CESG CERTIFICATION BODY

COMMON CRITERIA MAINTENANCE REPORT MR2
(supplementing Certification Report No. P184)

122-B

Clearswift Bastion II

Versions 2.0.0, 2.1.0 & 2.2.0

running on Trusted Solaris 8 4/01, 12/02, 7/03 & 2/04

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 CESG Certification Body 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
CLI	Command Line Interpreter
CS	Clearswift
DMZ	Demilitarized Zone
EAL	Evaluation Assurance Level
MR1	Maintenance Report No 1
SIA	Security Impact Analysis
SMC	Solaris Management Console
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,
DN11272/5, Issue 5.0, 29 May 2003.

c. CS Bastion II V2.2 Security Target (EAL4),
Clearswift,
DN11272/7, Issue 7, 13 September 2006.

d. Common Criteria Maintenance Report MR1 (supplementing Certification Report No. P184),
Clearswift Bastion II Version 2.0.0 Derivative (Version 2.1.0),
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, 5 November 2004.

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

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

g. CS Bastion Version 2.2.0 Security Impact Analysis,
Clearswift,
DN11529/1, Issue 1.0, 13 September, 2006.

h. Clearswift Bastion II Version 2.2 Installation Guide,
Clearswift,
DN11526/1, Issue 1.0, 18 August 2006.

i. Clearswift Bastion II Release 2.2.0 Release Notice,
Clearswift,
DN11528/1-RN, Issue 1.0, 18 August 2006.

j. Clearswift Bastion II Version 2.2 Administration Guide,
Clearswift,
DN11527/1, Issue 1.0, 18 August 2006.

k. Common Criteria Maintenance Report MR1 (supplementing Certification Report P170):
Sun Microsystems Inc, Trusted Solaris, Version 8 2/04,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, March 2006.

l. Sun Hardware Platform Guides (HPGs),
Sun Microsystems,
Solaris 8 4/01 Sun HPG: 806-7482-10,
Solaris 8 HW 12/02 Sun HPG: 816-7535-10,
Solaris 8 HW 7/03 Sun HPG: 817-1550-12,
Solaris 8 2/04 Sun HPG: 817-4347-10.

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 P184 [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 latest 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. The first derived version of the product for which assurance has subsequently been maintained [d] was:

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

6. The latest derived version of the product for which assurance has been maintained was:

- Clearswift Bastion II Version 2.2.0 running on Trusted Solaris 8 4/01, 12/02, 7/03 and 2/04.

7. The maintenance of the first derived version was described in Maintenance Report No 1 (MR1) [d]. The maintenance of the latest derived version is described in this document, which provides a summary of the incremental changes from MR1.

8. Note that for the latest maintained version, the main change to the scope of the TOE is the change of environment to Trusted Solaris 8 4/01, 12/02, 7/03 or 2/04. Otherwise, there are only minor generic changes between the respective Security Targets [b, c], extending to additional hardware platforms.

Assurance Continuity Process

9. The Common Criteria Recognition Arrangement (CCRA) [e] 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' [f].

10. The Assurance Continuity process is based on an Impact Analysis Report, also known as a Security Impact Analysis (SIA), produced by the Developer, which describes all the changes made to the product, together with the updated evaluation evidence, and assesses the security impact of each change. For Clearswift Bastion II Version 2.2.0, this SIA [g] has been examined by the CESG Certification Body, who produced this Maintenance Report.

11. The Developer, Clearswift Limited, has carried out full retesting on Clearswift Bastion II Version 2.2.0 running on Trusted Solaris 8 7/03 and 2/04, together with partial retesting on Trusted Solaris 8 4/01 and 12/02, and has considered all the assurance aspects detailed in 'Assurance Continuity: CCRA Requirements' [f].

Conclusions

12. The Certification Body accepts the decisions detailed in the SIA [g], which has assessed each change as being of ***minor*** impact, and concludes that the overall impact of all the changes is ***minor***. The Certification Body also accepts that the SIA meets the requirements for an Impact Analysis Report as specified in the 'Assurance Continuity: CCRA Requirements' [f].

13. After consideration of the SIA [g] and other visibility of the assurance continuity process given to the Certifier, the Certification Body has determined that EAL4 assurance outlined in Certification Report P184 [a] has been maintained for the latest derived version, Clearswift Bastion II Version 2.2.0. Only minor generic changes were required to the original Security Target [b] to reflect TOE version and platform changes.

