Security Problem Definition appropriate for application software, and as such is applicable to the Data Protection TOE.

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 with a reliable time clock 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 in compliance with the applied enterprise security policy.

4. Security Objectives

As with the Security Problem Definition, the Security Objectives have been drawn verbatim from [PPAS]. The PP offers additional information about the identified security objectives, but that has not been reproduced here and the PP should be consulted if there is interest in that material.

In general, the PP has presented a Security Objectives statement appropriate for application software, and as such is applicable to the Data Protector TOE.

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. 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.
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.
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.
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.
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.

4.2 Security Objectives for 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. IT Security Requirements

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

The SFRs have all been drawn from the *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([PPAS]) and from *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([FPTLS]). As a result, refinements and operations already performed in that PP are not identified here, rather the requirements have been copied from the PP and any residual operations have been completed herein. Of particular note, the PP makes a number of refinements and completes some of the SFR operations defined in the CC, and the PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in [PPAS].

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from [PPAS] or from [FPTLS]. These documents define the following extended SFRs and since they are not redefined in this ST, they should be consulted for more information in regard to these CC extensions.

- FCS_RBG_EXT.1: Random Bit Generation Services
- FCS_RBG_EXT.2: Random Bit Generation from Application
- FCS_CKM_EXT.1:Cryptographic Key Generation Services
- FCS_STO_EXT.1: Storage of Credentials
- FCS_TLS_EXT.1: TLS Protocol
- FCS_TLSC_EXT.1: TLS Client Protocol
- FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
- FCS_TLSC_EXT.5: TLS Client Support for Supported Groups Extension
- FCS_TLSS_EXT.1: TLS Server Protocol
- FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication
- FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
- FDP_NET_EXT.1: Network Communications
- FDP_DEC_EXT.1: Access to Platform Resources
- FIA_X509_EXT.1: X.509 Certificate Validation
- FIA_X509_EXT.2: X.509 Certificate Authentication
- FMT_MEC_EXT.1: Supported Configuration Mechanism
- FMT_CFG_EXT.1: Secure by Default Configuration
- FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information
- FPT_API_EXT.1: Use of Supported Services and APIs
- FPT_AEX_EXT.1: Anti-Exploitation Capabilities
- FPT_TUD_EXT.1: Integrity for Installation and Update
- FPT_TUD_EXT.2: Integrity for Installation and Update
- FPT_LIB_EXT.1: Use of Third Party Libraries
- FPT_IDV_EXT.1: Software Identification and Versions

- FTP_DIT_EXT.1: Protection of Data in Transit.

In addition, [PPAS] defines the following extended SAR:

- ALC_TSU_EXT.1: Timely Security Updates.

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the TOE.

Requirement Class	Requirement Component
FCS: Cryptographic support	FCS_CKM.1(1): Cryptographic Asymmetric Key Generation
	FCS_CKM_EXT.1: Cryptographic Key Generation Services
	FCS_CKM.2: Cryptographic Key Establishment
	FCS_COP.1(1): Cryptographic Operation Encryption/Decryption
	FCS_COP.1(2): Cryptographic Operation Hashing
	FCS_COP.1(3): Cryptographic Operation Signing
	FCS_COP.1(4): Cryptographic Operation - Keyed-Hash Message Authentication
	FCS_RBG_EXT.1: Random Bit Generation Services
	FCS_RBG_EXT.2: Random Bit Generation from Application
	FCS_STO_EXT.1: Storage of Credentials
	FCS_TLS_EXT.1: TLS Protocol
	FCS_TLSC_EXT.1: TLS Client Protocol
	FCS_TLSC_EXT.2: TLS Client Support for Mutual Authentication
	FCS_TLSC_EXT.5: TLS Client Support for Supported Groups Extension
	FCS_TLSS_EXT.1: TLS Server Protocol
	FCS_TLSS_EXT.2: TLS Server Support for Mutual Authentication
FDP: User Data Protection	FDP_DEC_EXT.1: Access to Platform Resources
	FDP_DAR_EXT.1: Encryption Of Sensitive Application Data
	FDP_NET_EXT.1: Network Communications
FIA: Identification and authentication	FIA_X509_EXT.1: X.509 Certificate Validation
	FIA_X509_EXT.2: X.509 Certificate Authentication
FMT: Security management	FMT_MEC_EXT.1: Supported Configuration Mechanism
	FMT_CFG_EXT.1: Secure by Default Configuration
	FMT_SMF.1 Specification of Management Functions
FPR: Privacy	FPR_ANO_EXT.1: User Consent for Transmission of Personally Identifiable Information
FPT: Protection of the TSF	FPT_API_EXT.1: Use of Supported Services and APIs
	FPT_AEX_EXT.1: Anti-Exploitation Capabilities
	FPT_IDV_EXT.1: Software Identification and Versions
	FPT_LIB_EXT.1: Use of Third Party Libraries
	FPT_TUD_EXT.1: Integrity for Installation and Update

Requirement Class	Requirement Component
	FPT_TUD_EXT.2: Integrity for Installation and Update
FTP: Trusted path/channels	FTP_DIT_EXT.1: Protection of Data in Transit

Table 1 TOE Security Functional Components

5.2.1 Cryptographic Support (FCS)

FCS_RBG_EXT.1 – Random Bit Generation Services

FCS_RBG_EXT.1.1 The application shall [
- ***implement DRBG functionality***

] for its cryptographic operations.

FCS_RBG_EXT.2 – 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 [
- ***256 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_CKM_EXT.1 – Cryptographic Key Generation Services

FCS_CKM_EXT.1.1 The application shall [
- ***implement asymmetric key generation***

].

FCS_CKM.1(1) – Cryptographic Asymmetric Key Generation

FCS_CKM.1.1(1) 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, P-384 and [P-521] 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 – 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: [
- ***[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) – 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***
- ***AES-GCM (as defined in NIST SP 800-38D) mode***

] and cryptographic key sizes [***128-bit, 256-bit***].

FCS_COP.1(2) – Cryptographic Operation Hashing

FCS_COP.1.1(2) The application shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm [

- ***SHA-256***
- ***SHA-384***

] and message digest sizes [

- ***256***
- ***384***

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

FCS_COP.1(3) – 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***

].

FCS_COP.1(4) – 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-384***

] with key sizes [**512 bits for SHA-256, 1024 bits for SHA-384**] and message digest sizes 256 and [***384***] bits that meet the following: FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard.

FCS_STO_EXT.1 – Storage of Credentials

FCS_STO_EXT.1.1 The application shall [

- ***invoke the functionality provided by the platform to securely store [RSA private keys, Data Protector user password encryption key]***
- ***implement functionality to securely store [Data Protector user passwords] according to [FCS_COP.1(1)]***

] to nonvolatile memory.

FCS_TLS_EXT.1 – TLS Protocol

FCS_TLS_EXT.1.1 The product shall implement [

- ***TLS as a client***
- ***TLS as a server***

].

FCS_TLSC_EXT.1 – TLS Client Protocol

Note, this SFR has been modified in accordance with TD0442.

