SSH Communications Security Corp.
Tectia 6.0

RSA Secured Implementation Guide
For Certificate Authority Products

Last Modified: July 16, 2008

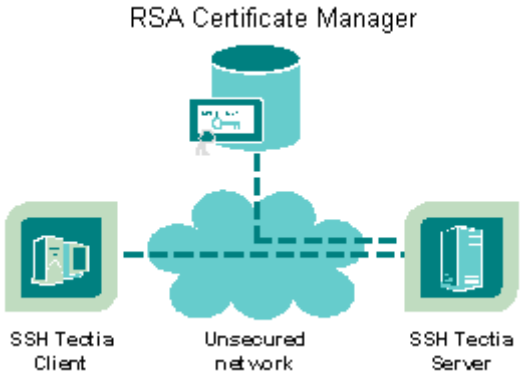
Partner Information

Product Information	
Partner Name	SSH Communications Security, Inc.
Web Site	www.ssh.com
Product Name	SSH Tectia Client SSH Tectia Server
Version & Platform	6.0.1 on Windows XP SP1 and Windows 2003 SP1 x64
Product Description	SSH Tectia Client/Server is the de facto standard enterprise security solution used by millions worldwide for secure file transfers, system administration and application connectivity throughout the network. SSH Tectia provides transparent, strong encryption, flexible authentication options, direct support for all major industry platforms, and superior performance, without requiring modifications to the existing infrastructure or applications. It also helps organizations meet regulatory compliance requirements, including a Federal Information Processing Standards (FIPS) 140-2 certified crypto algorithm for use in U.S. federal government applications. In addition, the commercially supported SSH Tectia solution with SSH Tectia Manager helps enterprises achieve compliance with PCI DDS and other government regulatory requirements.
Product Category	Authentication

Solution Summary

With the SSH Tectia solution, organizations can easily and cost-effectively leverage their existing digital certificate infrastructure, also known as PKI (Public Key Infrastructure). RSA Certificate Manager is an industry proven certificate manager providing digital certificate enrollment for not only SSH2 but also for Web services, E-mail, VPN. This best-of-breed solution offers full certificate lifecycle management.

Customers and prospects now wishing to use certificate authentication with SSH Tectia can do so with ease of implementation and can scale identity and key management throughout the entire enterprise. Optionally, customers can use SSH Tectia Manager (with its own internal CA) to deploy custom server and client configurations. These configurations can be deployed across the board to ensure scalable certificate authentication. Any server or client certificate can be easily revoked from the RSA Certificate Manager web console with immediate policy enforcement across your SSH Tectia environment.



Product Requirements

Partner Product Requirements: SSH Tectia Client	
CPU	No special requirements
Memory	No special requirements
Storage	50 MB
Firmware Version	N/A
Operating System	
Platform	**Required Patches**
Microsoft Windows XP (x86 and x64)	Service Pack 2
Microsoft Windows Vista (x86 and x64)	
Microsoft Windows Server 2003	
HP-UX (PA-RISC) 11iv1, 11iv2, 11iv3	
HP-UX (IA-64) 11iv2, 11iv3	
IBM AIX 5L (POWER) 5.2, 5.3	
Red Hat Enterprise Linux (x86 and x86-64) 3,4,5.5.1	
Sun Solaris (SPARC, 32-bit) 8,9,10	
Sun Solaris (x86-64) 10	
SUSE LINUX Enterprise Desktop (x86 and x86-64) 10	
SUSE LINUX Enterprise Server (x86 and x86-64) 9,10	
IBM z/OS (zSeries) 1.6, 1.7, 1.8, 1.9	

Partner Product Requirements: SSH Tectia Server	
CPU	No special requirements
Memory	1 GB RAM for hundreds of simultaneous tunnels
Storage	100 MB
Firmware Version	N/A

Operating System	
Platform	**Required Patches**
Microsoft Windows XP (x86 and x64)	Service Pack 2
Microsoft Windows Vista (x86 and x64)	
Microsoft Windows Server 2003	
HP-UX (PA-RISC) 11iv1, 11iv2, 11iv3	
HP-UX (IA-64) 11iv2, 11iv3	
IBM AIX 5L (POWER) 5.2, 5.3	
Red Hat Enterprise Linux (x86 and x86-64) 3,4,5.5.1	
Sun Solaris (SPARC, 32-bit) 8,9,10	
Sun Solaris (x86-64) 10	
SUSE LINUX Enterprise Desktop (x86 and x86-64) 10	
SUSE LINUX Enterprise Server (x86 and x86-64) 9,10	
IBM z/OS (zSeries) 1.6, 1.7, 1.8, 1.9	

