



# **CCT MARK**

## **IA Claims Document (ICD)**

### **AEP Netilla Security Platform**

### **Version 5.2.3.7**

CCT Mark Certificate Number: 2006/11/0016

CCT Mark Award expires on: 29 November 2008

Vendor Address:

AEP Networks Ltd  
Focus 31, West Wing, Cleveland Road  
Hemel Hempstead, Herts HP2 7BW  
United Kingdom

Vendor Website: [www.aepnetworks.com](http://www.aepnetworks.com)

Vendor Email: [info@aepnetworks.com](mailto:info@aepnetworks.com)

Vendor Telephone Number: +44 1442 458 600

# **1 Introduction**

## **1.1 Background**

This document outlines the Information Assurance (IA) claims made by AEP Networks, Inc in regard to the suitability of AEP Netilla Security Platform (NSP) for use by the UK Public Sector for secure, web-browser access to a broad range of business applications. With any PC or laptop, telecommuters, day extenders, branch office employees, business partners and a mobile sales force can quickly and securely reach virtually any resource used in the business.

## **1.2 Objectives**

The objectives of this ICD are to provide:

- A description of the AEP NSP and the expected environment including identification of any perceived threats and requirements upon the environment; and
- A statement of claims for the AEP NSP that will provide a countermeasure against the threats identified and thus tested against as part of the CCT Mark scheme.

## **1.3 Purpose of Document**

This document is the Initial Claims Document (ICD) for AEP NSP.

This ICD is the baseline document for the CCT Mark claims testing process of AEP NSP.

## **1.4 Structure**

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material;
- Section 2 contains the AEP NSP description and contains all the information related to the security of the AEP NSP.
- Section 3 details the claims that are made.

## 2 Product/Service Description

### 2.1 Product Identification

- Product Name: AEP Netilla Security Platform (NSP)
- Product Version: NSP-A, NSP-B, NSP-G
- Platform:

2.1.1 AEP NSP is supplied with the hardware on which it is to be installed, as shown in Figure 2.1. Claims testing will be performed on the AEP NSP.



Figure 2.1: AEP Netilla Security Platform

2.1.2 The Client operating system/browser combinations to be used in claims testing are shown in the table below:

Operating System	Browser
Microsoft Windows XP (SP2)	Internet Explorer 6.0.26, Mozilla 1.7.13, Firefox 1.5.0.7, Netscape 6.2.3, Netscape 7.2.0
Suse Linux 10.1	Mozilla 1.7.13, Firefox 1.5.0.7
Mac OSX Version 10.4.8	Safari Version 2.0.4 (419.3)

2.1.3 Further details of the services used in claims tested for each platform/browser combination are shown in the following table:

Browser			Service					
Name	Platform	JVM	SSL Tunnel	Thin-Client	Web	Admin	Idle	Periodic Reauth.
IE 6.0.26	Win32	MS	X	X	X	X	X	X
IE 6.0.26	Win32	Sun	X	X	X	X	X	X
Mozilla 1.7.13	Win32	Sun	X	X	X	X	X	X
Mozilla 1.7.13	Linux	Sun		X(4)	X	X		X
Netscape 7.2.0	Win32	Sun	X	X	X	X	X	X
Netscape 6.2.3	Win32	Sun	X	X(5)	X	X	X	X
Safari 2.0.4	Mac OSX	Apple		X(4)	X	X		
Firefox 1.5.0.7	Win32	Sun	X	X	X	X	X	X
Firefox 1.5.0.7	Linux	Sun		X(4)	X	X		X

**Notes:**

1. The exact versions of the operating systems for the platforms Win32, Linux and Mac OSX used in claims testing is specified in the Client Operating System/Browser table at paragraph 2.1.2 above.
2. All versions of Netscape and Mozilla do not properly handle the logout event for thin-client applications. Because of this, the user must close the browser after logging out before he/she can login again. This does not represent a security issue, as the user session is terminated within the NSP, but the Java applets do not properly handle this condition and fail to reinitialize upon the subsequent login.
3. The Port Forwarder which is part of the Web service has been tested on the following OS:browser combinations - WinXP SP1: MSIE 6, FF 1.0.4, Mozilla 1.7.5 and Linux: FF 1.0.4
4. The Client Drive Mapping and Universal Printing features for the Thin service are only compatible with Win32 platforms and are not supported under Mac OSX or Linux.

