UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P213

Clearswift Deep Secure

Release 2.0.0 E2
running on specified Clearswift Bastion platforms

Issue 1.0

February 2005

UK IT Security Evaluation and Certification Scheme, 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

Clearswift Deep Secure is a comprehensive e-mail management software suite supporting simultaneously SMTP and X.400 messaging protocols, including S/MIME signed and encrypted subscriber messages.

Clearswift Deep Secure Release 2.0.0 E2 has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the Clearswift Bastion platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Technical Manager of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorised	22 February 2005

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CC	Common Criteria
CLEF	Commercial Evaluation Facility
CSB2	Clearswift Bastion 2
CSDS	Clearswift Deep Secure
DAP	Directory Access Protocol
DISP	Directory Information Shadowing Protocol
DMZ	De-Militarised Zone
DSA	Directory System Agent
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
LSL	Labelling Support Library
MTA	Message Transfer Agent
PKI	Public Key Infrastructure
SFR	Security Functional Requirement
S/MIME	Secure Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SSL	Secure Sockets Layer
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
UKSP	United Kingdom Scheme Publication
VIC	Vendor Independent Cryptographic
VICI	Vendor Independent Cryptographic (Application Programming) Interface

(This page is intentionally left blank)

REFERENCES

a. Clearswift Deep Secure (CSDS) Security Target,
Clearswift Limited,
DN11240/4, Issue 4, 19 January 2005.

b. Common Criteria Certification Report P184, Clearswift Bastion II,
UK IT Security Evaluation and Certification Scheme,
P184, Issue 1.0, 12 June 2003.

c. Common Criteria Certification Report P170, Trusted Solaris Version 8 4/01,
UK IT Security Evaluation and Certification Scheme,
P170, Issue 3.0, 30 March 2004.

d. 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.

e. 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.

f. 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.

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

h. UK IT Security Evaluation and Certification Scheme CLEF Requirements,
Part I, Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02, Part I, Issue 4.0, April 2003.

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

j. Common Methodology for Information Technology Security Evaluation,
Part 2, Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CCIMB-2004-01-004, Version 2.2, January 2004.

k. Evaluation of Clearswift Deep Secure: LFL/T170 Evaluation Technical Report,
LogicaCMG CLEF,
310.EC114253:ETR.1, Issue 1.0, 11 February 2005.

l. Clearswift Deep Secure Installation Guide,
Clearswift Limited,
DN11407/1G, Issue 1.0, November 2004.

m. Clearswift Deep Secure Release 2.0.0 E2 Policy Servers Release Notice,
Clearswift Limited,
10 November 2004.

n. Clearswift Deep Secure ClearPoint Administration Guide,
Clearswift Limited,
DN11389/1, Issue 1.0, November 2004.

o. Clearswift Deep Secure Policy Servers Administration Guide,
Clearswift Limited,
DN11410/1, Issue 1.0, November 2004.

p. Clearswift Deep Secure PKI Configuration Administration Guide,
Clearswift Limited,
DN11409/1A, Issue 1.0A, November 2003.

q. Common Criteria Maintenance Report MR1, Clearswift Bastion II, Version 2.0.0
Derivative (Version 2.1.0) running on Trusted Solaris,
UK IT Security Evaluation and Certification Scheme,
Supplement to Certification Report P184, Issue 1.0, 5 November 2004.

r. Assurance Maintenance Status Summary: Sun Microsystems Inc., Trusted Solaris,
UK IT Security Evaluation and Certification Scheme,
Supplement to Certification Report P170, Issue 2.0, March 2004.

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Clearswift Deep Secure Release 2.0.0 E2 to the Sponsor, Clearswift Limited, 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 [Reference a] which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

Clearswift Deep Secure Release 2.0.0 E2.

This product is also described in this report as the Target of Evaluation (TOE), or as Clearswift Deep Secure. The Developer was Clearswift Limited.

4. Clearswift Deep Secure is a comprehensive e-mail management software suite supporting simultaneously SMTP and X.400 messaging protocols, including S/MIME signed and encrypted subscriber messages. The purpose of Clearswift Deep Secure is to provide controlled and audited flow of subscriber messages passing between two subscriber networks. Clearswift Deep Secure mediates the flow of a subscriber message in accordance with a specific entry in the current organisational security policy (the active Message Policy), which is determined from attributes of the subscriber message, including its originator and recipients.

