Kaseya US Sales, LLC

Virtual System Administrator Cryptographic Module

Software Version: 1.0

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 1
Document Version: 1.0

Prepared for:

Kaseya US Sales, LLC
901 N. Glebe Road, Suite 1010
Arlington, VA 22203
United States of America

Phone: +1 (415) 694-5700
http://www.kaseya.com

Prepared by:

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 (703) 267-6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Virtual System Administrator Cryptographic Module from Kaseya US Sales, LLC. This Security Policy describes how the Virtual System Administrator Cryptographic Module meets the security requirements of FIPS (Federal Information Processing Standards) 140-2 and how to run the module in a secure FIPS 140-2 mode. This policy was prepared as part of the Level 1 FIPS 140-2 validation of the module.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) details the U.S. and Canadian Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by National Institute of Standards and Technology (NIST) and Communication Security Establishment Canada (CSEC): http://csrc.nist.gov/groups/STM/index.html.

The Virtual System Administrator Cryptographic Module (VSACM) is referred to in this document as the Kaseya VSACM, crypto module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Kaseya website http://www.kaseya.com contains information on the full line of products from Kaseya.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package provided to the Cryptographic Module Testing Laboratory. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Model
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Kaseya. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Kaseya and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Kaseya.

2 Kaseya VSACM

2.1 Overview

Kaseya was founded with the goal of simplifying and automating Information Technology (IT) management, providing a single congruent and highly integrated solution which covers an ever-expanding set of IT management tasks. The Kaseya Virtual System Administrator (VSA) product is intended to satisfy this goal, providing automated, secure remote monitoring, management, and protection of IT resources.

The Kaseya Virtual System Administrator provides an IT automation framework allowing IT managers to proactively monitor, manage, maintain, and protect distributed IT resources using a single, integrated web-based interface. The services offered by Kaseya Virtual System Administrator are ever-broadening; as IT management services needs increase, so do the tools and services provided by the framework. In addition, the number of managed endpoints, which in this context are individual machines (laptops, desktops, servers, etc.), is also rapidly expanding. The current number of managed endpoints supported is approximately 20,000; however, Kaseya is moving quickly towards the ability to manage an unlimited number of endpoints.

2.1.1 Virtual System Administrator Server

The VSA Server is the central management component of the Kaseya Virtual System Administrator. As shown in Figure 1, the VSA Server includes the following components:

- KServer, which is the main Kaseya management application
- Microsoft IIS[1]
- ASP[2] framework
- Microsoft SQL[3] server, which communicates with a database through OLEDB (Object Linking and Embedding Database) and ODBC (Open Database Connectivity)
- Administrator authentication functionality implemented in JavaScript

The primary VSA Server administrative interface is provided via a web-based application, allowing remote access to the majority of administrative services. The web pages for the web-based Graphical User Interface (GUI) are served to administrator workstations via HTTP[4] or HTTPS[5]. In addition, the VSA also provides an API[6], allowing third-party application integration. The API exposes the majority of the actions and functionality available from the web GUI.

The KServer component contains the core set of VSA Server functionality, providing policy configuration and deployment to the Agents, who then use the policies to automatically manage their host endpoint. By using the management interfaces provided by the KServer component the following Kaseya Virtual System Administrator management services are realized:

- Endpoint policy creation and deployment
- Endpoint monitoring and auditing
- Automatic Agent deployment for new endpoints
- Endpoint antivirus and malware management
- Endpoint patch management

[1] Internet Information Services
[2] Active Server Pages
[3] Structured Query Language
[4] Hypertext Transfer Protocol
[5] Hypertext Transfer Protocol Secure
[6] Application Programming Interface

- Endpoint performance management

The KServer component also allows an operator to perform real-time audits, virus scans, and management actions such as manually setting up tasks for individual Agents.

