



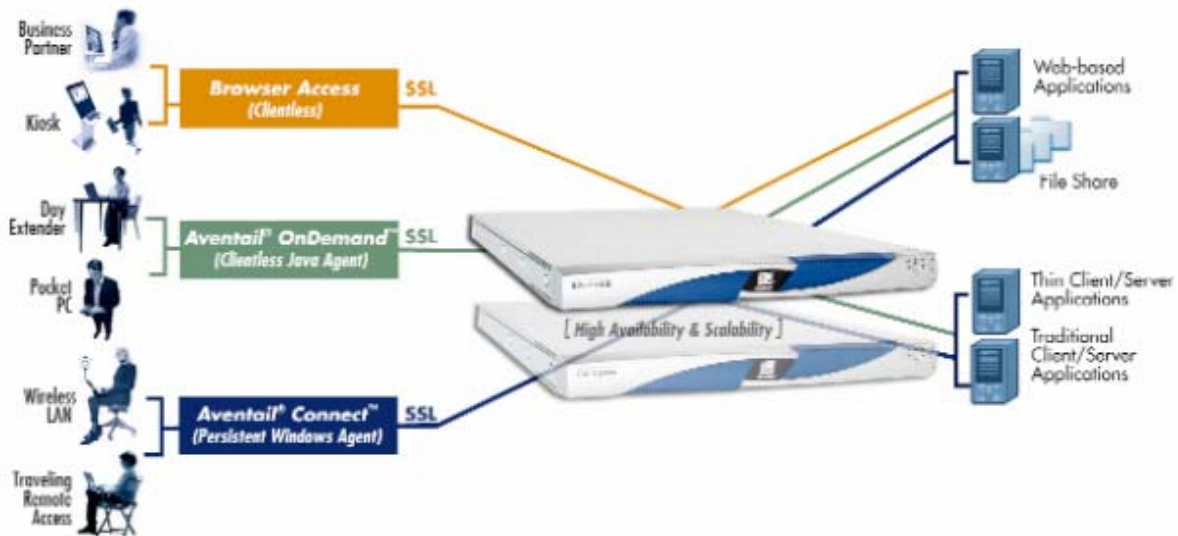
RSA Keon Ready Implementation Guide For PKI 3rd Party Applications

Aventail EX-1500

Last Modified Friday, March 19, 2004

1. Partner Information

Partner Name	Aventail
Web Site	http://aventail.com
Product Name	EX-1500™
Version & Platform	6.4.2
Product Description	The Aventail® EX-1500™ SSL VPN appliance provides your employees, partners, and customers with secure, anywhere access to the Web and client/server applications they need. In addition, the Aventail EX-1500 dramatically reduces the cost of deploying and managing your remote access VPN.
Product Category	Perimeter Defense
RSA Product Interaction	RSA Keon Certificate Authority



The Aventail / RSA Keon Certificate Authority (RSA KCA) solution provides certificate based authentication for remote users of the Aventail EX-1500. Users with private keys issued from the RSA KCA are authenticated by the Aventail EX-1500 via the ldap protocol.

2. Contact Information

	Sales contact	Support Contact
Email	info@aventail.com	aventailcustomerservice@aventail.com
Phone	1.877.AVENTAIL	N/A
Web	www.aventail.com	http://aventail.com/tech_support/default.asp

3. Product Requirements

Hardware requirements

Component Name: Aventail EX-1500	
Aventail EX-1500	Version 6.4.2

4. Product Configuration

RSA Keon CA's *installable* elements required for interoperability.

1. Keon CA must be configured to publish to an external repository. SunOne Directory Server v5.1 was utilized for this testing. Please refer to [RSA Secured Website](#) for information on publishing to this and other certificate repositories. No additional installable elements were necessary to achieve interoperability.

RSA Keon CA's *configurable* elements required for interoperability

1. The jurisdiction created to achieve interoperability should include at least the following **extension profiles**:
 - SSL Server**
 - Basic PKIX-Compliant End-Entity**
2. The external publishing values of the jurisdiction created to achieve interoperability should include an **end entity attribute** of **cn=uid**