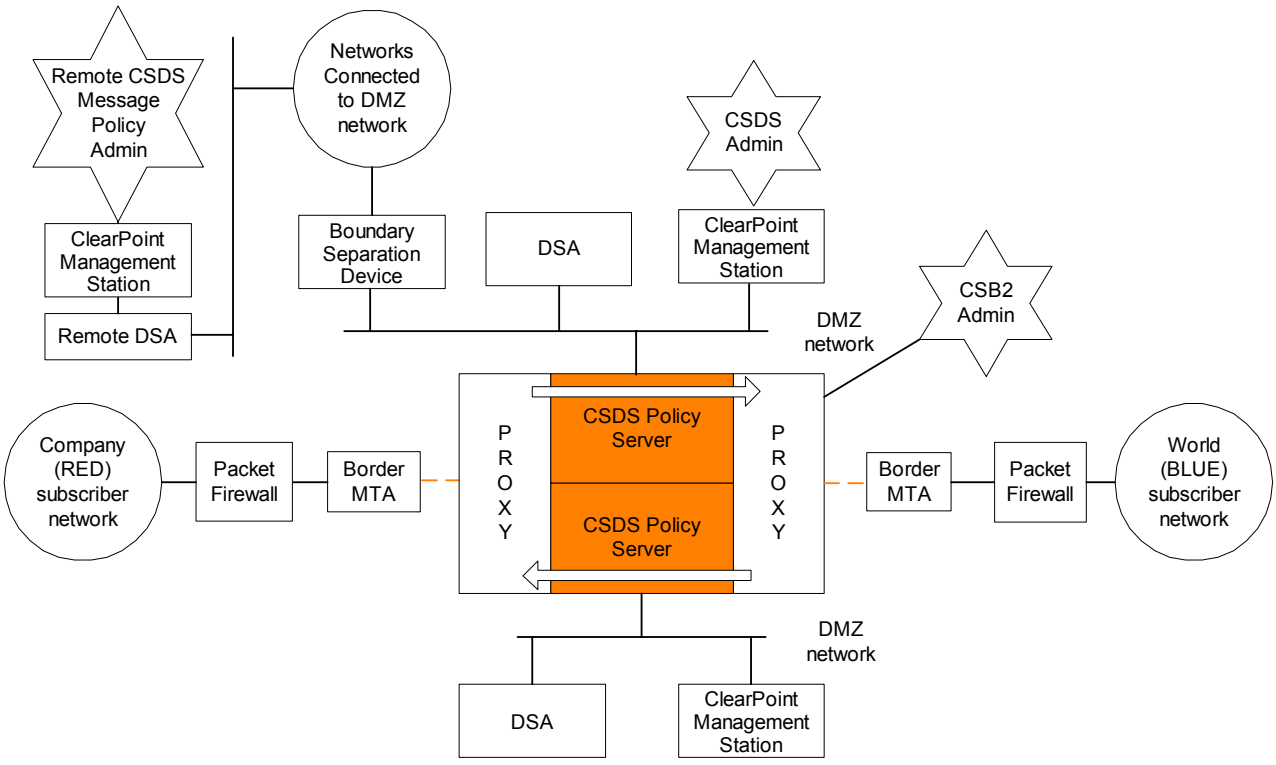
5. Each instance of Clearswift Deep Secure operates independently of any other instance, although any number of instances may be co-located and jointly managed.

6. Clearswift Deep Secure resides on and interfaces with a single Clearswift Bastion platform. Clearswift Bastion Version 2.0.0 has been evaluated and certified to Evaluation Assurance Level EAL4 [b] running on Trusted Solaris 8 4/01, which is also certified to EAL4 [c]. Clearswift Deep Secure also resides on assurance maintenance derivatives of these platforms [e.g. q, r].

7. The Clearswift Bastion platform provides Clearswift Deep Secure with two channels, one for each direction of message flow between the two subscriber networks, and assured separation between channels. Each Clearswift Bastion channel consists of two PROXY compartments (with X.400 and/or SMTP proxies) and a single VET compartment. The Clearswift Bastion platform also provides assured separation between each VET compartment and each of the two PROXY compartments, containing the SMTP or X.400 proxies, one for each subscriber network. The Clearswift Bastion platform forms part of the local IT environment of Clearswift Deep Secure.

8. Clearswift Deep Secure comprises two Policy Servers, one for each direction of message flow between the two subscriber networks, each residing in the VET compartment associated with the direction of message flow.

