Acronis SCS

Acronis SCS Cyber Backup 12.5 Hardened Edition Agent

v12.5

Security Target

Document Version: 6.0

Prepared for:

Acronis SCS

Acronis SCS
1225 W. Washington St., Suite 250
Tempe, AZ 85288
United States of America

Phone: +1 781 782 9000
www.acronisscs.com

Prepared by:

Corsec

Corsec Security, Inc.
12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the organization of the ST. The TOE is the Acronis SCS Cyber Backup 12.5 Hardened Edition Agent developed by Acronis SCS and will hereafter be referred to as the TOE throughout this document. The TOE is the Backup Agent component of the Acronis SCS Backup Agent solution, which consists of a Management Server and multiple Backup Agents. Backup Agents are responsible for performing specific backup, recovery, replication and data-manipulation tasks on their host machines. The Backup Agents are able to work independently from the Management Server to run their scheduled backup operations.

1.1 Purpose

This ST is divided into 10 sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Assurance Requirements (Section 6) – Presents the SARs met by the TOE.
- Security Functional Requirements (Section 7) – Presents the SFRs met by the TOE.
- TOE Summary Specification (Section 8) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 9) – Presents the conformance claims rationale for the selected PP.
- Acronyms (Section 10) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Acronis SCS Cyber Backup 12.5 Hardened Edition Agent Security Target*
ST Version	Version 6.0
ST Author	Corsec Security, Inc.
ST Publication Date	October 11, 2023
TOE Reference	Acronis SCS Cyber Backup 12.5 Hardened Edition Agent

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

Acronis SCS Cyber Backup 12.5 Hardened Edition Agent (also known as Acronis SCS Backup Agent) is part of an advanced data protection solution that provides reliable backup and recovery of physical, virtual, and cloud workloads with a wide range of storage options. It may be used to protect data residing on-premises, in remote locations, in the cloud, and on mobile devices. Centralized and remote management of backups is performed via the Management Server's web-based Management Console, with customizable dashboards, advanced reporting, and auditing. Backup Agents installed on protected platforms perform data backup and recovery of physical or virtual machines, hypervisors, applications, and mobile devices. Acronis SCS Backup Agent supports application-aware backup and recovery features for Oracle database, Microsoft Office 365, Microsoft Exchange, Microsoft SQL[1] Server, Microsoft SharePoint, and Microsoft Active Directory.

Acronis SCS Backup Agent may be deployed in an on-premise or cloud configuration. With the on-premise configuration, the Management Server is installed on a customer's local network. With the cloud configuration, it is installed in a secure Acronis Data Center.

Acronis SCS Backup Agent includes the Acronis SCS Cryptographic Library and Acronis SCS Protocol Library in both the Management Server and Backup Agents. They provide the underlying cryptographic and protocol functionality necessary to support the use of secure communications protocols, encrypted backups, and secure file sharing.

1.3.1 Product Components

The following paragraphs provide a brief description of the product components.

1.3.1.1 Management Server

The Management Server, which is in the TOE environment, provides the means to configure, monitor, and manage backups and provides the web server (Web UI) for the Management Console. The Management Server is comprised of a number of management services responsible for management functions of Acronis SCS Backup Agent. The Management Server also includes an API[2] Gateway to communicate with the Backup Agents. The Management Server does not actually perform backup, recovery, or other data-manipulation operations. These are performed by the Backup Agents installed on each protected machine.

1.3.1.2 Backup Agents

Backup Agents are installed as a number of services to perform the actual backup and recovery operations on each machine that requires protection. They are typically installed on each machine that requires protection and then added to the Management Server. However, they are able to operate independently from the Management Server. Backup Agents are supported on both Windows and Linux OS[3]s. Different agent types are used to protect different data sources, but they all share the same architecture, communication protocols, and the vast majority of the functionality.

[1] SQL – Structured Query Language
[2] API – Application Programming Interface
[3] OS – Operating System

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The software-only TOE is the Acronis SCS Cyber Backup 12.5 Hardened Edition Agent. It is a standalone software application that runs on both Windows and Linux operating systems and provides backup and restore functionality for the host machine. Its security features include securely storing the application token, using a digital signature to protect the integrity of the installation and update files, versioning the software with SWID tags, and using anti-exploitation capabilities such as not mapping memory to explicit addresses, file permission protections, and stack buffer overflow protections. It also secures communications between itself and the Management Server. The TOE implements the cryptographic functionality for cryptographic services, including TLS[4] v1.2, through its embedded Acronis SCS Cryptographic Library and Acronis SCS Protocol Library. The TOE also includes the separately downloaded version-check tool that will query the current version of the TOE and report if an update is available.

In the evaluated configuration, the TOE is setup in two configurations:

- Acronis SCS Backup Agent for Windows v12.5 software installed on a Windows 10 machine that is on a network connected to the Management Server in the TOE environment, and
- Acronis SCS Backup Agent for Linux v12.5 software installed on a RHEL v7.9 machine on a network connected to the Management Server in the TOE environment.

Note that both of these configurations can be setup and used on the same network and use the same Management Server without interfering with each other. Both setups will also include separate installations of the version-check tool on the same machine as the Backup Agent.

The Protection Profile for Application Software specifies several use cases that may be implemented by conformant TOEs. The Acronis SCS Cyber Backup 12.5 Hardened Edition Agent is considered to implement both content creation and content consumption.

1.4.1 TOE Environment

Table 2 defines the environmental component requirements. In the evaluated configuration, the TOE is provided as an Acronis SCS Backup Agent setup program. The TOE is installed on a computer running either Microsoft Windows 10 or RHEL v7.9.

Table 2 – Environmental Components

Component	Requirements
Management Server	This machine is used to host the Management Server software and Monitoring Service. The following are required: • Microsoft Windows Server 2016 OS • Acronis SCS Cyber Backup 12.5 Hardened Edition Server software with licenses • 200 MB[5] of RAM[6] and 1.7 GB[7] of free space on the system volume • Intel Xeon E-2136 (Coffee Lake) CPU[8] with AES-NI

[4] TLS – Transport Layer Security
[5] MB – Megabyte
[6] RAM – Random-Access Memory
[7] GB – Gigabyte
[8] CPU – Central Processing Unit

Component	Requirements
Windows Agent Computer	This machine is a general-purpose computer that will have the Windows Agent installed on it. The following are required: • Microsoft Windows 10 OS • 720 MB disk space and 130 MB RAM • Intel Core i7-8650U (Kaby Lake R) CPU with AES-NI
Linux Agent Computer	This machine is a general-purpose computer that will have the Linux Agent installed on it. The following are required: • RHEL v7.9 OS • 850 MB disk space and 150 MB RAM • Intel Core i5-8350U (Kaby Lake R) CPU with AES-NI
CA[9] Server	A CA server is used for certificate creation/signing and to host the CRL[10] for certificate validation. This connection is over HTTP[11]. No specific CA server is required as long as it follows RFC 5280.