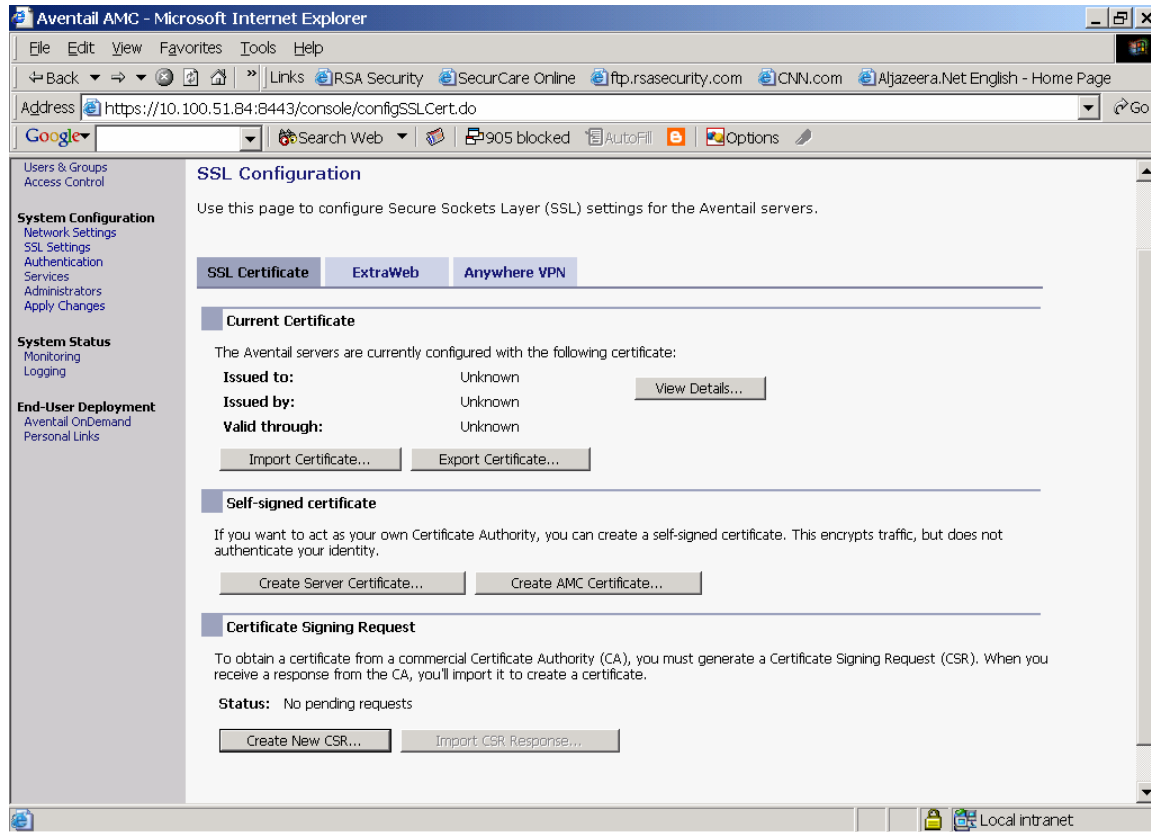
Partner product's *installable* elements required for interoperability

1. This guide assumes you've successfully installed and configured the Aventail EX-1500 by running the Aventail Setup Tool and have access to the Aventail Management Console (AMC). Please refer to the appropriate administration guides for detailed instructions.