FCS_TLSC_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a client that supports the cipher suites: [

- ***TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246***
- ***TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246***
- ***TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288***
- ***TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288***
- ***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***

] and also supports functionality for [

- ***mutual authentication***

].

FCS_TLSC_EXT.1.2 The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The product shall not establish a trusted channel if the server certificate is invalid [

- ***with no exceptions***

].

FCS_TLSC_EXT.2 – TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 The product shall support mutual authentication using X.509v3 certificates.

FCS_TLSC_EXT.5 – TLS Client Support for Supported Groups Extension

FCS_TLSC_EXT.5.1 The product shall present the Supported Groups Extension in the Client Hello with the supported groups [

- ***secp256r1,***
- ***secp384r1,***
- ***secp521r1***

].

FCS_TLSS_EXT.1 – TLS Server Protocol

Note, this SFR has been modified in accordance with TD0442.

FCS_TLSS_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [***no earlier TLS versions***] as a server that supports the cipher suites: [

- ***TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246***
- ***TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246***
- ***TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288***
- ***TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288***
- ***TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289***
- ***TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289***

] and no other cipher suites, and also supports functionality for [

- ***mutual authentication***

].

FCS_TLSS_EXT.1.2 The product shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0 and [***TLS 1.1***].

FCS_TLSS_EXT.1.3 The product shall perform key establishment for TLS using [

- ***Diffie-Hellman parameters with size [2048 bits]***
- ***ECDHE parameters using elliptic curves [secp256r1, secp384r1, secp521r1] and no other curves***

].

FCS_TLSS_EXT.2 – TLS Server Support for Mutual Authentication

FCS_TLSS_EXT.2.1 The product shall support authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.2 The product shall not establish a trusted channel if the client certificate is invalid.

FCS_TLSS_EXT.2.3 The product shall not establish a trusted channel if the Distinguished Name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match one of the expected identifiers for the client.

5.2.2 User Data Protection (FDP)

FDP_DAR_EXT.1 – Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1 The application shall [

- ***leverage platform-provided functionality to encrypt sensitive data***
- ***protect sensitive data in accordance with FCS_STO_EXT.1***

] in non-volatile memory.

FDP_DEC_EXT.1 – Access to Platform Resources

FDP_DEC_EXT.1.1 The application shall restrict its access to [

- ***network connectivity***

].

FDP_DEC_EXT.1.2 The application shall restrict its access to [

- ***no sensitive information repositories***

].

FDP_NET_EXT.1 – Network Communications

FDP_NET_EXT.1.1 The application shall restrict network communication to [

- ***[scheduled backup and restore operations]***

].

5.2.3 Identification and Authentication (FIA)

FIA_X509_EXT.1 – X.509 Certificate Validation

Note, this SFR has been modified in accordance with TD0505.

FIA_X509_EXT.1.1 The application shall [***implement functionality***] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The application shall validate the revocation status of the certificate using [***the Online Certificate Status Protocol (OCSP) as specified in RFC 2560***].
- 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.

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 – 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 [***allow the administrator to choose whether to accept the certificate in these cases***].

5.2.4 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 the application binaries and data files from modification by normal unprivileged users.

FMT_MEC_EXT.1 – Supported Configuration Mechanism

Note, this SFR has been modified in accordance with TD0437.

FMT_MEC_EXT.1.1 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 The TSF shall be capable of performing the following management functions [***/***

- ***Configure TLS cipher suites***
- ***Generate certificate signing requests***
- ***Manage X.509 certificates]***

].

5.2.5 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***

].

5.2.6 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 [**no exceptions**].
FPT_AEX_EXT.1.2	The application shall [• ***not allocate any memory region with both write and execute permissions***].
FPT_AEX_EXT.1.3	The application shall be compatible with security features provided by the platform vendor.
FPT_AEX_EXT.1.4	The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.
FPT_AEX_EXT.1.5	The application shall be built 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 [***provide the ability***] to query the current version of the application software.
FPT_TUD_EXT.1.3	The application shall not download, modify, replace or update its own binary code.
FPT_TUD_EXT.1.4	The application installation package and its updates shall be digitally signed such that its platform can cryptographically verify them prior to installation.
FPT_TUD_EXT.1.5	The application is distributed [***as an additional software package to the platform OS***]

FPT_TUD_EXT.2 – Integrity for Installation and Update

FPT_TUD_EXT.2.1	The application shall be distributed using the format of the platform-supported package manager.
FPT_TUD_EXT.2.2	The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_LIB_EXT.1 – Use of Third Party Libraries

FPT_LIB_EXT.1.1	The application shall be packaged with only [**third-party libraries listed in Appendix B**].

FPT_IDV_EXT.1 – Software Identification and Versions

FPT_IDV_EXT.1.1	The application shall be versioned with [***an identification string comprising the following elements:*** • ***a single letter identifying the product design/architecture level, followed by a "."*** • ***a major release version number, followed by a "."*** • ***a minor release version number***].

5.2.7 Trusted Path/Channels (FTP)

FTP_DIT_EXT.1 – Protection of Data in Transit

FTP_DIT_EXT.1.1	The application shall [• ***encrypt all transmitted [data] with [TLS as defined in the TLS package]***] between itself and another trusted IT product.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are reproduced verbatim from the [PPAS].

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
	ALC_TSU_EXT.1 Timely Security Updates
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 2 Assurance Components

These assurance requirements imply the following requirements from CC class ASE: Security Target Evaluation.

- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST introduction
- ASE_OBJ.1 Security objectives for the operational environment
- ASE_REQ.1 Stated security requirements
- ASE_TSS.1 TOE summary specification

Consequently, the assurance activities specified in [PPAS] apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the TOE security functions:

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted Path/Channels.

It also describes the processes put in place by the TOE vendor to provide timely security updates to the TOE as per the ALC_TSU_EXT.1 requirements of [PPAS].

6.1 Timely Security Updates

Micro Focus incorporates IT industry best practices during the product development lifecycle to ensure an appropriate focus on security. Micro Focus engineering and manufacturing practices are designed to meet product security requirements, protect Micro Focus intellectual property, and support Micro Focus product warranty requirements. In addition, when a new industry-wide security vulnerability is released, Micro Focus investigates its product line to determine the impact.

Micro Focus publishes Security Bulletins to report vulnerabilities identified in the TOE. Security Bulletins identify impacted product versions and the resolution, which could be a patch, an upgrade, or a configuration change. Customers can subscribe to receive real-time notifications of Micro Focus Security Bulletins and advisories.

Upon discovery of a vulnerability, the impact will be assessed for priority. Any critical security fixes (vulnerabilities with a CVSS v3 base score of 9.0-10.0) are given highest priority, with a target release of no more than 30 days. Lower-risk items are targeted for resolution in 90-180 days depending on priority and severity.

Customers can report security issues related to the TOE via the Micro Focus secure web site (https://www.microfocus.com/support-and-services/report-security/), or by sending encrypted email to security@microfocus.com using the Micro Focus PGP key.

6.2 Cryptographic Support

The TOE incorporates OpenSSL 1.0.2u-fips from OpenSuSE, with the FIPS Object Module v2.0.13 integrated into the OpenSSL core crypto library, to provide its cryptographic functionality.

