UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA MAINTENANCE REPORT MR1
(supplementing Certification Report No. P184)

Clearswift Bastion II

Version 2.0.0 Derivative (Version 2.1.0)

running on Trusted Solaris 8 12/02

Issue 1.0

5 November 2004

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 addendum to the original 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 addendum has been issued in accordance with the terms of this Arrangement.

The judgements contained in this report are those of the Qualified Certification Body which issued it. 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.

TABLE OF CONTENTS

Abbreviations

CCRA	Common Criteria Recognition Arrangement
CS	Clearswift
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
SIA	Security Impact Analysis
TOE	Target of Evaluation

References

a. Certification Report No. P184, CS Bastion II, running on Trusted Solaris 8 4/01 and specified Sun Workstations,
UK IT Security Evaluation and Certification Scheme,
Issue 1 .0, June 2003.

b. CS Bastion II Security Target (EAL4),
Clearswift Corporation,
DN11272/5, Issue 5.0, 29 May 2003.

c. CS Bastion 2.1 Security Target (EAL4),
Clearswift Corporation,
DN11272/6, Issue 6, 3 September 2004.

d. Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Members of the Agreement Group,
May 2000.

e. Assurance Continuity: CCRA Requirements,
Common Criteria Interpretation Management Board,
CCIMB-2004-02-09, Version 1.0, February 2004.

f. CS Bastion Version 2.1.0 Security Impact Analysis,
Clearswift Corporation,
DN11437/3, Issue 3, 1 November 2004.

g. Clearswift Bastion 2.1 Installation Guide,
Clearswift Corporation,
DN11420/1, Issue 1.0, 10 May 2004.

h. Clearswift Bastion 2.1 Release Notice,
Clearswift Corporation,
DN11430/1-RN, Issue 1.0, 7 May 2004.

i. Clearswift Bastion 2.1 Administration Guide,
Clearswift Corporation,
DN11421/1, Issue 1.0, 12 May 2004.

j. Assurance Maintenance Status Summary (supplementing Certification Report P170):
Sun Microsystems Inc, Trusted Solaris,
UK IT Security Evaluation and Certification Scheme,
Issue 2.0, March 2004.

k. Solaris 8 HW 12/02: Sun Hardware Platform Guide,
Sun Microsystems,
816-7535-10, Revision A, December 2002.
[http://www.sun.com/products-n-solutions/hardware/docs/pdf/816-7535-10.pdf]

Introduction

1. This Maintenance Report outlines the current status of the Assurance Continuity process for versions of Clearswift Bastion II, and is intended to assist prospective consumers when judging the suitability of the IT security of the versions of the product for their particular requirements.

2. The baseline for assurance maintenance was the Common Criteria evaluation, to the EAL4 Evaluation Assurance Level, of Clearswift Bastion II Version 2.0.0 running on Trusted Solaris 8 4/01.

3. Prospective consumers are advised to read this document in conjunction with:

- the Certification Report [Reference a] for the EAL4 evaluation of the original certified Target of Evaluation (TOE), to which this report is an addendum;
- the Security Target [b] of the certified TOE, which specifies the functional, environmental and assurance requirements for the evaluation; and
- the updated Security Target [c] of the maintained derivative.

Maintained Versions

4. The version of the product originally evaluated was:

- Clearswift Bastion II Version 2.0.0 running on Trusted Solaris 8 4/01.

5. This version of the product for which assurance has subsequently been maintained is:

- Clearswift Bastion II Version 2.1.0 running on Trusted Solaris 8 12/02.

6. Note that for the maintained version, the main change to the scope of the TOE is the change of environment from Trusted Solaris 8 4/01 to Trusted Solaris 8 12/02. Otherwise, there are only minor generic changes between the respective Security Targets [b, c], extending to additional hardware platforms.

Assurance Continuity Process

7. The Common Criteria Recognition Arrangement (CCRA) [d] has been established as a basis for the mutual recognition of the results of Common Criteria evaluations. The process of Assurance Continuity within Common Criteria is defined in the document 'Assurance Continuity: CCRA Requirements' [e].

8. The Assurance Continuity process is based on a Security Impact Analysis (SIA), produced by the Developer, which describes all the changes made to the product and assesses the security impact of each change. For Clearswift Bastion II Version 2.1.0, this SIA [f] has been examined by the UK IT Security Evaluation and Certification Scheme, Certification Body, who produced this Maintenance Report.