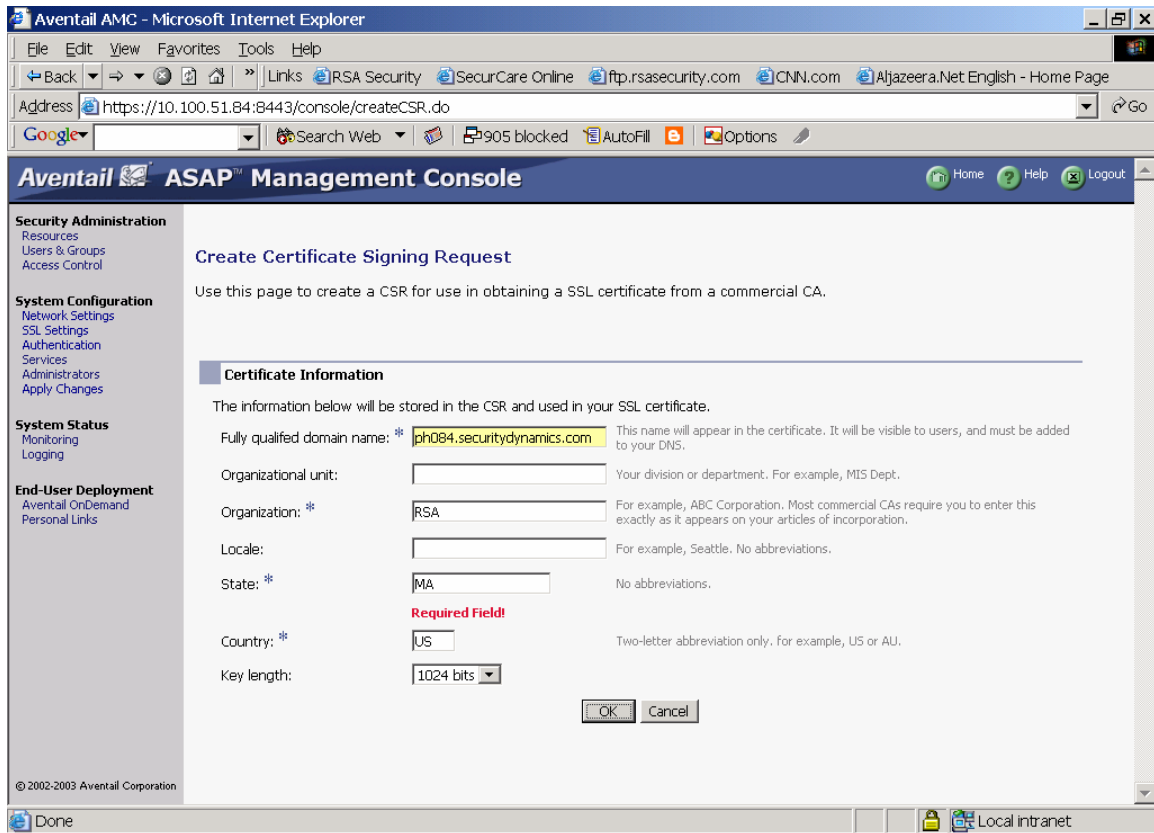
Partner product's *configurable* elements required for interoperability

1. Prepare the Aventail EX-1500 for use with an SSL Server Certificate

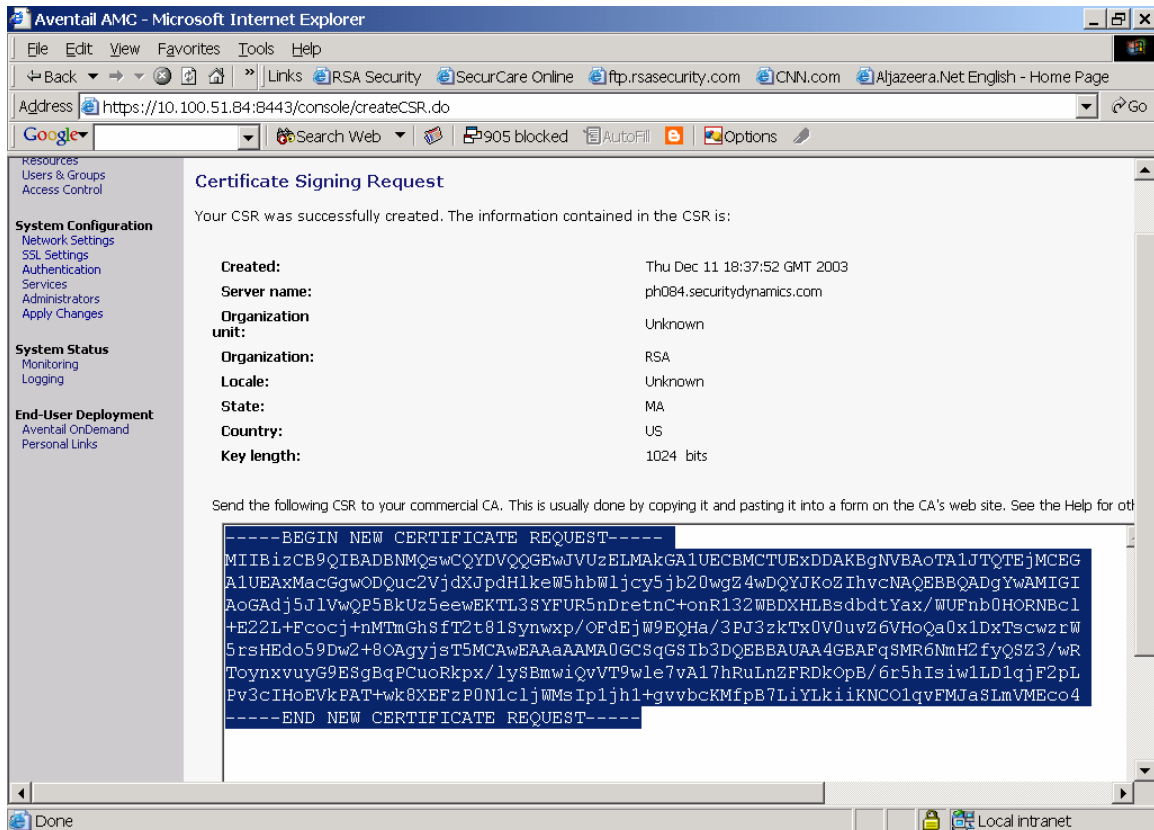
Generate a CSR at the AMC



Click on "Create New CSR"



Provide appropriate information and click OK.