2.1.2 Virtual System Administrator Agent

The Kaseya Virtual System Administrator Agents are software applications installed on the managed endpoints (Macintosh, Windows, or Linux-based General Purpose Computer (GPC)) and servers. Agents are the components which enact the endpoint management activities driven by VSA Server activities. The Agent management activities driven by the VSA Server typically include the following:

- Automated software patching
- Automated network policy enforcement
- Automated antivirus scans and definition updates
- Automated data backup and recovery
- Automated system inventory, monitoring, and reporting
- Remote control services

All Agent activities are driven by policies or requested tasks generated on the Virtual System Administrator Server; however, the Agent must first connect to the VSA Server. The VSA Server component acts solely as a server and will never initiate a connection to the Agent.

2.2 Security

The Kaseya Virtual System Administrator includes security functionality which provides both confidentiality and data authentication techniques to securely manage endpoints. This security functionality is described at a high-level in the following two sections.

2.2.1 VSA Server Security

The VSA Server uses security functionality over two different interfaces: (1) a TCP/IP[7] connection to securely communicate with and authenticate to the Agents and (2) the administrator HTTP/HTTPS interface which requires authentication:

- **Agent-to-VSA Server communication:** All data sent between the VSA Server and Agents is sent via Transmission Control Protocol (TCP). Before the data is sent, Agents are first authenticated to the VSA Server using a proprietary shared secret-based authentication mechanism which incorporates Secure Hashing Algorithm (SHA-256). Authenticated data is sent encrypted using the Advanced Encryption Standard (AES) block cipher within the VSA Server or Agent host computer and then sent over the TCP connection. In general, the data will consist of Agent control input, IT management policies, and Agent reporting data.
- **Administrator Authentication:** Services on the VSA Server can be accessed either locally or remotely. In order to securely authenticate an operator, the VSA Server uses a proprietary authentication mechanism incorporating the SHA-256. Within this mechanism, passwords entered on the Administrator PC (Personal Computer) are SHA-256 hashed before they are output. This ensures that the passwords are never output; only secure hashes of the passwords are output.

[7] Transmission Control Protocol/Internet Protocol

2.2.2 Agent Security

Agents communicate securely with the VSA Server over a TCP/IP port (default TCP port is 5721). The security provided over this interface is provided by a Kaseya-proprietary protocol which utilizes AES to provide confidentiality and authentication of the Agents to the VSA Server.

- **Authentication:** Authentication is provided via a proprietary shared secret-based authentication mechanism which incorporates SHA-256.
- **Confidential Communication:** All communications provided between the Agent and VSA Server are encrypted using AES, which is implemented by the Kaseya VSA Cryptographic Module.

Figure 1 provides an overview of the VSA system components and configuration, while Figure 2 below provides a logical diagram of the VSACM. Note that the cryptographic boundary is depicted in each figure with a red dotted line.