6.2.1 Random Bit Generation

The TOE includes the OpenSSL FIPS Object Module to implement DRBG functionality for its cryptographic operations. It uses the CTR_DRBG (AES) algorithm implemented by the OpenSSL FIPS Object Module to perform DRBG services in accordance with NIST Special Publication 800-90A. The TOE obtains the seed for its DRBG by calling the BCryptGenRandom API provided by the underlying Windows platform. BCryptGenRandom is the interface to the Windows random number generator.

The Random Bit Generation aspect of the Cryptographic Support security function satisfies the following security functional requirements:

- FCS_RBG_EXT.1—the TOE implements DRBG functionality for its cryptographic operations through the inclusion within Data Protector of the OpenSSL FIPS Object Module
- FCS_RBG_EXT.2—the TOE performs DRBG services using the CTR_DRBG (AES) provided by the OpenSSL FIPS Object Module.

6.2.2 Cryptographic Key Management

The TOE includes the OpenSSL FIPS Object Module to generate asymmetric key pairs.

The TOE generates asymmetric cryptographic keys in accordance with the following key generation algorithms and standards:

- RSA keys of 2048 bits or greater, in accordance with Appendix B.3 of FIPS 186-4, "Digital Signature Standard (DSS)". These keys are associated with X.509 certificates and used for entity authentication.
- ECC keys over NIST curves P-256, P-384 and P-521 in accordance with Appendix B.4 of FIPS PUB 186-4, "Digital Signature Standard (DSS). These keys are used for TLS key establishment.
- FFC schemes using cryptographic key sizes of 2048 bits or greater in accordance with Appendix B.1 of FIPS PUB 186-4, "Digital Signature Standard (DSS)". These keys are used for TLS key establishment.

The TOE supports the following key establishment schemes:

- Elliptic curve-based key establishment schemes—used when the TOE negotiates use of a TLS_ECDHE_* cipher suite
- Finite field-based key establishment schemes—used when the TOE negotiates use of a TLS_DHE_* cipher suite.

The Cryptographic Key Management aspect of the Cryptographic Support security function satisfies the following security functional requirements:

- FCS_CKM_EXT.1—the TOE implements asymmetric key generation through the inclusion within Data Protector of the OpenSSL FIPS Object Module
- FCS_CKM.1(1)—the TOE generates asymmetric cryptographic keys in accordance with the following key generation algorithms implemented by the OpenSSL FIPS Object Module: RSA; ECC; and FFC.
- FCS_CKM.2—the TOE implements functionality to perform cryptographic key establishment in accordance with the following cryptographic key establishment methods: Elliptic curve-based schemes; Finite field-based schemes.

6.2.3 Cryptographic Operations

The TOE includes NIST-validated cryptographic algorithms providing supporting cryptographic functions. The following functions have been certified in accordance with the identified standards.

Functions	**Standards**	**Certificates**
Asymmetric key generation (FCS_CKM.1(1))		
RSA (2048 bits or greater)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	C1643
ECDSA (P-256, P-384, P-521 curves)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4	C1643
DSA (2048 bits)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1	C1643
Cryptographic key establishment (FCS_CKM.2)		
Elliptic curve-based scheme	NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	C1643
Finite field-based scheme	NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	C1643

Functions	Standards	Certificates
Symmetric encryption/decryption (FCS_COP.1(1))		
AES CBC, GCM (128, 256 bits)	FIPS PUB 197 CBC as defined in NIST SP 800-38A GCM as defined in NIST SP 800-38D	C1643
Cryptographic hashing (FCS_COP.1(2))		
SHA-256, SHA-384	FIPS PUB 180-4	C1643
Cryptographic signature services (FCS_COP.1(3))		
RSA with 2048 bit modulus or greater	FIPS PUB 186-4	C1643
Keyed-hash message authentication (FCS_COP.1(4))		
HMAC-SHA-256, HMAC-SHA-384	FIPS Pub 198-1 FIPS Pub 180-4	C1643
Deterministic random bit generation (FCS_RBG_EXT.2)		
CTR_DRBG (AES)	NIST SP 800-90A	C1643

Table 3 Cryptographic Functions

The cryptographic hashing functions (SHA-256, SHA-384) are used in association with the related keyed-hash message authentication functions (HMAC-SHA-256, HMAC-SHA-384) to provide data integrity checking in the implementation of TLS and also in the verification of digital signatures associated with X.509v3 certificates.

The Cryptographic Operations aspect of the Cryptographic Support security function satisfies the following security functional requirements:

- FCS_COP.1(1)—the TOE performs symmetric encryption and decryption in accordance with AES operating in CBC and GCM modes with key sizes of 128 and 256 bits
- FCS_COP.1(2)—the TOE performs cryptographic hashing in accordance with SHA-256 and SHA-384 and message digest sizes of 256 bits and 384 bits respectively that meet FIPS Pub 180-4
- FCS_COP.1(3)—the TOE performs cryptographic signature services in accordance with RSA using 2048 bit keys that meet FIPS Pub 186-4
- FCS_COP.1(4)—the TOE performs keyed-hash message authentication in accordance with HMAC-SHA-256 and HMAC-SHA-384 with key sizes of 512 bits for HMAC-SHA-256 and 1024 bits for HMAC-SHA-384 and digest sizes of 256 bits and 384 bits respectively that meet FIPS Pub 198-1 and FIPS Pub 180-4.

6.2.4 Cryptographic Protocols

The TOE implements TLS v1.2 to protect communications between itself and other TOE instances (i.e., when acting as Cell Manager communicating to a Disk Agent or Media Agent, when acting as a Disk Agent communicating to a Media Agent, when acting as a Media Agent communicating to a Disk Agent), and rejects all attempts to connect using SSL or versions of TLS prior to v1.2. All communications between TOE instances use mutually authenticated TLS. The TOE supports the following TLS ciphersuites as both a TLS server and as a TLS client:

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289.

The TOE's implementation of TLS supports mutual authentication using X.509v3 certificates.

The TOE, when acting as a TLS server, performs key establishment for TLS as follows:

- When a DHE cipher suite is used, the TOE uses 2048-bit Diffie-Hellman parameters
- When an ECDHE cipher suite is used, the TOE uses the appropriate NIST curve as presented by the TLS client in the Supported Groups Extension of the Client Hello message. The TOE supports secp256r1, secp384r1 and secp521r1.

The TOE establishes reference identifiers for TLS certificate-based authentication based on the hostname (fully qualified domain name – FQDN) or IP address of the external IT entity (another TOE instance) with which it will communicate, configured during installation. As part of authentication in the establishment of TLS connectivity, the TOE will validate the reference identifier of the presented certificate (server or client). This is done through validation of the Common Name (CN) and Subject Alternative Name (SAN) certificate fields. The TOE does not support wildcard ("*") characters. The TOE verifies that the presented identifier matches the reference identifier according to RFC 6125 section 6, and establishes a trusted channel only if the presented certificate is valid. In addition, the TOE supports certificate pinning in relation to communications between Data Protector instances (i.e., communications occurring on port 5565). When a Data Protector instance is set up as a Disk Agent or a Media Agent, the administrator is presented with a certificate (assuming the certificate has passed all other checks, such as expiration, eku, and chaining). The administrator accepts the certificate, causing it to be "pinned". Subsequently, when a connection is attempted, the TOE instance performs all the regular checks on the certificate and then checks to make sure it is in the list of pinned certificates. If so, the connection succeeds; if not, the connection is denied.