5. Accessing the Citrix environment, via the thin-client proxy is unsupported for Netscape 6. This is due to a conflict between the version of Java that Citrix requires (1.4.2 or above) to run, and the versions of Java that Netscape 6 is compatible with.

2.1.4 In addition, the following table represents a matrix of individual browser features and which services require them. Note that some of the features may be optional for the service (for example, Intranet could use JavaScript if the backend application server requires it. In this case, the item will not be checked, as the service itself does not require JavaScript).

Feature	Framework	My Files	Intranet	Thin-Client	SSL Tunnel	Idle	P. Reauth.	Admin
Cookies	X	X						
JavaScript	X	X		X		X	X	X
Java		X		X		X		
ActiveX					X			
IE "Medium Security" Zone				X	X			
JavaScript Access to cookies			X(1)					

**Notes:**

1. If JavaScript and cookies are used in the remote site.
2. The feature requirements for any given service are the union between the "framework" component, as well as the requirements for the given service. Since the only requirements for the framework are cookie support and JavaScript, basically add these to the requirements for any other service to determine the service requirements.

**2.2 Product/Service Overview**

**2.2.1 General**

AEP NSP is an SSL VPN appliance that enables organisations to simply, securely and cost effectively provide users with web-browser based access to business applications – server-based (Windows, Citrix, UNIX/Linux and mainframe), web-based, client/server synchronization and file shares - from any location.

The product achieves this through a number of access mechanisms:

- **Web Reverse Proxy.** Web servers and applications with a browser interface on the private network are accessed as a client by the NSP product, which also acts as a client for the users logging in to access those servers. Translation of html traffic between the server and the client PC is enforced by the NSP product, so that no references to private side resources are available to the end user. Typically this will be used to provide e.g. Outlook web access for remote users. Access via the Web Reverse Proxy includes an option for intelligent port forwarding: a Java applet loaded onto the client PC acts as a local proxy, ensuring that traffic aimed at a specific port on the server side is translated into SSL-encrypted html traffic via port 443, which is then decrypted by the NSP product and forwarded in the clear to the correct port on the server.
- **Thin Client.** This access method is recommended for situations in which access is required from untrusted devices. It is a server based mechanism for access to e.g. terminal services and Unix/Linux servers. The NSP product runs window servers (such as X.11) internally, and interfaces to the private side resources, presenting to the client side just that information necessary to render the contents of window on the end user machine. The information to be rendered is sent to a Java applet on the client PC, using SSL.
- **Tunnelling.** This option provide pure network connectivity and is not recommended for general use, since the client PC is provided with a private side network address (subject to any Network Address Translation that may be in force), and the client is therefore provided with private side network level access, subject to control by NSP over the resources which are available to them. Tunnelling access is provided for Windows clients only, and administrator-level privileges are required to install the necessary client-side components.

The AEP NSP allows users remote access to multiple applications and file systems within the organisation via a portal home page, as follows:

- Users wishing to access any of the applications and resources that are available for access via the AEP NSP first enter the unique URL of the appliance in a web browser from any Internet connection, and are presented with a web-based login screen.
- The user enters their access credentials, and the request is processed by the NSP. Typically the NSP will query external authentication and authorisation servers, such as Windows Active Directory or LDAP, to confirm user identity. Strong authentication options, such as 2-factor or PKI, are also

supported.

- Upon successful authentication, the NSP polls external resource servers (such as mail servers), determines the specific server-based resources that the user or group member is authorised to access, and presents these resources as icons on a portal home page.
- Users can now remotely and securely access any of the applications, regardless of network-layer and application-layer issues.

The NSP controls access to applications and information on resource servers on the corporate network, through the concept of “V-Realms”. A V-Realm is a container for corporate security policies specifying identity, entitlements, environment and client integrity tests. Users are assigned to V-Realms. Users can only access applications and information according to the access rules applying to the V-Realm to which they are assigned.

The NSP is available in three different configurations, as follows (the only difference among models is in scalability (number of users) and not in security features):

- NSP-A. The NSP-A is designed to support up to 100 concurrent users;
- NSP-B. The NSP-B is designed to support from 100 to 250 concurrent users;
- NSP-G. The NSP-G is designed to support from 250 to 800 Thin Proxy users or from 250 to 1000 web and client/server users.