Product Configuration

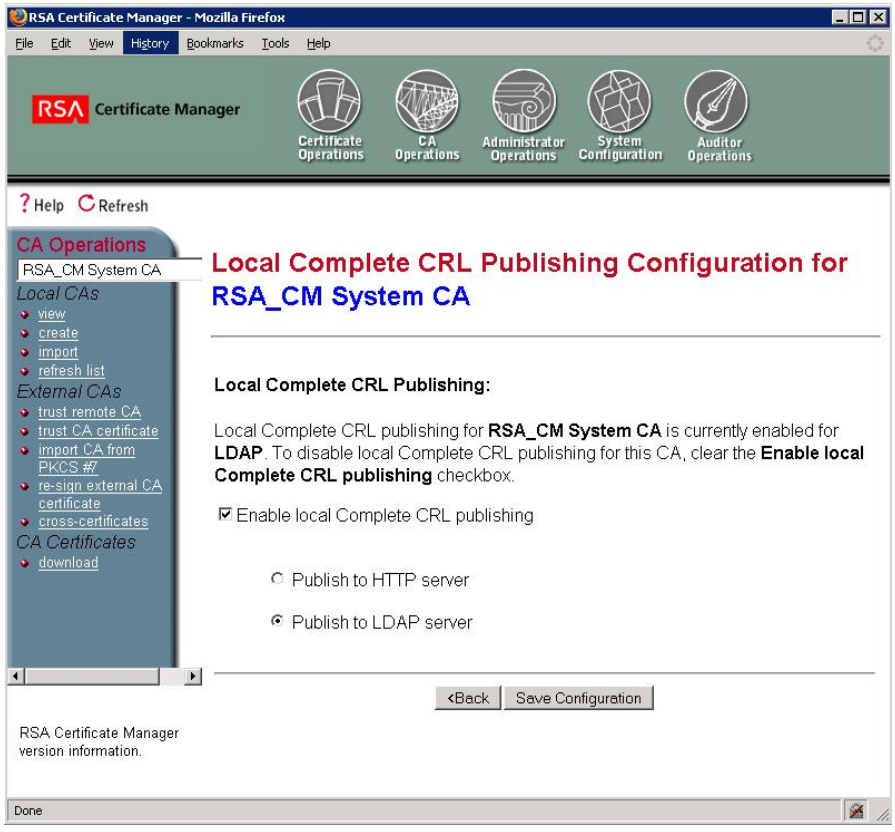
RSA Certificate Manager installable elements

RSA Certificate Manager 6.7

RSA Certificate Manager configurable elements

1. Configuration of CRL Publishing

- Browse to the RSA Certificate Manager Administration site.
- Choose CA Operations
- Select the appropriate CA and click **Local Complete CRL Publishing** in the CA Configuration section.
- Select Enable local Complete CRL publishing and Publish to LDAP server.
- Click Save Configuration and then OK to change the configuration of the chosen CA.



Partner Product Configuration

Partner product's installable elements

SSH Tectia Client/Server version 6.0 or later.

