**ASSURANCE MAINTENANCE REPORT MR3
(supplementing Certification Report No. CRP248)**

Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1

Version 9.3R1

Issue 1.0

April 2011

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT (ADDENDUM)

The IT products detailed below have been certified under the terms of the UK IT Security Evaluation and Certification Scheme and have met the specified Common Criteria (CC) requirements. The scope of the certification and the assumed usage environment are specified in the body of this report.

Sponsor:	Juniper Networks, Inc.	Developer:	Juniper Networks, Inc.
Products, Versions/Releases:	**MR3 Derived:** Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1 **Original:** Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1		
Platforms:	(See above)		
Description:	The Juniper platforms are designed as hardware devices, which perform all routing/switching functions internally to the device. All router/switch platforms are powered by the same JUNOS software, which provides management and control functions as well as all IP routing.		
CC Version:	Version 3.1		
CC Part 2:	Conformant	CC Part 3:	Conformant
EAL:	EAL3 augmented by ALC_FLR.3		
PP Conformance:	None		
Related CC Certificates:	P248		
Date Maintained:	8 April 2011		

The evaluation and maintenance was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation and maintenance was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], [ST3], 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 and maintained against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of an Assurance Maintenance Report and Certification Maintenance Addendum is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

TABLE OF CONTENTS

I. INTRODUCTION

Overview

1. This Assurance Maintenance Report (MR[1]) [MR3] states the outcome of the Common Criteria (CC) [CC] Assurance Continuity [AC] process for *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*, as summarised on page 2 'Certification Statement (Addendum)' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. The baseline for this Assurance Continuity (also known as Assurance Maintenance) report was the original CC evaluation of *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*. That version was certified to CC EAL3, augmented with ALC_FLR.3, in February 2009.

3. Prospective consumers are advised to read this document [MR3] in conjunction with the following documents (available on the CESG and CC websites):

   a) the Security Target [ST] for the original certified Target of Evaluation (TOE), which specifies the functional, environmental and assurance requirements for the evaluation;

   b) the Certification Report [CR] for the original certified TOE;

   c) the updated Security Target [ST3] for the third maintained derivative[2].

4. The Developer of the certified TOE, and the third derived maintained version, is detailed on page 2 'Certification Statement (Addendum)' of this report and elaborated further on the CESG website (www.cesg.gov.uk).

Maintained Versions

5. The version of the product originally evaluated was:

   • *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*

6. The third derived version of the product for which assurance is maintained is:

   • *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*

---

[1] Note that Assurance Maintenance Report (AMR) is sometimes abbreviated to Maintenance Report (MR).
[2] The third maintained derivative is directly associated with the baseline CC evaluation and is not associated with the first or second maintained derivatives.

7. The maintenance of the third derived version is described in this document [MR3], which provides a summary of the incremental changes from the previous certified version [CR]**Error! Reference source not found.**.

Assurance Continuity Process

8. The Common Criteria Recognition Arrangement (CCRA) [CCRA] has been established as a basis for the mutual recognition of the results of Common Criteria evaluations. The process of Assurance Continuity within the CC is defined in the document 'Assurance Continuity: CCRA Requirements' [AC] and UK specific aspects are presented in [UKSP03P2].

9. The Assurance Continuity process is based on an Impact Analysis Report (IAR) produced by the Developer. The IAR describes all the changes made to the product, together with the updated evaluation evidence, and assesses the security impact of each change. For *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*, the IAR [IAR3] has been examined by the CESG Certification Body (CB), who produced this Maintenance Report [MR3].

10. The Developer, Juniper Networks, Inc., has considered all the relevant assurance aspects detailed in 'Assurance Continuity: CCRA Requirements' [AC]. No retesting was required for *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* because:

   a) There were no changes in the TOE software images since the certified version [CR]**Error! Reference source not found.**.

   b) There were no changes to the TOE platforms listed in the security target [ST3] since the certified version [ST]**Error! Reference source not found.**.

General Points

11. Assurance Continuity addresses the security functionality claimed in the updated Security Target [ST3] with reference to the assumed environment specified. The assurance-maintained TOE configurations and platform environments are as specified by the modifications detailed in Chapter II of this report [MR3], in conjunction with the original Certification Report [CR]**Error! Reference source not found.**. Prospective consumers are advised to check that this matches their identified requirements.

II.   ASSURANCE MAINTENANCE

Analysis of Changes

12.   [IAR3]**Error! Reference source not found.** provides the Impact Analysis Report from *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* to *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*, and provides the Assurance Continuity rationale for the maintained TOE on the stated platforms. **Error! Reference source not found.**[IAR3] conforms to the Assurance Continuity requirements specified in [AC], in particular Chapters 4 and 5.