The Cryptographic Protocols aspect of the Cryptographic Support security function satisfies the following security functional requirements:

- FCS_TLS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.5, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2—the TOE implements TLS v1.2 in compliance with RFC 5246, with support for mutual authentication.

6.2.5 Credential Storage

The TOE stores the following persistent credentials that are used in meeting its security functional requirements:

- RSA private keys used by INET—these are used in authenticating TLS connections between INET agents on separate TOE instances. In the evaluated configuration, they are stored in the Windows certificate store.
- RSA private keys used by the Application Server—these are used in authenticating the Application Server to clients and are stored in the Application Server's trust store.
- User passwords—used to authenticate a claimed TOE user identity to the TOE. They are stored in the PostgreSQL database, encrypted using AES. The encryption key itself is, in the evaluated configuration, encrypted using the Windows Data Protection API (DPAPI).

The Credential Storage aspect of the Cryptographic Support security function satisfies the following security functional requirement:

- FCS_STO_EXT.1—the TOE includes mechanisms to securely store credentials in non-volatile memory.

6.3 User Data Protection

The [PPAS] defines "sensitive data" as follows: "Sensitive data may include all user or enterprise data or may be specific application data such as emails, messaging, documents, calendar items, and contacts. Sensitive data must minimally include PII, credentials, and keys. Sensitive data shall be identified in the application's TSS by the ST author." Based on this definition, the sensitive data stored by the TOE comprises any data backed up by a TOE instance operating as a Disk Agent and sent for storage to a TOE instance operating as a Media Agent, and the keys and credentials covered within the scope of FCS_STO_EXT.1 (see Section 6.2.5 above). The TOE relies on the BitLocker capability of the underlying Windows platform to encrypt all backup data written to non-volatile memory.

The TOE accesses the physical resources of its underlying platform for network connectivity. The guidance documentation identifies when the TOE requires network connectivity. The TOE does not access sensitive information repositories as defined and intended by [PPAS]. The TOE restricts network connectivity to:

- TSF-initiated—scheduled backup and restore operations.

The User Data Protection security function satisfies the following security functional requirements:

- FDP_DAR_EXT.1—the TOE leverages platform-provided functionality to encrypt stored backup data.
- FDP_DEC_EXT.1—the TOE's use of platform services is well understood by users prior to authorizing the TOE activity.
- FDP_NET_EXT.1—the TOE communicates over the network for well-defined purposes. Depending on the function, the use of network resources is user-initiated or initiated by the TOE itself.

6.4 Identification and Authentication

6.4.1 Certificate Authentication

The TOE uses X.509v3 certificates as defined in RFC 5280 to support authentication for TLS. The TOE supports mutual authentication of TLS connections to other TOE instances. The guidance documentation instructs the administrator on how to generate certificate signing requests, how to obtain custom certificates from a trusted authority, and how to load custom certificates, the trusted root CA certificate, and any intermediate CA certificates in the certificate chain onto the TOE platform. The TOE stores the certificates to be used for authenticating INET connections in a designated directory in the Windows filesystem.

The administrator can configure the TOE to accept or reject a connection if it is unable to establish a connection with an OCSP server to determine a certificate's revocation status. The guidance documentation provides instructions for configuring this behavior.

The Certificate Authentication aspect of the Identification and Authentication security function satisfies the following security functional requirement:

- FIA_X509_EXT.2—the TOE uses X.509 certificates to support authentication for TLS, and allows the administrator to configure whether to accept or reject a certificate when it cannot establish a connection to determine the certificate's validity.

6.4.2 Certificate Validation

When the TOE is installed, it generates its own certificate, but it can be configured to use external certificates.

The TOE performs RFC 5280 certificate validation and certificate path validation on all X.509 certificates presented to it for the purpose of TLS server authentication. The TOE supports a path length of at least three certificates.

The TOE validates a certification path by ensuring the presence of the basicConstraints extension with the CA flag set to TRUE for all CA certificates. The TOE will not treat a certificate as a CA certificate if the basicConstraints extension is not present or the CA flag is not set to TRUE. The certification path terminates with a trusted CA certificate designated as the Root CA.

The TOE validates X.509 certificates using the path validation algorithm defined in RFC 5280, which can be summarized as follows:

- The public key algorithm and parameters are checked
- The current date/time is checked against the validity period of the certificate
- The revocation status is checked
- The issuer name is checked to ensure that it equals the subject name of the previous certificate in the path
- Name constraints are checked, to make sure the subject name is within the permitted subtrees list of all previous CA certificates and not within the excluded subtrees list of any previous CA certificate
- The asserted certificate policy OIDs are checked against the permissible OIDs of the previous certificate, including any policy mapping equivalencies asserted by the previous certificate

- Policy constraints and basic constraints are checked, to ensure that any explicit policy requirements are not violated and that the certificate is a CA certificate, respectively
- The path length is checked to ensure that it does not exceed any maximum path length asserted in this or a previous certificate
- The key usage extension is checked
- Any other critical extensions are recognized and processed.

The certificate chain is validated to the root, and a revocation check is performed on each certificate (except the root certificate) using OCSP.

The TOE uses the following rules for validating 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.
- 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.

Certificates are not used for trusted updates or executable code integrity, and the TOE does not use S/MIME or support Certificate Management over CMS (CMC). Therefore, the TOE does not support the rules for validating certificates with the Code Signing purpose, Email Protection purpose, or CMC Registration Authority purpose in the extendedKeyUsage field, and this part of the requirement is trivially satisfied.

The Certificate Validation aspect of the Identification and Authentication security function satisfies the following security functional requirement:

- FIA_X509_EXT.1—the TOE validates X.509 certificates in accordance with specified validation rules.

6.5 Security Management

6.5.1 Secure by Default Configuration

Use of the TOE is restricted to configured TOE users. The TOE defines users based on the following attributes:

- Windows logon name
- Windows domain or workgroup
- System from which the user logs on (can use wildcard characters).

The TOE checks a user is a defined TOE user whenever the user attempts to start the TOE user interface or perform a specific task.

Each TOE user belongs to a single user group, which defines the user's rights to perform actions on the TOE (e.g., perform backup or restore operations). The TOE defines three default user groups—**admin**, **operator**, and **user**. The **admin** group has all user rights, while the **operator** and **user** groups have subsets of the **admin** user rights. A user in the **admin** group can create and manage new user groups and can modify the user rights associated with the **operator** and **user** groups (the user rights associated with the **admin** group cannot be modified).

