122-B

COMMON CRITERIA CERTIFICATION REPORT No. P229

SYMANTEC LIVESTATE DELIVERY Version 6.0.1

running on specified Microsoft Windows platforms

Issue 1.0

August 2006

Certification Body,
CESG, Hubble Road,
Cheltenham, GL51 0EX
United Kingdom

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

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement 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 contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

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	**Symantec Corporation**
Product and Version	**Symantec LiveState Delivery, Version 6.0.1**
Description	The evaluated version of this product remotely delivers software (operating systems, applications and programs) from centralized servers, across networks, to multiple desktop PCs or servers simultaneously.
CC Part 2	**extended**
CC Part 3	**conformant**
EAL	**EAL2**
CLEF	**BT**
Date authorised	**10 August 2006**

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 ([a] - [c]). The Scheme has established a 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 [d], 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 3 [g], the Common Evaluation Methodology (CEM) [h], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

TABLE OF CONTENTS

CERTIFICATION STATEMENT **2**
TABLE OF CONTENTS **3**
I. EXECUTIVE SUMMARY **4**
Introduction 4
Evaluated Product and TOE Scope 4
Protection Profile Conformance 4
Security Claims 5
Strength of Function Claims 5
Evaluation Conduct 5
Conclusions and Recommendations 6
II. PRODUCT SECURITY GUIDANCE **7**
Introduction 7
Delivery 7
Installation and Guidance Documentation 8
III. EVALUATED CONFIGURATION **9**
TOE Identification 9
TOE Documentation 10
TOE Scope 10
TOE Configuration 10
Environmental Requirements 11
Test Configuration 13
IV. PRODUCT SECURITY ARCHITECTURE **14**
Product Description and Architecture 14
Design Subsystems 15
Hardware and Firmware Dependencies 16
Product Interfaces 16
V. PRODUCT TESTING **17**
IT Product Testing 17
Vulnerability Analysis 18
Platform Issues 18
VI. REFERENCES **19**
VII. ABBREVIATIONS **21**

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Symantec LiveState Delivery, Version 6.0.1 to the Sponsor, Symantec Corporation, 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 [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:

   Symantec LiveState Delivery, Version 6.0.1.

4. The Developer was Symantec Corporation.

5. Symantec LiveState Delivery is a product for remotely delivering operating systems, applications and programs across networks to desktops, mobile PCs, handheld devices and servers. **(However, mobile PCs and handheld devices are outside the scope of the evaluation.)**

6. The evaluated product uses scheduled push-and-pull technology to deliver software from centralized servers to multiple PCs or servers simultaneously. It provides a suite of administrative tools that allow identified and authorised administrators (with a variety of roles) to manage the unattended deployment of business-critical software from centralized Windows servers to multiple PCs or servers simultaneously.

7. The evaluated subset and 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’.

8. An overview of the product and its security architecture are given in Chapter IV ‘Product Security Architecture’.

Protection Profile Conformance

9. The Security Target [d] does not claim conformance against any protection profiles.

Security Claims

10. The Security Target [d] specifies the TOE's security objectives, the threats which these objectives counter, and the Security Functional Requirements (SFRs) and security functions to elaborate the objectives. Most of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products.

11. There are two non-CC SFRs, stated in the Security Target [d] as explicit SFRs:

- FPT_SEP.1_EXP (TSF Domain Separation);
- FPT_STM.1_EXP (Reliable Time Stamps).

12. The TOE Security Policy is detailed in the Security Target [d].

13. The Security Target [d] states that there are no organizational security policies with which the TOE must comply.

14. Claims are primarily made for security functionality in the following areas:

a. **Identification:** The TOE identifies administrators by means of a username and authenticates them by means of a password mechanism.

b. **User Data Protection and Security Management:** All administrators are assigned a role that determines what functions they can access. There are five roles within the TOE.

c. **Audit:** The TOE records when administrators perform certain actions, noting what was performed, by whom and when. This function is active as long as the TOE's Configuration Server component is running. This function uses the time from the operating system on which the Configuration Server runs.

d. **Protection of TOE Security Functions:** The TOE provides self protection from untrusted entities. Functions that enforce TOE security always occur before other functions, to ensure that security is maintained.

