README
RSA Keon Validation Server 2.0

December 2003

Introduction

This document contains important information about RSA Keon Validation Server (Keon VS) 2.0. Read this document before installing the Keon VS 2.0 software.

This document contains the following information:

- Package Contents
- Hardware Requirements
- Software Requirements
- New Features and Changed Functionality
- Distribution Media Verification
- Limitations and Known Problems
- Getting Support and Service

Package Contents

You should have the following items in your RSA Keon Validation Server 2.0 package:

- One RSA Keon Validation Server 2.0 CD-ROM
- One copy of the *RSA Keon Validation Server Getting Started Guide*

Software

The RSA Keon Validation Server 2.0 CD-ROM contains:

- RSA Keon Validation Server 2.0 software for Solaris

Documentation

Product documentation comprises:

- *RSA Keon Validation Server Getting Started*
- Printable .pdf file of this README, located on the Keon VS CD-ROM
- Printable .pdf file of third party licences
- Printable .pdf files of the following documents, located on the Keon VS CD-ROM:
    - *RSA Keon Validation Server Getting Started*
    - *RSA Keon Validation Server Installation Guide*
    - *RSA Keon Validation Server Administrator's Guide*
    - *RSA Keon Validation Server Command Line Reference Manual*
- Online Help, accessible from the Keon VS administration interface

Note: In the event of a discrepancy, this README takes precedence over the RSA Keon Validation Server Installation Guide, RSA Keon Validation Server Administrator's Guide, RSA Keon Validation Server Command Line Reference Manual, and the online documentation.

Hardware Requirements

The minimum system configuration under Solaris is:

- Sun Enterprise Ultra 10S or equivalent.
- Sun Solaris 8 Operating Environment software.
- At least 256 MB of memory (RAM).
- Hard disk with at least 250 MB of free space for basic program installation. In addition, hard disk space to accommodate log file size should be considered.

Software Requirements

Keon VS supports Web-based administration with the following browsers:

- Microsoft Internet Explorer 6.0, with JavaScript enabled (UTF-8 encoding enabled by default), on Windows 2000 and Windows XP platforms
- Netscape Navigator 7.0, with JavaScript and UTF-8 encoding enabled, on Solaris platforms

Note: If you select the UTF-8 character set as the default, you will not need to select it again.

New Features

New features for Keon VS 2.0 include:

- Web-based administration through browser—administration of Keon VS 2.0 is provided through Microsoft Internet Explorer 6.0 and Netscape Navigator 7.0
- Audit logs and event logging—configuration of events to be logged and centralized logging
- Local revocation/reinstatement of certificates—ability to revoke and reinstate certificates stored locally with Keon VS
- Respect Service Locator extension—provides a system-wide overriding status source for certain requests
- Authenticated administration—three methods supported on a system-wide basis:
    - user ID and password
    - certificate authentication
    - user ID, password, and certificate authentication

- Signed media distribution—the Keon VS 2.0 CD-ROM has been digitally signed by RSA Security and the contents can be verified against modification, deletion, or addition before installation or upgrade (further explanation below in “Distribution Media Verification”)
- Starting and stopping of services through GUI—provide single action to start and stop the Keon VS OCSP Server
- Support for delta Certificate Revocation Lists (delta CRLs)—delta CRLs can be imported
- OCSP forwarding—Keon VS send its own client request to another OCSP Server and returns its own response
- More than one OCSP signer—supports multiple signers, each with multiple CA-issued certificates
- OCSP-based status sources—certificate status can be retrieved from another Keon VS installation or a third-party OCSP responder

Changed Functionality

Changed functionality in Keon VS 2.0 includes:

- vsadmin command line utility—additional commands added to support new functionality

Distribution Media Verification

For RSA Security customers with a SecurCare Online account, please visit `https://knowledge.rsasecurity.com/formslogin.asp` and log on with your username and password. After you've logged on, follow the links to **Documentation** > **Keon** > **KVS 2.0** > **Media Verification Utilities** to obtain your Keon VS 2.0 verification certificate and two MD5 checksums (those of the verification certificate and the Solaris version of the mediaverify utility). If you want a higher degree of assurance, you can contact your account manager to obtain the verification certificate and the MD5 checksums. For detailed instructions on how to verify your Keon VS 2.0 distribution media and, optionally, the verification certificate and the utility, see the *RSA Keon Validation Server Installation Guide*.

For RSA Security customers without a SecurCare Online account, please register for an account by visiting SecurCare Online at `https://knowledge.rsasecurity.com/formslogin.asp`. Click on ***To register, click here*** located under the username and password fields. Follow the instructions on the page, fill out the fields, and click the **Submit** button to register. Your username and password to access SecurCare Online will be e-mailed to you shortly. Then follow the instructions in the previous paragraph.

Limitations and Known Problems

This section describes limitations that exist in Keon VS 2.0. If workarounds exist, they are described.