The TOE relies on an embedded SQLite database to store configuration data that is downloaded from the Management Server. This database is part of the TOE.

[9] CA – Certificate Authority
[10] CRL – Certificate Revocation List
[11] HTTP – Hypertext Transfer Protocol

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.5.1 Physical Scope

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the software-only TOE and the constituents of the TOE environment.

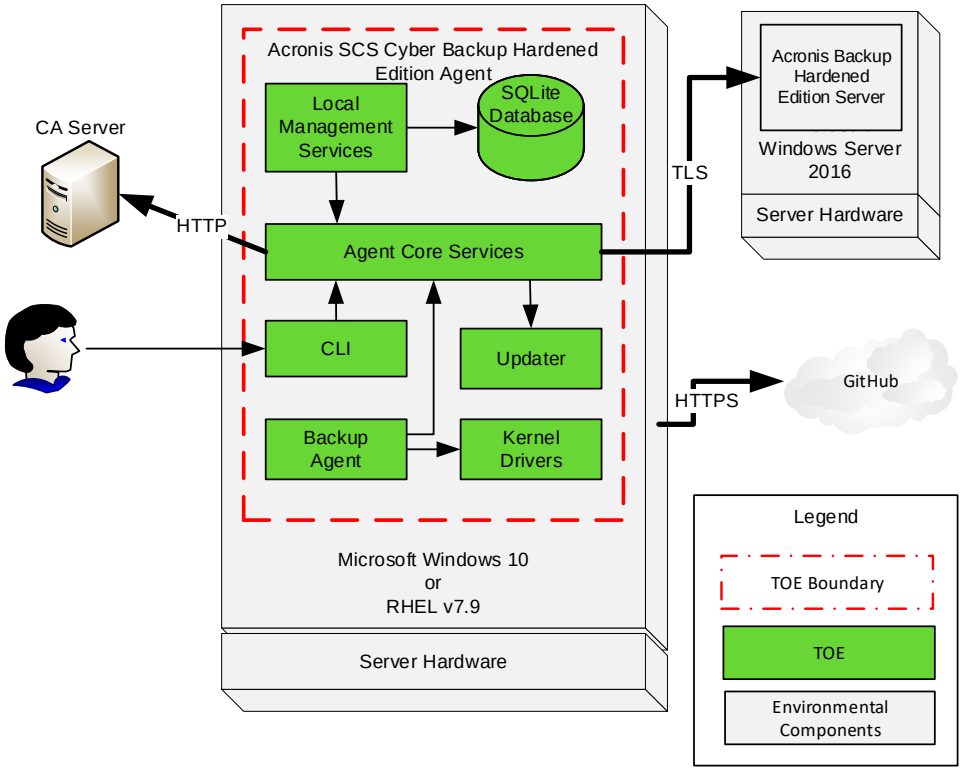

Figure 1 – Physical TOE Boundary

The TOE Boundary includes all the Acronis SCS developed parts of the Acronis SCS Cyber Backup 12.5 Hardened Edition Agent product. Any third-party source code or software that Acronis SCS has modified is considered to be TOE Software.

1.5.1.1 Guidance Documentation

Table 3 lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

Table 3 – Guidance Documentation

Document Name	Description
Acronis Cyber Backup SCS 12.5, Update 4.7	Contains steps for the basic initialization and setup of the TOE. Also contains guidance on how to use and maintain the TOE.
Acronis SCS Cyber Backup 12.5 Hardened Edition Agent Guidance Documentation Supplement Document Version: 0.7	Contains information regarding specific configuration for the TOE evaluated configuration.

1.5.2 Logical Scope

The logical boundary of the TOE is broken down into the following security classes, which are further described in Sections 7 and 8 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes.

1.5.2.1 Cryptographic Support

The TOE provides cryptographic functions to secure sessions between the Management Server and the TOE using TLS v1.2. The Acronis SCS Cryptographic Library and Acronis SCS Protocol Library are used to provide the required algorithms and protocols for all cryptographic operations. The TOE also stores its application token in the Windows Data Protection API (DPAPI) and the Linux keyring, depending on the OS.

1.5.2.2 User Data Protection

The TOE protects sensitive data in non-volatile memory according to the requirements in FCS_STO_EXT.1. The TOE restricts its access to network connectivity provided by the platform's hardware resources. Specifically, it will only use network connectivity for connections from itself to the Management Server and from itself to the CA server. The TOE does not access any of the platform's sensitive information repositories.

1.5.2.3 Identification and Authentication

To facilitate secure communications using TLS, the TOE provides a mechanism to validate X.509v3 certificates as defined by RFC[12] 5280. The TOE uses a CRL to check the certificate's revocation status and will not permit certificates to be used when the CRL is not available or if the certificate is invalid.

1.5.2.4 Security Management

The TOE does not provide default credentials. It uses the service accounts on the platform and does not have an authenticated user interface. The TOE does not provide any management features that write or change settings. Non-security-related settings are stored on the Management Server and are queried when performing tasks. The TOE and its data are protected against unauthorized access by default file permissions. Section 8.1.4 provides a list of security-relevant management functions provided by the TOE.

1.5.2.5 Privacy

The TOE does not transmit personally identifiable information (PII).

1.5.2.6 Protection of the TSF

The TOE does not allocate memory with both write and execute permissions and does not write user-modifiable files to directories that contain executable files. The TOE is compiled with the /GS flag to enable stack-based buffer overflow protection on the Windows Agent and Stack Smashing Protector (SSP) on the Linux Agent. Both agents are compatible with their platform's security features. The TOE uses standard platform APIs and includes only the third-party libraries it needs to perform its functionality. The TOE is versioned with SWID[13] tags that comply with the minimum requirements from ISO[14]/IEC[15] 19770-2:2015 and provides the ability to check for updates to the application software.