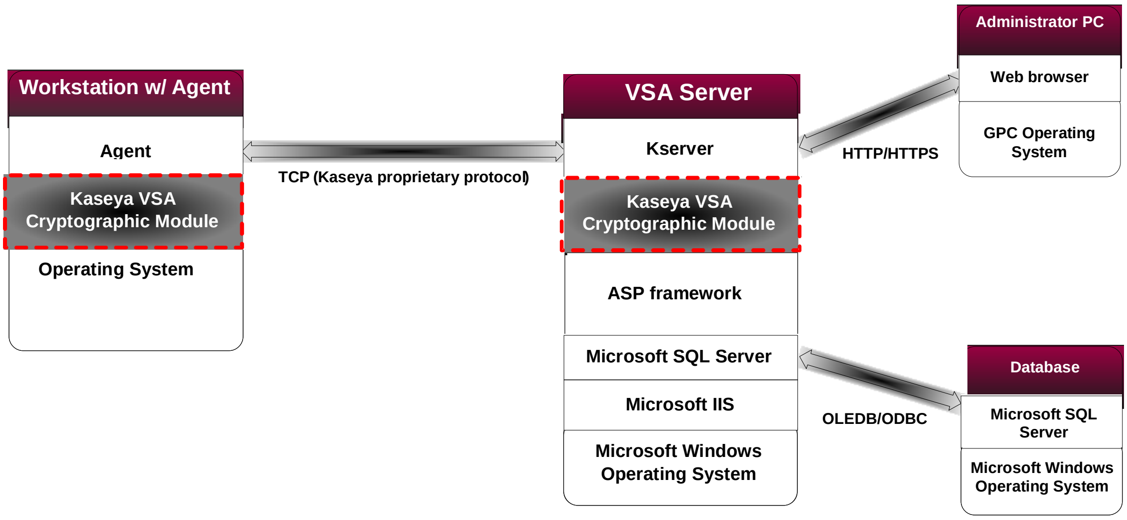

Figure 1 – Kaseya Virtual System Administrator System Overview

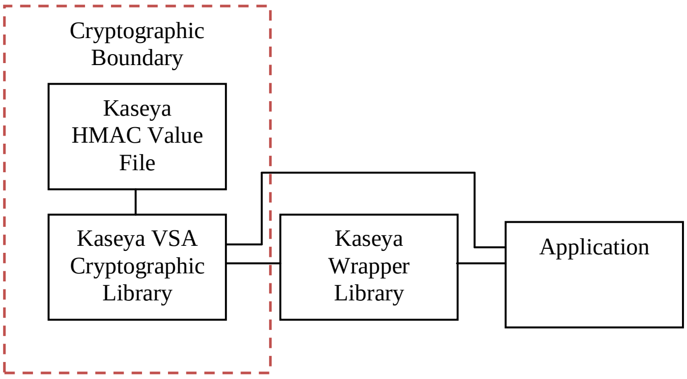

Figure 2 – Logical Block Diagram

The Virtual System Administrator Cryptographic Module is validated at the following FIPS 140-2 Section levels:

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC[8]	1
9	Self-tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A

[8] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

2.3 Module Specification

The Virtual System Administrator Cryptographic Module is a software-only module that meets overall level 1 FIPS 140-2 requirements. The logical cryptographic boundary of the Virtual System Administrator Cryptographic Module is defined as the following per operating platform:

Windows 7:	Kaseya VSA Cryptographic Library (libkacm.dll, libkacm_ksrv.dll),
Windows 2008:	Kaseya VSA Cryptographi Library Server Edition (libkacm.dll, libkacm_ksrv.dll)
Mac OS X:	Kaseya VSA Cryptographic Library (libkacm.dylib)
Linux RHEL[9] 5.5:	Kaseya VSA Cryptographic Library (libkacm.so.1)

2.4 Module Interfaces

The module supports the physical interfaces of a GPC, including the integrated circuits of the system board, the CPU (Central Processing Unit), network adapters, RAM (Random Access Memory), hard disk, device case, power supply, and fans. Other devices may be attached to the GPC, such as a display monitor, keyboard, mouse, printer, or storage media. See Figure 3 for a standard GPC block diagram.