13.   No major changes were made between the certified TOE and the third derived maintained version of the TOE: *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1.*

14.   The updated Security Target [ST3] and updated Secure Configuration Guide [SCG3] for CC consumers have incorporated changes to remove references to the use of the management GUIs and to ensure that access to the GUIs is disabled in the CC evaluated configuration. There were no bug fixes, since the TOE software and platforms had not changed. There were no changes to the development environment and hence no changes that impacted the ALC_FLR.3 augmentation.

15.   Consequently, only minor changes were required to the certified Security Target [ST]**Error! Reference source not found.** to obtain the Security Target for the third derived version [ST3].

Changes to Developer Evidence

16.   [IAR3] and [IAR3S] show that the evaluation documentation deliverables that were updated for *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* were as follows:

a)   Security Target [ST3]: updated from [ST].

b)   Secure Configuration Guide [SCG3]: updated from [SCG]**Error! Reference source not found.**.

17.   The CESG CB agreed with the Sponsor/Developer that a Vulnerability Analysis was not required because the only change provided reduced interfaces through which to manage the evaluated configuration of the TOE.

18.   All updates in the above documents were classified as *Minor*. There were no changes to any other evaluation documentation.

TOE Identification

19.   The maintained TOE is uniquely identified as:

> •   **Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1**

TOE Scope and TOE Configuration

20.   The TOE scope has been changed in Section 1.5 of [ST3], such that the management GUI is no longer in scope and access to the management GUI is disabled.

21.   The TOE configuration is defined in [SCG3].

TOE Documentation

22.   Apart from the Security Target [ST3] and the Secure Configuration Guide [SCG3], the TOE documentation has not changed.

TOE Environment

23.   Apart from moving the management GUI from the TOE to the environment, the rest of the defined environment has not changed and is defined in [ST3].

III. TOE TESTING

Vulnerability Analysis

24.   For the third maintained version, covered by this report, the CESG CB agreed with the Sponsor/Developer that a Vulnerability Analysis was not required because there was only a *Minor* change to the evaluated configuration of the TOE [IAR3].

25.   During the original evaluation, the Vulnerability Analysis was based on a search of public domain sources. As mentioned above, it was not necessary for that search to be repeated for the third maintained version. As the scope of the TOE and the deliverables were unchanged, the mitigation of these vulnerabilities was unchanged from that reported in [ETR].

26.   Chapter 5 of [IAR3] presents a justification that a search for vulnerabilities was not required.

27.   Therefore, no vulnerabilities were found between the certified version of the TOE and the third maintained version of the TOE.

TOE Testing

28.   No functional or penetration testing was required for the third derived version of the TOE because there were no changes in the TOE software images and no changes in the TOE platforms since the first derived version. The *Minor* change to the evaluated configuration did not require any testing.

IV. SUMMARY, CONCLUSIONS AND DISCLAIMERS

Summary

29.   The analyses in [IAR3] show that no major changes have been made to the TOE between the certified version and third derived version of *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*. Thus all changes are categorised as having a *Minor* impact and hence CC EAL3 augmented with ALC_FLR.3 assurance has been maintained.

Conclusions

30.   The CESG Certification Body accepts the decisions detailed in [IAR3] and [IAR3S]; and concludes that the overall impact of all the changes is *Minor*.

31.   The CESG Certification Body has therefore determined that EAL3 augmented with ALC_FLR.3 assurance, as outlined in Certification Report CRP248 [CR]**Error! Reference source not found.**, has been maintained for the third derived version, *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1*. Those conclusions are summarised in the 'Certification Statement (Addendum)' on Page 2 of this report.

32.   Prospective consumers of *Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1* should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST3]. The TOE should be used in accordance with the environmental assumptions specified in that Security Target. Prospective consumers are advised to check that the Security Functional Requirements (SFRs) and the evaluated configuration [SCG3] match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

33.   The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. A number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE are included in Certification Report CRP248 [CR]**Error! Reference source not found.**.

Disclaimers

34.   The Assurance Continuity process is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after the Assurance Continuity process has been completed. This Maintenance Report reflects the CESG Certification Body's view at the time of certification.

35.   Existing and prospective consumers should check regularly for themselves, in accordance with their Site Security Policy, whether any security vulnerabilities have been discovered since this

Report was issued and, if appropriate, should check with the vendor to see if any patches exist for the product and whether those patches have further assurance.

36.   The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

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

V.   REFERENCES

Common Criteria Documents

[AC]   Assurance Continuity: CCRA Requirements,
               Common Criteria Interpretation Management Board,
               CCIMB-2004-02-009, Version 1.0, February 2004.