Note: Only the NSP-G shall be tested as part of the claims testing.

### 2.2.2 Security Architecture

The NSP-G is a 1U-height, rack mount chassis, Intel CPU-based server with two RJ-45 10/100 Ethernet LAN ports, a serial console port, and one serial failover/cluster port. The appliance has an optional FIPS 140-1 certified Hardware Security Module (HSM) that plugs into a PCI slot in the main processor board.

Figure 2.2 illustrates how an NSP-G is used in a typical installation where it secures the datacenter resources in an enterprise for users who access these resources through remote connections via the Internet.

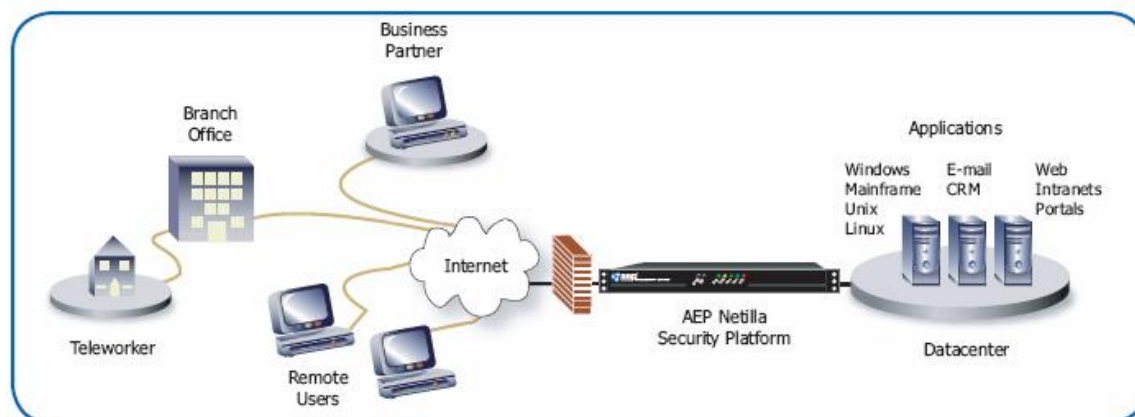


Figure 2.2: Typical AEP NSP environment

### 2.2.3 Hardware Requirements

The AEP NSP is supplied with the hardware on which the software shall be installed and therefore there are no further hardware requirements.

### 2.2.4 Software Requirements

The AEP NSP is supplied as a turnkey appliance with all the software necessary to provide the claimed functionality.

### 2.2.5 Out of Scope for Claims Testing

Only the Operating Systems and browsers listed in the table in Section 2.1 are in the scope of the CCT Mark testing.

When a user is initially connected to the network, an integrated Sygate Agent (SODA) Client Integrity suite is downloaded and launched on the client PC. SODA provides the capability to scan client PCs for security vulnerabilities in the installed OS (e.g. security settings, patch levels and updates). Clients that pass the integrity check are permitted to authenticate, while clients that fail are redirected to a failure web page. Whilst the loading and use of the SODA test results are within the scope of the product testing described here, the actual operation of the SODA suite (a third party product) is not.

The optional FIPS Hardware Security Module supported by the product is not within the scope of the testing.

The Activ Card and Aladdin authentication mechanisms, although supported by the product will not form part of the tests.

A Linux resource server is excluded from the scope of any of the claims, and did not form part of the test environment.

Forms-based authentication is excluded from the scope of the claims relating to authentication system support.

## **2.3 Usage Assumptions**

### **2.3.1 Assets**

Assets which are to be protected are corporate applications, files and client Personal Computer/laptop integrity.

### **2.3.2 Threat Scenario**

Threats to assets which are countered are:

- T1** Unauthorised individuals gaining access to sensitive data on untrusted computers after Users have completed their session.
- T2** Users neglecting to log-out from untrusted environments.
- T3** Malicious code residing on untrusted computers transferring onto the corporate internal network.
- T4** Negligent or malicious usage by the end-user damaging or compromising the integrity of the internal application.
- T5** Network level and Application level attacks originating from the external network and/or the internet.
- T6** Eavesdropping on communications.