[12] RFC – Request for Comments
[13] SWID – Software Identification
[14] ISO – International Organization for Standardization
[15] IEC – International Electrotechnical Commission

The TOE is distributed as an additional software package to the platform OS. The TOE is packaged such that its removal results in the deletion of all traces of the application, except for configuration settings, output files, and audit/log events. The TOE does not download, modify, replace or update its own binary code.

1.5.2.7 Trusted Path/Channels

The TOE provides trusted channels using its cryptographic functions to encrypt transmitted sensitive data. The TOE secures communications using TLS v1.2 between itself and the Management Server.

1.5.3 Product Physical/Logical Features and Functionality not included in the TOE

Features and Functionality that are not part of the evaluated configuration of the TOE are:

- Remote and cloud storage locations
- Cloud configuration deployments
- Functionality of the Management Server
- The backup features of the Agent
- Command line interface

1.5.4 Scope of Evaluation

The evaluation is limited in scope to the secure features described in the *Protection Profile for Application Software v1.4; October 07, 2021* (App PP) and the *Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019* (TLS-PKG) and detailed in Section 1.5.2.

2. Conformance Claims

This section provides the identification for any CC, PP, Technical Decisions (TD), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 9.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 extended; CC Part 3 extended; PP claim to the *Protection Profile for Application Software v1.4; October 07, 2021* conformant; *Functional Package for Transport Layer Security (TLS),* Version 1.1, 12 February 2019.
PP Identification	Exact Conformance[16] to the *Protection Profile for Application Software v1.4; October 07, 2021* and the *Functional Package for Transport Layer Security (TLS),* Version 1.1, 12 February 2019.

Table 5 - Relevant Technical Decisions

Technical Decisions	Applicable (Y/N)	Exclusion Rationale (if applicable)
AS PP		
TD0780 – FIA_X509_EXT.1 Test 4 Clarification	Yes	
TD0756 – Update for platform-provided full disk encryption	Yes	
TD0747 – Configuration Storage Option for Android	Yes	
TD0743 – FTP_DIT_EXT.1.1 Selection exclusivity	Yes	
TD0736 – Number of elements for iterations of FCS_HTTPS_EXT.1	No	The TOE does not claim FCS_HTTPS_EXT.1
TD0719 – ECD for PP APP v1.3 and 1.4	Yes	
TD0717 – Format changes for PP_APP_v1.4	Yes	
~~TD0669 – FIA_X509_EXT.1 Test 4 Interpretation~~	~~No~~	Archived by NIAP
TD0664 – Testing activity for FPT_TUD_EXT.2.2	Yes	
~~TD0659 – Change to Required NIST Curves for FCS_CKM.1/AK~~	~~Yes~~	Archived in TD0717
~~TD0655 – Mutual authentication in FTP_DIT_EXT.1 for SW App~~	~~No~~	Archived by NIAP
TD0650 – Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	No	The PP-Module added is not claimed by the TOE
TD0628 – Addition of Container Image to Package Format	Yes	
~~TD0626 – FCS_COP.1 Keyed Hash Selections~~	~~Yes~~	Archived in TD0717
~~TD0624 – Addition of DataStore for Storing and Setting Configuration Options~~	~~No~~	Archived by NIAP
TLS-PKG		
TD0770 – TLSS.2 connection with no client cert	No	The TOE does not claim FCS_TLSS_EXT.2
TD0739 – PKG_TLS_V1.1 has 2 different publication dates	No	The TOE only implements TLS as a client and is not a TLS server.
TD0726 – Corrections to (D)TLSS SFRs in TLS 1.1 FP	No	The TOE only implements TLS as a client and is not a TLS server.

[16] Exact Conformance is a type of strict conformance such that the set of SFRs and the SPD/Objectives are exactly as presented within the accepted PP and Extended PP without changes.

Technical Decisions	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0588 – Session Resumption Support in TLS package	No	The TOE does not claim FCS_TLSS_EXT.1
TD0513 – CA Certificate loading	Yes	
TD0499 – Testing with pinned certificates	No	The TOE does not support certificate pinning.
TD0469 – Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	No	The TOE does not claim FCS_TLSS_EXT.1
TD0442 – Updated TLS Ciphersuites for TLS Package	Yes	

3. Security Problem Definition

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statements for the TOE security environment's threats, assumptions, and Organizational Security Policies (OSPs) as identified in the App PP.

3.1 Threats

Table 6 describes the threats that the TOE is expected to address as defined in the App PP.

Table 6 – Threats

Threat	Description
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.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.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

3.2 Assumptions

Table 7 describes the assumptions that are assumed to exist in the TOE's operating environment as defined in the App PP.

Table 7 – Assumptions

Assumption	Description
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_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.
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.

3.3 Organizational Security Policies

There are no OSPs defined in the App PP.

4. Security Objectives

This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

Table 8 describes the security objectives that the TOE is required to meet as defined in the App PP.

Table 8 – Security Objectives for the TOE

Objective	Description
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. **Addressed by:** FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_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, FPR_ANO_EXT.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1, FCS_COP.1/Sig
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:** FCS_RBG_EXT.1, FCS_CKM_EXT.1, FTP_DIT_EXT.1, FCS_CKM.1/AK, FCS_CKM.2, FCS_COP.1/SKC, FCS_COP.1/Hash, FCS_COP.1/Sig, FCS_COP.1/KeyedHash, FCS_RBG_EXT.2, FDP_NET_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2
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:** FCS_RBG_EXT.1, FCS_STO_EXT.1, FDP_DAR_EXT.1, FCS_CKM.1/SK, FCS_COP.1/SKC, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RBG_EXT.2
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:** FCS_CKM_EXT.1, FCS_RBG_EXT.1, FCS_STO_EXT.1, FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1, FTP_DIT_EXT.1, FCS_CKM.1/AK, FCS_CKM.2, FIA_X509_EXT.1, FPT_TUD_EXT.2

4.2 Security Objectives for the Operational Environment

Table 9 describes the security objectives that the TOE's operating environment is required to meet as defined in the App PP.

Table 9 – Security Objectives for the Operational Environment

Assumption	Description
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

4.3 Security Objectives Rationale

Please refer to section 4.3 of the App PP for a description of how the assumptions, threats, and organizational security policies map to the security objectives defined in the App PP.

5. Extended Components

This section defines the extended SFRs and extended SARs met by the TOE.

