122-B

COMMON CRITERIA CERTIFICATION REPORT No. P228

Clearswift DeepSecure
Release 2.1
running on specified CSB2 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	**Clearswift**
Product and Version	**Clearswift DeepSecure Release 2.1**
Description	Clearswift DeepSecure is a comprehensive e-mail policy management software suite supporting simultaneously SMTP and X.400 messaging protocols, including S/MIME signed and encrypted subscriber messages.
CC Part 2	**Extended**
CC Part 3	**Conformant**
EAL	**EAL4**
CLEF	**BT CLEF**
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 itself first 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.

Trademarks:

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

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Clearswift DeepSecure (CSDS) Release 2.1 to the Sponsor, Clearswift, 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) [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:

> **Clearswift DeepSecure Release 2.1**, abbreviated as **DeepSecure 2.1** or **CSDS 2.1**.

4. The Developer was Clearswift, with some aspects of development subcontracted to Metanate and Softwire.

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

6. A CSDS deployment comprises one or more CSDS Servers, two or more ClearPoint management systems, and optionally one or more SPIF Editors. Each CSDS Server operates independently of any other CSDS Server, although any number of CSDS Servers may be co-located, with Policy Servers associated with the same direction of subscriber message flow being jointly managed. In general, Policy Server management functions must be performed from ClearPoint attached to the DMZ network or directly from a Clearswift Bastion 2 (CSB2) terminal. However, Message Policy and X.841 SPIFs may be modified from another network connected to the DMZ network.

7. 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’.

8. A CSDS Server resides on and interfaces with a single EAL4 certified CSB2/TSOL platform, which provides assured separation between the subscriber networks, and assured protection for Policy Servers from eavesdropping and message modification

attacks. CSB2 provides CSDS with two channels, one for each direction of subscriber message flow between the two subscriber networks, and assured separation between channels. Each CSB2 channel consists of two PROXY compartments (with X.400 and/or SMTP proxies) and a single CSB2 DMZ (VET) compartment. The CSB2/TSOL platform also provides assured separation between each CSB2 DMZ (VET) compartment and each of the two CSB2 PROXY compartments, containing the SMTP or X.400 proxies, one for each subscriber network. The CSB2/TSOL platform forms part of the local IT environment of the TOE.

9. A CSDS Server comprises two Policy Servers, one for each direction of message flow between the two subscriber networks, each residing in the CSB2 VET compartment associated with the direction of message flow.

10. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Protection Profile Conformance

11. The Security Target [d] did not claim conformance to any protection profile.

Security Claims

12. The Security Target [d] fully specifies the TOE's security objectives, the threats and Organisational Security Policies (OSPs) which these objectives counter and meet (respectively) 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.

13. The SFRs not taken from CC Part 2 are detailed in Section 5 of the Security Target (ST) [d].

14. The TOE security policy, the CSDS Message Flow Control Policy, is detailed in Section 5.1 of the ST [d]. The OSPs with which the TOE must comply are defined within Section 3.3 of the ST [d].

Strength of Function Claims

15. **There was no minimum Strength of Function (SoF) claim made**.

Evaluation Conduct

16. 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) [a] and UKSP 02 ([b], [c]). The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty's Government. As stated on page 1 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.

17. Although this was a re-evaluation, a significant portion of the TOE Security Functions and security environment, together with much of the supporting evaluation deliverables, was changed from that of Clearswift DeepSecure 2.0, Certification Report [i], which had previously been certified by the UK IT Security Evaluation and Certification Scheme to the CC EAL4 assurance level. For the evaluation of Clearswift DeepSecure 2.1, the Evaluators addressed every CEM [h] EAL4 work unit but made some use of Clearswift DeepSecure 2.0 evaluation results where these were valid for both Clearswift DeepSecure 2.1 and the CEM requirements.

18. 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], applying all relevant CC interpretations and all applicable previous evaluation results [n]. The results of this work, completed in August 2006, were reported in the ETR [l].

Conclusions and Recommendations

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

20. **Prospective consumers of Clearswift DeepSecure Release 2.1 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.

21. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III ‘Evaluated Configuration’.

22. **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.

23. **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 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

24. The following sections note considerations that are of particular relevance to consumers of the product.

Delivery

25. **On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery**.

26. The TOE is generally hand delivered, but can also be made available to consumers for download via FTP or delivered on CD-ROM or DVD-ROM. 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 with the Policy Server pre-installed, on a preconfigured 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. DeepSecure Policy Server is delivered and installed on a Clearswift Bastion platform, as part of the secure delivery process for Clearswift Bastion, as described in [j]. The ClearPoint and SPIF Editor components are installed at the customer site on the relevant platforms, as described in [v] and [w].

27. On receipt of the TOE, the consumer is recommended to check the contents of the delivery against the delivery note, as described in [j], and to verify the images used for installation by generating MD5 checksums for the objects received and comparing them with the MD5 hash values detailed in the relevant Release Notices ([o] - [r]).

Installation and Guidance Documentation

28. Secure installation, generation and start up of the TOE Policy Server are performed by qualified installers, and are described in the Installation Guide [s] and Release Notice [o]. The administration and use of the TOE Policy Server is described in [t] and [u].

29. Secure installation, generation and start up of ClearPoint and SPIF Editor[1] are described in [v] and [w], respectively, together with the description of the administration and use of these components.