After initial installation of the TOE, the **operator** and **user** groups are empty. The **admin** group contains the following users:

- CRS service account—this account is created during TOE installation and is limited to the TOE instance in the Cell Manager role
- User that installed Cell Manager—this will be the Windows administrator account on the Cell Manager host, or a user with Windows administrator privileges
- Local System on the Cell Manager.

Each configured TOE user has an associated password that is defined when the user account is created. However, the user is not required to enter this password when accessing the TOE via the GUI or CLI and the password is not used

in the evaluated configuration. The password is used in association with the user account for REST API access, which is excluded from the evaluated configuration. The TOE does not install with default credentials.

6.5.2 Supported Configuration Mechanism

The administrator sets the following options during initial configuration of the TOE:

- Name and password for Windows account under which TOE services run
- FIPS mode of operation
- OCSP certificate revocation checking functionality.

The following configuration options are maintained in the Windows Registry:

- Inet port
- Cell Manager name

The digital certificates and the TOE environment configuration are stored in files within `C:\ProgramData\OmniBack\` and its sub-directories.

6.5.3 Specification of Management Functions

The TOE provides the following security management functions:

- Configure supported TLS cipher suites
- Generate certificate signing requests
- Manage X.509 certificates.

The Security Management security function satisfies the following security functional requirements:

- FMT_CFG_EXT.1—the TOE requires credentials to be defined before use. The TOE is protected from direct modification by untrusted users via its host OS platform.
- FMT_MEC_EXT.1—configuration settings for the TOE are stored in the Windows registry and in configuration files stored in `C:\ProgramData\`.
- FMT_SMF.1—the GUI and CLI can be used by administrators to configure TOE settings.

6.6 Privacy

The TOE does not collect Personally Identifiable Information (PII) from administrators or users. As such, it does not transmit PII over a network.

The Privacy security function satisfies the following security functional requirement:

- FPR_ANO_EXT.1—the TOE does not transmit PII over a network.

6.7 Protection of the TSF

6.7.1 Anti-Exploitation Capabilities

The TOE implementation is compatible with anti-exploitation mechanisms implemented in the underlying Windows platform. The TOE relies fully on the underlying Windows platform to perform memory mapping. There is no situation where the TOE maps memory to an explicit address or requests a memory mapping with both write and execute permissions. The TOE runs successfully with process exploit mitigations enabled on the underlying Windows Server platform.

The TOE does not write user-modifiable files to directories containing executable files, including the TOE's installation directory.

Executables (i.e., `.exe` and `.dll` files) intended to run on a Windows platform indicate to the operating system they are compatible with address space layout randomization (ASLR) by linking with the /DYNAMICBASE flag. This flag has been enabled by default since Visual Studio 2010. In addition, the operating system can be configured to force

mandatory ASLR on executables that have not been linked with /DYNAMICBASE, on a system-wide or per-process basis.

The TOE executables have been compiled with the /GS (GuardStack) flag, which protects against stack-based buffer overflow in the compiled program.

6.7.2 Supported APIs and Third-Party Libraries

The TOE uses only documented platform APIs. Appendix A lists the APIs used by the TOE. The TOE also makes use of third-party libraries. Appendix B lists the libraries used by the TOE.

6.7.3 Software Identification and Versioning

The TOE is identified as Micro Focus Data Protector Premium Edition, release 2020.05, software version A.10.70. The software versioning format was adopted from the HP-UX platform due to historical reasons. The initial letter ("A") represents the first design/architecture of the product and it changes only if there is a fundamental transformation in a new version. The first part of the version number ("10") refers to a major version and it will be changed when there is a major enhancement from the previous version. The second part ("70") refers to the minor version and it will be incremented by 10, for every minor version release that contains enhancements and defect fixes.

6.7.4 Trusted Update

The administrator can query the current installed version of the TOE from the GUI. The TOE guidance documentation describes the procedure for administrators to check for the availability of TOE updates. The administrator visits the Micro Focus Software Licenses and Downloads Portal to download an upgrade package. The TOE is distributed as a set of files in the standard Windows Installer (.MSI) format, along with a setup program. All files are signed by the Micro Focus code-signing service. A TOE update succeeds only if the digitally signed update is verified by Data Protector. Additionally, the administrator can verify the digital signature of the setup program and the MSI files using SignTool from Microsoft (https://docs.microsoft.com/en-us/dotnet/framework/tools/signtool-exe), as follows: `signtool verify /pa <path_to_msi/setup_file>`.

The procedures for uninstalling the TOE are such that all traces of the TOE are removed from the operational environment, with the exception of configuration settings, output files, and log files.

Updating the TOE software is the only method of changing its executable code—it does not change its own code.

The Protection of the TSF security function satisfies the following security functional requirements:

- FPT_AEX_EXT.1—the TOE interacts with its host OS platform in a manner that does not expose the system to memory-related exploitation.
- FPT_API_EXT.1—the TOE uses only documented platform APIs.
- FPT_LIB_EXT.1—the third-party libraries packaged with the TOE are identified and all serve a necessary purpose.
- FPT_IDV_EXT.1—the TOE is versioned based on its year and month of release.
- FPT_TUD_EXT.1, FPT_TUD_EXT.2—the TOE can be updated through installation packages. Updates are signed by the vendor and validated by the host OS platform prior to installation.

6.8 Trusted Path/Channels

All data transmitted between TOE instances is assumed to be sensitive data.

A TOE instance protects all data it communicates with other TOE instances using TLS.

The Trusted Path/Channels security function satisfies the following security functional requirement:

- FTP_DIT_EXT.1—the TOE encrypts all transmitted data with TLS.

7. Protection Profile Claims

This ST is conformant to the *Protection Profile for Application Software*, Version 1.3, 1 March 2019 ([PPAS]) and to *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 12 February 2019 ([FPTLS]), including the following selection-based SFRs:

- FCS_CKM.1(1)
- FCS_CKM.2
- FCS_COP.1(1)
- FCS_COP.1(2)
- FCS_COP.1(3)
- FCS_COP.1(4)
- FCS_TLSC_EXT.1
- FCS_TLSC_EXT.2
- FCS_TLSC_EXT.5
- FCS_TLSS_EXT.1
- FCS_TLSS_EXT.2
- FCS_RBG_EXT.2
- FIA_X509_EXT.1
- FIA_X509_EXT.2.

As explained in Section 3, Security Problem Definition, the Security Problem Definition of [PPAS] has been copied verbatim into this ST.

As explained in Section 4, Security Objectives, the Security Objectives of [PPAS] have been copied verbatim into this ST.

All claimed SFRs are defined in [PPAS] or in [FPTLS]. All mandatory SFRs are claimed. No optional or objective SFRs are claimed. Selection-based SFR claims are consistent with the selections made in the mandatory SFRs that prompt their inclusion.

8. Rationale

This Security Target reproduces the [PPAS] Security Problem Definition and Security Objectives. The Security Target makes no additions to the [PPAS] assumptions. [PPAS] and [FPTLS] SFRs have been reproduced with the PP operations completed. Operations on the security requirements follow [PPAS] and [FPTLS] application notes and assurance activities as appropriate. The proper set of selection-based requirements have been claimed based on the selections made in the mandatory requirements. Consequently, the claims made by this Security Target are sufficient to address the TOE's security problem. Rationale for the sufficiency of the TOE Summary Specification is provided below.