Strength of Function Claims

15. **The minimum Strength of Function (SoF) was SoF-Basic.** This was claimed for SFR FIA_UAU.2, in respect of the authentication mechanism using passwords. **The Certification Body has determined that this claim was met.**

16. Products such as Symantec LiveState Delivery are intended to be used in various environments and used to connect networks with different levels of trust in the users. The SoF of SoF-Basic for the TOE will be appropriate to a number of deployments, in government and other organisations.

Evaluation Conduct

17. The Certification Body monitored the evaluation which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work,

completed in June 2006, were reported in the ETR [i]. The Certification Body requested further details and, following the CLEF's satisfactory responses, the Certification Body produced this Certification Report.

Conclusions and Recommendations

18. The conclusions of the Certification Body are summarized in the Certification Statement on page 2.

19. **Prospective consumers of Symantec LiveState Delivery, Version 6.0.1, should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d]**. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

20. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III 'Evaluated Configuration'.

21. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II 'Product Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

22. The product provides some features that were not within the scope of the evaluation, as identified in Chapter III 'Evaluated Configuration'. **Those features should therefore not be used if the TOE is to comply with its evaluated configuration.**

23. If any changes are proposed to the TOE's functionality, or to components that were examined during the evaluation, such changes should be handled under the Assurance Continuity Scheme. If the change falls outside the scope of Assurance Continuity, a partial or complete re-evaluation of the product should be performed.

24. **Certification is not a guarantee of freedom from security vulnerabilities**; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

25. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

26. **On receipt of the TOE, the consumer is recommended to check that the evaluated version (as detailed in Chapter III) has been supplied, and to check that the security of the TOE has not been compromised in delivery**.

27. Symantec ships the TOE (including its CD-ROMs, documentation, etc) in a sealed box to a Symantec authorised reseller. Consumers are required to order the TOE from a reputable supplier (i.e. a Symantec authorised reseller), who then ships the sealed box to the consumer by registered delivery, using a reputable delivery firm.

28. When consumers receive the TOE, they are required to follow the process detailed in the Certified Release Notes [j].

29. The following measures provide security for delivery of the TOE and its guidance documentation:

    a. The delivery firm's outer box is sealed with a tamper-evident, clear label.

    b. The Symantec inner box contains:

        i. A tamper-evident, sealed CD-ROM case containing two CD-ROMs:

            - Symantec LiveState Delivery, Version 6.0.1. This CD-ROM includes the Reference Guide [l].
            - Symantec LiveState Delivery Package Manager, Version 6.0.1. (This was not within the scope of the evaluation, as identified in Chapter III 'Evaluated Configuration'. **It should therefore not be used if the TOE is to comply with its evaluated configuration**.)

        ii. Implementation Guide [k].

    c. Consumers should download the Certified Release Notes [j] in PDF format from Symantec's website at www.symantec.com. (Note: There are also other release notes for the product on that website so, for the evaluated configuration of the TOE, the consumer should take care to download the Certified Release Notes.)

30. The primary considerations governing the security of web-based delivery of the Certified Release Notes [j] are as follows:

    a. standard procedures associated with a well-managed web interface must be followed;

    b. the Certified Release Notes are downloaded as a PDF file.

Installation and Guidance Documentation

31. Guidance is provided in the following documents:

- Certified Release Notes [j];
- Implementation Guide [k];
- Reference Guide [l].

32. The **Certified Release Notes** [j] describe the procedures that must be followed to install and configure the product in its evaluated configuration, and to operate it securely, and they provide warnings that identify unevaluated functionality. They also describe the procedures that must be followed to configure the environment. Hence it is recommended that these notes are read first.

33. The **Implementation Guide** [k] provides general details concerning installation of Symantec LiveState Delivery, such as setting up a BOOTstrap Protocol (BOOTP) environment or a Dynamic Host Configuration Protocol (DHCP) environment.