[CC]   Common Criteria for Information Technology Security Evaluation,
               (comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1]   Common Criteria for Information Technology Security Evaluation,
               Part 1, Introduction and General Model,
               Common Criteria Maintenance Board,
               CCMB-2006-09-001, Version 3.1 R1, September 2006.

[CC2]   Common Criteria for Information Technology Security Evaluation,
               Part 2, Security Functional Requirements,
               Common Criteria Maintenance Board,
               CCMB-2007-09-002, Version 3.1 R2, September 2007.

[CC3]   Common Criteria for Information Technology Security Evaluation,
               Part 3, Security Assurance Requirements,
               Common Criteria Maintenance Board,
               CCMB-2007-09-003, Version 3.1 R2, September 2007.

[CCRA]   Arrangement on the Recognition of Common Criteria Certificates in the Field of
               Information Technology Security,
               Participants in the Arrangement Group,
               May 2000.

[CEM]   Common Methodology for Information Technology Security Evaluation,
               Evaluation Methodology,
               Common Criteria Maintenance Board,
               CCMB-2007-09-004, Version 3.1 R2, September 2007.

[MRA]   Mutual Recognition Agreement of Information Technology Security Evaluation
               Certificates,
               Management Committee,
               Senior Officials Group – Information Systems Security (SOG-IS),
               Version 3.0, January 2010 (effective April 2010).

UK IT Security Evaluation and Certification Scheme Documents

[UKSP00]   Abbreviations and References,
               UK IT Security Evaluation and Certification Scheme,
               UKSP 00, Issue 1.6, December 2009.

[UKSP01]   UK Scheme Publication No. 1: Description of the Scheme,
               UK IT Security Evaluation and Certification Scheme,
               UKSP 01, Issue 6.3, December 2009.

[UKSP02P1]	UK Scheme Publication No. 2: CLEF Requirements, Part I – Start Up and Operation, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part I, Issue 4.2, December 2009.
[UKSP02P2]	UK Scheme Publication No. 2: CLEF Requirements, Part II – Conduct of an Evaluation, UK IT Security Evaluation and Certification Scheme, UKSP 02: Part II, Issue 2.4, December 2009.
[UKSP03P1]	UK Scheme Publication No. 3: Sponsor's Guide, Part I – General Introduction, UK IT Security Evaluation and Certification Scheme, UKSP 03: Part I, Issue 2.2, December 2009.
[UKSP03P2]	UK Scheme Publication No. 3: Sponsor's Guide, Part II – Assurance Continuity, UK IT Security Evaluation and Certification Scheme, UKSP 03: Part II, Issue 1.0, December 2009.

Evaluated Version (Original)

[CR]	Certification Report No. CRP248, UK IT Security Evaluation and Certification Scheme, Issue 1.0, February 2009.
[ETR]	Evaluation Technical Report: Juniper Networks Services Routers running JUNOS 9.3R1, BT CLEF, LFS/T556/ETR, Issue 1.0, 15 January 2009.
[SCG]	Secure Configuration Guide for Common Criteria and JUNOS-FIPS, Juniper Networks, Inc., Release 9.3, January 2009.
[ST]	Security Target for Juniper Networks M7i, M10i, M40e, M120, M320, T320, T640, T1600, MX240, MX480 and MX960 Services Routers and EX3200, EX4200 Switches running JUNOS 9.3R1, Juniper Networks, Inc., Version 1.0, 13 January 2009.

Third Derived Version

[IAR3]	Impact Analysis Report JUNOS 8.5 & 9.3, Icon Security Ltd. for Juniper Networks, Inc., Version 1.2, 5 April 2011.
[IAR3S]	Review Form (Supplement to [IAR3]), CESG Certification Body and Icon Security Ltd., CB/110209/ISL/AC, Issue 1.1, 11 April 2011.

[SCG3]   Secure Configuration Guide for Common Criteria and JUNOS-FIPS, Release 9.3,
             Juniper Networks, Inc.,
             Revision 5, 31 March 2011.

[ST3]   Security Target for Juniper Networks EX3200 and EX4200 Switches
             running JUNOS 9.3R2,
             Juniper Networks, Inc.,
             Version 1.4, 05 April 2011.

[MR3]   *(this document)*

VI. ABBREVIATIONS

This list contains only abbreviations that are specific to the TOE. It does not include well-known IT terms (such as GUI, HTML) or standard CC abbreviations (such as TOE, TSF; see CC Part 1 [CC1]) or Scheme abbreviations (such as CESG, CLEF; see [UKSP00]).

FIPS   Federal Information Processing Standard

JUNOS   Juniper Operating System