5.1 Extended TOE Security Functional Components

Table 12 in section 7.2 below identifies the extended SFRs implemented by the TOE. These extended SFRs' definitions are not repeated in this ST because they are taken directly from the App PP, PP_APP_v1.4-ECD[17], and TLS-PKG.

5.2 Extended TOE Security Assurance Components

Table 10 identifies the extended SARs claimed for the TOE. These extended SARs' definitions are taken directly from the App PP and are not repeated in this ST.

Table 10 – Extended TOE Security Assurance Components

Name	Description
ALC_TSU_EXT.1	Timely Security Updates

[17] Added to meet TD0719 and include the PP_APP_V1.4-ECD.pdf

6. Security Assurance Requirements

The App PP identifies the SARs to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

This section lists the set of SARs that are required in evaluations against the App PP. The App PP is conformant to Parts 2 (extended) and 3 (extended) of CC V3.1, Revision 5.

As a functional package, the TLS Package does not define its own SARs. The expectation is that all SARs required by the App PP will apply to the entire TOE, including the portions addressed by the TLS Package. Consequently, the evaluation activities specified in the App PP apply to the entire TOE evaluation, including any changes made to them by subsequent NIAP Technical Decisions as summarized in Section1.2.

The TLS Package does contain evaluation activities for how to evaluate its SFR claims as part of the evaluation of AES_TSS.1, AGD_OPE.1, AGD_PRE.1, and ATE_IND.1. All Security Functional Requirement specified by the TLS Package will be evaluated in the manner specified in that package.

The TOE security assurance requirements are identified in Table 11.

Table 11 – Security Assurance Requirements

Assurance Requirements	
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.1)
	Security requirements (ASE_REQ.1)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM[18] coverage (ALC_CMS.1)
	Timely Security Updates (ALC_TSU_EXT.1)
Tests (ATE)	Independent testing – Conformance (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)

[18] CM – Configuration Management

7. Security Functional Requirements

The individual SFRs are specified in the sections below. SFRs in this section are mandatory SFRs that any conformant TOE must meet. Based on selections made in these SFRs, it will also be necessary to include some of the selection-based SFRs in Appendix B. Optional or Objective SFRs may also be adopted from those listed in Appendix A and Appendix C respectively.

The Assurance Activities defined in App PP describe actions that the evaluator will take in order to determine compliance of a particular TOE with the SFRs. The content of these Assurance Activities will therefore provide more insight into deliverables required from TOE Developers.

7.1 Conventions

The conventions used in descriptions of the SFRs are as follows:

- Refinement: Indicated with bold text (e.g., [**refinement**]).
- Selection: Indicated with underlined text surrounded by brackets (e.g., [selection]).
- Assignment: Indicated with italicized text surrounded by brackets (e.g., [*assignment*]).
- Assignment within a Selection: Indicated with italicized and underlined text surrounded by brackets (e.g., [*assignment within a selection*]).
- Refinement within a Selection: Indicated with bold and underlined text surrounded by brackets (e.g., [**assignment within a selection**]).
- **Iteration** operation: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."
- Extended SFRs are identified by having a label 'EXT' at the end of the SFR name.

Operations such as assignments and selections performed by the PP author are identified as shown above; however, they do not appear within brackets. This is done intentionally to delineate between selections or assignments made by the PP author and those made by the ST author. No refinements have been made by the ST author other than grammatical and formatting corrections, or those made in places where a table reference differs from that of the PP.

7.2 Security Functional Requirements

This section specifies the SFRs for the TOE and organizes the SFRs by CC class. Table 12 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement. Note that some column headers use the following abbreviations: S=Selection; A=Assignment; R=Refinement; I=Iteration.

Table 12 – TOE Security Functional Requirements

Name	Description	S	A	R	I
Required SFRs					
FCS_RBG_EXT.1	Random Bit Generation Services	✓			
FCS_CKM_EXT.1	Cryptographic Key Generation Services	✓			
FCS_STO_EXT.1	Storage of Credentials	✓	✓		
FDP_DAR_EXT.1	Encryption of Sensitive Application Data	✓			
FDP_DEC_EXT.1	Access to Platform Resources	✓	✓		

Name	Description	S	A	R	I
FDP_NET_EXT.1	Network Communications	✓	✓		
FMT_CFG_EXT.1	Secure by Default Configuration				
FMT_MEC_EXT.1	Supported Configuration Mechanism				
FMT_SMF.1	Specification of Management Functions	✓	✓		
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information	✓			
FPT_AEX_EXT.1	Anti-Exploitation Capabilities	✓	✓		
FPT_API_EXT.1	Use of Supported Services and APIs				
FPT_IDV_EXT.1	Software Identification and Versions	✓	✓		
FPT_LIB_EXT.1	User of Third Party Libraries		✓		
FPT_TUD_EXT.1	Integrity for Installation and Update	✓			
FTP_DIT_EXT.1	Protection of Data in Transit	✓			
Selection-based SFRs					
FCS_CKM.1/AK	Cryptographic Asymmetric Key Generation	✓		✓	✓
FCS_CKM.2	Cryptographic Key Establishment	✓		✓	
FCS_COP.1/SKC	Cryptographic Operation – Encryption/Decryption	✓		✓	✓
FCS_COP.1/Hash	Cryptographic Operation – Hashing	✓		✓	✓
FCS_COP.1/Sig	Cryptographic Operation – Signing	✓		✓	✓
FCS_COP.1/KeyedHash	Cryptographic Operation – Keyed-Hash Message Authentication	✓	✓	✓	✓
FCS_RBG_EXT.2	Random Bit Generation from Application	✓			
FCS_TLS_EXT.1	TLS Protocol	✓			
FCS_TLSC_EXT.1	TLS Client Protocol	✓			
FCS_TLSC_EXT.4	TLS Client Support for Renegotiation				
FCS_TLSC_EXT.5	TLS Client Support for Supported Groups Extension	✓			
FIA_X509_EXT.1	X.509 Certificate Validation	✓			
FIA_X509_EXT.2	X.509 Certificate Authentication	✓			
FPT_TUD_EXT.2	Integrity for Installation and Update				

7.2.1 Class FCS: Cryptographic Support

FCS_CKM.1/AK Cryptographic Asymmetric Key Generation

***FCS_CKM.1.1*/AK**

The application shall [

- *implement functionality*

] **to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm** [

- ***[RSA[19] schemes]*** *using cryptographic key sizes of* ***2048 bit or greater*** *that meet the following:* ***[FIPS PUB[20] 186-4, "Digital Signature Standard (DSS)", Appendix B.3]***,

[19] RSA – Rivest, Shamir, Adleman

[20] PUB – Publication

- ***[ECC[21] schemes]*** *using [**"NIST[22] curves" P-384 and [P-256, P-521]** that meet the following: **FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4]*[23]

].