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 4 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Cryptographic support	User Data Protection	Identification and authentication	Security management	Protection of the TSF	Trusted path/channels	Privacy
FCS_CKM.1(1)	X						
FCS_CKM_EXT.1	X						
FCS_CKM.2	X						
FCS_COP.1(1)	X						
FCS_COP.1(2)	X						
FCS_COP.1(3)	X						
FCS_COP.1(4)	X						
FCS_RBG_EXT.1	X						
FCS_RBG_EXT.2	X						
FCS_STO_EXT.1	X						
FCS_TLS_EXT.1	X						
FCS_TLSC_EXT.1	X						
FCS_TLSC_EXT.2	X						
FCS_TLSC_EXT.5	X						

	Cryptographic support	User Data Protection	Identification and authentication	Security management	Protection of the TSF	Trusted path/channels	Privacy
FCS_TLSS_EXT.1	X						
FCS_TLSS_EXT.2	X						
FDP_DAR_EXT.1		X					
FDP_DEC_EXT.1		X					
FDP_NET_EXT.1		X					
FIA_X509_EXT.1			X				
FIA_X509_EXT.2			X				
FMT_MEC_EXT.1				X			
FMT_CFG_EXT.1				X			
FMT_SMF.1				X			
FPR_ANO_EXT.1							X
FPT_API_EXT.1					X		
FPT_AEX_EXT.1					X		
FPT_TUD_EXT.1					X		
FPT_TUD_EXT.2					X		
FPT_LIB_EXT.1					X		
FPT_IDV_EXT.1					X		
FTP_DIT_EXT.1						X	

Table 4 Security Functions vs. Requirements Mapping

Appendix A: APIs

The following is the list of Windows system APIs used by the TOE.

WSAGetLastError

ntohl

ntohs

htonl

inet_ntoa

gethostbyname

send

SetStdHandle

lstrlenA

WriteFile

SetFilePointerEx

SetEndOfFile

LocalFree

FormatMessageA

GetSystemInfo

DeviceIoControl

CreateFileW

SetConsoleCtrlHandler

GetFileAttributesW

FileTimeToSystemTime

ReadFile

FlushFileBuffers

SetFilePointer

WideCharToMultiByte

lstrlenW

ReleaseSemaphore

UnmapViewOfFile

ReleaseMutex

WaitForSingleObject

FindClose

TlsGetValue

TlsSetValue

TlsFree

IsValidCodePage

FreeLibrary

DeleteFileW

FindFirstFileW

FindNextFileW

GetFileInformationByHandle

LockFileEx

RemoveDirectoryW

UnlockFileEx

SetHandleInformation

FormatMessageW

GetStdHandle

GetFileType

GetTempPathW

GetHandleInformation

HeapAlloc

GetProcessHeap

GetConsoleMode

SetConsoleMode

FileTimeToLocalFileTime

GetFileSize

MultiByteToWideChar

SetEvent

CreateThread

DeleteCriticalSection

CreateProcessA

MapViewOfFile

ConnectNamedPipe

DisconnectNamedPipe

SetNamedPipeHandleState

ResetEvent

WaitForSingleObjectEx

ResumeThread

DuplicateHandle

CloseHandle

GetCurrentProcess

SetLastError

GetTickCount

GetProcessTimes

GetCurrentThreadId

GetCurrentProcessId

GetSystemTimeAsFileTime

Sleep

QueryPerformanceFrequency

QueryPerformanceCounter

GetProcAddress

GetLastError

TlsAlloc

LeaveCriticalSection

EnterCriticalSection

InitializeCriticalSection

SetErrorMode

TerminateProcess

WaitForMultipleObjects

GetOverlappedResult

PeekNamedPipe

CreatePipe

GlobalMemoryStatusEx

GetTimeZoneInformation

SystemTimeToFileTime

GetProcessIoCounters

OpenProcess

GetCurrentThread

GetExitCodeProcess

LocalFileTimeToFileTime

InitializeAcl

GetLengthSid

FreeSid

DuplicateToken

AllocateAndInitializeSid

AdjustTokenPrivileges

AddAccessAllowedAce

OpenThreadToken

SetThreadToken

DeleteService

ControlService

IsValidSid

InitializeSid

GetTokenInformation

GetSidSubAuthority

EqualSid

OpenProcessToken

IsTextUnicode

SetSecurityDescriptorGroup

SetSecurityDescriptorOwner

CreateProcessAsUserA

IsValidSecurityDescriptor

QueryServiceStatus

CloseServiceHandle

CloseEventLog

RegCloseKey

SetSecurityDescriptorDacl

InitializeSecurityDescriptor

CryptQueryObject

CertGetNameStringW

CertFreeCertificateContext

CertFindCertificateInStore

CertCloseStore

CryptMsgGetParam

CryptMsgClose

CryptUnprotectData

CryptProtectData

CryptBinaryToStringA

CertOpenStore

getnameinfo

WSAEventSelect

WSAIoctl

freeaddrinfo

getaddrinfo

WinVerifyTrust

DeregisterEventSource

GetExitCodeThread

SizeofResource

LoadStringA
SetKernelObjectSecurity
ioctlsocket
socket
gethostbyaddr
listen
WSAStartup
WSACleanup
inet_addr
accept
getpeername
getsockname
bind
closesocket
connect
WSASetLastError
gethostname
htons
shutdown
sendto
select
WNetCloseEnum
SetupCloseInfFile
SetFileAttributesW
HeapReAlloc
HeapFree
HeapSize
GetACP
GetOEMCP
GlobalAlloc
GlobalFree
InvalidateRect
IsWindow
GetFocus
SetCursor
GetSystemMetrics
GetActiveWindow

GetSysColor
SetActiveWindow
GetParent
ScreenToClient
GetCursorPos
GetWindowRect
GetDC
ReleaseDC
RedrawWindow
LockWindowUpdate
GetWindowDC
EnableWindow
SendMessageW
GetClientRect
SetWindowTextW
UpdateWindow
SetParent
CreateCompatibleDC
StretchBlt
SHGetSpecialFolderLocation
SHGetMalloc
StrCmpW
CoUninitialize
CoCreateInstance
CoInitialize
PathFileExistsW
GetVersionExA
GetFileTime
SetFileTime
SetWaitableTimer
GetComputerNameExA
GetLocalTime
CryptGenRandom
LsaNtStatusToWinError
LsaRemoveAccountRights
LsaAddAccountRights
LsaEnumerateAccountRights