9. The Developer, Clearswift Limited, has carried out full retesting on Clearswift Bastion II Version 2.1.0 and has considered all the assurance aspects detailed in 'Assurance Continuity: CCRA Requirements' [e].

10. The Certification Body accepts the decisions detailed in the SIA, which has assessed each change as being of ***minor*** impact, and concludes that the overall impact of all the changes is ***minor***.

11. After consideration of the SIA [f] and other visibility of the assurance continuity process given to the Certifier, the Certification Body has determined that EAL4 assurance has been maintained for the derived version, Clearswift Bastion II Version 2.1.0.

General Points

12. Assurance continuity addresses the security functionality claimed in the Security Target [c] with reference to the assumed environment specified. The assurance maintained configurations are as specified by the modifications specified in this Report in conjunction with the original Certification Report [a]. Prospective consumers are advised to check that this matches their identified requirements.

13. The assurance continuity process is not a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the assurance continuity process has been completed. Existing and prospective consumers should check for themselves whether any security vulnerabilities have been discovered since this Report and, if appropriate, should check with the vendor to see if any patches exist for the product.

Analysis of Changes

14. There are no new TOE Security Policy enforcing components in Clearswift Bastion II Version 2.1.0. There are no changes to the high-level design and no changes to any TOE Security Policy enforcing code.

15. Changes between Clearswift Bastion II Version 2.0.0 and Version 2.1.0 fall into the following categories.

- Changes due to the software port to the revised environment, which moves from Trusted Solaris 8 4/01 to Trusted Solaris 8 12/02 and associated hardware.
- Resolution of bugs raised since the original evaluation.
- Enhancements.
- Changes to the resolution of Observations raised in the original evaluation.

These changes are summarized in the sections below, corresponding to matching sections in the SIA [f].

Changes due to the Software Port

16. The prime need for change to the product was to enable it to run in the revised Environment detailed below under 'TOE Environment', and specifically to run under Trusted Solaris 8 12/02. Changes are detailed in the table below.

Item	Description of Change	Related Changes
Environment change	Change environment from Trusted Solaris 8 4/01 to Trusted Solaris 8 12/02.	▪ Complete re-test under Trusted Solaris 8 12/02. ▪ Generic changes to documentation.
Partition sizes	Change recommended disk partition sizes to 32 or 40 GB.	▪ Minor update to design documents.
Text based install	Additional information included in the Installation Guide	[None]
Remove *syslog* error message	Change *csbtsol* package of the SYSGEN subsys tem to remove superfluous files.	[None]
Diskette installation	Diskette installation method removed to avoid erroneous behaviour of Trusted Solaris installation.	▪ Minor update to design documents. ▪ Obsolete files only needed for diskette installation were deleted from the SYSGEN implementation.
Platform lists	Changes to shell scripts in the SYSGEN subsystem to reflect platforms tested.	[None]

Resolution of Bugs

17. The following minor changes were made.

Item	Description of Change	Related Changes
Etherleak vulnerability	Release Notice modified to include a warning.	▪ Update to the Vulnerability Analysis (with no adverse results).
Copyright	Copyright notice changed from 'DERA' to 'QinetiQ' in SYSGEN subsystem.	[None]
Network interfaces	Note added to operational documentation to recommend disconnection from networks while in single-user mode.	▪ Changes to Test Scripts. ▪ Update to the Vulnerability Analysis (with no adverse results).
Installation Guide	Improvements to wording.	[None]
Administration Guide	Correction of minor errors.	[None]

Enhancements

18. The four enhancement changes are listed below.

Item	Description of Change	Related Changes
Poll period granularity.	The Trusted Messaging Subsystem was changed to support poll periods down to 1 millisecond.	▪ Design documents changed, with minor changes to the TOE interfaces. ▪ Implementation of confgen script adjusted to manipulate poll-periods in milliseconds. ▪ Test Scripts changed to reflect poll periods in milliseconds. ▪ Update to the Vulnerability Analysis (with no adverse results).
Configurable poll period	The RUNCTRL subsystem now prompts the administrator to supply a poll period (previously 5 seconds, by default).	▪ Design documents changed, with minor changes to the TOE interfaces. ▪ Test Scripts changed to verify correct configuration of poll periods. ▪ New test added. ▪ Installation Guide and Administrators Guide updated.