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: [

- **RSA-based key establishment schemes** that meets the following: **RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1",**
- **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",**

].

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall [

- implement asymmetric key generation

].

FCS_COP.1/SKC Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/SKC

The **application** shall perform [*encryption/decryption*][24] in accordance with a specified cryptographic algorithm [

- AES[25]-GCM[26] (as defined in NIST SP[27] 800-38D) mode

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

FCS_COP.1/Hash Cryptographic Operation – Hashing

FCS_COP.1.1/Hash

The **application** shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [

- SHA[28]-256
- SHA-384

] and **message digest** sizes [

- 256
- 384

] **bits** that meet the following: [FIPS Pub 180-4][29].

---

[21] ECC – Elliptic Curve Cryptography
[22] NIST – National Institute of Standards and Technology
[23] Non-impactful updates as per TD0717: Format changes for PP_APP_v1.4
[24] Updated as per TD0717: format changes for PP_APP_V1.4
[25] AES – Advanced Encryption Standard
[26] GCM – Galois Counter Mode
[27] SP – Special Publication
[28] SHA – Secure Hash Algorithm
[29] Non-impactful updates as per TD0717: Format changes for PP_APP_v1.4

FCS_COP.1/Sig Cryptographic Operation – Signing

FCS_COP.1.1/Sig

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

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

].[30]

FCS_COP.1/KeyedHash Cryptographic Operation – Keyed-Hash Message Authentication

FCS_COP.1.1/KeyedHash

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

- HMAC[31]-SHA-256
- HMAC-SHA-384

] and [

- *no other algorithms*

] with key sizes [*256, 384*] and message digest sizes 256 and [384] **and** [no other size] **bits** that meet the following: [FIPS Pub 198-1, '*The Keyed-Hash Message Authentication Code'* and FIPS Pub 180-4 '*Secure Hash Standard'*.][32]

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [implement DRBG[33] 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[34]_DRBG (AES)].

FCS_RBG_EXT.2.2

The deterministic RBG[35] shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [a hardware-based 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_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1

The application shall [invoke the functionality provided by the platform to securely store [*the application token*]] to non-volatile memory.

FCS_TLS_EXT.1 TLS Protocol

FCS_TLS_EXT.1.1

The product shall implement [TLS as a client].

---

[30] Updated as per TD0717: format changes for PP_APP_V1.4

[31] HMAC – Hash-based Message Authentication Code

[32] Updated as per TD0717: Format changes for PP_APP_V1.4

[33] DRBG – Deterministic Random Bit Generator

[34] CTR – Counter Mode

[35] RBG – Random Bit Generation

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1

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

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE[36]_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,

] and also supports functionality for [session renegotiation].

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.4 TLS Client Support for Renegotiation

FCS_TLSC_EXT.4.1

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

FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension

FCS_TLS_EXT.5.1

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

- secp256r1,
- secp384r1,
- secp521r1,

].

7.2.2 Class FDP: User Data Protection

FDP_DAR_EXT.1 Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1

The application shall [protect sensitive data in accordance with FCS_STO_EXT.1] in non-volatile memory.[37]

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].

[36] ECDHE – Elliptic Curve Diffie Hellman Ephemeral

[37] TD0756: Update for platform-provided full disk encryption applies

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- [*application-initiated TLS connections to the Management Server for configuration updates and HTTP network communication for access to a CA server*]

].

7.2.3 Class FIA: Identification and Authentication

FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1

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

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field.
- The application shall validate the revocation status of the certificate using [CRL as specified in RFC 5280 Section 6.3]
- The application shall validate the extendedKeyUsage (EKU) 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 EKU 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 EKU 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 EKU 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 EKU field.[38]
  - 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 EKU 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.

[38] TD0780: FIA_X509_EXT.1 Test 4 Clarification Applies

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 [not accept the certificate].

7.2.4 Class FMT: Security Management

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

FMT_MEC_EXT.1.1

The application shall [invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.][39]

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [

- *no management functions*]

].

7.2.5 Class FPR: Privacy

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].

7.2.6 Class FPT: Protection of the TSF

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 [*OpenSSL runtime integrity test*].

FPT_AEX_EXT.1.2

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

[39] Non-impactful updates as a result of TD0747: Configuration Storage Option for Android as there is no change to how it is evaluated

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_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1

The application shall be versioned with [SWID tags that comply with minimum requirements from ISO/IEC 19770-2:2015].

FPT_LIB_EXT.1 User of Third Party Libraries

FPT_LIB_EXT.1.1

The application shall be packaged with only [*the list of third-party libraries in Appendix B: Included Third-Party Libraries*].

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1

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

FPT_TUD_EXT.1.2

The application shall [leverage the platform] 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 ~~it's~~ the application 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].[40]

[40] Updated as per TD0628: Addition of Container Image to Package Format

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_TUD_EXT.2.3

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

7.2.7 Class FTP: Trusted Path/Channel

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall [

- *encrypt all transmitted [sensitive data] with [TLS as a client as defined in the Functional Package for TLS for [the Management Server][41]]*

] between itself and another trusted IT[42] product.