34. The **Reference Guide** [l] provides instructions on how to operate and configure the Configuration Server and the Command Center (including all of its services) once the Symantec LiveState Delivery product has been installed.

35. The intended audience of the installation and guidance documents is the administrator.

III. EVALUATED CONFIGURATION

TOE Identification

36. The TOE is identified as:

Symantec LiveState Delivery, Version 6.0.1.

37. The TOE components are:

a. Symantec LiveState Delivery 6.0.1 Configuration Server;

b. Symantec LiveState Delivery 6.0.1 Command Center;

c. the Agents, namely:

- Symantec LiveState Delivery 6.0.1 Agent For Windows;
- Symantec LiveState Delivery 6.0.1 Boot Agent;
- Symantec LiveState Delivery 6.0.1 Pre-OS Agent.

38. The Configuration Server component stores the packages to be assigned and, when instructed by an administrator, it connects to a Managed Computer and installs or uninstalls a package. This component also stores the log files, which can be examined by an administrator via the operating system.

39. The Command Center component is the administrative interface to the TOE. It presents a GUI that allows an administrator to instruct the Configuration Server component.

40. The Agent for Windows component resides on a Managed Computer and performs any installation and/or configuration of packages that is required, as instructed by the Configuration Server component. To enable the Agent For Windows component to be installed on a Managed Computer by the Configuration Server component, the Boot Agent component and the Pre-OS Agent component must be downloaded to the Managed Computer component.

41. Figure 1-1 shows the components and scope of the TOE:

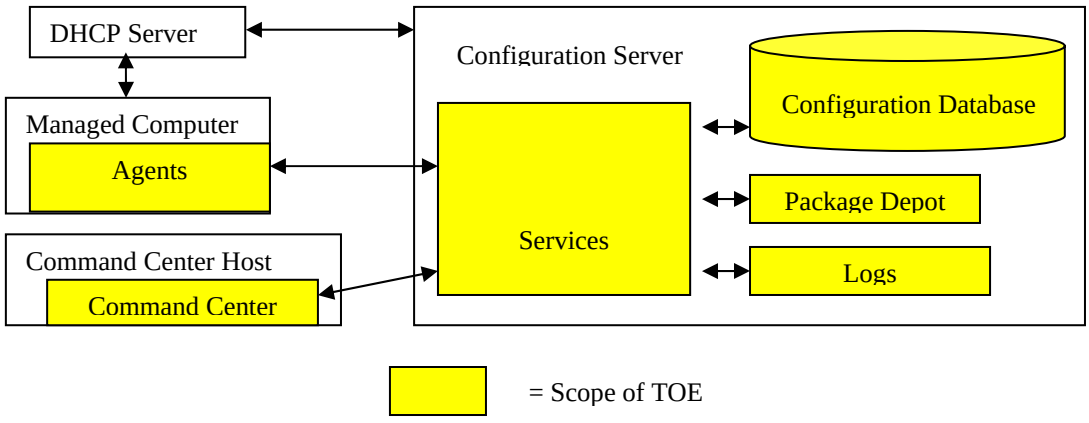

Figure 1-1: Components and Scope of the TOE

TOE Documentation

42. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'.

TOE Scope

43. The TOE is identified above under 'TOE Identification'.

44. The product remotely delivers operating systems, applications and programs across networks to desktops, mobile PCs, handheld devices and servers. **However, it should be noted that only desktops and servers as managed computers running Windows are within the scope of the evaluation.**

45. **Mobile PCs and handheld devices are outside the scope of the TOE and hence were not evaluated**.