### **2.3.3 Expected Operational Environment**

It is expected that the AEP NSP will be employed within infrastructures that enable user access to both terminal server-based and web-based applications. The AEP NSP is normally connected to the LAN between the corporate datacenter assets and the firewall as shown in Figure 2.2.

### **2.3.4 Organisational Security Policies**

The AEP NSP is intended to support remote access control organisational policies in securing the connection from external, untrusted environments.

### **2.3.5 Security Requirements on the Environment**

The AEP NSP uses its ACCM technology to supply the SSL encryption. The AEP NSP is deployed inside the enterprise firewall as shown in Figure 2.2. The browser and client OS combinations are shown in the tables in section 2.1.

The device is intended to be operated in an environment which includes security management with three levels of administrative access: administrator, remote administrator, and maintenance.

### 3 Security Claims for the IA Product or Service

The Security features of the AEP NSP are as follows:

#### 3.1 Claims Statements

Ref	Claims Statement
	<b>Encryption</b>
<b>CS1</b>	All outgoing (session) data is encrypted.
<b>CS2</b>	Authentication data requested from the user is encrypted.
	<b>Authentication System Support</b>
<b>CS3</b>	Authentication is performed by the AEP NSP Appliance at the network access perimeter. The following protocols are supported: <ul style="list-style-type: none"> <li>• Microsoft Windows NT/2000/2003 – SMB/Active Directory;</li> <li>• RADIUS and RADIUS Groups;</li> <li>• LDAP (Open LDAP, Novell eDirectory, IPlanet);</li> <li>• Vasco Digipass (Built-in server);</li> <li>• RSA SecurID;</li> <li>• Kerberos;</li> <li>• Client side certificates with revocation.</li> </ul>
	<b>V-Realm Architecture</b>
<b>CS4</b>	AEP's advanced V-Realms client controls access to applications and information. A V-Realm is a container for corporate security policies specifying identity, entitlements, environment and client integrity tests. Users are assigned to V-Realms. Users can only access applications and information according to the access rules applied to the V-Realm to which they are assigned.
<b>CS5</b>	Different authentication and client integrity rules can be applied to each V-Realm.
<b>CS6</b>	The V-Realm architecture supports the following group memberships by accessing: <ul style="list-style-type: none"> <li>• Microsoft Windows Global groups (Domain/SMB);</li> <li>• LDAP (including Active Directory);</li> <li>• RADIUS;</li> <li>• Local groups.</li> </ul>
<b>CS7</b>	A simple, easy-to-use mechanism is provided to enable changes to V-Realm rules (stages) and membership.

Ref	Claims Statement
	<b>Inactivity Time-outs</b>
<b>CS8</b>	The AEP NSP can be configured to apply a timeout parameter to automatically timeout user sessions to ensure that the sessions do not live indefinitely if users neglect to log off.
	<b>Inactivity Re-authentication</b>
<b>CS9</b>	To ensure that only legitimate users continue to work from an NSP session, the NSP can be configured to periodically request user passwords; failure to re-authenticate successfully immediately terminates the NSP session.
	<b>Client Machine Identification (CMID)</b>
<b>CS10</b>	<p>CMID authentication creates a unique profile (based on CPU, memory, network card addresses and other information) to uniquely identify a specific client device. CMID profiles are associated with users. CMID authentication is used by the NSP to authorise specific PCs, and to deny access requests from unauthorised PCs.</p> <p>The first time the user logs in to the NSP, the NSP creates a profile of administrator-defined information and alerts the NSP administrator to approve the machine.</p> <p>The CMID feature only works with Win32 platforms.</p>
<b>CS11</b>	Subsequent logins must match this unique signature or access is denied.
<b>CS12</b>	Logins from users on PCs which have not been profiled and approved are rejected.
	<b>Endpoint Security</b>
<b>CS13</b>	<p>Client PCs are protected from information downloaded onto them during the session, information which can be deleted, including:</p> <ul style="list-style-type: none"> <li>• Temporary files;</li> <li>• Browser cache;</li> <li>• Downloaded files, pages, URLs;</li> <li>• Cookies;</li> <li>• History information.</li> </ul>