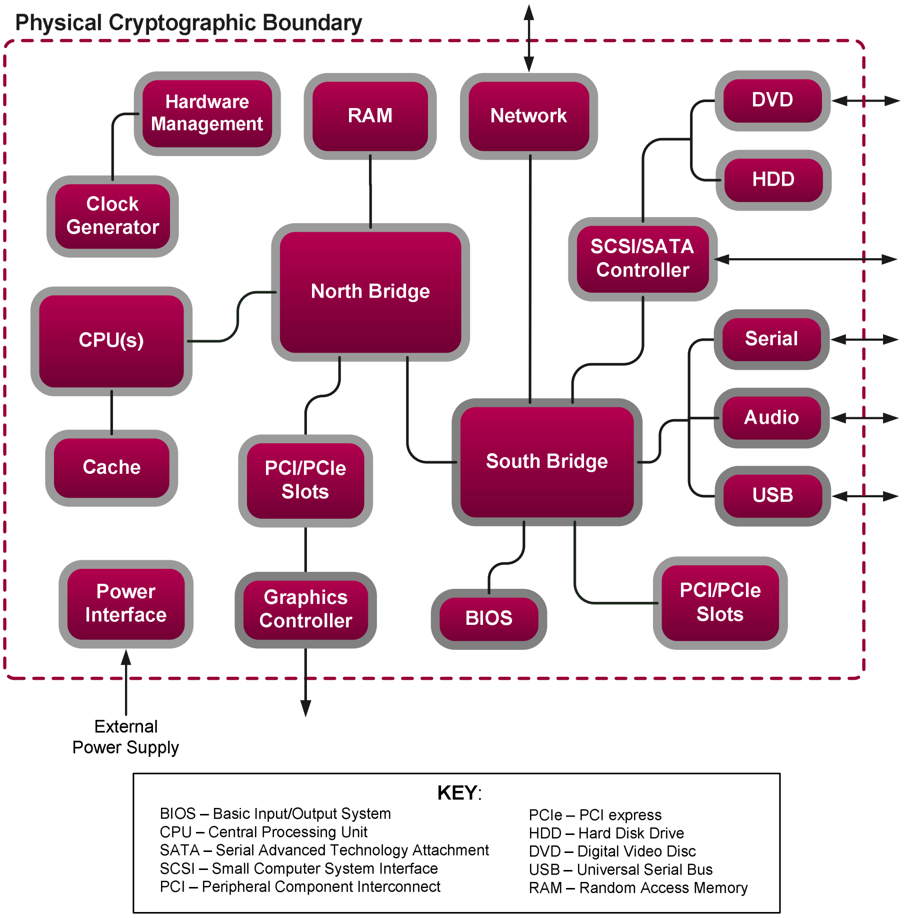

Figure 3 – GPC Block Diagram

[9] RHEL – Red Hat Enterprise Linux

The modules interfaces are provided by the logical API supported by Kaseya Cryptographic Library, which provides the data input, data output, control input, and status output logical interfaces defined by FIPS 140-2. These logical interfaces are shown in Figure 3 above. The mapping of logical interfaces to the physical ports of the GPC is provided in Table 2 below

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Physical Interface	Logical Interface Description
Data Input	USB ports (keyboard, mouse, data), network ports, serial ports, SCSI/SATA ports, DVD drive	Arguments for library functions that specify plaintext data, ciphertext, digital signatures, cryptographic keys (plaintext or encrypted), initialization vectors, and passwords that are to be input to and processed by the cryptographic module.
Data Output	Monitor, USB ports, network ports, serial ports, SCSI/SATA ports, audio ports, DVD drive	Arguments for library functions that receive plaintext data, ciphertext data, digital signatures, cryptographic keys (plaintext or encrypted), and initialization vectors from the cryptographic module.
Control Input	USB ports (keyboard, mouse), network ports, serial ports, power switch	Arguments for library functions that initiate and control the operation of the module, such as arguments that specify commands and control data (e.g., algorithms, algorithm modes, digest type, or module settings).
Status Output	Monitor, network ports, serial ports, Audio	Function return codes, error codes, or output arguments that receive status information used to indicate the status of the cryptographic module.

2.5 Roles, Services, and Authentication

The module does not support authentication; all roles are implicitly assumed. There are two roles in the module (as required by FIPS 140-2) that operators may assume: a Crypto Officer role and a User role.

2.5.1 Crypto Officer Role

The Crypto Officer role has the ability to initialize and terminate the module. Descriptions of the services available to the Crypto Officer role are provided in the table below.

Table 3 – Mapping of Crypto Officer Role's Services to Inputs, Outputs, CSPs (Critical Security Parameter), and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Crypto Enable	Initiates Power-on Self-Tests. All other functions will not execute until this service has been invoked and successfully returns.	API Command	Status	None

Service	Description	Input	Output	CSP and Type of Access
Crypto Disable	Disables the crypto services; "Crypto Enable" will need to be invoked to re-enable them.	API Command	Status	None

2.5.2 User Role

The User role has the ability to perform basic cryptographic operations such as encrypt, decrypt, generate random, and hash. Descriptions of the services available to the User role are provided in the table below.