Cut the CSR from the page and leave on clipboard or copy to file.

looks similar to this:

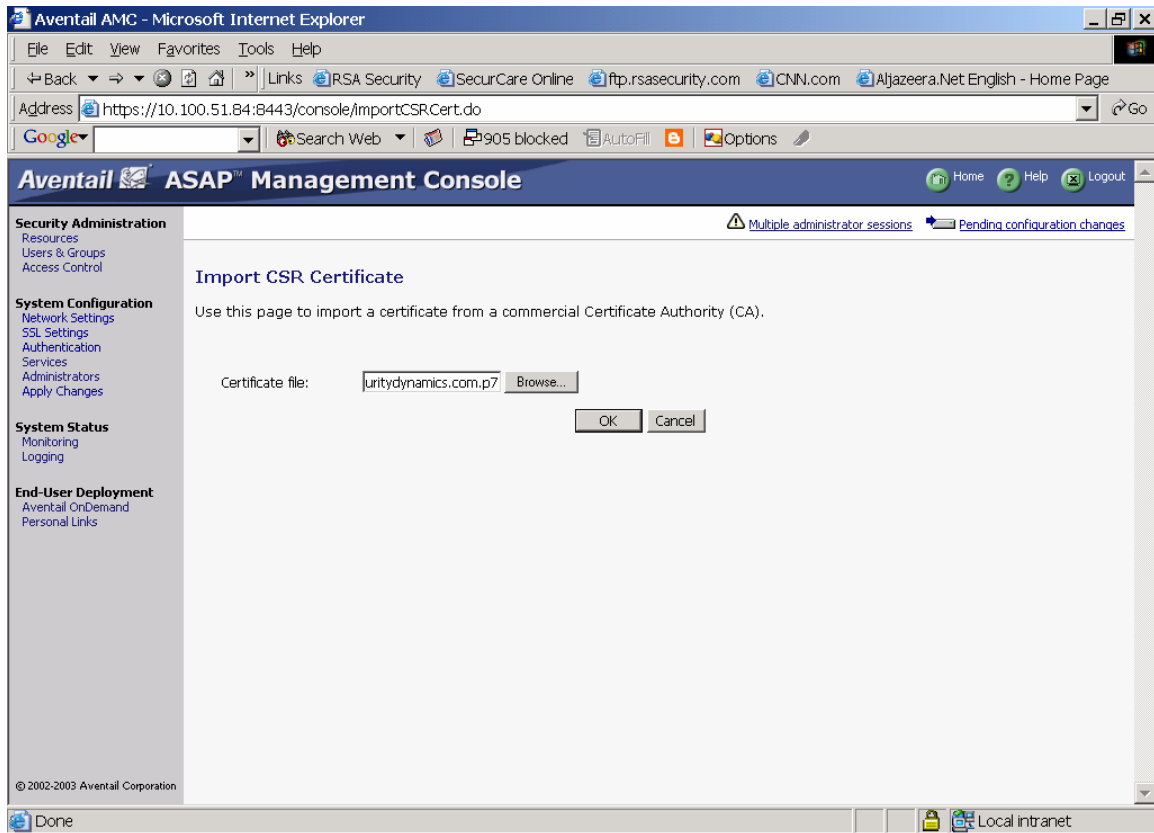
```
-----BEGIN NEW CERTIFICATE REQUEST-----  
...  
-----END NEW CERTIFICATE REQUEST-----
```

Put the text of the message here:

