122

CERTIFICATION REPORT No. CRP264

Kaseya Virtual System Administrator
Version 6.2.1.0
running on Multiple Platforms

Issue 1.0

February 2012

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.

Sponsor:	Kaseya International Ltd	Developer:	Kaseya International Ltd
Product and Version:	Kaseya Virtual System Administrator Version 6.2.1.0		
Platform:	Multiple		
Description:	The Kaseya Virtual System Administrator provides IT managers with the capability to monitor, manage, and maintain distributed IT networks.		
CC Version:	Version 3.1		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL2 Augmented by ALC_FLR.2		
PP Conformance:	None		
CLEF:	SiVenture		
FIPS 140-2	Level 1 Crypto Module Validation is covered by the following FIPS 140-2 validation certificates numbers: ***(TBD)***.		
CC Certificate:	P264	Date Certified:	16 February 2012

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo

CC logo

SOGIS MRA logo

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Kaseya Virtual System Administrator Version 6.2.1.0 to the Sponsor, Kaseya International Ltd., as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC **EAL2** augmented by ALC_FLR.2 on 20 January 2012:

- Kaseya Virtual System Administrator Version 6.2.1.0 running on multiple platforms. (The Kaseya Agent component can be installed on servers, desktops and laptops of various operating systems, such as: Microsoft Windows XP, Vista, 2008 and 7; Apple Macintosh OSX Version 10.3.9 and above; and Linux. The Kaseya Server component can be installed on Microsoft Windows 2003 Server or 2008 Server.)

4. The Kaseya Virtual System Administrator (hereinafter also referred to as 'VSA') provides IT managers with the capability to monitor, manage, and maintain distributed IT networks. The Developer was Kaseya International Ltd.

5. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

6. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in Section 1.4 of [ST].

Protection Profile Conformance

7. The Security Target [ST] does not claim conformance to any protection profile.

Security Claims

8. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which those Objectives counter and the Security Functional Requirements (SFRs) and TOE Security Functions that elaborate the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of that standard facilitates comparison with other evaluated products.

9. The Security Target [ST] specifies two extended SFR components, consisting of EXT_SMS_ARP.1 (for Security Alarms) and EXT_SMS_SDC.1 (for System Data Collection).

10. The TOE security policies are detailed in [ST]. The environmental assumptions related to the *operating environment* are detailed in Chapter III (in ‘Environmental Requirements’) of this report.

Evaluation Conduct

11. The CESG Certification Body monitored the evaluation, which was performed by the SiVenture Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of that work, completed in January 2012 were reported in the Evaluation Technical Report [ETR] and [ETRsupp].

Special Configuration Requirements

12. In the evaluated configuration, the following checkboxes need to be deselected in order to make sure that these options are not visible to the end user in the Agent Menu:

a) Disable Remote Control – By deselecting this option, the end user will not have the option or checkbox within the Kaseya Agent Menu to disable remote control access of the managed device.

b) Set Account – By deselecting this option, the end user will not have the option or checkbox within the Kaseya Agent Menu to set the IP address or hostname of the Kaseya Server.

c) Exit – By deselecting this option, the end user will not have the Kaseya Agent Menu option or checkbox within the Kaseya Agent Menu to be able to terminate the agent service on the managed device.

13. In order to comply with the evaluated configuration for Common Criteria, the Kaseya Server must be configured in FIPS mode, which provides proprietary cryptographic functions to protect TSF data from disclosure or modification while in transit from the Kaseya Agent to the Server. Level 1 Crypto Module Validation is covered by the following FIPS 140-2 [FIPS 140-2] validation certificate numbers: ***(TBD[2])***.

Conclusions and Recommendations

14. The conclusions of the CESG Certification Body are summarised on page 2 ‘Certification Statement’ of this report.

15. Prospective consumers of Kaseya Virtual System Administrator Version 6.2.1.0 should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

[2] This document will be updated with respect to the outcome of the latest FIPS 140-2 validation of the cryptographic module used by the TOE when it completes in the Cryptographic Module Validation Program (CMVP).

16. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

17. The Kaseya Server can be installed on Microsoft Windows 2003 Server or 2008 Server.

18. The Kaseya Agent can be installed on: Microsoft Windows XP, Vista, 2008 and 7; Apple Macintosh OSX Version 10.3.9 and above; and Linux. (Although it can also be installed on Windows 98, Me, NT and 2000, such use is not recommended by the CESG Certification Body, as Microsoft no longer issues security patches for those operating systems.)

19. In addition, the Evaluators' comments and recommendations are as follows:

a) Prior to installation and operation the end-user must be aware of OE.MANAGE and OE.PROTECT, as secure installation and operation is dependent on those objectives being satisfied.

b) Installation should only be carried out after reading the Guidance Supplement [GUIDESUP], to ensure that the product is installed in its Evaluated Configuration.

c) Customers should adhere closely to the administrative guidance, to maintain security.

Disclaimers

20. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

21. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

22. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

23. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

24. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

25. The following sections provide guidance of particular relevance to purchasers of the TOE.

Delivery

26. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised during delivery.

27. The delivery process is as follows:

- The customer downloads the product as a free trial download from the Kaseya web site
- The customer will install the product by running the KaseyaVSA.exe executable.
- To use the product beyond the 30-day trial period, the customer must purchase licensing from Kaseya. Upon purchase, Kaseya generates a unique license code for the customer, which is used to activate the software for long-term use.
- The customer is able to extend the license by logging into the VSA Administrator Console. Under System > License Manager > General tab, the customer may click the 'Update Code…' button in order to enter a new license code or reapply an existing license code.
- The customer's VSA Server communicates with the Kaseya license server by sending encrypted, digitally signed data via Hypertext Transfer Protocol (HTTP). Data transmitted from the VSA Server is signed using the VSA Server's unique authorised certificate. Data transferred from the Kaseya license server is signed using the Kaseya public certificate.

28. When the TOE is downloaded via Kaseya's website, a SHA-1 hash is provided to the customer on the product download page and also in the Guidance Supplement pdf (which enables the end user to check that the correct hash value is being used by comparing the value on the download page with the value in the Guidance Supplement). To confirm the downloaded TOE's integrity, a SHA-1 hash utility should be used to calculate a SHA-1 hash for the downloaded TOE. If the calculated SHA-1 hash matches the SHA-1 hash provided on Kaseya's website, the TOE downloaded correctly. Should the TOE fail the SHA-1 hash procedure, the customer should download the TOE again and re-check the SHA-1 hash. If the failure persists, the customer should contact Kaseya customer support.

Installation and Guidance Documentation

29. The Installation and Secure Configuration documentation is as follows:

a) [INSTALL]

b) [GUIDESUP]

30. The User Guide and Administration Guide documentation is as follows:

a) [ADMIN]

III. EVALUATED CONFIGURATION

TOE Identification

31. The TOE is Kaseya Virtual System Administrator Version 6.2.1.0, which consists of:

a) Kaseya Server v6.2.1.0; and

b) Kaseya Agent v6.2.1.0.

TOE Documentation

32. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

33. All guidance documentation is available online and can be downloaded in .pdf format from Kaseya's web site: http://help.kaseya.com/WebHelp/EN/VSA/6010000/. Links to various online help resources can be found by going to the 'Kaseya® Virtual System Administrator™ Online User Assistance' section of the online help. All online help and user guides are published to the help.kaseya.com website and can be viewed or downloaded by customers.

TOE Scope

34. The TOE Scope is defined in Sections 1.5.1 and 1.5.2 of the Security Target [ST]. Section 1.5.3 of [ST] defines functionality that is outside the TOE Scope; most significantly, the API interface.

TOE Configuration

35. The evaluated configuration of the TOE is defined in [GUIDESUP].

Environmental Requirements

36. The environmental assumptions for the TOE are stated in [ST] Section 3.3.

37. The TOE was evaluated running on the following representative platforms:

a) Kaseya Server: Windows Server 2003.