9. A single instance of Clearswift Deep Secure is connected to two subscriber networks. One network is designated the 'Company' network (generally the network that is part of the organisation that controls Clearswift Deep Secure). The other network is designated the 'World' network. The Company network is labelled RED; the World network is labelled BLUE. Connection is via the PROXY compartments of the Clearswift Bastion platform, as shown in the following diagram:



Single CSDS (coloured area = two instances of Policy Server)
Also illustrates location of administrators (remote shown for only one Policy Server)

10. It is assumed that a packet firewall is used to protect Clearswift Deep Secure and its Clearswift Bastion platform from low level attacks, such as denial of service, from each subscriber network if it is considered hostile. A border Message Transfer Agent (MTA) would normally be used to concentrate subscriber message traffic.

11. As stated above, Clearswift Deep Secure comprises two Policy Servers, one for each direction of message flow between the two subscriber networks. Each Policy Server resides in a separate VET compartment and must be connected to a separate DMZ network. Each DMZ network must contain a ClearPoint Management Station for management of the associated Policy

Server. Selection and activation of a specific Message Policy, management of message queues and stop/re-start of the Policy Engine must be performed directly using the ClearPoint Management Station on the DMZ network. Definition and modification of Message Policy may be performed using the ClearPoint Management Station on the DMZ network (either directly or via a Directory System Agent (DSA) on the DMZ network) or remotely from a ClearPoint Management Station on another network connected to the DMZ network (via DSAs on the remote and DMZ networks which are synchronized with Directory replication). Each Policy Server is thus configured for exclusively direct or DSA-based definition and modification of Message Policy.

12. Direct communication between the local ClearPoint Management Station and the Policy Server is over SSL (this configuration of ClearPoint allows all management operations, subject to the roles assigned to individual administrators).

13. Communication between a ClearPoint Management Station and a DSA uses DAP or LDAP (this configuration of ClearPoint only allows definition and configuration of Message Policy). Message Policies, each with an associated information integrity attribute (a digital signature), can be downloaded from the DSA on the DMZ network to the Policy Server. The Policy Server validates the integrity of each Message Policy, and authenticates the Administrator.

14. It is assumed that the DMZ network is protected from attacks from connected networks by an appropriately assured boundary separation device, e.g. a packet firewall and application level firewall. Protection is assumed to be provided against unauthorised access attempts and denial of service attacks.

15. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

16. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

17. Logically, the TOE comprises the following aspects of Clearswift Deep Secure message-flow management functionality:

a. Accurate identification and validation of all originator/recipient pairings (relationships) per message. A valid pairing must fall within the domains defined by, and controlled by, the active Message Policy.

b. Invocation of all necessary message-flow mediation checks (on the message elements derived from preliminary message unpacking) in accordance with per-relationship policy requirements. The checks result in zero or more policy event triggers.

c. Correct application of cryptographic operations, security label checking operations and virus scanning. For these functions the TOE boundary extends to the correct handling of calls to the underlying external libraries, which provide the basic functions on which these policy operations depend.

d. Release, deletion or queuing for manual inspection of messages as required by policy event triggers.

e. Invocation of excluded supplementary message handling actions (see paragraph 18) as required by policy event triggers.

f. Release or deletion of messages in accordance with manual inspection directives.

g. Logging of associated audit records.

h. Accurate routing and delivery of released messages, including internally generated notifications, to the correct subscriber network interface.

i. Separation, on the Clearswift Deep Secure policy server, of the management roles defined for manipulation of message queues and Message Policies.

j. Application, on the Clearswift Deep Secure policy server, of the TOE security management functions (updating, selecting, activating Message Policy, managing messages in queues and stopping/starting a Policy Engine).

18. Functionality excluded from the TOE includes:

a. Correct unpacking of messages into message elements, and reassembly of message elements into output messages.

b. The mediation checks applied to message elements (some of which use external libraries for virus scanning, cryptography and formal security labels).

c. Actions to remove, replace or annotate message content, as required by policy event triggers.

d. Actions to generate notification messages, as required by policy event triggers.

e. Actions to generate inbound or outbound archives, as required by policy event triggers.

f. The management interface running on ClearPoint Management Stations.

19. The environment of the TOE is assumed to be one of the certified or assurance maintained combinations of Clearswift Bastion 2 [b, q] in a Trusted Solaris 8 Operating System [c, r] context specified in Annex A.