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

[1] The X.841 package for formal security label support together with the associated SPIF Editor are part of the TOE and are optional within a deployment.

III. EVALUATED CONFIGURATION

TOE Identification

31. The TOE consists of:

Clearswift DeepSecure Release 2.1:

a. Policy Server, Policy Engine Vn 5.1.0.65 (Pkg Vn 3.20.52)

b. X.841 Label support library for Solaris: Vn 2.03.00 (Pkg Vn 3.20.50)

c. ClearPoint v5.1.40.0

d. X.841 Label support library for Windows: Vn 2.03.00

e. SPIF Editor v1.08

32. The TOE software is made available on CD-ROM/DVD-ROM or via FTP download. The versions of the components used by the Policy Engine are recorded in the system log file. Alternatively the versions of the packages can be gained using the "pkginfo" command on Solaris. The version of ClearPoint and the SPIF Editor can be gained via the Help > About menu.

TOE Documentation

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

- Installation Guide [s];
- Policy Servers Administration Guide [t];
- PKI Configuration Administration Guide [u];
- ClearPoint Administration Guide [v];
- SPIF Editor Administration Guide [w];
- System Planning Guide [x];
- Release Notices [o]-[r].

34. The guidance documentation is distributed together with the TOE software.

TOE Scope

35. A CSDS Server comprises two Policy Servers, one Policy Server for each direction of subscriber message flow between the two subscriber networks, each

residing in the CSB2 VET compartment associated with the direction of subscriber message flow.

36. A Policy Server comprises the following components:

- Policy Engine;
- External Libraries (environment);
- X.841 LSL (optional formal security label subsystem);
- Q-handler Service;
- Administration Service;
- Directory Synchronisation Agent;
- PKI Configuration Utility.

37. ClearPoint management station comprises the following components:

- ClearPoint GUI;
- External Libraries (environment).

38. A SPIF Editor platform comprises the following components:

- SPIF Editor GUI;
- External Libraries (environment).

39. The SPIF Editor is an optional component that provides configuration used by the X.841 LSL, which is an optional External Library for the Policy Server and ClearPoint.

40. Items excluded from the TOE include the following external libraries that may be invoked by the Policy Engine to perform additional checks and actions:

- data type recognition, decomposition, text extraction, macro detection and re-composition subsystem;
- textual analysis subsystem;
- virus scanner subsystem;
- spam detection subsystem;
- formal security label subsystem (other than the X.841 LSL, which is included in the TOE);

- cryptographic subsystem.

41. The cryptographic subsystem is also used by the Administration Service, the Directory Synchronisation Agent, the PKI Configuration Utility, the X.841 LSL option for the formal security label subsystem, ClearPoint and the SPIF Editor.

42. The Directory Synchronisation Agent is part of the Policy Server. It supports administration, using ClearPoint in Directory-mode, of the Message Policy by authorised CSDS Directory-mode Administrators, who are permitted to define and modify the behaviour of a Message Policy that is stored in an X.500 (or LDAP) Directory, which forms part of the TOE environment. It also supports administration of malicious code definition and spam definition updates stored in a Directory by IT Environment administrators using a Directory Synchronisation Uploader.

43. Items excluded from the TOE also include the following:

- The encompassing system environments:
    - CSB2/TSOL platform for CSDS Server (including SMTP or X.400 proxies)
    - Internet Explorer on Microsoft Windows for ClearPoint
    - A JAVA VM on Microsoft Windows, Linux or Solaris for the SPIF Editor
- Certification Authority software to create X.509 Certificates and Certificate Revocation Lists, and publish these into an X.500 (or LDAP) Directory
- The CSDS Directory Synchronisation Uploader for uploading malicious code definition and spam definition updates into an X.500 (or LDAP) Directory
- X.500 (or LDAP) Directory Servers[2]
- Border MTAs
- Boundary Separation devices
- Packet firewalls.

TOE Configuration

44. The evaluated TOE configuration is as follows:

45. A single CSDS Server is connected to two subscriber networks. One network is designated the ‘Company’ network (generally the network that is part of the organisation that controls the TOE); 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 CSB2/TSOL platform.

[2] The ST [d] uses the term Directory System Agent, as defined in X.500, in place of Directory Server.

46. There can be multiple instances of a CSDS Server within a given network, comprising a CSDS Server farm. These all operate independently, with the option of synchronising policies between the servers via a ClearPoint or Directory Server.