General Points

14. Assurance continuity addresses the security functionality claimed in the Security Target [c] with reference to the assumed environment specified. The assurance maintained TOE configurations and platform environments are as specified by the modifications detailed in this Report (see 'TOE Identification' and 'TOE Environment') in conjunction with the original Certification Report [a]. Prospective consumers are advised to check that this matches their identified requirements.

15. 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

16. There are no new TOE Security Policy enforcing components in Clearswift Bastion II Version 2.2.0. There are no changes to the functional specification, high-level design and low-level design and no changes to any TOE Security Policy enforcing code.

17. Changes between Clearswift Bastion II Version 2.1.0 and Version 2.2.0 fall into the following categories.

- Changes directly or indirectly related to extending the TOE environment to Trusted Solaris 8 4/01, 12/02, 7/03 and 2/04 platforms and associated Sun hardware.

- Issues raised or revisited since the maintenance of Clearswift Bastion II Version 2.1.0.

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

Changes due to Requirement for Multiple Trusted Solaris 8 Platforms

18. 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 4/01, 12/02, 7/03 or 2/04. The changes are summarized in the table below.

Item	Description of Change	Related Changes
Environment change	Extend TOE environment from Trusted Solaris 8 4/01 and 12/02 to Trusted Solaris 8 4/01, 12/02, 7/03 and 2/04.	▪ Complete re-test on Trusted Solaris 8 7/03 and 2/04. ▪ Retest of updated installation procedures on Trusted Solaris 8 4/01 and 12/02. ▪ Generic changes to documentation and Test Plan updated. ▪ Repackaging of TOE components; new version numbers.
SMC command tool failure	New procedure and guidance in Installation Guide to install Trusted Solaris evaluated patches.	▪ Test of updated installation procedures on Trusted Solaris 8 7/03.
No Trusted Solaris patch procedures	New procedure in Installation and Administration Guides to install Trusted Solaris evaluated patches.	▪ Test extended to confirm new patch installation procedure. ▪ Test of updated installation procedures.
Patch import issues	Revised procedures in Installation and Administration Guides to install Trusted Solaris evaluated patches using only CD delivery.	▪ None.
Platform list	Changes to shell scripts in the SYSGEN subsystem to reflect platforms tested.	▪ Retest of updated installation scripts on Trusted Solaris 8 4/01, 12/02, 7/03 and 2/04.

Issues Raised or Revisited Since Clearswift Bastion II Version 2.1.0

19. The following minor changes were made.

Item	Description of Change	Related Changes
ARCHIVE script version number	Add version number to ARCHIVE script	▪ Re-test on Trusted Solaris 8 7/03 and 2/04.
Release Notice Package Version	Release Notice updated to quote TOE package versions	▪ Test of updated installation procedures on Trusted Solaris 8 7/03 and 2/04.

Item	Description of Change	Related Changes
Reboot bug 1	New test to confirm TOE behaviour due to a reboot bug.	▪ Re-test on Trusted Solaris 8 7/03 and 2/04.
Reboot bug 2	New test to confirm TOE behaviour due to another reboot bug.	▪ Re-test on Trusted Solaris 8 7/03 and 2/04.
SNMP daemon disablement	Changes to shell scripts in the SYSGEN subsystem to harden the Trusted Solaris platforms.	▪ Re-test on Trusted Solaris 8 7/03 and 2/04.
NIC Etherleak vulnerability	Installation Guide modified to repeat a warning already in the Release Notice.	▪ None.
Disk partitioning	Installation Guide updated to provide more flexible guidance on disk partitioning strategies.	▪ Test Plan updated to cover different disk partitioning strategies. ▪ Re-test on Trusted Solaris 8 7/03 and 2/04.
VET packaging issue	No change required following analysis.	▪ None.
VET and PROXY combinations	Test Plan updated to cover different combinations of VET and PROXY subsystems.	▪ Re-test on Trusted Solaris 8 7/03 and 2/04.
Write-cache enablement	Release Notice updated to include reference to Trusted Solaris procedures for write-cache enablement/disablement.	▪ Test Plan updated ▪ Re-test on Trusted Solaris 8 7/03 and 2/04.
SMC CLI integration	No change required following analysis.	▪ None.
Installation Guide typos	Changes to cross references in Installation Guide.	▪ None.
Poll period log	Change to correct process that reports poll period as seconds rather than milliseconds in log message.	▪ Re-test on Trusted Solaris 8 7/03 and 2/04.