Protection Profile Conformance

20. The Security Target [a] did not claim conformance to any protection profile.

Assurance

21. The Security Target [a] specified the assurance requirements for the evaluation. Predefined Evaluation Assurance Level EAL4 was used. CC Part 3 [f] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [d].

Strength of Function Claims

22. There was no claim for minimum Strength of Function.

Security Policy

23. The TOE Security Policy, including the Clearswift Deep Secure Message Flow Control Policy, is expressed implicitly within the Security Functional Requirements (SFRs) detailed in Section 5.1 of the Security Target [a].

24. The Organizational Security Policies with which the TOE must comply are defined within Section 3.3 of the Security Target [a].

Security Claims

25. The Security Target [a] fully specifies the TOE's security objectives, the threats which these objectives counter and the SFRs and security functions to elaborate the objectives. Some of the SFRs are taken from CC Part 2 [e]; use of this standard facilitates comparison with other evaluated products.

26. The SFRs not taken from CC Part 2 are as follows.

a. FCS_COP.1X, *Calls to cryptographic operations*, which requires properly formed calls to symmetric and asymmetric encryption and digital signature operations, depending on the CC Part 2 SFR FCS_COP.1.

b. FDP_LCK.1X, *Calls to label checking operations*, which requires properly formed calls to message security label validity and clearance checking operations, dependent on the explicitly stated environmental SFR FDP_LCK.2X.

c. FIA_UAU.2X, *User authentication before any action*, which requires each user to be successfully authenticated by appropriate calls to cryptographic operations before allowing any other TSF-mediated actions on behalf of that user, depending on FCS_COP.1X.

d. FIA_UID.2X, *User identification before any action,* which requires each user to identify itself by appropriate calls to cryptographic operations before allowing any other TSF-mediated actions on behalf of that user, hierarchical to the CC Part 2 SFR FIA_UID.1 and dependent on FCS_COP.1X.

e. FMC_VSF.1X, *Calls to virus scanner filters*, which requires properly formed calls to Virus Scanner Filters, dependent on the explicitly stated environmental SFR FMC_VSF.2X.

f. FMT_MSA.3X, *Static attribute initialization*, which requires enforcement of the Message Flow Control Policy to ensure that no subscriber message flow is permitted prior to the selection and activation of a Message Policy, depending on the CC Part 2 SFR FMT_MSA.1. (This is a modified version of the CC Part 2 SFR FMT_MSA.3.)

27. In addition to these, the following SFRs for the IT environment are not taken from CC Part 2.

a. FDP_LCK.2X, *Label checking operations*, which requires the IT environment to check the validity of a given message security label and to check that the label is dominated by a specified clearance.

b. FMC_VSF.2X, *Virus scanner filters*, which requires the IT environment to scan message elements in order to detect malicious code corresponding to a set of malicious code definitions.

Evaluation Conduct

28. 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 [g-i]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

29. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], 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 [f] and the Common Evaluation Methodology [j].

30. The Certification Body monitored the evaluation which was carried out by the LogicaCMG Commercial Evaluation Facility (CLEF). The evaluation was completed when the CLEF submitted the final Evaluation Technical Report (ETR) [k] to the Certification Body in February 2005. The Certification Body then produced this Certification Report.

General Points

31. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. 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.

32. 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 products and whether such patches have been evaluated and certified.

33. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

34. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [k] under the CC Part 3 [f] headings. The following sections note considerations that are of particular relevance to consumers.

Delivery

35. Secure delivery of the TOE is described in the delivery procedures, detailed in Section 3 of the Installation Guide [l], which describes the process of releasing the TOE to consumers.

36. Following confirmation of an order, a Clearswift Deep Secure CD-ROM containing a copy of the TOE and its guidance documentation [m, o][1] is packed with the Clearswift Bastion media in Clearswift-branded packages with a tamper-resistant seal to form an installation kit. If requested by the customer, the installation kit will also include Trusted Solaris media and documentation, supplied in Sun's original packaging.

37. Clearswift Deep Secure is delivered and installed on a Clearswift Bastion platform, as part of the secure delivery process for Clearswift Bastion, as described in [b]. The TOE with delivery note is hand delivered to the consumer - either as an installation kit for use by the Clearswift or Clearswift trained consumer installation team at the consumer site, or as a pre-installed, pre-configured system including the platform (i.e. Clearswift Bastion, Trusted Solaris and required hardware). Hand delivery by a trusted person ensures that the TOE is not susceptible to tampering during delivery.