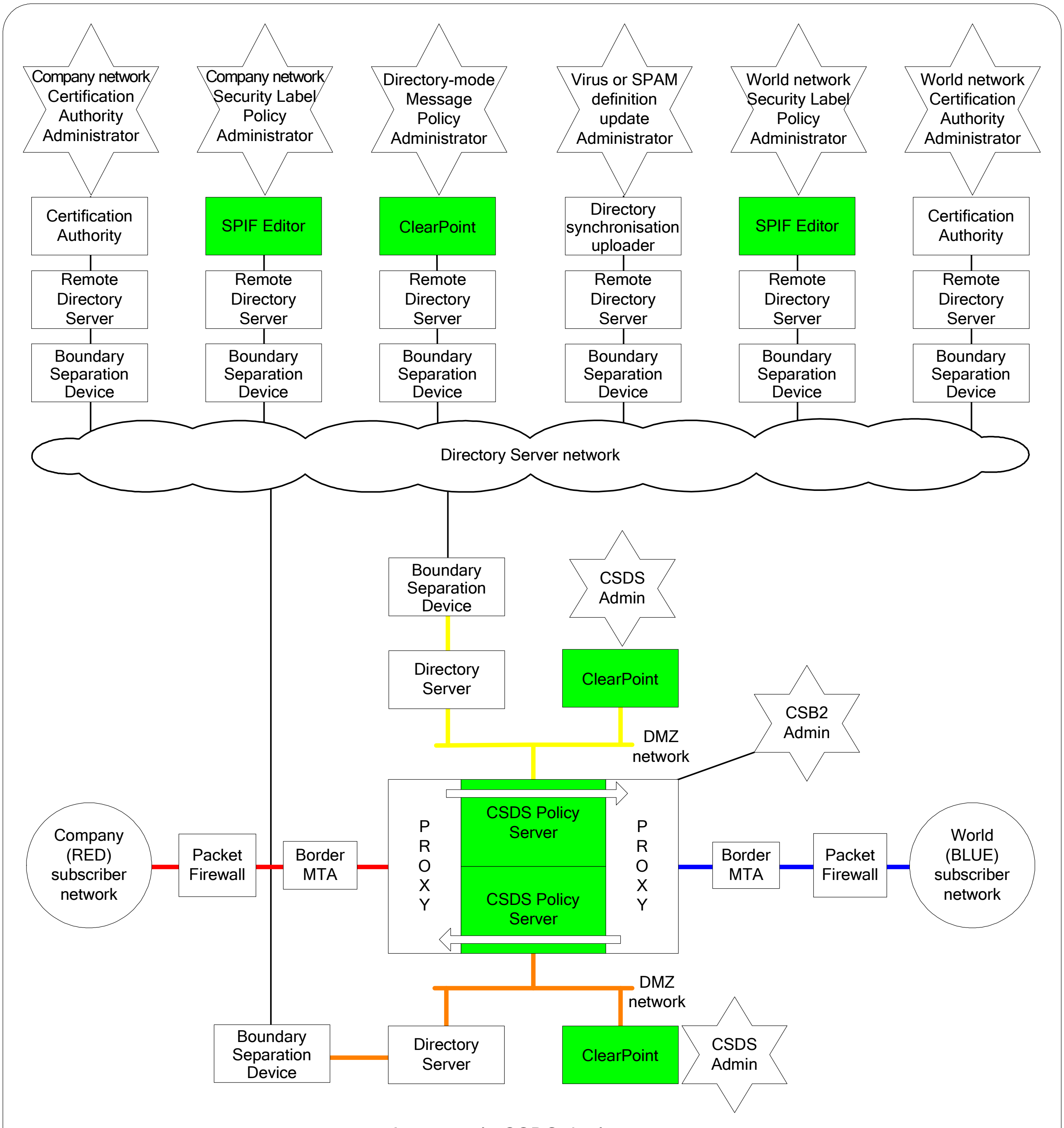
47. ClearPoint management systems can connect to Policy Servers on a DMZ network, or to Directory Servers. If installed, a SPIF Editor can only be connected via a Directory Server. A ClearPoint connected directly to a Policy Server is said to be operating in *Server-mode*, while one connected to a Directory Server is said to be operating in *Directory-mode*. The administrators authenticated by ClearPoint are similarly identified as Server-mode or Directory-mode administrators. Directory Servers on remote networks can replicate data through appropriately assured Boundary Separation Devices to Directory Servers on DMZ networks.

48. The following diagram overleaf shows an example of a single instance of Clearswift DeepSecure, showing remote management systems. It is assumed that each remote management system is in a different location, each directly connected to a Directory Server which is itself connected to a (distributed) network of Directory Servers through an appropriately assured Boundary Separation Device. If some remote management systems are in the same location they can share access to a common Directory Server (not illustrated). Each DMZ network is also connected to this network of Directory Servers, again through an appropriately assured Boundary Separation Device. The network of Directory Servers may contain other Boundary Separation Devices within it (not illustrated) if it spans different security domains.

49. It is assumed that a packet firewall is used to protect Clearswift DeepSecure and its Clearswift Bastion/TSOL 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.

50. Direct communication between ClearPoint and a Policy Server on the DMZ network is over SSL (this configuration of ClearPoint allows all management operations, subject to the roles assigned to individual administrators).

51. Communication between ClearPoint and a Directory Server 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 Directory Server on the DMZ network to the Policy Server. The Policy Server validates the integrity of each Message Policy, and authenticates the Administrator who created or modified that Policy.


Company network Certification Authority Administrator
Company network Security Label Policy Administrator
Directory-mode Message Policy Administrator
Virus or SPAM definition update Administrator
World network Security Label Policy Administrator
World network Certification Authority Administrator
Certification Authority
SPIF Editor
ClearPoint
Directory synchronisation uploader
SPIF Editor
Certification Authority
Remote Directory Server
Boundary Separation Device
Directory Server network
Boundary Separation Device
CSDS Admin
Directory Server
ClearPoint
DMZ network
CSB2 Admin
Company (RED) subscriber network
Packet Firewall
Border MTA
P R O X Y
CSDS Policy Server
CSDS Policy Server
P R O X Y
Border MTA
Packet Firewall
World (BLUE) subscriber network
DMZ network
Boundary Separation Device
Directory Server
ClearPoint
CSDS Admin

An example CSDS deployment
(TOE is within coloured areas: CSDS Policy Servers, ClearPoint and SPIF Editors)
Also illustrates location of administrators

This is just a single example of one of the many permitted configurations of a deployed TOE.