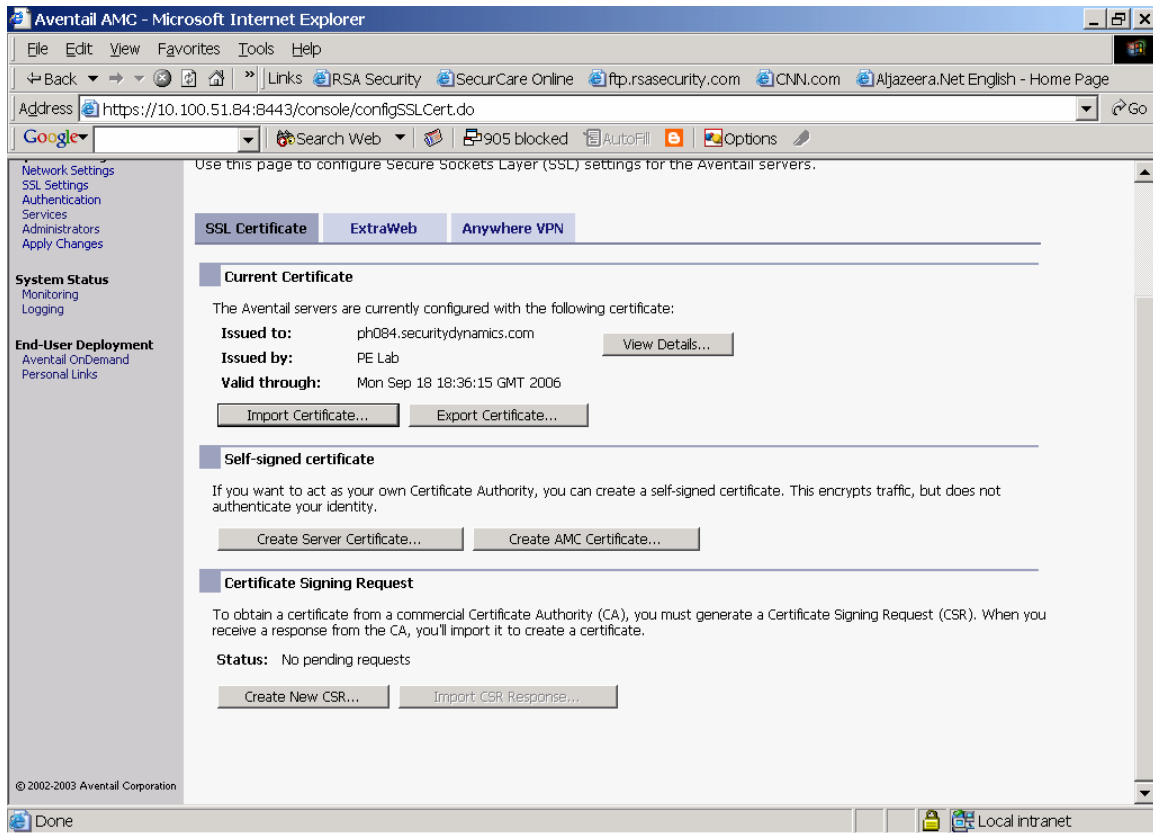
```
-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIBizCB9QIBADBNMQswCQQYDVQQGEwJVUzELMAkGA1UECBMCTUExDDAKBgNVBAoTA1JTRTEjMCEG  
A1UEAxMacGwODQuc2VjdXJpdH1keW5hbWljcy5jb20wgZ4wDQYJKoZIhvcNAQEBBQADgYwAMIGI  
AoGAdj5JlVwQP5BkUz5eewEKTLSsYFUR5nDretnC+onR132WBDXHLBsdbdtYax/WUFnb0HORNbc1  
+E22L+Fcocj+nMTmGhsfT2t81synwpx/OFdeJW9EQHa/3PJ3zkTx0V0uvZ6VHoQa0x1DxTscwzrW  
5rsHEdo59Dw2+8OAgysT5MCAwEAAaAAMA0GCSqGSIb3DQEBBAAUAA4GBAFqSMR6NmH2fyQSZ3/wR  
ToynxvuyG9ESgBqPCuoRkpx/lySBmwiQvVT9wle7vA17hRuLnZFRDkOpB/6r5hIsiw1LD1qjF2pL  
Pv3cIHoEVkPAT+wkBXEFzP0N1cljWMSIp1jh1+gvvbcKMfpB7LiYLkiiKNC01qvFMJaSLmVMEco4  
-----END NEW CERTIFICATE REQUEST-----
```

The request contents will be displayed after you click submit.
They will then be placed into the request queue.

At the appropriate RSA Keon CA jurisdiction, submit the csr for signing. Once submitted, save the PKCS#7 response to a file.



Import the PKCS#7 response at the AMC. Click OK.



This RSA Keon CA server certificate is now installed and will be used to create an SSL connection.

