



# **CCT Mark Test Report Summary**

## **Juniper Networks Secure Access Family**

### **Secure Access 4000-FIPS & Secure Access 6000-FIPS**

#### **Version 5.4R2.1**

Test Laboratory:

LogicaCMG  
Chaucer House  
The Office Park  
Springfield Drive  
Leatherhead, Surrey  
KT22 7LP

Vendor:

Juniper Networks (UK) Limited  
Building 1 Aviator Park  
Station Road  
Addlestone  
Surrey  
KT15 2PG

Test Report Summary Issue Date: 24 April 2007

Further details about the claims tested are included in the Information Assurance Claims Document (CCT Mark Certificate Number 2007/04/0020) published on the CCT Mark website ([www.cctmark.gov.uk](http://www.cctmark.gov.uk))

## 1. Test Result

- 1.1 All the security claims specified in [ICD] were tested successfully. The CSIA claims testing of Juniper Networks Secure Access Family 5.4R2.1 by LogicaCMG concluded that the claims made within [ICD] are valid for this IA Product.

## 2. References

[ICD] IA Claims Document published on the CCT Mark website for Juniper Networks Secure Access Family, Secure Access 4000-FIPS & Secure Access 6000-FIPS, Version 5.4R2.1

[JNSA4000] Juniper Network Secure Access 4000 - FIPS Datasheet, Version 100160-003, Nov 2006

[JNSA6000] Juniper Network Secure Access 6000 - FIPS Datasheet, Version 100161-003, Nov 2006

[SAFIPS] Juniper Networks Secure Access – Quick Start Guide, Release 5.4, 2006

[SAFRURI] Secure Access 6000 Field-Replaceable Units Removal and Installation, Release B, 2005

[SAG] Secure Access Administration Guide, Release 5.4, 2006

## 3. Scope of Testing

- 3.1 The product was tested against the all of the claims and test objectives made in the [ICD]. The SA-4000-FIPS version 5.4R2.1 and SA-6000-FIPS version IVEOS 5.4R2.1 were both tested.
- 3.2 Windows XP SP2 and Windows 2000 SP4 were used as the Client operating systems for the Windows testing. Red Hat Enterprise Server ES4 was used as the Client operating system for the Linux testing. Various backend authentication and application servers were also provided.
- 3.3 The tests were conducted at the Vendor's premises in Addlestone, Surrey by LogicaCMG.

- 3.4 The following products and platform combinations were tested, but the claims statements in the [ICD] make it clear which of the operating systems platforms are fully supported by the product.

<b>Product</b>	<b>Client Operating System</b>	<b>Browser</b>
SA-4000-FIPS	Windows XP Professional SP2	Internet Explorer v6.0
	Windows 2000 SP4	Internet Explorer v6.0
	Red Hat Enterprise Server ES4	Firefox 1.5
SA-6000-FIPS	Windows XP Professional SP3	Internet Explorer v6.0
	Windows 2000 SP4	Internet Explorer v6.0
	Red Hat Enterprise Server ES4	Firefox 1.5

#### **4. Ease of Use**

- 4.1 The installation of SA4000-FIPS and SA6000-FIPS Version 5.4R2.1 was straightforward consisting of easy to follow on screen instructions after the initial connections to the various interfaces.
- 4.2 During the first installation of the Secure Access FIPS system, the IVE serial console walks the user through the process of creating a security world through the serial console. A security world is a key management system used by Secure Access FIPS.
- 4.3 There were no issues or difficulties associated with the product. It was also easy to implement changes to the policy that govern the operation of the product.
- 4.4 Juniper recommends that customer installations of the SA4000-FIPS and SA-6000 – FIPS are performed by certified partners who have trained engineers, as the IT environment in which it is installed can be complex.

#### **5. Quality of User and Administration Documentation**

- 5.1 The current set of administrator documentation comprises of [SAFIPS] and [SAG].
- 5.2 The guidance documentation [SAFIPS] supplied with the products was generally straightforward and easy to use. [SAFIPS] is the standard document that is sent to customers when they first purchase the products. It contains information on installing the hardware, performing basic setup and licensing and configuring the SA. This document contains information on the other FIPS units as well as outlining all of the functions located on the IVE.

- 5.3 [JNSA4000] and [JNSA6000] are datasheets for the SA 4000 and SA 6000 units. They contain information surrounding the units, as well as summarise the values of the units. The final pages of each document state the specifications of the units. This is particularly useful as each contains a wide range of information, including details regarding the upgrade options, panel display, ports, power, environment, safety and emissions, warranty and more. These documents are useful for getting a better understanding of the benefits of this IVE and then comparing against others.
- 5.4 [SAFRURI] is a guide which relates to the SA 6000 unit. It contains information about installation and unit removals. [SAFRURI] contains detailed data surrounding hard disk, power supply and cooling fans. These are the main differentiators from the SA 4000 unit in that with the SA 6000 unit they can be removed and replaced.
- 5.5 [SAG] is a very detailed administration guide. It provides a vast amount of literature concerning many aspects of the IVE. Screenshots and additional notes are provided to give users a better understanding of the terminology and use.
- 5.6 Overall, the documentation set is suitable for the purposes of installation, configuration, administration and general use.
- 5.7 The vendor also has a web site that provides significant additional information in the form of FAQs (Frequently Asked Questions) and datasheets.

## 6. Resistance to Publicly Known Vulnerabilities

- 6.1 The evaluators performed a search for any publicly known vulnerabilities that may affect the product under evaluation. However, none were found.

## 7. Validation of Existing Assurance Certificates

- 7.1 The existing assurance certificates specified in the [ICD] have been validated for the relevant version of the IA Product which has been claims tested.
- 7.2 The FIPS140-2 Level 3 Compliant nCipher HSM PCI 4000 – Certificate #536 has been validated; please see the links below:

Listing:

<http://csrc.nist.gov/cryptval/140-1/1401val2005.htm>

Report:

<http://csrc.nist.gov/cryptval/140-1/140sp/140sp536.pdf>

## 8. Disclaimer

- 8.1 CSIA Claims Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the IS Product, IS Service or the Information Systems environment supporting the IS Product or IS Service. The issue of a Test Report Summary is not an endorsement of a product or service.
- 8.2 This Test Report Summary serves solely to summarise the results of the testing carried out for the CCT Mark Scheme and should not be taken as an endorsement or otherwise of the IS product or IS Service.

## 9. Abbreviations

<b>Acronym</b>	<b>Description</b>
CCT	CSIA Claims Test
CSIA	Central Sponsor for Information Assurance
FIPS	Federal Information Processing Standards
IA	Information Assurance
ICD	Information Assurance Claims Document
IVE	Instant Virtual Extranet
SA	Secure Access
SP	Service Pack