[41] TD0743: FTP_DIT_EXT.1.1 Selection exclusivity applies

[42] IT – Information Technology

8. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

8.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 13 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Function	SFR	Description
Cryptographic Support	FCS_CKM.1/AK	Cryptographic Asymmetric Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM_EXT.1	Cryptographic Key Generation Services
	FCS_COP.1/SKC	Cryptographic Operation – Encryption/Decryption
	FCS_COP.1/Hash	Cryptographic Operation – Hashing
	FCS_COP.1/Sig	Cryptographic Operation – Signing
	FCS_COP.1/KeyedHash	Cryptographic Operation – Keyed-Hash Message
	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.4	TLS Client Support for Renegotiation
	FCS_TLSC_EXT.5	TLS Client Support for Supported Groups Extension
User Data Protection	FDP_DAR_EXT.1	Encryption of Sensitive Application Data
	FDP_DEC_EXT.1	Access to Platform Resources
	FDP_NET_EXT.1	Network Communications
Identification and Authentication	FIA_X509_EXT.1	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
Security Management	FMT_CFG_EXT.1	Secure by Default Configuration
	FMT_MEC_EXT.1	Supported Configuration Mechanism
	FMT_SMF.1	Specification of Management Functions
Privacy	FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
Protection of the TSF	FPT_AEX_EXT.1	Anti-Exploitation Capabilities
	FPT_API_EXT.1	Use of Supported Services and APIs
	FPT_IDV_EXT.1	Software Identification and Versions

TOE Security Function	SFR	Description
	FPT_LIB_EXT.1	User of Third Party Libraries
	FPT_TUD_EXT.1	Integrity for Installation and Update
	FPT_TUD_EXT.2	Integrity for Installation and Update
Trusted Path / Channels	FTP_DIT_EXT.1	Protection of Data in Transit

8.1.1 Cryptographic Support

The TOE implements the Acronis SCS Cryptographic Library to provide the required algorithms for all cryptographic operations. Each of the cryptographic algorithms supported by the TOE have been tested and certified by the CAVP[43]. See Table 14 below for the cryptographic operations implemented by the TOE.

Table 14 – Cryptographic Algorithms and Key Sizes

Cryptographic Operation	Usage	Algorithm	Key Lengths / Curves / Moduli	Certificate
Encryption/Decryption	TLS	AES-GCM	128, 256	CAVP C1351 CAVP A4299
Key Pair Generation	TLS	RSA	2048, 3072	CAVP C1351 CAVP A4299
		ECDSA	NIST P curves with sizes 256, 384, and 521	CAVP C1351 CAVP A4299
Digital Signature Generation Digital Signature Verification	TLS	RSA	2048, 3072	CAVP C1351 CAVP A4299
Key Establishment	TLS	RSA	2048, 3072, 4096	None
		ECDHE	NIST P curves with sizes 256, 384, and 521	CAVP C1351 CAVP A4299
Message Digest	TLS	SHA-256, SHA-384	256, 384	CAVP C1351 CAVP A4299
Message Authentication	TLS	HMAC-SHA-256, HMAC-SHA-384	256, 384	CAVP C1351 CAVP A4299
Deterministic Random Bit Generation	DRBG	CTR_DRBG (AES)	256	CAVP C1351 CAVP A4299

FCS_CKM_EXT.1 and FCS_CKM.1/AK

The TOE implements asymmetric key generation. The schemes implemented by the TOE to generate asymmetric cryptographic keys for key establishment and entity authentication are the RSA and ECC schemes. The RSA keys and key sizes listed in Table 14 are generated for key establishment and entity authentication for TLS. The ECDHE keys and NIST P curves listed in Table 14 are generated for key establishment and entity authentication for TLS. Both RSA and ECC key generation schemes that are implemented by the TOE meet FIPS PUB 186-4.

FCS_CKM.2

The TOE implements both RSA and elliptic curve-based key establishment schemes for TLS. The RSA-based schemes meet RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017. The elliptic-curve based schemes for ECDHE meet NIST SP-800 56A. The key sizes and curves used for the key establishment schemes are listed in Table 14.

[43] CAVP – Cryptographic Algorithm Validation Program

FCS_COP.1/SKC
The TOE performs AES encryption and decryption for TLS v1.2 trusted channel communications. The AES algorithm operates in GCM mode with key sizes of 128 and 256 bits. In TLS sessions, the TOE acts as a TLS client for connections to the Management Server from itself. Please refer to **FCS_TLSC_EXT.1** for more information on the implementation of the TLS protocol.

FCS_COP.1/Hash and FCS_COP.1/KeyedHash
Hashing services are performed by the TOE with the SHA-256 and SHA-384 algorithms and the message digest sizes of 256 and 384 in accordance with FIPS Pub 180-4. The hash functions are used with other TOE cryptographic functions, including digital signature verification and MACs[44]. The HMAC-SHA-256 cryptographic algorithm uses the SHA-256 hash function with a cryptographic key size of 256 bits and 256-bit message digest size in accordance with FIPS Pub 198-1. The HMAC-SHA-384 cryptographic algorithm uses the SHA-384 hash function with a cryptographic key size of 384 bits and 384-bit message digest size in accordance with FIPS Pub 198-1.

FCS_COP.1/Sig
For signature generation and verification, the TOE uses the RSA algorithm. The RSA algorithm meets FIPS PUB 186-4 Section 4 and uses the key sizes of 2048 and 3072 bits. The RSA algorithm is used for TLS connections.

FCS_RBG_EXT.1 and FCS_RBG_EXT.2
The TOE implements the SP 800-90A CTR_DRBG (AES) for all deterministic random bit generation services. The CTR_DRBG is seeded with a minimum of 256 bits of entropy via RDRAND that accumulates entropy from the Intel DRNG. The entropy received from the Intel DRNG is assumed to be 100% entropic. The amount of entropy used to seed the CTR_DRBG corresponds to the greatest security strength of the algorithms included in the ST (AES-256). Refer to Tables 2 and 3 of NIST SP 800-57A for more information on the algorithm security strengths.

FCS_STO_EXT.1
The TOE leverages the Windows Data Protection API (DPAPI) to securely store the TOE's application token for the Windows Agent. On Linux, the application token is securely stored using the Linux keyring. The application token is used by the TOE to identify itself to the Management Server when downloading configuration settings. The initial application token is generated by the Management Server when the TOE is installed and added as a device to the Management Server.

FCS_TLS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.4, and FCS_TLSC_EXT.5
The TOE only implements TLS as a client and is not a TLS server.

The TOE implements client-side TLS v1.2 for secure connections from itself to the Management Server. The client-side TLS v1.2 connections support the following cipher suites:

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

The TOE looks for the common name in the subject name or the DNS name in the Subject Alternative Name (SAN) of the server's certificate as the identifier for the Management Server. The reference identifier is established during installation when the Management Server's name is entered in the connection information. Use of IP addresses and wildcards as the identifiers is supported but are discouraged as identifiers. When constructing the

[44] MAC – Message Authentication Code

certificate, the SAN is mandated for IP identifiers and not mandated for DNS identifiers. The use of certificate pinning is not supported.