Environmental Requirements

52. Threat agents may be persons, or active IT entities (e.g. processes). CSDS may be attacked from subscriber networks, from networks with connection to the DMZ networks, from a DMZ network or locally via a CSB2/TSOL terminal. Threat agents are:

a. authorised users of subscriber networks, or intervening networks, or persons who gain unauthorised access to such networks. They may or may not have legitimate access to email facilities with authorisation to communicate with other networks via CSDS. They may be careless or inexperienced users of the email facilities, users motivated to make casual attempts to breach the email export policy, or persons that are motivated to make concerted attempts to breach the email export policy or attack CSDS, but have a low attack potential (expertise, opportunity, resources)

b. authorised administrators of CSDS, CSB2 and TSOL. They are trusted, competent and trained to use (in accordance with their role, a subset of) the administration facilities of CSDS, CSB2 & TSOL in an appropriate manner. They are nevertheless human, and may inadvertently mis-configure a complicated policy. (There is a finite risk that they may, due to pressure of work or for illicit purposes, attempt to access administration facilities outside of their role)

c. authorised users of networks used to connect the DMZ network with a remote management network, or persons who gain unauthorised access to such networks. They may be users motivated to make casual attempts to modify email policy, or persons that are motivated to make concerted attempts to breach the email policy or attack CSDS, but have a low attack potential (expertise, opportunity, resources)

d. CSDS software. An error in the construction or configuration of CSDS may cause an accidental breach of security. Untrusted third party software may attempt deliberate breach of security.

53. As a boundary protection device, CSDS protects not only TOE assets, but also assets in the connected subscriber networks. Assets are therefore: information, facilities and resources on the connected networks; subscriber messages being processed by the TOE; other TOE/TSF data, including notifications, audit data and Message Policies; TOE/TSF functions, including Policy Engine and queue management.

54. There are a number of secure usage assumptions relating to the environment. These are detailed in the Security Target [d]. Specifically the following must be provided in the evaluated configuration:

a. CSDS is assumed to be located in an environment that physically protects it against unauthorised access to subscriber and management information stored or in transit through CSDS.

55. The environmental configuration is as follows.

a. The platform of the Policy Server is assumed to be one of the certified or assurance maintained combinations of Clearswift Bastion 2 in a Trusted Solaris 8 operating system context specified in Section 2.7.2 and Annex J of the ST [d].

b. The platform of the SPIF Editor is assumed to be SUN Java Runtime Environment (JRE) 1.4.2 or future upwards compatible versions of Java conformant JVM, running on Windows, Linux or Solaris platform as specified in Section 2.7.2 and Annex L of the ST [d].

c. The platform of ClearPoint is assumed to be Internet Explorer (V6.0) on Windows, as specified in Section 2.7.2 and Annex K of the ST [d].

Evaluator Test Configuration

56. The following platforms were used for evaluator testing, and were confirmed to be a consistent, representative subset of the configurations used for developer testing (see Paragraphs 77 to 88).

57. The Policy Server runs on a single Sun SPARC platform[3] with a certified or assurance maintained combination of Sun Trusted Solaris 8 and Clearswift Bastion 2.

58. The platform combinations of Sun Trusted Solaris 8 and Clearswift Bastion 2 used for testing the Policy Server were:

- CSB2.1 running on TSOL8, Sun SPARC 12/02;
- CSB2.2 running on TSOL8, Sun SPARC 2/04;
- CSB2.2 running on TSOL8, Sun SPARC 7/03.

59. ClearPoint platforms used for testing were Windows Server 2003 R2 Standard Edition, and Windows XP Professional, Service Pack 2, both with Internet Explorer v6.0.

60. SPIF Editor platforms (running JRE v1.4.2_10) used for testing were:

- Windows XP Professional (64 bit), Service Pack 2;
- Linux Mandrake (kernel v2.6.8.1-12mdk);
- Solaris 10.

61. The TOE was tested on different platform combinations of Policy Server, ClearPoint and SPIF Editor as detailed in the following test configurations[4]:

[3] Sun SPARC platform includes Sun SPARC workstations and Sun SPARC servers, and is also referenced as Sun SPARC.

Test Config	Policy Server configuration	ClearPoint	SPIF Editor
1	Clearswift Bastion 2.2, running on Trusted Solaris 8 (hardware 2/04), on SUN Fire V240 Server	Directory-mode: Windows Server 2003 R2 Standard Edition (32bit), with Internet Explorer v6.0 Server-mode: Windows XP PRO Service Pack 2	Solaris 10, with JRE 1.4.2
2	Clearswift Bastion 2.2, running on Trusted Solaris 8 (hardware 7/03), on SUN Blade 150	Directory-mode: Windows Server 2003 R2 Standard Edition (32bit), with Internet Explorer v6.0 Server-mode: Windows XP PRO Service Pack 2	Linux Mandrake (kernel v2.6.8.1-12mdk), with JRE 1.4.2
3	Clearswift Bastion 2.1, running on Trusted Solaris 8 (hardware 12/02), on SUN Blade 150	Directory-mode: Windows Server 2003 R2 Standard Edition (32bit), with Internet Explorer v6.0 Server-mode: Windows XP PRO Service Pack 2	Windows XP Professional (64 bit), Service Pack 2, with JRE 1.4.2

62. The evaluator's tests used the following libraries:

- VIC Library: Cryptomathic PrimeInk Premium VIC for CSDS2.1 Vn 2.3.0 (Pkg Vn 3.20.50);

- LSL : X.841 Label Support Library for Solaris Vn 2.3.0 (Pkg Vn 3.20.50);

- Sophos virus scanner for CSDS (Vn 1.0.0) with Sophos SAVI Virus Scanner for Solaris Issue May 2006.