Ref	Claims Statement
<b>CS14</b>	<p>When a user is initially connected to the network, an integrated Sygate Agent (SODA) Client Integrity suite is downloaded and launched on the client PC. Clients that pass the integrity check are permitted to authenticate, while clients that fail are redirected to a failure web page.</p> <p>The SODA Client Integrity suite only works with Win32 platforms.</p>
<b>CS15</b>	<p>Client integrity scanning using SODA can be configured in a continual “polling” manner throughout the life of the user session. Whenever a failure notice is received by the NSP the session is terminated and the client is directed to a failure web page.</p>
<b>Tunnelling</b>	
<b>CS16</b>	<p>The AEP NSP provides secure network level access for remote users, using SSL tunneling.</p>
<b>CS17</b>	<p>The AEP NSP has a session-based firewall that applies policy rules on a per-user basis for applications using the SSL tunnel mode access method.</p>
<b>Thin Client Proxy</b>	
<b>CS18</b>	<p>The NSP’s thin-client proxy allows a remote user using a PC/browser to access Citrix, and Windows Terminal Services farms securely over an SSL VPN.</p>
<b>CS19</b>	<p>The thin proxy also provides client-drive mapping.</p>
<b>Web Reverse Proxy</b>	
<b>CS20</b>	<p>The NSP protects “private side” web servers in the private network with Web reverse proxy technology. At no time is the end-user directly connected to a “private side” network resource.</p>
<b>CS21</b>	<p>NSP allows administrators to set up access control to servers, and paths on a user or group basis.</p>
<b>Intelligent Port Forwarding</b>	
<b>CS22</b>	<p>The NSP supports “intelligent” Port Forwarding, which is useful for organizations that prefer to use the Microsoft native RDP client or native Citrix ICA client. A java client application dynamically installed on a remote user’s Windows PC encapsulates and encrypts all the traffic in SSL and forwards it to the NSP at the enterprise side of the network, where it can be deciphered and delivered to a terminal server or Citrix MetaFrame server.</p>

Ref	Claims Statement
	<b>Logging and Reporting</b>
<b>CS23</b>	<p>The Event Logging mechanism logs and records security events. The Security events logged include:</p> <ul style="list-style-type: none"> <li>• Login success or failure;</li> <li>• Security policy, i.e. attempts to access a URL that is not authorised; and</li> <li>• Password changes.</li> </ul>
<b>CS24</b>	<p>The Event Logging mechanism records security events in Syslog format and SNMP traps.</p>
	<b>Single Sign On</b>
<b>CS25</b>	<p>The AEP NSP provides Single Sign On enforcement capabilities. Credentials can be collected during the initial login and used when selecting applications later on during the session so users are not re-prompted for login information.</p>
	<b>Automatic Application Launch</b>
<b>CS26</b>	<p>The NSP can be configured to automatically launch specific applications immediately upon initial login. This feature can be assigned on a per-V-Realm basis.</p>
	<b>Management</b>
<b>CS27</b>	<p>The AEP NSP supports three levels of administrative access: administrator, remote administrator, and maintenance.</p>
<b>CS28</b>	<p>The product supports a remote administrative interface which can be enabled and disabled by a local authorised individual.</p>

### 3.2 Existing Assurance Certificates

None.

## Annex A: Glossary of Terms

<b>Terms</b>	<b>Definitions</b>
AEP NSP	AEP Netilla Security Platform
ACCM	Asynchronous Control Character Map
CCT Mark	CSIA Claims Tested Mark
CSIA	Central Sponsor for Information Assurance
ICD	Information Assurance Claims Document
FIPS	Federal Information Processing Standards
JVM	Java Virtual Machine
LDAP	Lightweight Directory Access Protocol
LAN	Local Area Network
OS	Operating System
PC	Personal Computer
PCI	Peripheral Component Interconnect
PKI	Public Key Infrastructure
SMB	Server Message Block
SSL	Secure Sockets Layer
SODA	Sygate On-demand Agent
SP	Service Pack
URL	Uniform Resource Locator
VPN	Virtual Private Network
Win32	Microsoft Windows 32-bit Operating Systems

## **Annex B: Marketing Statement to be Used**

The AEP Netilla Security Platform (NSP) is an SSL VPN appliance that enables organizations to simply, securely, and cost effectively provide users with browser-based access to corporate applications and files from through the security and convenience of a web browser. With any browser enabled computer, telecommuters, branch office employees, business partners and a mobile sales force can quickly and securely reach virtually any resource used in your business.