If the server's certificate is not valid, the TOE will not establish a connection.

The TOE also supports functionality for session renegotiation. The TOE supports the `renegotiation_info` TLS extension in accordance with RFC 5746. It includes the `renegotiation_info` extension in `ClientHello` messages.

The TOE uses its Acronis SCS Cryptographic Library to support elliptic curves in TLS and presents the Supported Groups Extension in the `ClientHello` with NIST curves secp256r1, secp384r1, and secp521r1.

TOE Security Functional Requirements Satisfied: FCS_CKM.1/AK, FCS_CKM.2, FCS_CKM_EXT.1, FCS_COP.1/SKC, FCS_COP.1/Hash, FCS_COP.1/Sig, FCS_COP.1/KeyedHash, FCS_RBG_EXT.1, FCS_RBG_EXT.2, FCS_STO_EXT.1, FCS_TLS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.4, FCS_TLSC_EXT.5

8.1.2 User Data Protection

FDP_DAR_EXT.1
The TOE protects sensitive data in accordance with FCS_STO_EXT.1 when it is stored in non-volatile memory. The application token used to identify the TOE to the Management Server is the only sensitive data that the TOE stores. No other forms of sensitive data are stored by the TOE. The TOE runs as a service in the evaluated configuration and does not require any user credentials to operate.

FDP_DEC_EXT.1 and FDP_NET_EXT.1
The TOE restricts its access to platform hardware resources to network connectivity. This is for the TLS connections described in FCS_TLSC_EXT.1 and the HTTP connections to the CA server in the TOE environment. The TLS connection includes the TOE initiating a TLS v1.2 connection to the Management Server's API Gateway. The TOE initiates communication with the CA server when performing certificate revocation checking. The ports utilized by the TOE are as follows:

- Port 9877: Management Server authentication and token retrieval
- Port 7780: Asynchronous communication between the Management Server and the TOE

The TOE does not access any of the sensitive information repositories on the host platform.

TOE Security Functional Requirements Satisfied: FDP_DAR_EXT.1, FDP_DEC_EXT.1, FDP_NET_EXT.1

8.1.3 Identification and Authentication

FIA_X509_EXT.1 and FIA_X509_EXT.2
The TOE uses X.509v3 certificates as defined by RFC 5280 when it acts as a TLS client for TLS. The TOE does not support TLS mutual authentication but will validate the Management Server's certificate before establishing a connection. The TOE implements the following rules when validating the Management Server's certificate when connecting to it:

- Certificate validation and certificate path validation as per RFC 5280.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.

- The application shall validate that any CA certificate includes the `caSigning` purpose in the key usage field.
- The application shall validate the revocation status of the certificate using a CRL as specified in RFC 5280 Section 6.3.
- The application shall reject expired certificates.
- The application shall validate the extendedKeyUsage field according to the following rules:
    - 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.

If the TOE cannot establish a connection to the CA server's CRL to determine the revocation status of a certificate, it does not accept the certificate.

TOE Security Functional Requirements Satisfied: FIA_X509_EXT.1, FIA_X509_EXT.2

8.1.4 Security Management

FMT_CFG_EXT.1
The TOE does not install with any default credentials. Rather, it uses the platform's service accounts to run and is available to any user logged into the platform. It is configured by default with file permissions that protect the application binaries and data files from modification by normal unprivileged users. This prevents a standard user from modifying the application or its data files.

FMT_MEC_EXT.1
The TOE does not store or set any security-related settings. Non-security-related settings are stored on the Management Server and are queried when performing tasks. The TOE does not provide any management features that write or change settings.

FMT_SMF.1
The TOE does not perform any management functions.

TOE Security Functional Requirements Satisfied: FMT_CFG_EXT.1, FMT_MEC_EXT.1, FMT_SMF.1

8.1.5 Privacy

FPR_ANO_EXT.1
The products primary function is to backup and restore data, which may include PII. The TOE does not prompt for or require user-supplied PII to perform its designed functionality, nor does it transmit any such PII over a network; therefore, the requirement does not apply to this PII.

TOE Security Functional Requirements Satisfied: FPR_ANO_EXT.1

8.1.6 Protection of the TSF

FPT_AEX_EXT.1
The TOE does not make requests to map memory at an explicit address, except for the OpenSSL integrity test, and is compiled with ASLR enabled. The TOE does not allocate any memory regions with write and execute permissions. The TOE is compatible with the platform's security features. More specifically, the application can run successfully with Windows Defender Exploit Guard configured with the following minimum mitigations enabled: Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The TOE is also compatible with SELinux enabled and in enforcing mode. The TOE does not write user-modifiable files to directories that contain executable files. The Windows Agent is compiled with the /GS flag enabled by default for stack-based buffer overflow protection and the /NXCOMPAT flag to enable DEP protections for the application. The Linux Agent uses the __stack_chk_fail symbol in ELF executable files for stack-based buffer overflow protection.

FPT_API_EXT.1
The TOE uses only the documented platform APIs listed in Appendix A: Supported Platform APIs.

FPT_IDV_EXT.1
The TOE is versioned with SWID tags that comply with the minimum requirements from ISO/IEC 19770-2:2015.

FPT_LIB_EXT.1
The TOE is packaged with the third-party libraries listed in Appendix B: Included Third-Party Libraries.

FPT_TUD_EXT.1.1 and FPT_TUD_EXT.1.2
The TOE leverages the platform to check for updates and patches to the application software. To check for an update, the user of the platform runs a set of commands. If the version in the Acronis repository matches the version of the TOE, then no action is required. If the version in the repository is greater than the TOE version, then the updated should be downloaded to the platform.

FPT_TUD_EXT.1.3 and FPT_TUD_EXT.1.4
The TOE does not download, modify, replace or update its own binary code. The TOE's Windows and Linux installation packages and its updates are digitally signed so that the platform can verify their signatures before installation. The packages are digitally signed using a 2048-bit RSA key and SHA-256 digest algorithm. The authorized sources of the Linux and Windows installer signatures are Acronis International GmbH, issued by GlobalSign and Acronis SCS, Inc., issued by DigiCert respectively.

FPT_TUD_EXT.1.5 and FPT_TUD_EXT.2
The TOE is distributed as an additional software package to the platform OS. The Windows Agent is packaged in the standard executable (.exe) format and the Linux Agent is packaged as an executable binary (.x86_64). The TOE is 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.