- Command line virus scanner for CSDS (Vn 1.0.0) with ClamAV command line scanner for Solaris v0.88.

63. Within the test configurations the following components are installed in the environment:

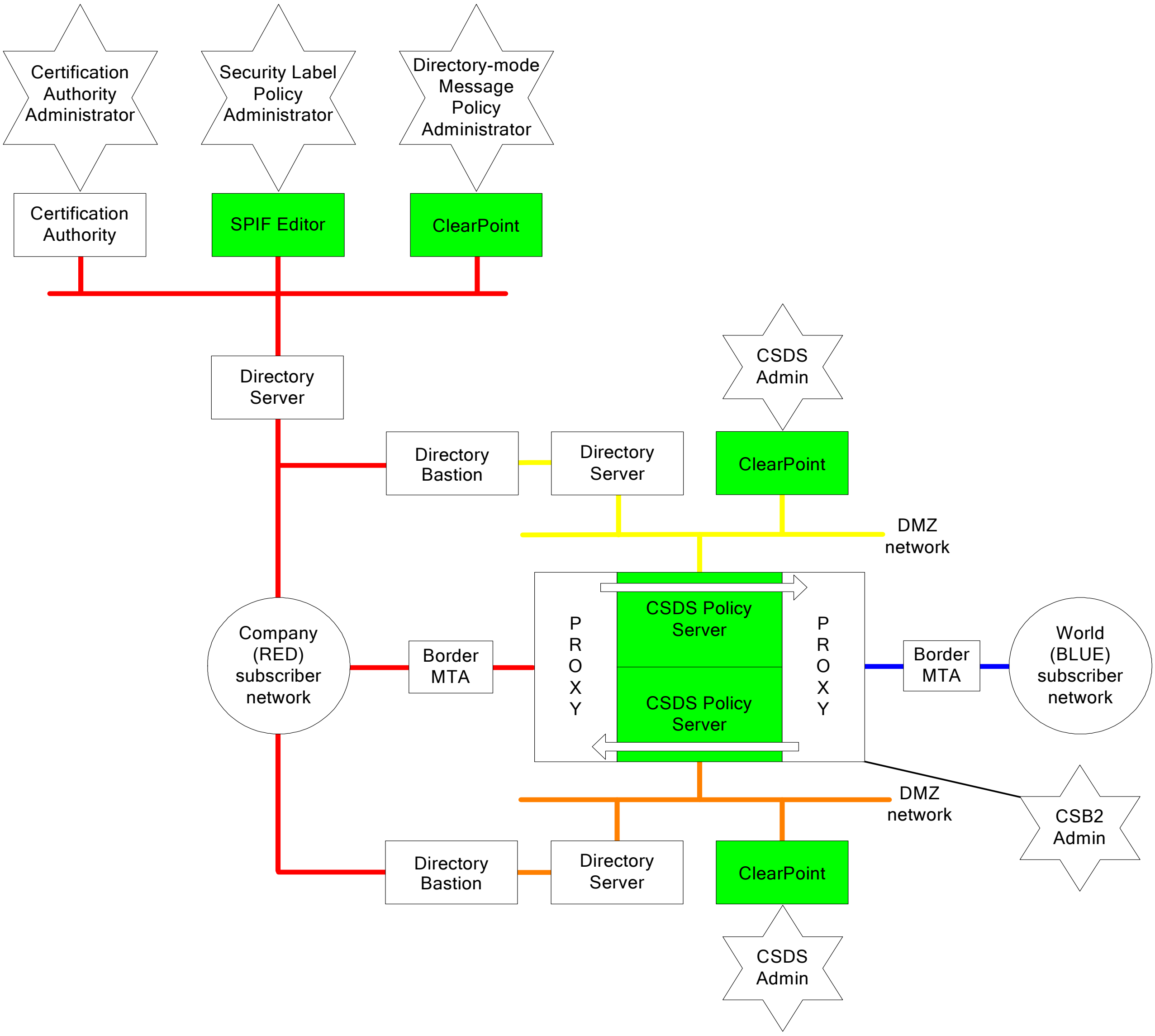
- Boundary separation devices protecting the DMZ network were Directory Bastions running Clearswift Bastion 2 configured with DISP (X.525) vet and proxy software;

- Border MTAs were Clearswift FlashPoint Server (Release 6.1.9) for X.400 and Exim (v4.43) for SMTP running on Fedora Core 3 Linux;

- Directory Servers were running either Data Connection DC Directory Server (v3.0.00), eB2Bcom View 500 (Release 5.3) or ISODE Directory Server (Release 11.3.1.0).

[4] See paragraphs 90 to 101 for assertions related to other platform combinations.