Title	Description	Workaround (if available)
Installation Related Issues		
Unable to install Keon VS if white spaces are used when entering the installation path.	When installing Keon VS, if white spaces are used at the beginning of the installation path Keon VS will not install.	When installing Keon VS, do not use white spaces at the beginning of the installation path.
Keon VS fails to start if only one passphrase for a TLS key changed.	You cannot change the passphrase of one TLS key only due to the passphrase prompting regime in place for server startup.	Change the passphrases of all TLS keys en masse (to the same value). If using an nCipher HSM, change the nCipher PIN to the same value. The passphrases and PIN must meet the same criteria (at least eight characters with at least one alphabetic and one numeric character).
Keon VS fails to start if nCipher selected in installation when no nCipher connected.	If you select nCipher as the cryptographic provider during the installation when there is no nCipher HSM connected to the machine, the installation appears successful. However, no TLS certificate or key files are created and Keon VS services will fail to start up after you run the startupVS script.	Select nCipher as the cryptographic provider only if there is an nCipher HSM connected to the machine where you are installing Keon VS.
Browser Support Issues		
Certain entries in Selected list may be overwritten using Netscape 7.	When using the Netscape 7 browser, certain entries in the Selected list may be overwritten when entries from the Available list are added (for example, on the Edit Purposes for CA page). The Selected list now appears with one less entry that cannot selected.	For editing purposes for a CA, use the command line utility, `SetCAPurposes`.
Unable to download OCSP signer certificate request to a file when administering Keon VS through Microsoft Internet Explorer 6.	If your Keon VS installation resides on a Solaris machine and you administer Keon VS through Microsoft Internet Explorer 6, you cannot download the OCSP signer certificate request to a file. The error message, similar to the following, is displayed: `IE cannot download SignerCertRequestEdit.do from sparc-31.x509.com. IE was not able to open this internet site. The requested site is either unavailable or cannot be found. Please try again later.`	Copy the request from the screen (including headers) and paste it into a text file.
Keon VS GUI Related Issues		
Search pages refresh as search parameters changed.	As you change each of the search parameters (search object, criteria, and text) on a search page, the page refreshes.	Enter the search data in the following order: search text, criteria, object. Then click the Search button.

Title	Description	Workaround (if available)
Cannot import large CRL through Keon VS GUI.	You cannot successfully import certificate revocation lists larger than 1 MB into Keon VS through the GUI. An unexpected exception occurs and an error message is displayed. No information is logged to the audit log or trace log files.	To import revocation lists larger than 1MB, use the vsadmin command line utility.
Logout not disabled when user authentication by certificate only.	If you Keon VS for user authentication by certificates only and you click Logout in the menu bar, a new page is displayed with the message 'You are successfully logged out'; however, you can access the Keon VS GUI again by clicking the browser's Back button.	
Path Prefix entry not required for manual revocation list-based status source.	For a manual revocation list-based status source, the path prefix field on the 'Configure Advanced Settings' page is not required.	
Maximum value for refresh time and grace period.	On the 'Configure Advanced Settings' page for status sources, if you enter a value greater than 2147483647 seconds in the refresh time or grace period, an incorrect value is stored in the database.	The maximum refresh time or grace period is 2147483647 seconds (35791394 minutes, 596523 hours, 24855 days, or 3550 weeks).
Support for international character sets not fully supported.	The use of international characters in nicknames of CAs, signers, signer certificates, and status sources is not supported.	Avoid the use of international characters.
Replaced signer certificate no longer default.	If you replace the default signer certificate, the default designation is lost.	After replacing the default signer certificate, set the signer certificate to be the default on the 'Manage Signer Certificates' page.
vsadmin Related Issues		
Keon VS rejects re-signed System CA.	If the System CA certificate is externally resigned by a self-signed CA certificate containing a Basic Constraints extension (where the Path Constraint is set to none), there is an error message displayed trying to run vsadmin commands.	Use a CA with a positive Path Length Constraint in the Basic Constraints extension.
OCSP Signer Certificate Issues		
After deleting CA's configured signer certificate, responses for that CA are 'unknown'.	If a CA-issued signer certificate is deleted, any CAs that were explicitly configured to use that certificate will return 'unknown' status for all status requests until their signer certificate is re- configured and the configuration is saved. CA's that are using automatic selection or default for their signer are not impacted.	For each CA that was explicitly using the deleted signer certificate, re-configure to use another signer certificate or to use the automatic selection or default options.