Item	Description of Change	Related Changes
Improved Guidance	Included extra advice for commonly required networking configurations - in Administration and Installation Guides.	▪ Design documents trivially changed. ▪ Some Test Scripts modified and one new test added. ▪ Revised Misuse Analysis (with no adverse results).
More Testing	Test Scripts extended to cover more possible environmental configurations, including end-to-end traffic flow through multiple TOEs in parallel, to remove the caveat in the Certification Report that stated such configurations had not been tested.	[None]

Changes to OR Resolutions

19. The original evaluation raised some Observation Reports of minor significance and proposed various solutions which were accepted by the Certification Body. Clearswift Bastion II Version 2.1.0 includes improved resolution for five of these Observation Reports, as listed below.

Item	Description of Change	Related Changes
Incorrect version numbers.	Comments in *label_encoding* file of the SYSGEN subsystem changed.	▪ Release Notice adjusted. ▪ Design documents trivially updated. ▪ Test Scripts trivially updated.
Audit_class needs updating at end of install.	*Audit_class* script of the SYSGEN subsystem changed.	▪ Installation Guide adjusted to remove a section on hand-editing.
Fail after re-boot command.	Trusted Messaging Subsystem *csbrun* component fixed to make it less sensitive to *process-id* files left on the system.	[None]
Csblaunch does not report ARCHIVE failures.	Archive subsystem, *csbrun* component modified to wait a few seconds longer before checking for successful *csbarchive* start-up.	[None]
Csbarchive failure.	Fixed not to fail when disc space has been filled.	▪ Release Notice adjusted.

Changes to Developer Evidence

20. There are no changes to the High Level Design or to the Security Target, other than minor generic changes. Changes to the Low Level Design, test documentation and other TOE documentation have been listed above in the descriptions of the individual changes.

21. The Installation Guide, Administration Guide and Release Notice have been updated to reflect the changes made to the product and its method of secure use, as indicated in the tables above.

22. The Misuse Analysis and Vulnerability Analysis have both been updated as part of the process of producing the SIA as listed above in the descriptions of the individual changes.

23. The Multi-Platform Rationale has also been updated to cover the hardware platforms supported by Solaris 8 12/02. Although Solaris now supports platforms with up to 128 processors, Clearswift Bastion uses at most two processors. It has only been tested on single and dual processor platforms.

24. The generic changes referred to throughout this document are the minor documentation changes such as changes to the Version numbers for Clearswift Bastion II and the Version numbers for the Trusted Solaris Environment. (Version numbers for Clearswift Bastion are sometimes referred to as Release numbers.)

TOE Identification

25. The maintained TOE is uniquely identified as:

Clearswift Bastion II Version 2.1.0, otherwise known as CS Bastion Version 2.1

26. The TOE is available on CD-ROM, or can be supplied pre-installed and pre-packaged.

27. Details of the TOE Security Policy enforcing components of the TOE in the derived version are listed in Appendix A of the SIA [f].

TOE Documentation

28. The guidance documents, which are included on the TOE CD-ROM, are:

- Clearswift Bastion 2.1 Installation Guide [g].
- Clearswift Bastion 2.1 Release Notice [h].
- Clearswift Bastion 2.1 Administration Guide [i].

TOE Environment

29. The defined Environment for Clearswift Bastion II Version 2.1.0 is as follows.

a) SUN Trusted Solaris 8 12/02 in its assurance maintained configuration [j] on any single SUN SPARC Workstation supported by the Operating System [k], with specific SUN-tested Network Interface Cards[1].

b) Interfaces to the two subscriber networks mediated by Clearswift Bastion II.

c) Either one or two channels, each having between zero and four network interfaces to the extended DMZs.

d) A pair of proxies.

[1] Only interface cards tested successfully against the etherleak vulnerability can be used. These are listed at http://www.kb.cert.org/vuls/id/JPLA-5BGNYP.

IT Product Testing

30. Clearswift Bastion II Version 2.0.0 was tested on three specific platforms running Trusted Solaris 8 4/01. The Developers carried out a complete re-test of the maintained Version 2.1.0 on each of the following two platforms running Trusted Solaris 8 12/02:

- A Sun Blade 150, with OpenBoot Version 4.6, UltraSPARC IIe Single 650 MHz processor, 256MB memory, 40GB disc, using an X1034A Sun Quad FastEthernet PCI Adapter Card.
- A Sun Fire V240, with OpenBoot Version 4.11.4, UltraSPARC IIIi Single 1002 MHz processor, 1024MB memory, 32GB disc, using an integral Sun Gigabit Ethernet Adapter Card.

31. For the derived TOE, Version 2.1.0, the CS Bastion II Version 2.0.0 tests were supplemented with additional tests as indicated in this Report.