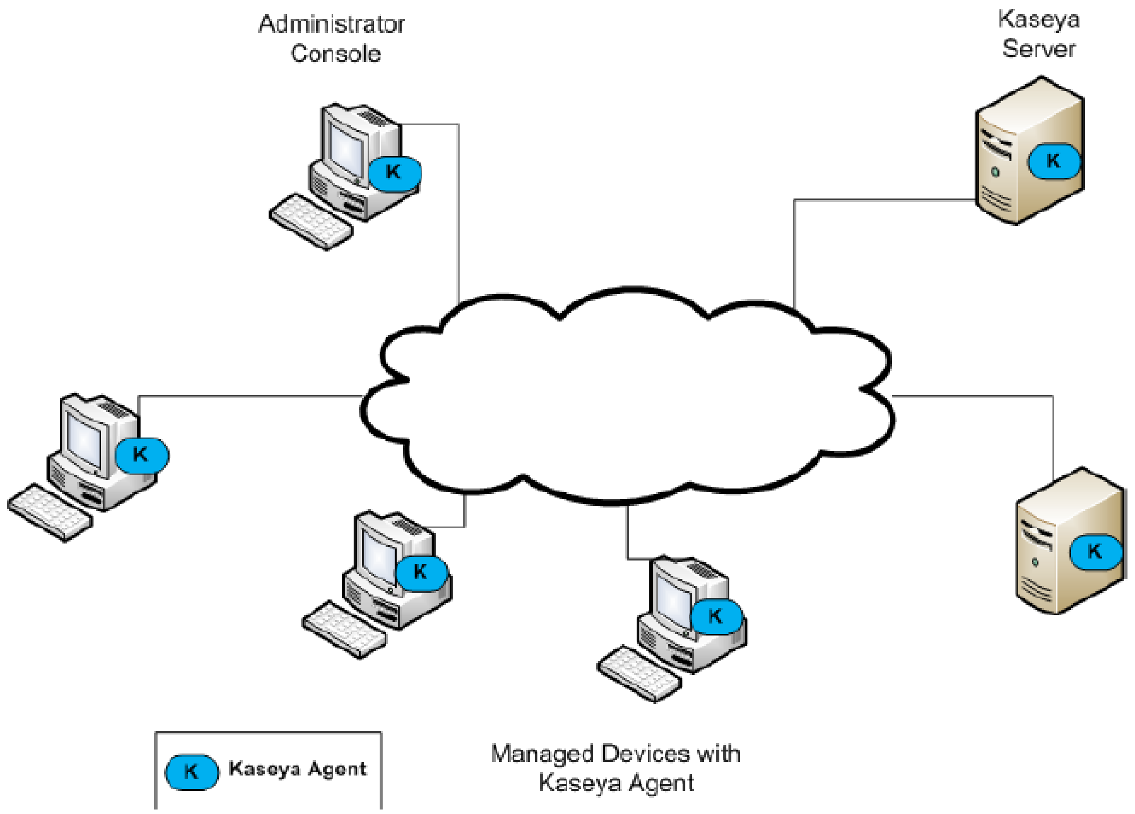
b) Kaseya Agents: Windows agent running on a Dell Inspiron and Windows agent running on an Intel Classmate PC. *(Note that other platforms, such as Macintosh OSX and Linux, can also be used.)*

38. The environmental IT configuration is as follows:

a) The Kaseya Server hardware. The Kaseya Server relies upon the IT environment to provide protection of data transfer between the Administrator web-based GUI and the Kaseya Server TOE components.

b) An administrator workstation with a web browser.

39. The diagram below shows a simple, sample deployment of the TOE.



Test Configuration

40. The Developers used the following configuration for their testing:

a) Kaseya Server v6.2.1.0 installed on a Windows Server 2003 host, compliant to the minimum software and hardware requirements.

b) Kaseya Agent v6.2.1.0 installed on a Windows XP host, compliant to the minimum software and hardware requirements.

c) Tester Workstation with a web browser, compliant to the minimum software requirements.

41. The Evaluators used the following configuration for their testing:

a) Kaseya Server v6.2.1.0 installed on a Windows Server 2003 host, compliant to the minimum software and hardware requirements.

b) Kaseya Agent v6.2.1.0 installed on a Dell Inspiron, compliant to the minimum software and hardware requirements.

c) Kaseya Agent v6.2.1.0 installed on an Intel Classmate PC.