LsaOpenPolicy

LsaClose

ImpersonateLoggedOnUser

CLSIDFromString

GetAdaptersInfo

BackupWrite

BackupRead

ExitThread

GetProcessMemoryInfo

GetVolumeInformationW

MessageBeep

GetDlgCtrlID

UnionRect

IsRectEmpty

IsWindowVisible

KillTimer

SetTimer

GetStockObject

DisableThreadLibraryCalls

LoadLibraryA

GetStringTypeExW

GetStringTypeExA

LoadStringW

arm_init

arm_getid

arm_start

arm_stop

arm_end

SnmpUtilVarBindListFree

inet_pton

inet_ntop

GetDIBits

GetDeviceCaps

DeleteObject

CreateCompatibleBitmap

OpenCluster

ClusterResourceControl

OfflineClusterResource

OnlineClusterResource

GetClusterResourceState

CloseClusterResource

OpenClusterResource

ClusterCloseEnum

ClusterEnum

ClusterOpenEnum

CloseCluster

LockFile

UnlockFile

GetSystemTime

GetLogicalDrives

SetPriorityClass

ExitProcess

CoInitializeSecurity

CoTaskMemFree

StringFromGUID2

CreatePopupMenu

PtInRect

CreateMenu

DrawIconEx

CreateDIBSection

SelectObject

DeleteDC

CompareFileTime

TerminateThread

AllocConsole

GetModuleFileNameA

CopySid

UuidCreate

BackupClusterDatabase

GetClusterQuorumResource

NetShareGetInfo

NetShareDel

NetShareAdd

NetApiBufferFree

NetShareEnum

LocalAlloc

BackupSeek

VirtualAlloc

VirtualFree

ReadFileEx

CancelIo

FindVolumeClose

GetThreadTimes

GetSidSubAuthorityCount

GetSidIdentifierAuthority

GetSecurityDescriptorLength

ConvertSecurityDescriptorToStringSecurityDescriptorA

CoSetProxyBlanket

GetStorageDependencyInformation

SetServiceStatus

SetupDiEnumDeviceInterfaces

SetupDiDestroyDeviceInfoList

RestoreClusterDatabase

FlushViewOfFile

RegSetKeySecurity

RegGetKeySecurity

RegFlushKey

IsValidAcl

GetSecurityDescriptorDacl

GetSecurityDescriptorControl

GetAce

TranslateMessage

GetKeyState

GetSubMenu

ClientToScreen

GetWindow

CreateToolhelp32Snapshot

DebugBreak

Process32FirstW

Process32NextW

GetDlgItem

GetNextDlgTabItem

SetFocus

Netbios

WTSFreeMemory

FindVolumeMountPointClose

FreeConsole

OpenThread

CoInitializeEx

GetLocaleInfoEx

EnumProcesses

GetModuleBaseNameA

LoadResource

LockResource

MulDiv

CallNextHookEx

DestroyMenu

EnableMenuItem

EndDialog

GetWindowLongPtrA

MoveWindow

SendMessageA

SetWindowLongPtrA

SetWindowPos

SetWindowsHookExA

ShowWindow

TrackPopupMenu

UnhookWindowsHookEx

InflateRect

InvertRect

ReleaseCapture

AcquireSRWLockExclusive

AcquireSRWLockShared

ReleaseSRWLockExclusive

ReleaseSRWLockShared

CallWindowProcA

GetDesktopWindow

GetWindowLongA

MsgWaitForMultipleObjects

SetWindowLongA

FreeResource

GetEnvironmentStrings

GetVersion

GlobalLock

GlobalUnlock

BCryptGenRandom

Appendix B: Third Party Libraries

The following table lists the third-party libraries that are packaged with the TOE. It identifies the library name, version number, and source.

3rd Party Product Name	Company Name
gsoap 2.8 [HPE] [Genivia]	Genivia
Data Domain DD Boost 3.4.0.2	Dell EMC
JRE HP-UX 8.0.15 [Hewlett Packard]	Hewlett Packard
Microsoft Visual Studio and C++ Redist (2013) [Microsoft]	Microsoft
Microsoft Visual Studio and C++ Redist (2017) VC_redist.x64.exe [Microsoft]	Microsoft
NetApp Manageability SDK 9.5 [NetApp]	NetApp
Virtual Disk Development Kit (VDDK) 6.7 U1 [VMware]	VMware
activemq-all 5.15.9 [Apache.org]	Apache.org
Commons BeanUtils 1.9.3 [Apache.org]	Apache.org
Commons Codec 1.2 [Apache.org]	Apache.org
Commons Codec 1.9 [Apache.org]	Apache.org
Commons Collections 3.2.2 [Apache.org]	Apache.org
Commons IO 1.3.2 [Apache.org]	Apache.org
Commons Logging 1.1.1 [Apache.org]	Apache.org
HTTPClient 4.5.8 [Apache.org]	Apache.org
log4j 1.2.15 [Apache.org]	Apache.org
log4j 1.2.17 [Apache.org]	Apache.org
Log4j API 2.10.0 [Apache.org]	Apache.org
Log4j API 2.7 [Apache.org]	Apache.org
Log4j Core 2.10.0 [Apache.org]	Apache.org
Log4j Core 2.11.2 [Apache.org]	Apache.org
Log4net 1.2.10 [Apache.org]	Apache.org
Zulu OpenJDK 8u212 (Linux 64-bit) [Azul Systems]	Azul Systems
Zulu OpenJDK 8u212 (Win 64-bit) [Azul Systems]	Azul Systems
Boost C++ Libraries 1.44 [Boost.org]	Boost.org
Boost C++ Libraries 1.65.0 [Boost.org]	Boost.org
Boost C++ Libraries-regex 1.44 [Boost.org]	Boost.org
Boost C++ Libraries-string 1.44 [Boost.org]	Boost.org
Boost C++ Libraries-test 1.44 [Boost.org]	Boost.org
Bouncy Castle bcpkix-jdk15on 1.62 [Bouncy Castle.org]	Bouncy Castle.org
libcurl 7.50.2 [cURLhaxx]	cURLhaxx
Dom4j 1.6.1 [Dom4j.org]	Dom4j.org
FileSaver.js 1.3.3 [Eli Grey]	Eli Grey
jackson-annotations 2.9.8 [FasterXML]	FasterXML
jackson-core 2.9.8 [FasterXML]	FasterXML
Jackson-core-asl 1.9.13 [FasterXML]	FasterXML
jackson-databind 2.9.8 [FasterXML]	FasterXML
Jackson-dataformat csv 2.7.0 [FasterXML]	FasterXML