Partner product's configurable elements

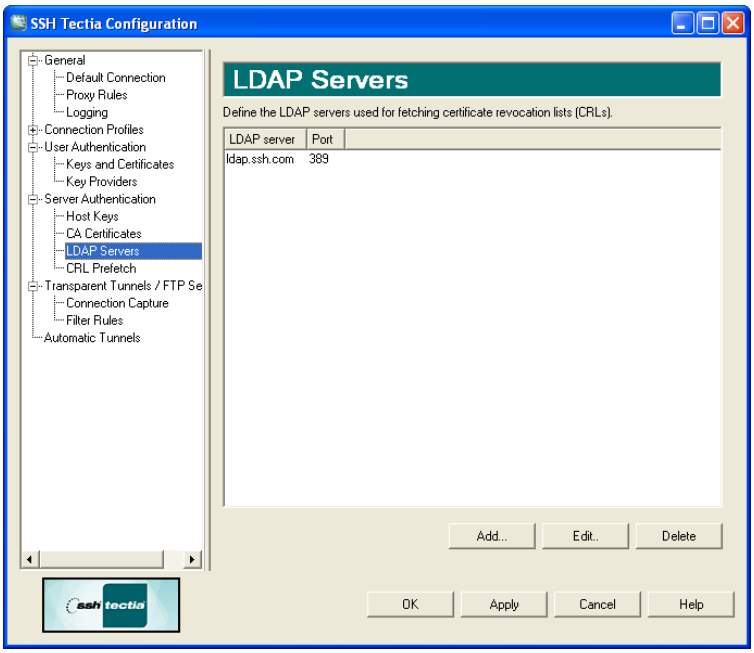
Refer to the RSA Certificate Manager Administrator documentation to ensure the necessary setup for certificate compatibility with SSH Tectia Client/Server/ConnectSecure. This includes CRL distribution points, client certificate extensions (e.g. RFC822 email extension) as the server will need to map a certificate attribute to a user account.

CRL Checking Mechanism

If SSH Tectia Server authenticates using certificates and the certificate does not contain the LDAP url as CRL DistributionPoints extension, the location of LDAP server must be defined on the client side. Corresponding if the SSH Tectia Server user wants to authenticate using certificates, the location of the LDAP server must be defined on the server side.

Ensure that you have the SSH Tectia Client software installed correctly on the system prior to moving to the configuration steps.

1. Open SSH Tectia Configuration window and select **LDAP Servers** under **Server Authentication**.
2. Click Add and enter LDAP server address.



3. On SSH Tectia for Unix simply add the following text to your configuration file:

```
<cert-validation end-point-identity-check="NO">
          <ldap-server address="ldap.ssh.com" port="389"/>
      </cert-validation>
```

Certificates can only be valid if the issuer is trusted. The issuer can be trusted directly or through path verification. Trusted CA certificates into SSH Tectia by first exporting them from a web browser and then importing them into SSH Tectia Client and/or Server.

Partner product client's installable elements

No other 3rd party components required.

Partner product client's configurable elements

Server-side Certificate Mapping:

Certificate authentication is a part of the public-key authentication method. Enable public-key authentication in the ssh-server-config.xml file and create rules that specify which certificates authorize logging into which accounts.

The following is an example of certificate authentication rules in the ssh-server-config.xml file:

```
<authentication-methods>
  <authentication action="allow" repeat-block="yes">
    <auth-publickey />
    <authentication action="allow">
      <selector>
         <certificate field="ca-list" pattern="exa-ca1,exa-ca2" />
         <certificate field="issuer-name" pattern="C=FI, O=SSH, CN=*" />
         <certificate field="subject-name" pattern="C=FI, O=SSH, CN=%username%"
/>
         <certificate field="serial-number" pattern="123456" />
         <certificate field="altname-email" pattern="%username%@ssh.com" />
         <certificate field="altname-upn" pattern="%username-without-
domain%@ssh" />
      </selector>
    </authentication>
  <authentication action="deny" />
</authentication>
</authentication-methods>
```

Partner product operational elements

The CA certificate exporting is done in the following way with Microsoft Internet Explorer:

1. Choose Tools -> Internet Options.
2. Click the Content tab.
3. Click Certificates
4. Choose the desired CA certificate(s) under Intermediate Certification Authorities or Trusted Root Certification Authorities.
5. Click the Export button and then Next.
6. Choose the export format to be either DER encoded binary X.509 (.CER) or Cryptographic Message Syntax Standard – PKCS #7 (.P7B) and click Next.
7. Specify the name of the file you want to export and then click **Next**, and **Finish**.
8. Alternatively the CA certificates can be downloaded from the RSA Certificate Manager Certificate Authority Enrollment Server.
9. Browse to the enrollment page, and choose CA options.
10. From the Save a CA Certificate or a CRL Signer Certificate to a File section select the certificate authority from the drop down menu.
11. Select the format of the certificate to be either PKCS #7 or DER-encoded certificate.
12. Click Save CA Cert…

Importing CA certificates to SSH Tectia Client is described in detail below:

SSH Tectia Client/ConnectSecure for Windows

1. Open SSH Tectia Configuration window.
2. Select CA Certificates under Server Authentication.
3. Click **Add** to import required CA certificate(s).