2. Ensure proper Roots files are loaded on the appliance.

- The ca.cert file in the /usr/local/aventail/etc should contain any roots keys from CAs that issued certificates to users who authenticate using client certificates.
- The ldapca.cert file in /usr/local/aventail/etc should contain any roots keys from CAs that issued SSL certificates used on back-end LDAP servers accessed using secure LDAP (LDAPS).
- The backendca.cert file in /usr/local/extraweb/etc should contain any roots keys from CAs that issued SSL certificates in use on the back-end secure Web servers (HTTPS) managed by ExtraWeb server.

NOTE - Detailed information can be found regarding these files in the EX-1500 Administration and Installation Guide.

3. Configure Aventail EX-1500 for Client Certificate Auth SSL

*Note - Before configuring this authentication method, it may be a good idea to ensure that users are able to authenticate using LDAP Username/Password before attempting to authenticate with a cert. Detailed instructions on this authentication method can be found in the **Aventail EX-1500 Installation and Administration Guide.***

Aventail refers to this authentication method as LDAP with Digital Certificates. Detailed instructions on the configuration of this authentication type can be found in the **Aventail EX-1500 Installation and Administration Guide.**

The following screenshot is a sample configuration for this authentication method as entered into the AMC.

Aventail ASAP Management Console Home Help Logout

Security Administration
Resources
Users & Groups
Access Control

System Configuration
Network Settings
SSL Settings
Authentication
Services
Administrators
Apply Changes

System Status
Monitoring
Logging

End-User Deployment
Aventail OnDemand
Personal Links

Configure LDAP Authentication

Use this page to configure authentication settings for an LDAP server.

Credential type: Digital Certificates

Name:

Description:

General

Roots file: [View roots file details](#)

Maximum chain length:

LDAP

LDAP server:

Login DN:

Password:

Search base:

Matching LDAP Attributes

Attribute mapping:

Certificate attribute:

Group attribute:

Fast groups

Advanced

Enable LDAP referrals

Server timeout: seconds

LDAP over SSL

Use SSL to secure LDAP connection

SSL roots file: [View SSL roots file details](#)

Match certificate CN against LDAP server name

Maximum chain length:

OK Cancel

5. Product Operation

RSA Keon CA operational elements

Certificates presented to the Aventail EX-1500 are extracted from the local Cryptographic Service Provider (CSP). As such, RSA SecurID Passage was used to store the private key and present it for successful authentication. Although RSA SecurID Passage is mentioned in this document, integration is actually achieved through the browser on the local PC. Please refer to <http://www.rsasecurity.com/support> for supported browsers.

The private key is then presented to the EX-1500 where it is presented to the certificate repository and checked against the public key information. The EX-1500 will search for the appropriate **uid** for the user. Please ensure the jurisdiction has the **end entity attribute** of **cn=uid** (see section 4).

6. Certification Checklist for 3rd Party Applications

Date Tested: Jan 5, 2004

Product	Tested Version
RSA Keon Certificate Authority	6.5.1
RSA Keon Web Passport	N/A
RSA SecurID Passage	3.5.1
Aventail EX-1500	6.4.2

Test Case	Result		
Certificate Enrollment			
P10 Certificate Request	P		
P7 Response installed correctly	P		
CMP Certificate Request	N/A		
CMP Response installed correctly	N/A		
SCEP Certificate Request	N/A		
SCEP Response installed correctly	N/A		
Import Certificate			
Import PKCS#12 envelope	N/A		
Import via cut & paste	N/A		
Install Root Certificate via cut/paste	P		
Install SubCA Certificate via cut/paste	P		
Install Root Certificate via SCEP	N/A		
Install SubCA Certificate via SCEP	N/A		
Verify Certificate chain is installed	P		
Certificate Usage			
	Sign	Encrypt	SSL
S/MIME	N/A	N/A	
Document and Files	N/A	N/A	
SSL Client Authentication			P
LDAP Support			
Name lookup	N/A		
Certificate retrieval	N/A		
Status Check of Certificate			
	OCSP	CRL	Other
Success with a valid certificate	N/A	N/A	N/A
Fails with a revoked certificate	N/A	N/A	N/A
Fails with a suspended certificate	N/A	N/A	N/A
Pass with a re-instated certificate	N/A	N/A	N/A
RSA Keon Web Passport / RSA SecurID Passage Support			
Access certificates via MS CAPI (Internet Explorer)		Passage	KWP
		P	N/A

JRV

*P=Pass or Yes F=Fail N/A=Non-available function

7. Known Issues

There are no known issues with this implementation.