Title	Description	Workaround (if available)
Automatic signer certificate selection fails after previously unknown CA becomes known to Keon VS.	If you import a CA-issued signer certificate and the CA is not known to Keon VS, and then import that CA's certificate (the CA is now known to Keon VS), the automatic signer certificate selection fails. Keon VS will respond to any OCSP requests against certificates issued by this recently known CA as an internal error.	For automatic selection of signer certificates to work, all of the multiple certificates must be deleted and only one of them imported again.
User Authentication Issues		
Unable to log into Keon VS GUI with certificate authentication only if users stored in LDAP directory.	If you are using an LDAP directory to store users and you configured user authentication by certificates only, users cannot log into the Keon VS GUI due to an deficiency in the application server used to manage users (Tomcat 4.1.27).	Use another user authentication method or store users in the Keon VS database instead of LDAP.
nCipher Issues		
Use of 4096-bit key size for OCSP signer causes errors.	When creating an OCSP signer with the native nCipher library to generate a 4096-bit key results in error message: `System Error : <command-name> has failed : Received fatal alert: bad_record_mac` The nfast server may stop functioning properly at this point. Keon VS cannot perform any further nCipher cryptographic operations until the nFast Server service is restarted. This is caused by an nCipher bug where generation of 4096-bit keys may sometimes fail. Attempting the operation again may succeed. Sometimes the nfast server may require a restart on older nCipher units.	Restart the nfast server and Keon VS, then try to create another signer with a 4096-bit nCipher-based key.
OCSP Server Issues		
Keon VS uses cached responses for a longer time than specified.	On the 'OCSP Configuration' page, you can configure Keon VS to reuse cached reponse for individual CAs for a specified time period. However, Keon VS is reusing the cached response for a longer time period.	Use cache response timeout values longer than 90 seconds.
Cached response information not logged by Keon VS.	The following information is not logged in the cached response log entry in the audit log file: • OCSP response status • Time of OCSP response • Certificate status values	
Keon VS continues to reuse cached responses after disabled.	If you remove a CA from the list of CAs using cached responses, Keon VS continues to reuse cached responses for that CA.	Restart Keon VS services and Keon VS stops using cached responses for that CA.

Title	Description	Workaround (if available)
Status not updated for suspended self-signed CA.	A self-signed CA that is suspended in its own revocation list no longer refreshes its status information. This means that all certificate requests for that CA will be 'revoked', regardless of the certificate's actual status. However, if the CA is reinstated, Keon VS will never retrieve the updated revocation lists and will continue returning 'revoked' status.	Refresh the self-signed CA's revocation lists through the Keon VS GUI (on the 'Manage Revocation Lists' page) or the command line utility (vsadmin).
Keon VS Operations Issues		
Reusing responses returns nonceless responses for requests with nonces.	If response reuse is on and a cached (nonceless) response exists for a certificate, when an OCSP request with a nonce is made for the same certificate, the cached (nonceless) response is returned instead of a fresh response. A response is only cached when a nonceless request is received, thus this problem only arises in an environment where some OCSP clients use nonces and others do not.	Disable response reuse in environments where at least one OCSP client uses nonces in requests.
Unable to access Keon VS GUI or vsadmin utility after 4096-bit key size used.	If you replace the server certificates for accessing the Keon VS GUI or the vsadmin command line utility with those using a 4096-bit key, you cannot access the GUI or use the utility. The following cannot use 4096-bit keys: • `VSAdmin.key` • `admin.p12` • `guiadmin.p12`	Do not use 4096-bit keys for `VSAdmin.key`, `admin.p12`, and `guiadmin.p12`.
Certificate status returned incorrect when CA purpose set to only one value.	If you set a CA's purpose to only "verify OCSP clients", then the OCSP response returned by Keon VS is an `unauthorized` OCSP error. A successful OCSP response containing an `unknown` certificate status is the expected behaviour. If you set a CA's purpose to only "provide certificate status", then the OCSP response returned by Keon VS is a successful OCSP response containing the actual certificate status. The expected behaviour is an `unauthorized` OCSP error.	

Getting Support and Service

SecurCare Online `https://knowledge.rsasecurity.com`

Customer Support Information `www.rsasecurity.com/support`

Trademarks

Trademarks

ACE/Agent, ACE/Server, Because Knowledge is Security, BSAFE, ClearTrust, Keon, RC2, RC4, RC5, RSA, the RSA logo, RSA Secured, RSA Security, SecurCare, SecurID, Smart Rules, The Most Trusted Name in e-Security, and Virtual Business Units are registered trademarks, and e-Titlement, the RSA Secured logo, SecurWorld, and Transaction Authority are trademarks of RSA Security Inc. in the U.S and/or other countries.

Netscape Navigator and Netscape Enterprise Server are registered trademarks of Netscape Communications Corp; Microsoft Internet Explorer, Microsoft Internet Information Server, Microsoft Outlook, Windows NT and Windows 2000 are registered trademarks of Microsoft Corp; Solaris and Java are registered trademarks of Sun Microsystems, Inc.; nFast, nShield, nForce, and KeySafe are registered trademarks of nCipher Corporation, Ltd. Other product and service names mentioned herein may be the trademarks of their respective companies.