38. On receipt of the TOE, the consumer is recommended to check the contents of the delivery against the delivery note, as described in [b], and to check that the evaluated version has been supplied as detailed in the Release Notice [m].

Installation and Guidance Documentation

39. Secure installation, generation and start up of the TOE are described in the Installation Guide [l][1] and Release Notice [m].

40. Administration and use of the TOE is described in the Clearswift Deep Secure Administration Guides [n-p][1].

41. Note that all human interaction with the TOE is by authorised administrators and that user guidance is therefore not applicable.

[1] [l] is supplied only to qualified installers. [n, p] are supplied with their respective ClearPoint and PKI products.

Strength of Function

42. There was no Strength of Function claim for the TOE. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE and that a Strength of Function claim was not required.

Vulnerability Analysis

43. The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. No exploitable vulnerabilities were identified in the construction of the TOE or from the public domain sources.

Platform and Environmental Issues

44. The environment of the TOE is assumed to be one of the two certified or assurance maintained combinations of Clearswift Bastion 2 [b, q] in a Trusted Solaris 8 Operating System [c, r] context as specified in Annex A. The Developer and Evaluator testing summarized in Annex C covered both of these two combinations.

45. The Evaluators agreed with a Developer assertion that use of the TOE with a future assurance maintained derivative of Clearswift Bastion 2 (on specified version(s) of Trusted Solaris) would involve only a low risk of the security of the TOE being undermined. This was based on a rationale which argued that:

- the TOE makes straightforward use of Clearswift Bastion 2 interfaces (associated only with Bastion queues and VET compartments)

- the TOE uses standard Solaris programming interfaces and functions (e.g. file management and syslog) that are designed to be consistent between different Trusted Solaris 8 derivatives; Clearswift programming standards would ensure that these interfaces and functions are used consistently throughout the TOE and Clearswift Bastion 2, and this usage would be tested under the assurance maintenance of Clearswift Bastion 2.

46. Details of the specific Sun SPARC Workstations that also form part of the TOE environment are included in the Clearswift Bastion 2 documentation [b, q]. All TOE communication with the hardware platform is via Clearswift Bastion and/or standard Solaris programming interfaces and functions. As part of the Clearswift Bastion evaluation [b] and assurance maintenance [q], the Sponsor supplied a hardware Multi-Platform Rationale that examined the impact of platform variations. The Evaluators confirmed that this rationale was also applicable to the evaluation of Clearswift Deep Secure. The Developer and Evaluator testing summarised in Annex C supported this Multi-Platform Rationale.

47. The Vendor Independent Cryptographic (VIC) subsystems, Labelling Support Library (LSL) subsystems and virus scanners used in the test configurations are specified in Annex A. The Developer asserts that the Developer testing summarized in Annex C will be used to test the TOE with other such VIC subsystems, LSL subsystems and virus scanners. The Evaluators considered this testing to be thorough and appropriate to support the assertions of Annexes A, B and C of the Security Target [a] which were additional to the security claims made for the TOE.

III. EVALUATION OUTCOME

Certification Result

48. After due consideration of the ETR [k], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Clearswift Deep Secure Release 2.0.0 E2 meets the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL4 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on the Clearswift Bastion platforms specified in Annex A.

Recommendations

49. Prospective consumers of Clearswift Deep Secure should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

50. The TOE should be delivered, installed, configured and used in accordance with the supporting guidance documentation [l-p] included in the evaluated configuration.

51. Particular care should be taken to secure any onward connections from the local DMZ, including those for remote TOE management.

52. Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under 'TOE Scope' and 'Evaluation Findings'. However, the Certification Body recommends that any evaluated or assurance-maintained security patches to Clearswift Deep Secure, Clearswift Bastion 2 and Trusted Solaris 8 are applied if they counter vulnerabilities relevant to the security of the TOE.

53. The Certification Body also recommends that any security patches relevant to the ClearPoint Management Station and any infrastructure (e.g. the DSAs and boundary separation devices) on the DMZ networks supporting local and remote TOE management are also applied to counter vulnerabilities relevant to the secure management of the TOE.

54. With regard to the Developer assertion of paragraph 45, it is recommended that Maintenance Reports for future assurance maintained derivatives are consulted, e.g. to confirm on which version of Trusted Solaris 8 a future derivative of Clearswift Bastion 2 has been assurance maintained.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE is uniquely defined as:

   Clearswift Deep Secure Release 2.0.0 E2 Pkg Vn 2.02.37, also termed in this report as Clearswift Deep Secure (CSDS). It is marketed as Clearswift Deep Secure Release 2.0.0 E2.