Table 4 – Mapping of User Role's Services to Inputs, Outputs, CSPs, and Type of Access

Service	Description	Input	Output	CSP and Type of Access
Generate Random	Create a random number of a specified bit length.	Size	Random	Read DRBG Seed, 'V', and 'key'
Zeroize	Overwrites a CSP that was sent into the crypto module by a previous call. Zeroes will be written in the memory location that held the CSP and then the memory is freed.	Memory Address	None	Write All CSPs
Encrypt File	Encrypts the specified file using AES 256-bit in CTR (Counter) mode and writes the encrypted data into an output file.	Plaintext File, Key	Encrypted File	Read AES Key
Decrypt File	Decrypts the specified file and writes the plaintext data into an output file.	Encrypted File, Key	Plaintext File	Read AES Key
Encrypt Buffer	Encrypts an input buffer of data using AES 256-bit CTR mode and writes the encrypted data into an output buffer.	Buffer, Key	Encrypted Buffer	Read AES Key
Decrypt Buffer	Decrypts an input buffer of data and writes the decrypted data into an output buffer.	Encrypted Buffer, Key	Plaintext Buffer	Read AES Key

Service	Description	Input	Output	CSP and Type of Access
Hash File	Hashes the specified file using SHA-256 and returns the hash result in an output file.	File	Hash	None
Hash Buffer	Hashes an input buffer using SHA-256 and returns the hash result in an output buffer.	Buffer	Hash	None
Key Wrap	Encrypts a specified key in accordance with the AES Key Wrap specification.	Key Encryption Key, Key	Encrypted Key	Read AES Key Read, Execute AES KEK
Key Unwrap	Decrypts a specified key in accordance with the AES Key Wrap specification.	Key Encryption Key, Encrypted Key	Key	Read AES Key Read, Execute AES KEK
HMAC File	Create an HMAC hash for a specified file using HMAC SHA-256.	HMAC key, file	Hash	Read HMAC Key
HMAC SHA-256 Buffer	Set stream buffer using HMAC SHA-256	Data	Buffer data, Status	Read HMAC Key
Error	Provide error notifications.	API Command	Status	None
Data Parameter Validation	Verify the provided parameters for a given function are valid.	Data Parameter	Status	None
Crypto Module Integrity Check	Verify the software integrity of the crypto module.	HMAC, HMAC Key	Status	Read HMAC Key
Get File Descriptors	Opens the given file name and returns their associated file descriptors	File	File Descriptors	None
Initialize Cipher Context	Initialize AES Stream Cipher	Data	Status, Ciphertext	Read AES Key
Clean Up Cipher Context	Finalize AES Stream Cipher	Data	Status	None
Stream Based Encryption	Stream cipher encryption	Data	Status, Ciphertext	Read AES Key
Stream Based Decryption	Stream cipher decryption	Data	Status, Plaintext Data	Read AES Key

In addition to the above services, the Show Status and Self-tests services are also available to both roles; neither service has any access to any CSPs.

2.5.3 Non-Approved Services

When the module is operating in the non-Approved mode of operation (described in Section 3.2.3), the following additional service is available to the operator of the module, which uses the non-Approved AES-CBC mode. This service is only available in the non-Approved mode of operation.

- Encrypt and Decrypt with AES-CBC Mode

2.6 Physical Security

Virtual System Administrator Cryptographic Module is a software-only module. For the purposes of FIPS 140-2, the module is defined as a multiple-chip standalone cryptographic module, which is reflective of the GPC on which the module is installed. As a result, physical security is not applicable.

2.7 Operational Environment

The Virtual System Administrator Cryptographic Module was tested and found to be compliant with FIPS 140-2 requirements on the following platforms:

- MAC OS X v10.6.8,
- Windows 7 (32-bit and 64-bit),
- Windows Server 2008, and
- Red Hat Enterprise Linux 5.5 (32-bit and 64-bit)

Kaseya affirms that the module also executes in its FIPS-Approved manner (as described in this Security Policy) on other Operating Systems that are binary-compatible to those on which the module was tested; however no assurance can be made as to the correct operation of the module under these operational environments:

- Microsoft Windows NT, 2000, XP, XP Pro, 2003, 2003 R2, Vista, 2008, 2008 R2, 7
- Apple Mac OS X version 10.3.9 or above
- SuSE Linux Enterprise 10 and 11, Red Hat Enterprise Linux 5.4/5.5, Ubuntu 8.04-10.4, and OpenSuSE

2.8 Cryptographic Key Management

The module implements the FIPS-Approved algorithms listed in Table 5 below.