46. **Also, the following features of the product are outside the scope of the TOE and hence were not evaluated:**

- **Wizards;**
- **Remote Administration;**
- **Live Update Support;**
- **Replicator;**
- **Web Admin;**
- **Multiplatform (Java) Agent;**
- **Web Self Service;**
- **Pocket PC agent;**
- **Wake On LAN Proxy;**
- **Locator;**
- **User Profile Manager;**
- **Image Delivery;**
- **LiveState Delivery Enterprise Manager;**
- **LiveState Delivery Package Manager;**
- **Client Migration;**
- **AutoInstall;**
- **Auto Discover Agent.**

TOE Configuration

47. In the TOE configuration, the Configuration Server component and the Command Center component run on two physically separate machines in the network:

    a. the Configuration Server component is installed on a **Windows 2000 (Service Pack (SP) 4))** operating system;

    b. the Command Center component is installed on a **Windows XP Professional (SP2)** operating system;

c. the Agent components are installed on a client machine (a **Windows XP Professional (SP2)** operating system in the evaluated configuration) by the Configuration Server component.

48. The operating systems and hardware platforms are part of the environment.

49. The product's data exchange is based on the IP protocol. The product can be set up in either BOOTP or DHCP environments; DHCP dynamically allocates IP addresses to computers on a LAN. For the evaluated configuration, a DHCP environment must be used, and the DHCP server must be configured with the specified options, to allow the Boot Agent to be downloaded from the Configuration Server to a Managed Computer.

50. For the evaluated configuration, PXE-compatible network cards were used and the TOE was on a network that was not connected to any other network.

51. Figure 1-2 shows the TOE components within a typical network of a Configuration Server, a Command Center, a DHCP Server and several Managed Computers:

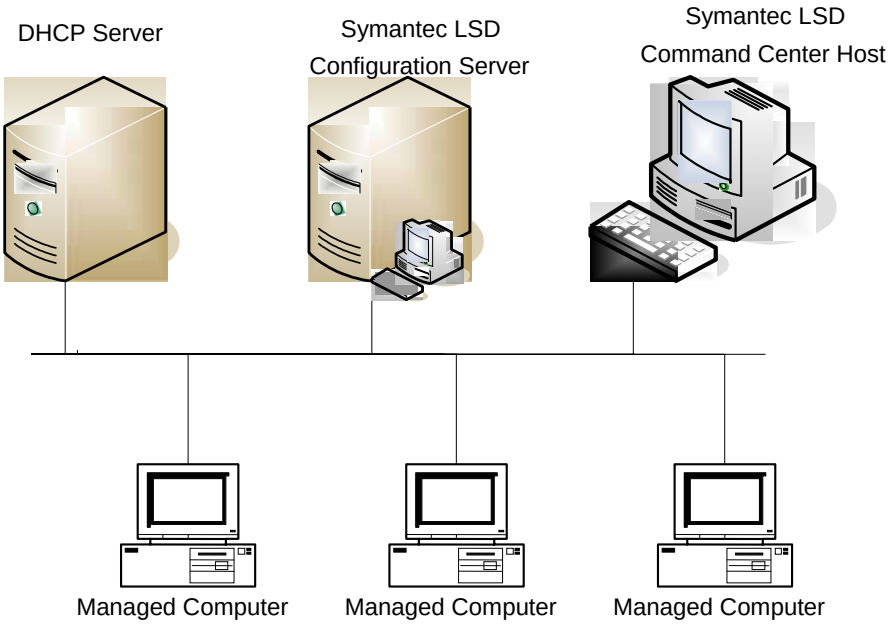

Figure 1-2: Network Environment for the TOE

52. The operating system running the Configuration Server (i.e. Windows 2000 (SP4)) provides a number of supporting mechanisms which provide the security requirements for the environment of the TOE:

a. The operating system provides for domain separation by correctly handling different processes and their memory management.

b. The system clock, provided by the underlying hardware (through the operating system) is used to generate audit timestamps.

c. Controlled access to system data, and the services that maintain and configure the data, is provided. Stored audit records are protected, as only administrators have access to the Configuration Server's operating system.

d. The audit records are stored in operating system files, which can be accessed by administrators in order to review and manage the audit trail.

Environmental Requirements

53. The Security Target [d] identifies the threats that are met by the environment, or are met collectively by the TOE and the environment.