Changes to Developer Evidence

20. There were no changes to the Functional Specification, High-Level Design or Low-Level Design and no changes to the Security Target, other than minor generic changes. Changes to the test documentation and other TOE documentation have been summarised 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 required no changes.

23. The Multi-Platform Rationale has also been updated to cover the hardware platforms supported by Trusted Solaris 8 4/01, 12/02, 7/03 and 2/04 and reflected mainly minor generic changes. Although Solaris now supports platforms with up to 128 processors, Clearswift Bastion II has only been tested on single and dual processor platforms and the Rationale has been updated to reflect the configurations tested. The Rationale has also been updated to reflect one addition to the UltraSPARC processor range and an extension to the range in processor speed. These extensions have been tested as summarised in the Trusted Solaris 8 Maintenance Report MR1 [k].

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 2.2.0, otherwise known as CS Bastion Version 2.2

26. The maintained TOE includes the following software:

- csbtsol package Version 4.00.00.
- csbcore package Version 4.00.00.
- csblaunch Version 1.02.01 (part of csbcore).
- csbarchtidy Version 1.02.00 (part of csbcore).

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

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

TOE Documentation

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

- Clearswift Bastion II Version 2.2 Installation Guide [h].
- Clearswift Bastion II Release 2.2.0 Release Notice [i].
- Clearswift Bastion II Version 2.2 Administration Guide [j].

TOE Environment

30. The defined Environment for Clearswift Bastion II Version 2.2.0 is as follows.

a) Sun Trusted Solaris 8 4/01, 12/02, 7/03 or 2/04 in its assurance maintained configuration [k] on any single Sun SPARC platform supported by the operating system [l] 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

31. Clearswift Bastion II Version 2.0.0 was tested on three specific platforms running Trusted Solaris 8 4/01 [a].

32. The Developers carried out a complete re-test of the maintained Version 2.2.0 on each of the following four platforms running Trusted Solaris 8 variants as indicated:

- A SunBlade 150, with OpenBoot PROM Version 4.10.6, UltraSPARC IIe Single 650 MHz processor, 1024MB memory, 80GB disc, using an X1034A Sun Quad FastEthernet PCI Adapter Card, running Trusted Solaris 8 7/03.

- A SunFire 280R, with OpenBoot PROM Version 4.2, UltraSPARC III Dual 750 MHz processor, 4096MB memory, 2x32GB discs, using an X1034A Sun Quad FastEthernet PCI Adapter Card, running Trusted Solaris 8 2/04.

- A SunFire V240, with OpenBoot PROM Version 4.13.2, UltraSPARC IIIi Dual 1280 MHz processor, 2048MB memory, 2x73GB discs, using an integral Sun Gigabit Ethernet Adapter Card, running Trusted Solaris 8 7/03.

- A SunFire V210, with OpenBoot PROM Version 4.13.2, UltraSPARC IIIi Single 1336 MHz processor, 1024MB memory, 73GB disc, using an integral Sun Gigabit Ethernet Adapter Card, running Trusted Solaris 8 2/04.

33. The Developers also carried out a partial re-test, covering installation and administrative tests only, of the maintained Version 2.2.0 on each of the following three platforms running Trusted Solaris 8:

- A SunBlade 100, with OpenBoot PROM Version 4.5, UltraSPARC IIe Single 500 MHz processor, 256MB memory, 18GB disc, using an X1034A Sun Quad FastEthernet PCI Adapter Card, running Trusted Solaris 8 12/02.

- A SunBlade 150, with OpenBoot PROM Version 4.10.6, UltraSPARC IIe Single 650 MHz processor, 1024MB memory, 80GB disc, using an X1034A Sun Quad FastEthernet PCI Adapter Card, running Trusted Solaris 8 4/01.

- A SunFire 280R, with OpenBoot PROM Version 4.2, UltraSPARC III Dual 750 MHz processor, 4096MB memory, 2x32GB discs, using an X1034A Sun Quad FastEthernet PCI Adapter Card, running Trusted Solaris 8 12/02.

34. For the derived TOE, Version 2.2.0, the CS Bastion II Version 2.0.0 test suite was supplemented with new tests as summarised in the Change Tables of this Report.