64. The following diagram shows the basic configuration used during evaluator testing activities, as used for individual tests. The CSDS Servers were configured in a server farm, but only a single CSDS Server was used within any one test.



CSDS deployment used in evaluator testing
(TOE is within coloured areas: CSDS Server, ClearPoint and SPIF Editor)
Also illustrates location of administrators

IV. PRODUCT SECURITY ARCHITECTURE

65. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

66. As described in the Section 'TOE Scope' above, the TOE is comprised of a Policy Server, ClearPoint and SPIF Editor.

67. The Policy Engine component of the Policy Server is responsible for managing and auditing the flow of subscriber messages between subscriber networks, performing protocol conformance checks and message decomposition and recomposition. The Policy Engine is also responsible for the invocation of appropriate rules, performing the policy checks and actions (except for those parts explicitly identified as performed by plug-ins or external libraries), in accordance with the active Message Policy. Message security labels may be extracted in accordance with proprietary standards for informal (text) labels, or with specified standards RFC 2634, STANAG 4406 and X.411 for formal (ASN.1 binary encoded) labels, as detailed in ST [d]. Encrypted messages are decrypted in order to perform the required mediation, and then re-encrypted if required. Decrypted messages are protected from unauthorised access by the CSB2/TSOL platform assured separation and role mechanisms.

68. The directly connected ClearPoint 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 DeepSecure Administrator.

69. ClearPoint can modify and store Message Policy on a Directory Server. The Directory Server where Message Policy is stored may be a remote Directory Server, in which case Directory replication may be used so that the Directory Server 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 Directory Server 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 DeepSecure Message Policy Administrator who modified it. No data can be uploaded from the Policy Server to the Directory Server. The Policy Server initiates all connections, and provides authentication to the Directory Server if required.

70. The SPIF Editor comprises policy management software with an intuitive GUI interface, which allows an X.841 Security (Label) Policy Administrator to define or modify an X.841 Security (Label) Policy Information File (SPIF) and store this in a Directory Server.

Design Subsystems

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

a. Policy Server

i. Policy Engine: Manages and audits the flow of subscriber messages between subscriber networks, and invokes appropriate rules (checks and actions), in accordance with the active Message Policy.

ii. Q-handler Service: Responsible for the association of Policy Engine queues with CSB2 queues in accordance with the direction of subscriber message flow through the Policy Server.

iii. Administration Service. The administrative module of the CSDS system, supporting administration by ClearPoint in Server-mode, of Message Policies and Policy Engine queues, archives, audit logs and diagnostic logs.

iv. Directory Synchronisation Agent: Responsible for regularly downloading data from the Directory Server, supporting administration of Message Policies by ClearPoint in Directory-mode.

v. PKI Configuration Utility: A configuration tool to manage identification and authentication details (crypto tokens containing private keys, certificate trust points, Administrators' certificates with permitted roles and privileges).

vi. X.841 LSL (Optional, but is within the TOE): The LSL library checks the validity of a formal security label, checks that the label is dominated by clearance, translates a value of a formal security label into a value in another security policy and provides a text rendition of the value of a formal security label.

vii. A4L: Provides data and message translation services, including ASN.1 encoding/decoding, character set translation, X.400 message rendering.

b. ClearPoint

i. LOGON Provides front end user interface for specified management functions and provides initial processing of user input prior to the initialisation of the main ClearPoint UI (managed by VIEWS).

ii. VIEWS Populates the Folder View tree according to the Message Policy and Policy Server COM objects. Manages a number of views used to display and edit content in the Contents View.

iii. OBJSTORE Provides an object store to store the COM object representation of a Message Policy, Policy Server LDIF, etc.

iv. COMMSAGENT Provide a communication interface for interaction with Directory Servers and Policy Servers.

v. X.841 LSL. Renders Clearance and Security Label parameters for each Security Policy (SPIF) in ClearPoint's Message Policy management GUI and for each message from a Policy Server queue that ClearPoint displays.

vi. A4L Provides data and message translation services, including ASN.1 encoding/decoding, character set translation, X.400 message rendering.

c. SPIF Editor

i. UIMGR Provides all immediate user UI functions.

ii. CSUPP Coordinates data management, storage and re-use. It also manages direct interfaces to the X.841 LSL and A4L modules. (Re-compiled for each platform on which the SPIF Editor is supported.)

iii. A4L Library to encode SPIFs from internal data structures into ASN.1 format.

iv. X.841 LSL Library to decode SPIFs from ASN.1 form into internal representation. (Only uses some internal components of the X.841 LSL, does not use the generic LSL as used by Policy Engine.)

72. The X.841 LSL and A4L subsystems are common among each of the TOE components.

Hardware and Firmware Dependencies

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

Product Interfaces

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

- Clearswift Bastion;
- Trusted Solaris (used by all subsystems of the Policy Server);
- Administrator at ClearPoint and SPIF Editor;
- Administrator on CSB2, e.g. through PKICONFIG Utility;
- Cryptographic operations library;

- Formal security label checking library;
- Virus scanning library and other Policy Engine Plug-in APIs (i.e. data type recognition, textual analysis and spam detection).

75. The TSFI also provides interfaces between distributed TOE components, in the following manner:

- SPIF Editor and Policy Server via Directory Server;
- ClearPoint and Policy Server via SOAP/SSL.