IV. PRODUCT ARCHITECTURE

Introduction

42. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

43. Kaseya Virtual Systems Administrator is an IT Systems Management system that comprises of the Kaseya Agents and Kaseya Server with a web-based Administrator Console.

Kaseya Agents

44. VSA manages machines by installing a software client called the Kaseya Agent on a managed device. The Kaseya Agent is a system service or a daemon that does not require the user to be logged on for the Agent to function and does not require a reboot for the Agent to be installed. The Agent is configurable and can be totally invisible to the end user.

45. The Kaseya Agents are software applications installed on managed devices. Agents are the components which enact the machine management activities driven by Kaseya Server activities. 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 Kaseya Server. The Kaseya Server component acting solely as a server will never initiate a connection to the Agent.

Kaseya Server

46. The Kaseya Server contains the majority of the Kaseya-developed logic and functionality to provide the VSA services. The Kaseya Server performs the authentication for all administrators and ensures that all automated tasks that have been scheduled by administrators are performed. The Kaseya Server accepts configuration information and instructions via the web-based Administrator Console to change policies or settings on managed devices as well as instructions to perform scans on the managed devices. In addition to the Administrator Console, the VSA also has an API that allows third party application integration. The API exposes the majority of the actions and functionality available from the web GUI.

47. The Kaseya Server uses proprietary cryptographic software to provide protection of data transfer between the Kaseya Server and the Agents.

48. The Microsoft SQL database is the data repository for IT policies, collected information about the IT network, and VSA configuration information. Kaseya VSA is an IT Systems Management system that is comprised of the Kaseya Agents and Kaseya Server with a web-based Administrator Console.

TOE Design Subsystems

49. The TOE subsystems, and their security features/functionality, are as follows:

a) Kaseya Server:

- Kaseya Server Administrative Subsystem (SFR-enforcing). The Management Interface accepts configuration information and instructions via the web-based Management Interface to change policies or settings on managed devices as well as instructions to perform scans on the managed devices. The Kaseya Server relies on the Web Server which is external to the TOE to provide secure SSL communications between the Kaseya Server Administrative Subsystem and the VSA Console Web Browser. Security-relevant administrator actions taken in the Management Interface are logged. The configuration settings are written to the SQL Server database which is external to the TOE.

- Kaseya Server System Management Subsystem (SFR-enforcing). This subsystem analyses the scanned information that was collected by the Scan Interface on the Agent System Management Subsystem. This is data that is received from Agents and is written to the SQL database. The Kaseya Server System Management Subsystem reads the data from the database and takes action on items that have been flagged as alarm candidates by the Agent System Management Subsystem. When programmable alarms are triggered, the Kaseya Server System Management Subsystem executes email notifications, procedures, and job ticketing for problems and state changes that have been configured by the VSA Administrator within the Management Interface.

- Kaseya Server Cryptographic Subsystem (SFR-enforcing). This subsystem provides the cryptographic functionality for the Kaseya Server. The cryptographic functions provide a secured communications channel between the Kaseya Server and Agent in order to protect TSF data that is transferred between them. It also provides the hashing mechanism of the password when users are authenticating through the Management Interface within the Kaseya Server Administrative Subsystem

- Authentication Subsystem (SFR-supporting). This subsystem provides Windows domain Active Directory server identification and authentication functionality for the Kaseya Server. The Kaseya Server offers the ability for a VSA administrator to login via their Windows domain logon credentials. Once the user is successfully identified and authenticated, they are then able to gain access to the TOE.

b) Kaseya Agent:

- Kaseya Agent Administrative Subsystem (SFR-enforcing). A user logs in directly into a managed device with a Kaseya Agent installed on it via the Identification and Authentication functionality provided by the Operating System. Once identified and authenticated by the Operating System, the machine user can click the Agent icon which gives the machine user access to the Agent menu. The Agent Administrative Subsystem provides a GUI menu, called the Agent Menu Interface, that allows the machine user to make a few configuration changes to the Kaseya Agent.

- Kaseya Agent System Management Subsystem (SFR-enforcing). This subsystem scans the local device for asset inventory information such as system information, hardware information, operating system, and software applications. In addition, if LANWatch is turned on, then SNMP trap information (as well as information about other devices on the local subnet) is collected. This information is collected and stored in log files on the local device.