54. The Security Target [d] makes physical, personnel and connectivity assumptions, as follows:

a. (A.PHYSEC): It is assumed that the Configuration Server and the Command Center Host are physically protected to prevent unauthorised use / user access.

b. (A.REMOS): It is assumed that the platforms (i.e. any hardware platforms, and operating systems, that have a component of the TOE installed on them) are delivered to the user's site, installed and administered in a secure manner.

c. (A.TRUST): It is assumed that the users of the network on which the TOE is installed are trusted not to connect that network to any other network

d. (A.NOEVIL): It is assumed that authorised administrators for the TOE and platforms (i.e. any hardware platforms, and operating systems, that have a component of the TOE installed on them) are non-hostile and follow all administrator guidance; however, they are capable of error.

e. (A.LOWEXP): It is assumed that the threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered to be low.

f. (A.COMMS): It is assumed that the communication links between the TOE components are physically protected.

g. (A.ONENET): It is assumed that the network on which the TOE is installed is not connected to any other network.

55. The product is intended to be used in a variety of low threat environments, to distribute operating systems, applications and programs with different levels of trust in the users. The EAL2 assurance level will be appropriate to a number of deployments, in both government and other organisations, where the overall threat is considered low – as defined by assumptions A.LOWEXP and A.ONENET above.

Test Configuration

56. The environmental configuration used by the Developer, and the Evaluators, to test the TOE is summarised in Table 1-1:

Machine running the Configuration Server	
Hardware	Dell PowerEdge 6400
Processor	Intel Quad 550MHz Xeon Pentium III
Memory	4GB RAM
Drive(s)	34GB HDD; CD-ROM drive
NIC(s)	Intel Pro/1000 Gigabit Server Adapter
Operating System	Windows 2000 Advanced Server SP4
TOE Software	*Symantec LiveState Delivery 6.0.1 Configuration Server*
Machine running the Command Center	
Hardware	HP Compaq D330
Processor	Intel Pentium IV 2.8GHz
Memory	1GB RAM
Drive(s)	75GB HDD; CD-ROM drive
NIC(s)	HP Gigabit Ethernet Controller
Operating System	Windows XP Professional SP2
TOE Software	*Symantec LiveState Delivery 6.0.1 Command Center*
Machine hosting the Client	
Hardware	IBM 819175G
Processor	Intel Celeron 2.4GHz
Memory	128MB RAM
Drive(s)	40GB HDD
NIC(s)	Intel Pro/100 VE Network Controller
Operating System	Windows XP Professional SP2
TOE Software	*the Agents, namely:* • *Symantec LiveState Delivery 6.0.1 Agent For Windows;* • *Symantec LiveState Delivery 6.0.1 Boot Agent;* • *Symantec LiveState Delivery 6.0.1 Pre-OS Agent.*
Other Network Equipment:	
DHCP Server	
Hardware	Compaq Deskpro
Processor	Intel Pentium III 1.4GHz
Memory	768MB RAM
Drive(s)	144GB HDD
NIC(s)	3Com EtherLink XL 10/100 PCI
Operating System	Windows 2003 Enterprise Edition SP1
Router	
Hardware	Bay Networks Accelar 1100R-A

Table 1-1: Environmental Configuration (Developer's Tests & Evaluators' Tests)

IV. PRODUCT SECURITY ARCHITECTURE

Product Description and Architecture

57. The product consists of three main architectural features (see Figure 1-1):

    a. The **Configuration Server**, which:

    - supplies a package depot with all operating systems and applications delivered to Managed Computer(s);
    - supplies the configuration database for tracking all installation and configuration actions on Managed Computer(s);
    - supplies services for remotely administering PCs over the network;
    - generates and stores the log files that are generated by the product.

    b. The **Command Center**, which is used to administer Managed Computer(s) and to manage the Configuration Server. The Command Center is also used to install the Agents onto the Managed Computer(s).

    c. The **Managed Computer(s)**, on which the Agents reside and perform any installation and/or configuration that is required. The Agents query the Configuration Server to discover what tasks are scheduled to be performed, download the packages required, and execute the tasks.