76. The TOE, major IT environment components and TSFI are depicted in the diagram in Section ‘TOE Configuration’ above.

V. PRODUCT TESTING

IT Product Testing

77. The Developer’s Test Plan included 294 tests covering all SFRs, all TOE high level subsystems (identified in Section ‘Design Subsystems‘ above), all security functions and the TSFI (as detailed in Section ‘Product Interfaces‘ above). It included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. A further 110 tests were also included, which while not directly related to SFRs, demonstrate features of DeepSecure 2.1. The Developer’s testing also included comprehensive testing that malformed messages are handled correctly, using extensive test suites from NISCC for X.400, ASN.1, MIME and S/MIME.

78. The Developer’s testing used 4 different combinations of Sun Trusted Solaris, Clearswift Bastion 2 and Sun SPARC platforms specifically configured to address the platform variations. These included the three combinations of Sun Trusted Solaris and Clearswift Bastion 2 specified in Paragraph 58. The Developer’s testing used 5 different Windows platforms for ClearPoint, including both 32- and 64-bit architecture. These included the two Windows platforms specified in Paragraph 59. The Developer’s testing also used 9 different platforms for the SPIF Editor, including Windows, Solaris and Linux. These included the three platforms specified in Paragraph 60.

79. In total the Developer performed 9 test runs with various combinations of platforms for the TOE components. The full set of tests were run on 4 of the platform combinations, which included Clearswift Bastion 2.2 running on all certified/assurance maintained combinations of Trusted Solaris/Sun SPARC hardware. Partial runs were completed on the remaining 5 platform combinations focusing on the tests relating to ClearPoint and SPIF Editor management functionality, to reflect the variation in the associated platforms.

80. All tests run on each platform used the versions of TOE components detailed in Paragraph 31.

81. Identical results were obtained on each platform and satisfactorily demonstrated the correct operation of the TOE in all platform variation conditions.

82. Developer testing utilized a number of network configurations. Each configuration consisted of 3 or more co-located Sun SPARC platforms, 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 and Directory Server, covering both the Server-mode and Directory-mode configuration options for ClearPoint.

83. The above Developer's testing also covered the VIC subsystems, LSL subsystems and virus scanners listed in Section 'Evaluator Test Configuration'.

84. The Evaluator's testing used test configurations 1 to 3, as detailed in Section 'Evaluator Test Configuration', in conjunction with the TOE software detailed in Paragraph 31. The Evaluators witnessed the full installation and configuration of the TOE on test configuration 1 and confirmed that test configurations 2 and 3 were consistent with that specified in the Security Target [d].

85. The Developer tests were comprehensive. To validate the Developer's testing, the Evaluators therefore repeated a sample of 30 Developer tests on test configuration 1 (where relevant to SMTP) and test configuration 3 (where relevant to X.400). Together, these exercised 10% of the Developer's tests. The test results were identical to those produced by the Developer.

86. The Evaluators devised a further set of 10 independent functional tests, different to those performed by the Developer, on test configuration 1 to test the TOE independently. No anomalies were found. The Evaluators, in conjunction with the Developer and Certification Body, also devised a set of 8 penetration tests on test configurations 1 to 3 to address potential vulnerabilities considered during the course of the evaluation. No vulnerabilities or errors were detected.

87. 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.

88. Further evidence of the correct operation of the TOE's platform (i.e. Clearswift Bastion and Trusted Solaris 8 on specified Sun SPARC platforms) is reported in [j] - [l].

Vulnerability Analysis

89. 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

90. As detailed in Paragraph 55, there are three aspects of environment forming the platform for the TOE components. These are addressed in turn in the following.

91. The **platform of the Policy Server** is assumed to be one of the current or future certified or assurance maintained combinations of Clearswift Bastion 2 ([j] - [l]) in a Trusted Solaris 8 Operating System context as specified in Section 'Evaluator Test Configuration'. The Developer and Evaluator testing summarized in Section 'IT Product Testing' covered both of these two combinations.

92. The Evaluators agreed with the Developer assertion that use of the TOE Policy Server 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:

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

b. 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;

c. 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.

93. 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 2 evaluation [j] and assurance maintenance ([k] and [l]), the Sponsor supplied a hardware Multi-Platform Rationale that examined the impact of Sun SPARC platform variations. The Evaluators confirmed that this rationale was also applicable to the evaluation of Clearswift DeepSecure. The Developer and Evaluator testing summarised in Section 'IT Product Testing' supported this Multi-Platform Rationale.

94. The **platform of ClearPoint** is assumed to be Internet Explorer v6.0 on one of the Microsoft Windows operating systems specified in Section 2.7.2 of ST [d].

95. The Evaluators agreed with the Developer assertion that use of the TOE ClearPoint component with a future upwards compatible version of Internet Explorer and alternative versions of Microsoft Windows operating systems would involve only a low risk of the security of the TOE being undermined. This was based on a rationale which argued that:

a. ClearPoint uses standard Internet Explorer and Windows programming interfaces and functions that are designed to be consistent between different versions;

b. Clearswift programming standards would ensure that these interfaces and functions are used consistently throughout ClearPoint;

c. ClearPoint's only security critical dependency on the ClearPoint platform is for the protection of the CSDS Server-mode Administrators' and CSDS Directory-mode Administrators' private keys, which may be protected using Windows security functions, or other alternatives (e.g. storage on a smart card).

96. The Developer and Evaluator testing summarised in Section 'IT Product Testing' supported this Multi-Platform Rationale, verifying consistent operation of the ClearPoint TOE component across the various platforms sampled.