SSH Tectia Client/ConnectSecure for Unix

1. Copy the PKCS #7 package to the /etc/ssh2 directory on the SSH Tectia Client system.
2. Extract the certificates from the PKCS #7 package using the ssh-keygen-g3 utility:

   % ssh-keygen-g3 -7 <name-of-the-package>

   Note: DER encoded binary certificates can be used directly.

3. Edit the ssh-broker-config.xml configuration file to include the CA certificate

```
<cert-validation end-point-identity-check="yes">
  <ca-certificate name="ssh_ca1" file="ssh_ca1.crt"
                  disable-crls="no" />
</cert-validation>
```

   Note: CRL usage should only be disabled for testing purposes. Otherwise it is highly recommended to always use CRLs.

Partner product client operational elements

User Certificate Enrollment

1. Browse to the RSA Certificate Manager enrollment page and select Make a certificate request.
2. Fill out the certificate request form and click the submit option.
3. Next the browser will generate a private key. Click OK to start the generation.
4. Give your password/PIN for browser security database, and then click OK.
5. If the request has been successfully received, you will see a confirmation page.

Importing Certificate

The certificate import is done by first exporting the certificate from the browser and then importing into SSH Tectia. Note you can also configure the SSH Tectia Client/ConnectSecure to use certificates from the MSCAPI store.

The exporting is done in the following way with Microsoft Internet Explorer:

1. Choose Tools -> Internet Options.
2. Click the Content tab.
3. Click Certificates.
4. Choose the desired certificate under Personal.
5. Click Export and then Next.

6. Choose the export the private key and click Next.
7. The certificate can only be imported in PKCS #12 format. Select first and/or third check boxes also if desired and click Next.
8. Type and confirm the password and click Next.
9. Specify the file name, click Next and Finish.

Importing into SSH Tectia Client on Windows:

1. Open SSH Tectia Configuration window.
2. Select Keys and Certificates under User Authentication and click Add.
3. Select the .PFX file containing the private key and certificate you just exported.
4. Give the password needed for PFX integrity check and click **OK**.
5. Type and confirm passphrase to protect the private key and click **OK**.

Importing into SSH Tectia Client on Unix:

1. Extract the user certificate from a PKCS #12 package using the ssh-keygen-g3 into an SSH2 private/public key pair.

   Ssh-keygen-g3 –k <mycertificate.pfx>

2. Edit either your user-specific or system-wide ssh-broker-config.xml file to use the new certificate. e.g.

```
<key-stores>
          <key-store type=”software”
init=”key_files(/u/exa/cert.crt,/u/exa/cert)” />
</key-stores>
```

Certification Checklist for Certificate Authorities

Date Tested: July 16, 2008

Product	Operating System	Tested Version
RSA Certificate Manager	Microsoft Windows 2003 Server R2	6.7
SSH Tectia Client	Microsoft Windows XP SP2	6.0.1
SSH Tectia Server	Microsoft Windows Server 2003 R2	6.0.1

Interoperability Certification Checklist

Test Case			Results
Certificate Enrollment			
P10 Certificate Request			✓
P7 Response installed correctly			N/A
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			✓
Import via cut & paste			N/A
Install Root Certificate via cut/paste			N/A
Install SubCA Certificate via cut/paste			N/A
Install Root Certificate via SCEP			N/A
Install SubCA Certificate via SCEP			N/A
Verify Certificate chain is installed			N/A
Certificate Usage			
Alternative Names			
RFC822Name			✓
	Sign	Encrypt	SSL
S/MIME	N/A	N/A	N/A
Document and Files	N/A	N/A	N/A
SSL Client Authentication	N/A	N/A	N/A
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
Fails with a revoked certificate	N/A	✓	N/A
Fails with a suspended certificate	N/A	✓	N/A
Pass with a re-instated certificate	N/A	✓	N/A

RSA Remote Authentication Utility / RSA Sign-On Manager Access certificates via MS CAPI (Internet Explorer)	RAU	SOM
	N/A	N/A

DRP / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function