TOE Security Functional Requirements Satisfied: FPT_AEX_EXT.1, FPT_API_EXT.1, FPT_IDV_EXT.1, FPT_LIB_EXT.1, FPT_TUD_EXT.1, FPT_TUD_EXT.2

8.1.7 Trusted Path/Channels

FTP_DIT_EXT.1
The TOE encrypts all transmitted sensitive data between itself and the Management Server with TLSv1.2. Please refer to the section **FCS_TLSC_EXT.1** for more details. Sensitive data is defined as all data except communications with the CA server to check for certificate revocation.

The Acronis Managed Machine Service provides backup, recovery, replication, retention, and validation functionality. The port used by this service is port 9850, and it is required to be running for the TOE to function.
TOE Security Functional Requirements Satisfied: FTP_DIT_EXT.1

8.2 Timely Security Updates

To keep the TOE secure, Acronis SCS plans to fix security issues depending on the following severity:

- Critical: hotfix and workaround are immediately required.
- High: hotfix or nearest update, if update is within 3-4 weeks (15-20 business days).
- Low-Medium: next major version or update.

Issue severity is calculated according to CVSSv3 methodology. For some issues a custom severity can be set by security team when CVSSv3 is not appropriate. For example, privacy issues may be prioritized far higher than the CVSS score.

If issue was reported by a 3rd-party and therefore is subject to public disclosure, the fixes are released within the negotiated disclosure period.

Acronis SCS discloses the following information for vulnerabilities:

- Release Notes will contain information that security issues were fixed in a specific release or update.
- Release Notes will contain issue IDs and severity in a qualitative form if they are worth mentioning.
- In special cases, the details of security issues may be disclosed to customers when it's important to let customers know if their systems/data are at risk.
- Acronis SCS will not disclose details of vulnerabilities in documentation.

The Acronis SCS Support team notifies customers about security issues related to the TOE in following cases:

1. Issue severity is Critical
2. Issue severity is High and the issue is known to 3rd-party (external report or a known exploitation).

The notification will be sent to the most relevant group of customers and include enough information to understand the following:

1. The risk associated with the issue
2. Conditions under which a customer's system is vulnerable
3. Necessary steps to mitigate the risk

Customers that purchase the TOE may email appsupport@acronisscs.com to report security issues pertaining to the TOE. A public key and disclosure policy are posted to the Acronis SCS GitHub (https://github.com/acronisscs/public_disclosure) for use in securing the contents of any security related email.

Any update that is released, related to security fixes or not, is deployed to the Acronis SCS website for download. Customers may refer to the email or use the check for update process to see if a new version is available for their installation. Updates can then be downloaded and applied to the TOE as needed.

9. Rationale

9.1 Conformance Claims Rationale

This Security Target extends Part 2 and extends to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 5. This ST conforms to the App PP and TLS-PKG.

9.1.1 Variance Between the PP and this ST

There is no variance between the App PP, TLS-PKG, and this ST.

9.1.2 Security Assurance Requirements Rationale

The assumptions, threats, OSPs, and objectives defined in this ST are those specified in the App PP and TLS-PKG. This ST maintains exact conformance to the App PP and TLS-PKG, including the assurance requirements listed in Section 5 of the App PP. The TOE is a standalone application that runs on a Windows and Linux desktop platforms and is applicable to the App PP and TLS-PKG.

10. Acronyms

Table 15 defines the acronyms used throughout this document.

Table 15 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
App PP	Protection Profile for Application Software v1.4; October 07, 2021
ASLR	Address Space Layout Randomization
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
CFG	Control Flow Guard
CM	Configuration Management
CTR	Counter Mode
DEP	Data Execution Protection
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EAF	Export address filtering
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie Hellman Ephemeral
FIPS	Federal Information Processing Standard
GB	Gigabyte
GCM	Galois Counter Mode
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IAF	Import address filtering
ID	Identification
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
CCTL	Common Criteria Testing Laboratory
MAC	Message Authentication Code
MB	Megabyte
N/A	Not Applicable
NIST	National Institute of Standards and Technology

Acronym	Definition
OS	Operating System
OSP	Organizational Security Policy
PII	Personally Identifiable Information
PP	Protection Profile
PUB	Publication
RAM	Random Access Memory
RBG	Random Bit Generation
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
SWID	Software Identification
TD	Technical Decisions
TLS	Transport Layer Security
TLS-PKG	Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019
TOE	Target of Evaluation
UI	User Interface
VM	Virtual Machine

Appendix A: Supported Platform APIs

The following is a list of the supported platform APIs that the TOE uses:

- For Windows:
  - ReadFile
  - WriteFile
  - NtQueryInformationFile
  - UnlockFile
  - LockFile
  - Send
  - Recv
  - RegQueryInfoKeyA
  - RegOpenKey
  - RegSetInfoKey
  - RegQueryValue
  - RegCloseKey
  - RegQueryMutlipleValueKey
  - ExitThread
  - CreateThread
- For Linux:
  - mount
  - mkdir
  - exec
  - mv
  - sudo
  - chroot
  - uname
  - gawk
  - echo
  - cp

Appendix B: Included Third-party Libraries

Table 16 provides a list of the included third-party libraries that the Windows Agent uses.

Table 16 – Included Third-party Windows Libraries

Library	Library	Library
curl.dll	libevent.dll	re2.dll
expat.dll	libmagic.dll	sqlite3.dll
python35.dll	xerces_c.dll	tcmalloc.dll
icu38.dll	mspack.dll	ulxmlrpcpp.dll
icudt38.dll	onig.dll	winpthreads4.dll
libcrypto10.dll	libssl10.dll	

Table 17 provides a list of the included third-party libraries that the Linux Agent uses.

Table 17 – Included Third-party Linux Libraries

Library	Library	Library
_ctypes.so	libcurl.so	libsqlite3.so
_multiprocessing.so	libdbus-1.so	libssl10.so
_psycopg.so	liblibevent.so	libtcmalloc.so
_socket.so	libexpat.so	ujson.so
_sqlite3.so	libjwt.so	libulxmlrpcpp.so
_ssl.so	pyexpat.so	unicodedata.so
libaio.so	libpython35.so	libunwind.so
libcrypto10.so	libre2.so	libzstd.so
libicu38.so	select.so	liblibcrypto10.so
libicudt38.so	liblibssl10.so	

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com