2. The TOE software is available on CD-ROM, which is labelled with the TOE version number. Only parts of this software were evaluated; for further details, see the 'TOE Scope' section in the main body of the Report.

TOE Documentation

3. The supporting guidance documents evaluated were:

   - the Installation Guide [l] – supplied only to qualified installers
   - the Release Notes [m]
   - the ClearPoint Administration Guide [n]
   - the Policy Servers Administration Guide [o]
   - the PKI Configuration Administration Guide [p]

4. Further discussion of the guidance documents is provided above under the heading ‘Installation and Guidance Documentation’.

TOE Configuration

5. The TOE should be configured in accordance with the guidance documents identified in paragraph 3 above.

6. The evaluated configuration covers two options, whereby distribution of Message Policy is either directly from a ClearPoint Management Station on the DMZ network or via DSAs.[2]

Environmental Configuration

7. The evaluated TOE runs on a single Sun SPARC workstation with a certified or assurance maintained combination of Sun Trusted Solaris 8 and Clearswift Bastion 2.

8. The combinations[3] of Sun Trusted Solaris 8 and Clearswift Bastion 2 applicable to the certification of the TOE are:

   - Clearswift Bastion 2 [b] on Trusted Solaris 8 4/01 [c]
   - Clearswift Bastion 2.1 [q] on Trusted Solaris 8 12/02 [r]

---

[2] Equivalent configuration options exist for distribution of virus definition updates.

[3] See paragraph 45 for assertions related to other platform combinations.

9. Details of the specific Sun SPARC Workstations that form part of the TOE environment are included in the Clearswift Bastion 2 documentation [b, q].

Environmental Test Configuration

10. The TOE was tested on the following configurations of Sun SPARC workstation, Sun Trusted Solaris 8 and Clearswift Bastion 2:

Test Config	Platform	Software Environment	Memory	Disc Size	Network Interface Card
1	Sun Blade 100 UltraSPARC IIe Single 500MHz OpenBoot V4.3	Clearswift Bastion 2 Trusted Solaris 8 4/01	256MB[4]	18GB	One X1034A Sun Quad FastEthernet PCI Adapter card
2	Sun Fire 280R UltraSPARC III Dual 750MHz OpenBoot V4.2	Clearswift Bastion 2 Trusted Solaris 8 4/01	4GB	2x32GB	One X1034A Sun Quad FastEthernet PCI Adapter card
3	Sun Blade 150 UltraSPARC IIe Single 650MHz OpenBoot V4.6	Clearswift Bastion 2.1 Trusted Solaris 8 12/02	256MB	40GB	One X1034A Sun Quad FastEthernet PCI Adapter card
4	Sun Fire 280R UltraSPARC III Dual 750MHz OpenBoot V4.2	Clearswift Bastion 2.1 Trusted Solaris 8 12/02	4GB	2x32GB	One X1034A Sun Quad FastEthernet PCI Adapter card

11. Each test configuration used one of the following VIC subsystems (each subsystem incorporating an external cryptographic library):

- Cryptomathic PrimeInk Premium VIC for Clearswift Deep Secure Pkg Vn 1.0.07
- S/MIME Freeware Library VIC for Clearswift Deep Secure Pkg Vn 3.00.36
- Null VIC for Clearswift Deep Secure Pkg Vn 3.0.36

12. Each test configuration used one of the following LSL subsystems (each subsystem incorporating an external label checking library):

- X.841 LSL for Clearswift Deep Secure Pkg Vn 3.00.36
- Null LSL for Clearswift Deep Secure Pkg Vn 3.00.36

13. Each test configuration used between zero and four virus scanners, including the following:

- Sophos SAVI Virus Scanner, issues January 2003, June 2003 and September 2003
- CSAV Command AV for Solaris, Vn 4.70.0

14. ClearPoint software Version 4.7.6.35 was installed on the ClearPoint Management stations used in the test configurations.

[4] For evaluator testing this system was replaced with an identical system containing 1GB memory.

15. Within the test configurations, boundary separation devices protecting the DMZ network were Directory Bastions running Clearswift Bastion 2 configured with DISP (X.525) vet and proxy software.