- Kaseya Agent Cryptographic Subsystem (SFR-enforcing). This subsystem provides cryptographic functionality to the Agent. This allows for an encrypted session between the Kaseya Server and Agent which protects the data that is sent from the Kaseya Agent to the Kaseya Server.

- A/D Interface Subsystem (SFR-supporting). This subsystem provides the functionality to call the Windows domain server – Active Directory.

TOE Dependencies

50. The TOE depends on the underlying operating system (see paragraphs 17 – 18 for the operating systems).

TOE Interfaces

51. The external TOE Security Functions Interface (TSFI) is described as follows:

a) Management Interface. This interface accepts configuration information and instructions via the web-based VSA Console Web Browser to change policies or settings on managed devices as well as instructions to perform scans on the managed devices. The Management Interface presents the login screen of the Management Interface via a web browser to an administrative user to input their username and password. Security-relevant administrator actions taken in the Management Interface are logged.

b) Agent Menu Interface. This interface is shown as an icon in the taskbar by default. The machine user can perform updates to the Agent Settings through the Agent Menu Interface menu. The user displays the Agent Menu Interface by right-clicking the agent icon in the system tray of the managed device. An example of functionality available through this interface is that the user is able to initiate a full check-in to the Kaseya Server. A full check-in occurs when an agent completes the processing of any and all outstanding tasks.

V. TOE TESTING

TOE Testing

52. The Developer's tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- all Security Functions (SFs);
- the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

53. The Developer's tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly.

54. The Developer's test configuration is detailed in Chapter III (in 'Test Configuration') of this report.

55. The Evaluators devised and ran a total of 28 independent functional tests, different from those performed by the Developer. No anomalies were found.

56. The Evaluators also devised and ran a total of 5 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities were detected.

57. The Evaluators performed all of their tests on the evaluated configuration. Details of the test set-up are provided in Chapter III (in 'Test Configuration') of this report.

58. The Evaluators finished running their penetration tests on 29 September 2011.

Vulnerability Analysis

59. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

Platform Issues

60. The TOE was evaluated on the platforms described in Chapter III. However all platforms described in [ST] can be used, namely:

a) The Kaseya Agent can be installed on: Microsoft Windows XP, Vista, 2008 and 7; Apple Macintosh OSX Version 10.3.9 and above; and Linux. (It can also be installed on Windows 98, Me, NT and 2000, but they are no longer patched by Microsoft.)

b) The Kaseya Server can be installed on Windows 2003 Server or 2008 Server.

VI. REFERENCES

[ADMIN] Virtual System Administrator, User Guide,
Kaseya International Ltd.,
Version 6.2, 19 January 2012.

[CC] Common Criteria for Information Technology Security Evaluation
(comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Components,
Common Criteria Maintenance Board,
CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Components,
Common Criteria Maintenance Board,
CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Participants in the Arrangement Group,
May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2009-07-004, Version 3.1 R3, July 2009.

[ETR] Evaluation Technical Report,
SiVenture CLEF,
LFV/T013/ETR, Issue 1.3, 20 January 2012.

[ETRsupp] LFV/T013 ETR Supplement,
SiVenture CLEF,
LFV/T013/ETRsupp, Issue 1.0, 6 February 2012.

[FIPS 140-2] Security Requirements for Cryptographic Modules,
Federal Information Processing Standard Publication,
FIPS PUB 140-2, 25 May 2001.

[GUIDESUP] Virtual Systems Administrator v6.2.1.0 Guidance Document Supplement,
Kaseya International Ltd.,
Version 1.1, 4 November 2011.

[INSTALL] Kaseya Server Installation and Update User Guide,
Kaseya International Ltd.,
Version 6.2, 19 January 2012.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8 January 2010 (effective April 2010).

[ST] Virtual Systems Administrator v6.2.1.0 Security Target,
Kaseya International Ltd.,
Version 1.1, 4 November 2011.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.2, December 2009.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard CC abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00].

CMVP	Cryptographic Module Validation Program
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSL	Secure Lockets Layer
VSA	Virtual System Administrator