58. The administration of a Symantec LiveState Delivery network is an asynchronous operation. Authorised administrators deploy software to managed computers by first copying that software (via CD-ROM or by other means such as FTP) to the package depot on the Configuration Server and then scheduling tasks to be executed from that server.

59. Tasks are performed by the Agents on targeted Managed Computers at a defined time, or the product pushes tasks that are immediately performed on Managed Computers. Completed work is reported back to the Configuration Server. The authorized administrators can then use the Command Center to determine the status of the Managed Computers.

60. The product's data exchange is based on IP. The product can be set up in either BOOTP or DHCP environments.

61. A Managed Computer must be installed with a PXE-compatible network card and, when booted from the network, it receives an IP address from the DHCP Server. In addition, the Managed Computer receives the name of the Boot Agent and the IP Address of the Configuration Server (these details require configuration of the DHCP Server options, as detailed in the guidance documentation identified above under 'Installation and Guidance Documentation').

62. The Managed Computer then requests the download of the Boot Agent from the Configuration Server. The Boot Agent runs in memory on the Managed Computer,

and requests the download of both the Pre-OS Agent and Agent For Windows, also from the Configuration Server.

63. Once the Agent For Windows has been downloaded onto the Managed Computer, it is then possible to install operating system and other software applications on to the Managed Computer by assigning packages.

64. The Administrator assigns a package to a Managed Computer using the Command Center. Once assigned, the Configuration Server communicates with the Agent For Windows on the Managed Computer, in order to download and run the package on the Managed Computer. A package needs to be created for each item of software that is required to be installed on the Managed Computer – whether this is an operating system or application.

65. Figure 1-1 above shows the components and scope of the TOE. Figure 1-2 above shows the TOE components within a typical network environment for the TOE.

Design Subsystems

66. The high level design subsystems of the TOE are:

a. **Command Center.** Administrators access the TOE through this subsystem, which is a GUI interface snap-in to Microsoft Management Console, providing a tree-structure interface across all Windows management functions.

b. **LiveState Services.** The TOE is accessed and changed via this subsystem. This subsystem manages the configuration database and its consistency by providing controlled access to its data by means of the Database Business Logic subsystem.

c. **Database Business Logic.** This subsystem verifies data in the Configuration Database and verifies action integrity requests made by the Command Center subsystem.

d. **Configuration Database.** This subsystem stores all LiveState data. The database allows data to be accessed, read or written.

e. **Log Files.** This subsystem generates various detailed log files that provide an audit trail of actions performed by administrators, services and agents.

f. **Package Depot Files.** This subsystem contains the directory and data for the configuration packages which are deployed on the Managed Computers.

g. **Agent for Windows.** This subsystem controls the execution of software installation, action and configuration packages on Managed Computers.

h. **Pre-OS Agent.** This subsystem runs on a Managed Computer and establishes an IP stack for downloads. It partitions and formats the hard disk, transfers DOS system files to the system partition and downloads configuration files.

i. **Pre-OS Boot File.** This subsystem establishes communication with the Configuration Server in order to determine the value of the Managed Computer's net boot flag.

Hardware and Firmware Dependencies

67. The TOE is software only; it has no hardware or firmware components.

68. The TOE depends on hardware and firmware in its environment as follows:

a. **interrupts and exceptions.** The hardware is relied upon to raise device interrupts to the CPU. When these interrupts are received, the current context is saved and the interrupt is identified and serviced. Then the saved context is restored and processing continues. Exceptions (i.e. unexpected events, such as divide by zero) are handled in a similar manner to interrupts.

b. **memory allocation.** The Configuration Server's operating system allocates memory from its virtual address space, when memory is needed by the TOE software.

c. **system clock.** The system clock provided by the underlying hardware is used for calculating timestamps used by the TOE software for audit trails, checking the validity of service requests based on time constraints, etc.