97. The **platform of the SPIF Editor** is assumed to be Java Runtime Environment 1.4.2, running on one of the Microsoft Windows, Linux or Solaris operating systems specified in Section 2.7.2 of ST [d].

98. The Evaluators agreed with the Developer assertion that use of the TOE SPIF Editor component with a future upwards compatible versions of Java conformant JVM and alternative versions of Microsoft Windows, Linux and Solaris operating systems would involve only a low risk of the security of the TOE being undermined. This was based on a rationale which argued that:

a. SPIF Editor uses standard JVM, Windows Linux and Solaris programming interfaces and functions that are designed to be consistent between different versions;

b. Clearswift programming standards would ensure that these interfaces and functions are used consistently throughout SPIF Editor;

c. SPIF Editor's only security critical dependency on the SPIF Editor Platform is for the protection of the X.841 Security (Label) Policy Administrator's private key, which may be protected using the platform system security functions, or other alternatives (e.g. storage on a smart card).

99. The Developer and Evaluator testing summarised in Section 'IT Product Testing' supported this Multi-Platform Rationale, verifying consistent operation of the SPIF Editor TOE component across the various platforms sampled.

100. Other TOE IT environment components include the following external libraries, details of which are provided in Section 2.7.1 of ST [d]:

- VIC
- LSL
- Data Type Recognition
- Textual Analysis
- Virus Scanner
- Spam Detection

101. The versions of libraries used in the test configurations are detailed in Section 'Evaluator Test Configuration'. The Developer asserts that the Developer testing summarized in Section 'IT Product Testing' will be used to test the TOE with other such external libraries. The Evaluators considered this testing to be thorough and appropriate to support the assertions of Annexes D through I, inclusive of the Security Target [d] which were additional to the security claims made for the TOE.

VI. REFERENCES

References to protocol standards included the CR are implicitly to the version specified in the ST References section and are not repeated here.

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[b] CLEF Requirements – Start Up 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 2.0, December 2005.

[d] DeepSecure (CSDS) Release 2.1Security Target,
Clearswift Ltd,
DN11488/1, Issue 1, 28 July 2006.

[e] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB -2005-08-004, Version 2.3, August 2005.

[i] Common Criteria Certification Report No. P213,
Clearswift Deep Secure Release 2.0.0 E2,
UK IT Security Evaluation and Certification Scheme,
P213, Issue 1.0, February 2005.

[j] Common Criteria Certification Report No. P184, Clearswift Bastion II,
UK IT Security Evaluation and Certification Scheme,
P184, Issue 1.0, June 2003.

[k] Common Criteria Maintenance Report MR1, (Supplementing Certification Report No. P184),
Clearswift Bastion II (Version 2.1.0),
UK IT Security Evaluation and Certification Scheme,
P184 MR1, Issue 1.0, 5 November 2004.

[l] Common Criteria Maintenance Report MR2, (Supplementing Certification Report No. P184),
Clearswift Bastion II (2.2.0),
UK IT Security Evaluation and Certification Scheme,
P184 MR2, Issue 1.0, August 2006.

[m] Evaluation Technical Report,
BT CLEF,
LFS/T514, Issue 1.0, August 2006.

[n] Evaluation of Clearswift DeepSecure: LFL/T170 Evaluation Technical Report,
LogicaCMG CLEF,
310.EC114253:ETR.1, Issue 1.0, 11 February 2005.

[o] Release Notice, Clearswift DeepSecure, Release 2.1, Policy Server,
Clearswift Ltd,
DN11610/1.

[p] Release Notice, Clearswift DeepSecure, Release 2.1, ClearPoint,
Clearswift Ltd,
DN11611/1.

[q] Release Notice, Clearswift DeepSecure, Release 2.1, X.841 Security Label Support Library,
Clearswift Ltd,
DN11612/1.

[r] Release Notice, Clearswift DeepSecure, SPIF Editor, Release 1.0,
Clearswift Ltd,
DN11613/1.

[s] Installation Guide, DeepSecure Release 2.1,
Clearswift Ltd,
DN11583/1.

[t] Policy Servers Administration Guide, DeepSecure 2.1,
Clearswift Ltd,
DN11545/1.

[u] PKI Configuration Administration Guide, DeepSecure 2.1,
Clearswift Ltd,
DN11546/1.

[v] ClearPoint Administration Guide, DeepSecure 2.1,
Clearswift Ltd,
DN11547/1.

[w] SPIF Editor Administration Guide, DeepSecure 2.1,
Clearswift Ltd,
DN11548/1.

[x] Clearswift DeepSecure System Planning Guide, DeepSecure 2.1,
Clearswift Ltd,
DN11591/1.

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)

COM	Component Object Model
CSB2	Clearswift Bastion II
CSDS	Clearswift DeepSecure
DAP	Directory Access Protocol
DISP	Directory Information Shadowing Protocol
LDAP	Lightweight Directory Access Protocol
LSL	(Security) Label Support Library
MTA	Message Transfer Agent
NISCC	National Infrastructure Security Co-ordination Centre
SPIF	Security (Label) Policy Information File
TSOL	Trusted Solaris
TSOL8	Trusted Solaris 8
VIC	Vendor Independent Cryptographic (Library)
VICI	Vendor Independent Cryptographic API