Table 5 – FIPS-Approved Algorithm Implementations

Algorithm	Certificate Number
AES ECB[10], CTR[11] modes; 256-bit keys (DRBG Implementation)	1989
AES ECB, CTR modes; 256-bit keys (VSACM Implementation)	1988
SHA-256	1744
HMAC-SHA-256	1202

[10] Electronic Code Book

[11] Counter

SP 800-90A CTR_DRBG	185

The module provides the following non-FIPS-Approved algorithm, which is not allowed for use in a FIPS-Approved mode of operation:

- AES-CBC (non-compliant)

Additionally, the following algorithm is allowed in the FIPS-Approved mode for key wrapping:

- AES (Cert. #1989, key wrapping)

The module supports the critical security parameters listed in Table 6 below.

Table 6 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key Type	Generation / Input	Output	Storage	Zeroization	Use
AES Key	Generated Within the Physical Boundary; Input Electronically in Plaintext via API Call	Wrapped via AES KEK[12]	Plaintext in volatile memory	By calling the Zeroize function in the API	Data confidentiality
AES KEK	Generated Within the Physical Boundary; Input Electronically in Plaintext via API Call	N/A	Plaintext in volatile memory	By calling the Zeroize function in the API	Wrapping AES Keys
HMAC Key	Generated Within the Physical Boundary; Input Electronically in Plaintext via API Call	N/A	Plaintext in volatile memory	By calling the Zeroize function in the API	Keyed hashing
DRBG Seed	Generated Within the Physical Boundary; Input Electronically	Never	Plaintext in volatile memory	Zeroize function; Module reset	Generate random values
DRBG 'V' Value	Generated Within the Physical Boundary; Input Electronically	Never	Plaintext in volatile memory	Zeroize function; Module reset	Used for SP 800-90 CTR_DRBG
DRBG 'key' Value	Generated Within the Physical Boundary; Input Electronically	Never	Plaintext in volatile memory	Zeroize function; Module reset	Used for SP 800-90 CTR_DRBG

[12] KEK – Key Encryption Key

2.9 EMI/EMC

The test platforms used to perform operational testing comply with the EMI/EMC requirements of the FIPS 140-2 standard.

2.10 Self-Tests

The Virtual System Administrator Cryptographic Module performs all self-tests required by FIPS 140-2 requirements at power-up. If the module encounters an error during a power-up or conditional self-test, the module will write the appropriate error message to an error log and then continue to unload itself from memory. In order to restart the module, the host system or calling application should be restarted. Should this operation fail to bring the module to an operational state, the module must be reinstalled following the directions in Section 3 of this Security Policy.

See Table 7 for a description of all self-tests performed at power-up.

Table 7 – Power-Up Tests and Descriptions

Power-Up Test	Description
AES KAT[13] (VSACM Implementation)	Individual Known Answer Tests for VSACM AES implementation
AES KAT (DRBG Implementation)	Individual Known Answer Tests for DRBG AES implementation
SHA-256 KAT	Known Answer Test for SHA-256
HMAC-SHA-256 KAT	Known Answer Test for HMAC-SHA-256
SP 800-90A CTR_DRBG KAT	Known Answer Test for SP 800-90A CTR_DRBG
Software Integrity Test	HMAC SHA-256 verifications of the crypto module

The Virtual System Administrator Cryptographic Module performs all conditional self-tests required by FIPS 140-2. See Table 8 for a description of all conditional tests.

Table 8 – Conditional Tests and Descriptions

Conditional Test	Description
Continuous DRBG Test	Continuous test performed to ensure no two consecutively generated values are the same, which would indicate a DRBG failure

The Kaseya VSACM implements the SP 800-90 CTR_DRBG as its random number generator. This DRBG employs two critical functions which must also be tested on a regular basis to ensure the security of the SP 800-90 DRBG. Therefore, the critical function tests listed in Table 9 are also implemented by the crypto module.

Table 9 – Critical Function Tests and Descriptions

Critical Function Test	Description
DRBG Instantiate Test	Test performed prior to instantiating a new DRBG.
DRBG Reseed Test	Test performed prior to instantiating a new DRBG

[13] KAT – Known Answer Test

	or before reseeding an existing DRBG.