Product Interfaces

69. The external interfaces (i.e. the TOE Security Functions Interface (TSFI)) are:

a. **Interface between the administrator and the Command Center:** the Command Center provides the administrator with a tree-structure interface to administer Managed Computers and the Configuration Server.

b. **Interface between the TOE and the operating system (from the Command Center, the Configuration Server and the Agent For Windows):** the Command Center, the Configuration Server (LiveState Services subsystem) and the Agent For Windows all interface with their local operating system, in order to communicate (e.g. to download packages).

c. **Interface between the Pre-OS Agent and the Managed Computer:** the Pre-OS Agent interacts with the Managed Computer (specifically the BIOS and the hard disc).

d. **Interface between the pre-OS boot file and the Managed Computer:** the pre-OS boot file interacts with the Managed Computer (specifically the PXE-enabled NIC and the BIOS).

V. PRODUCT TESTING

IT Product Testing

70. During their on-site testing, the evaluators used the guidance in [j], [k] and [l] in order to install and generate a secure configuration, and to start-up the TOE.

71. The environmental configuration used by the Evaluators to test the TOE was equivalent to that used by the Developer to test the TOE, as summarised in Table 1-1 above.

72. The TOE was tested against the set of external interfaces that comprise the TSFI, as listed above under 'Product Interfaces'.

73. The Developer performed tests using all aspects of the TSFI. Those tests also exercised:

    a. all related security functions specified in the Security Target [d];

    b. all high level design subsystems identified above under 'Design Subsystems'.

74. The majority of the developer tests were automated and driven through a set of Rational Robot scripts; other than this no specialist tools or techniques were used. The rest of the Developer's testing was performed manually, following test scripts; those scripts contained all procedures necessary to repeat the tests and, where appropriate, provided a description of any external stimulus required.

75. The Evaluators performed the following independent testing:

    a. A sample of the Developer's tests was repeated, to validate the Developer's testing. The sample was at least 20% of the Developer's total security testing, and included tests from all functional areas, tests on all of the hardware models and tests performed by the Developer's different test engineers.

    b. For each interface of the TSFI, a test that was different from those performed by the Developer was devised wherever possible.

    Independent tests were thus performed for the majority of security functions.

76. The Evaluators also devised and performed penetration tests, wherever needed, to confirm the non-exploitability of potential vulnerabilities that had been noted during the evaluation.

77. The evaluators did not use any specific evaluation tools during the evaluation, except for the automated scripts used when repeating the developer tests (as noted in paragraph 74 above).

Vulnerability Analysis

78. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on both public domain sources and the visibility of the TOE given by the evaluation process.

Platform Issues

79. Platform issues are covered above under 'TOE Configuration' and 'Environmental Requirements'.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

[b] CLEF Requirements - Startup and Operation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.1, October 2003.

[d] Security Target for Symantec LiveState Delivery version 6.0.1,
Symantec Corporation,
Symantec LiveState Delivery\ST, Issue 1.2, 9 August 2006.

[e] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-001, Version 2.2, January 2004.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-002, Version 2.2, January 2004.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-003, Version 2.2, January 2004.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2004-01-004, Version 2.2, January 2004.

[i] Evaluation Technical Report,
BT CLEF,
LFS/T483/ETR, Issue 1.0, 28 June 2006.

[j] Release Notes - The Certified Symantec LiveState Delivery version 6.0.1,
Symantec Corporation,
Issue 1.9, 9 August 2006.

[k] Symantec LiveState Delivery Implementation Guide,
Symantec Corporation,
Part No. 10368644, Documentation Version 6.0, 2005.

[l] Symantec LiveState Delivery Reference Guide,
Symantec Corporation,
Documentation Version 6.0, 2005.

VII. ABBREVIATIONS

This list does not include well known IT terms such as LAN, GUI, PC, HTML, ... or standard Common Criteria abbreviations such as TOE, TSF, ... (See Common Criteria Part 1 [e], Section 2.3.)

BOOTP	BOOTstrap Protocol
DHCP	Dynamic Host Configuration Protocol
SP	Service Pack

This page is intentionally blank