3rd Party Product Name	Company Name
Jackson-dataformat ion 2.9.6 [FasterXML]	FasterXML
freebsd 1.72 [FreeBSD Project]	FreeBSD Project
Angular 1.2 [Github]	Github
Angular Bootstrap Calendar 0.27.5 [Github]	Github
Angular-Download 4.3.0 [Github]	Github
AngularJS-Toaster 0.4.3 [Github]	Github
Angular-Local-Storage 0.0.2 [Github]	Github
Angular-translate 1.1.1 [Github]	Github
angular-ui-bootstrap-aps 0.10.0 [Github]	Github
Bootstrap 3.0.3 [Github]	Github
CmdLine 1.8 [Github]	Github
Fuse 2.5.3 [Github]	Github
Jansson 2.4 [Github]	Github
Jasmine 1.3.1 [Github]	Github
Java Mail 1.4.4 [Github] [Github]	Github
Java Mail API 1.6.1 [Github]	Github
java-jwt 3.4.0 [Github]	Github
Jaxen 1.1.6 [Github]	Github
Joda-Time 2.9.9 [Github]	Github
jQuery Treeview Plugin 0.1 [Github]	Github
jQuery-timepicker-addon 1.2.10 [Github]	Github
jUnit 4.12 [Github]	Github
MutationObserver.js 0.3.2 [Github]	Github
netlib-java 1.1.2 [Github]	Github
ng-Grid 2.08 [Github]	Github
ng-Table 0.3.1 [Github]	Github
node-js 0.8.6 [Github]	Github
Snappy 1.0.4 [Github]	Github
springfox-swagger2 2.9.2 [Github]	Github
springfox-swagger-ui 2.9.2 [Github]	Github
StAXON 1.3 [Github]	Github
tableSorter 2.0.5b [Github]	Github
uuid 2.18 [MIT License] [Github]	Github
UXAspects 1.6.8 [Github]	Github
WinDPAPI4J 1.0 [Github]	Github
Jersey Core 1.19.4 [Glassfish]	Glassfish
Servlet-api 4.0.1 [Glassfish]	Glassfish
gcc runtimes 4.5.2 [GNU.org]	GNU.org
libgcc_s 4.5.2 [GNU.org]	GNU.org
libiconv 1.9.2 [GNU.org]	GNU.org
libstdc++ 4.5.2 [GNU.org]	GNU.org
Microsoft C Runtime library	Microsoft

3rd Party Product Name	Company Name
Oracle Client 11.1.0.7.0	Oracle
OpenJDK 1.8.0_242	OpenJDK
Chromium Embedded Framework 3.3202.1733 [Google Code]	Google Code
GSON 2.0 [Google Code]	Google Code
json-simple 1.1 [Google Code]	Google Code
Mkisofs 2.01 [Google Code]	Google Code
html2canvas 1.0.0-alpha.12 [Hertzen]	Hertzen
ICU4C 3.8-1 [ICU (International Components for Unicode) Project]	ICU (International Components for Unicode) Project
ICU4C 3.8-3 [ICU (International Components for Unicode) Project]	ICU (International Components for Unicode) Project
ICU4C 4.4.1 [ICU (International Components for Unicode) Project]	ICU (International Components for Unicode) Project
PDFjet 5.75 [Innovatics, Inc.]	Innovatics, Inc.
Expat XML Parser 1.95.6 [James Clark]	James Clark
Expat XML Parser 1.95.8 [James Clark]	James Clark
Jboss 7.1.1 [JBoss.org]	JBoss.org
resteasy-cdi 3.0.26.Final [JBoss.org]	JBoss.org
resteasy-links 3.0.26.Final [JBoss.org]	JBoss.org
jQuery 2.1.4 [jQuery]	jQuery
jQuery blockUI 2.66.0 [jQuery]	jQuery
jQuery Core 1.4.4 [jQuery]	jQuery
jQuery UI 1.12.1 [jQuery]	jQuery
jQuery UI 1.8.7 [jQuery]	jQuery
jQuery UI Layout 1.3.0 [jQuery]	jQuery
JSON 0.6.0 [json.org]	json.org
JSONcpp 0.6.0 [json.org]	json.org
jsTree 3.0.0 [jsTree]	jsTree
Keycloak 2.5.5 [Keycloak]	Keycloak
libssh2 1.7.0 [Libssh2.org]	Libssh2.org
dp-reporting-prediction [Open Source Bundle] 1.0 [Micro Focus]	Micro Focus
TypeScript 0.9.5 [Microsoft]	Microsoft
Moment.js 2.10.6 [Momentjs.com]	Momentjs.com
Moment.js 2.4.0 [Momentjs.com]	Momentjs.com
javax.json-api 1.0 [MVN Repository]	MVN Repository
Net-SNMP 5.6 [Net-SNMP.org]	Net-SNMP.org
ngx-translate/Core 8.0.0 [NGX-translate]	NGX-translate
ngx-translate/http-loader 2.0.0 [NGX-translate]	NGX-translate
OpenLDAP 2.2.29 [OpenLDAP Foundation]	OpenLDAP Foundation
OpenSSL 1.0.2u [OpenSSL.org]	OpenSSL.org
Perl 5.24.2 [Perl.org]	Perl.org
Poco C++ Libraries 1.7.4 [Pocoproject.org]	Pocoproject.org
PostgreSQL 11.5 [PostgreSQL]	PostgreSQL

3rd Party Product Name	Company Name
EFI Linux Boot Loader (Elilo) 3.14 [Sourceforge.net]	Sourceforge.net
Weka 3.0 [Sourceforge.net]	Sourceforge.net
Weka-core 3.0 [Sourceforge.net]	Sourceforge.net
Weka-mtj 3.0 [Sourceforge.net]	Sourceforge.net
Weka-Pentaho 3.0 [Sourceforge.net]	Sourceforge.net
Weka-timeseriesforecasting 3.0 [Sourceforge.net]	Sourceforge.net
spring-batch-infrastructure 4.1.2.RELEASE [Springframework.org]	Springframework.org
spring-boot-maven-plugin 2.1.4.RELEASE [Springframework.org]	Springframework.org
spring-boot-starter-web 2.1.4.RELEASE [Springframework.org]	Springframework.org
spring-core 5.1.6.RELEASE [Springframework.org]	Springframework.org
springframework-spring-beans 4.3.9 [Springframework.org]	Springframework.org
Springframework-spring-boot-autoconfigure 2.1.4.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-boot-starter 2.1.4.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-boot-starter-aop 2.1.4.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-boot-starter-jdbc 1.5.9.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-boot-starter-jdbc 2.1.4.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-boot-starter-log4j2 2.1.4.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-boot-starter-mail 2.1.4.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-boot-starter-test 2.1.4.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-context 4.3.14.RELEASE [Springframework.org]	Springframework.org
Springframework-spring-context-support 4.3.14.RELEASE [Springframework.org]	Springframework.org
springframework-spring-web 4.3.9 [Springframework.org]	Springframework.org
SQLite 3.7.3 [SQLite.org]	SQLite.org
Talend OFSDI talend_file_enhanced_20070724 1 [Talend]	Talend
Talend OSFDI advancedPersistentLookupLib 1 [Talend]	Talend
Talend OSFDI routines 1 [Talend]	Talend
Talend OSFDI talendcsv 1 [Talend]	Talend
Glib 2.16.4 [The GNOME Project]	The GNOME Project
Pegasus (basis for HP WEBM Services product) 2.11.0 [The Open Group]	The Open Group
QT (framework) 4.8.4 [The QT Company]	The QT Company
QT Webkit 4.8.4 [The QT Company]	The QT Company
QT win migrate 2.8 [The QT Company]	The QT Company
Wildfly 18.0.1 [wildfly.org]	wildfly.org
libxml2 2.6.30 [XMLsoft.org]	XMLsoft.org
zlib 1.2.3 [Zlib.net]	Zlib.net
zlib 1.2.3-5 [Zlib.net]	Zlib.net

3rd Party Product Name	Company Name
zlib 1.2.8 [Zlib.net]	Zlib.net