If any of the above self-tests fail, the module will enter into an error state and no cryptographic services will be available.

2.11 Design Assurance

A combination of Subversion (SVN), version 1.6.5, and Author-it Enterprise Authoring Platform (EAP) version 5.4 are used to provide configuration management for the Virtual System Administrator Cryptographic Module and related documentation. These software solutions provide access control, versioning, and logging.

2.12 Mitigation of Other Attacks

The module has not been designed to mitigate any attacks beyond the scope of FIPS 140-2 requirements.

3 Secure Operation

The Virtual System Administrator Cryptographic Module meets Level 1 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

3.1 Initial Setup

The Virtual System Administrator Cryptographic Module does not require any additional configuration once it has been properly installed and initialized per the guidance provided in Section 3.2 below.

3.2 Crypto Officer Guidance

The Virtual System Administrator Cryptographic Module is provided in the installation package of the Virtual System Administrator Server and Virtual System Administrator Agent. The module is installed onto a system during the installation of these products. The Crypto Officer is required to install the dynamic library components of the VSACM and their HMAC signature counter-parts in the same directory.

3.2.1 Initialization

To place the module into FIPS mode, the calling application must invoke "__kacm_crypto_enable" upon startup to initialize the VSACM. If being called through the Kaseya wrapper library, then "kacm_start" must be called upon startup. After FIPS mode has been enabled, the CO shall ensure that AES CBC mode is not used during operation. Use of this algorithm will cause the module to operate in a Non-Approved mode. See Section 3.2.3 for further details.

3.2.2 Management

The module is a cryptographic library and as such, the single-user of the module is the calling application. The application itself may service multiple operators, but the module itself will only provide services to the associated loading application. When providing service to a server, the server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients. The operating system itself prevents operators from circumventing the single-user enforcement mechanism, as the module runs in separate instances.

3.2.3 Non-Approved Mode of Operation

The Virtual System Administrator Cryptographic Module contains both an Approved and Non-Approved mode of operation. Instructions on how to place the module into an Approved mode of operation are available in Section 3.2.1. To take the module out of an Approved mode of operation, the CO can call "_kacm_crypto_disable". To operate the module in a Non-Approved mode of operation, the CO must do the following:

1. Call "register_cipher()" to register the AES-256 cipher
2. Call "register_hash()" to register the SHA-256 hash
3. Set two global variables pointing the chosen cipher and hash algorithms

When operating in a Non-Approved mode, the module provides all cryptographic algorithms listed in Table 5 in a non-compliant form, with the addition of AES in CBC mode. Additionally, the services listed in Table 3 and Table 4 are available to the user of the module and can be run in a non-Approved form. Section 2.5.3 presents an additional service, which is available to the operator of the module only in the non-Approved mode. AES can be used in CBC mode for encrypt and decrypt operations of files and buffers, in the non-Approved mode. While operating in the non-Approved mode, all module services are available to all operators with access to the module.

3.3 User Guidance

No additional guidance is required for the User.

4 Acronyms

Table 10 lists the acronyms used throughout this document.

Table 10 – Acronyms

Acronym	Definition
API	Application Programming Interface
ASP	Active Server Pages
BIOS	Basic Input/Output System
CMVP	Cryptographic Module Validation Program
CPU	Central Processing Unit
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
CTR	Counter
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
DVD	Digital Video Disc
EAP	Enterprise Authoring Platform
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
GPC	General Purpose Computer
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology
KAT	Known Answer Test
MAC	Macintosh
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
ODBC	Open Database Connectivity

Acronym	Definition
OLEDB	Object Linking and Embedding Database
OS	Operating System
PC	Personal Computer
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
RAM	Random Access Memory
RHEL	Red Hat Enterprise Linux
RSA	Rivest Shamir and Adleman
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SVN	SubVersion
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
USB	Universal Serial Bus
VSA	Virtual System Administrator
VSACM	Virtual System Administrator Cryptographic Module
VSS	Visual Source Safe

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Hwy, Suite 220
Fairfax, VA 22033
United States of America

Phone: (703) 267-6050
Email: info@corsec.com
http://www.corsec.com