16. Further details of the use of the test configurations by the Developer and Evaluators are provided in Annex C.

(This page is intentionally left blank)

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of the report and in Annex A.

Architectural Features

2. Clearswift Deep Secure resides on and interfaces with a single Clearswift Bastion platform.

3. The Clearswift Bastion platform provides Clearswift Deep Secure with two channels, one for each direction of message flow between the two subscriber networks, and assured separation between channels. Each Clearswift Bastion channel consists of two PROXY compartments (with X.400 and/or SMTP proxies) and a single VET compartment. The Clearswift Bastion platform also provides assured separation between each VET compartment and each of the two PROXY compartments, containing the SMTP or X.400 proxies, one for each subscriber network. The Clearswift Bastion platform forms part of the local IT environment of Clearswift Deep Secure.

4. Clearswift Deep Secure comprises two Policy Servers, one for each direction of message flow between the two subscriber networks, each residing in the VET compartment associated with the direction of message flow.

5. Physically the TOE comprises those software components of a Clearswift Deep Secure Policy Server which provide the logical functionality specified under the 'TOE Scope' section in the main body of the report, specifically:

a. The Policy Engine, except the exclusions identified in the next paragraph;

b. The Administration process (including a DSA synchronisation agent), excluding the Cryptographic Subsystem; and

c. The Queue Manager.

Environmental Features

6. The TOE excludes the following software components, which form the TOE IT environment:

a. The Policy Engine embedded modules that implement:

i. Message decomposition and re-composition functions; and

ii. policy mediation check functions and policy action functions,

as listed under the logical description of the 'TOE Scope' section in the main body of the report.

b. The Clearswift Deep Secure Policy Engine external libraries for:

i. virus scanning;

ii. cryptography; and

iii. formal security labels.

c. The encompassing system environment (Clearswift Bastion and Trusted Solaris).

d. ClearPoint Management Stations.

e. X.500 Directory Servers (DSAs).

f. Certification Authority software to create X.509 Certificates and Certificate Revocation Lists.

g. The Clearswift Deep Secure Directory Synchronisation Agent for uploading virus definition updates into a remote X.500 Directory Server.

h. Border MTAs.

i. Boundary Separation devices.

Design Subsystems

7. The high level design subsystems of the TOE are as follows.

a. MGADMIN, the administrative server of Clearswift Deep Secure, which provides role authentication, stop/start of ENGINE, and management of logs, queues and policy changes.

b. ENGINE. This subsystem recursively decrypts and decomposes the data, identifies originators, resolves policy, splits messages, applies policy checks and actions, re-encrypts and re-composes data and updates the audit trail.

c. DSSYNC, which is the directory synchronization agent for configurations requiring policy distribution or virus updates via an X.500 or LDAP directory in the DMZ network.

d. CSBIF, which provides the interface with Clearswift Bastion.

e. CTRLSCRIPTS. This is a set of scripts which supports the administration of the MGADMIN and ENGINE subsystems.

8. Several components of the Clearswift Deep Secure product are in the environment of the TOE, including the Policy Engine embedded modules and external libraries noted in subparagraphs 6.a and 6.b above.

Hardware and Firmware Dependencies

9. The TOE includes no hardware or firmware components. Clearswift Deep Secure is embedded in the Clearswift Bastion VET compartment software which forms part of its environment. The hardware and firmware dependencies of Clearswift Deep Secure are identical to those of Clearswift Bastion detailed in the associated Certification Report [b].

TOE Security Function Interface (TSFI)

10. The TSFI provides the interfaces between the TOE and:

- Clearswift Bastion
- Trusted Solaris (used by all subsystems)
- ClearPoint Management Station (in the DMZ)
- Policy Engine embedded modules noted in subparagraph 6.a above
- Cryptographic operations library[5]
- Formal security label checking library
- Virus scanning library

11. The local ClearPoint Management Station on the DMZ network can modify and load Message Policy onto the Policy Server; and ClearPoint commands can select active policy, stop/start Policy Engine, inspect Manual queues and individual messages contained within, and release or discard held messages, etc. All these interactions are conveyed by authenticated SSL. The Vendor independent Cryptographic Application Programming Interface (VICI) is used to authenticate the Clearswift Deep Secure Administrator.

12. The ClearPoint Management Station can modify and store Message Policy on a DSA. The DSA where Message Policy is stored may be a remote DSA, in which case Directory replication may be used so that the DSA on the DMZ network holds a copy of the remotely mastered data. Message Policies, each with an associated integrity information attribute (a digital signature), are downloaded from the DSA on the DMZ network to the Policy Server. The VICI is used to validate the integrity of each Message Policy, and to authenticate the Clearswift Deep Secure Message Policy Administrator who modified it. No data can be uploaded from the Policy Server to the DSA. The Policy Server initiates all connections, and provides authentication to the DSA if required.

13. The Policy Engine embedded modules and the three libraries listed above are bound with the TOE at run-time, and thus share some memory and stack. No architectural separation mechanisms exist to enforce non-interference, but a degree of protection is provided by object orientated encapsulation principles that are employed consistently at all interfaces to ensure TOE data structures are protected as private or read-only data.

[5] The interface to the DSAs is via the cryptographic operations library.

(This page is intentionally left blank)

ANNEX C: PRODUCT TESTING

IT Product Testing and Test Configurations

1. The Developer's Test Plan included 128 tests covering all SFRs, all TOE high level subsystems (identified in Annex B), all security functions and the TSFI (as detailed in Annex B). It included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. It also included tests to check the installation and configuration of the TOE, the administrative functions and the message flow management functions.

2. The Developer's testing used 3 different Sun SPARC Workstations specifically configured to address the hardware platform variations. It also used the two combinations of Sun Trusted Solaris and Clearswift Bastion 2 specified in Annex A paragraph 8. This resulted in test configurations 1-4 specified in Annex A. The full set of tests was run on each platform for Build Pkg Vn 2.02.36. Except for one minor difference, identical results were obtained on each platform and satisfactorily demonstrated the correct operation of the TOE in all platform variation conditions.

3. Subsequent to these tests, the Clearswift Deep Secure software was updated to address a communications protocol vulnerability. A subset of 37 tests was therefore rerun on 2 test configurations (1 and 4) using TOE Build Pkg Vn 2.02.37 to check the updated protocol and the correction of the minor difference, together with some regression tests. Identical results were obtained on each platform, which satisfactorily demonstrated the correct operation of the TOE.

4. Developer testing utilized a number of network configurations. Each configuration consisted of 3 or more co-located Sun SPARC workstations, situated between 2 representative subscriber networks, and sharing 2 DMZ networks. Each subscriber network included several subscriber host computers handling test mail messages and test tools, together with an MTA. Each subscriber host could therefore examine incoming and outgoing mail messages in either traffic flow direction. For each direction of message flow, a DMZ network was used for communication with both a ClearPoint Management Station and DSA, covering the two configuration options noted in Annex A paragraph 6. This test configuration facilitated the testing of not only the TOE and the TSFI, but also the correct operation of the local and remote ClearPoint functionality (which was not included in the TOE).

5. The above Developer's testing also covered the VIC subsystems, LSL subsystems and virus scanners listed in Annex A.

6. The Evaluator's testing used test configurations 1 and 4 in conjunction with TOE Build Pkg Vn 2.02.37. The Evaluators witnessed the full installation and configuration of the TOE on test configuration 1 and confirmed that test configurations 1 and 4 were consistent with that specified in the Security Target [a].

7. The Developer tests were comprehensive. To validate the Developer's testing, the Evaluators therefore witnessed the repeat of a sample of 31 developer tests on test configuration 1 and a different sample of 21 tests on test configuration 4 covering areas that had not been regression tested by the Developer. Together, these exercised over 40% of the Developer's Tests. The test results were identical to those produced by the Developer.

8. The Evaluators devised a further set of 6 independent functional tests, different to those performed by the Developer, on test configurations 1 and 4 to test the TOE independently. No anomalies were found. The Evaluators, in conjunction with the Developer and Certification Body, also devised a set of 11 penetration tests on test configuration 1 to address potential vulnerabilities considered during the course of the evaluation. No vulnerabilities or errors were detected.

9. The penetration tests related to the administration networks included examining TOE behaviour related to the handling of abnormal Message Policy files and the loss of specific services on the DMZ network.

10. Due to the comprehensiveness of the Developer tests, the Evaluators used only one virus scanner in their configuration (SOPHOS SAVI, September 2003) and only one VIC library (S/MIME Freeware Library). Their tests covered the two configuration options noted in Annex A paragraph 6.

11. Further evidence of the correct operation of the TOE's platform (i.e. Clearswift Bastion and Trusted Solaris 8 on specified Sun SPARC Workstations) is reported in [b, c, q and r].