

# **Red Hat Certificate System 7.3 Release Notes**

## **7.3**

**ISBN: N/A**

**Publication date:**

## Red Hat Certificate System 7.3 Release Notes

---

These release notes contain important information related to Red Hat Certificate System 7.3 that may not be currently available in the Product Manuals. You should read these Release Notes in their entirety before deploying Red Hat Certificate System 7.3.



---

## Red Hat Certificate System 7.3 Release Notes :

Copyright © 2008 Red Hat, Inc.

Copyright © 2008 Red Hat. This material may only be distributed subject to the terms and conditions set forth in the Open Publication License, V1.0 or later with the restrictions noted below (the latest version of the OPL is presently available at <http://www.opencontent.org/openpub>).

Distribution of substantively modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative of the work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

Red Hat and the Red Hat "Shadow Man" logo are registered trademarks of Red Hat, Inc. in the United States and other countries.

All other trademarks referenced herein are the property of their respective owners.

The GPG fingerprint of the security@redhat.com key is:

CA 20 86 86 2B D6 9D FC 65 F6 EC C4 21 91 80 CD DB 42 A6 0E

1801 Varsity Drive  
Raleigh, NC 27606-2072  
USA  
Phone: +1 919 754 3700  
Phone: 888 733 4281  
Fax: +1 919 754 3701  
PO Box 13588  
Research Triangle Park, NC 27709  
USA

---



---

1. Introduction .....	1
2. New Features in Red Hat Certificate System 7.3 .....	3
1. Registration Authority .....	3
1.1. Enrollment Types .....	3
1.2. RA Roles .....	3
2. SCEP .....	4
3. Auto-enrollment Proxy .....	4
3. Deployment Notes .....	7
1. Server Support .....	7
1.1. Server Requirements .....	7
1.2. Red Hat Enterprise Linux Considerations .....	7
2. Client Support .....	8
3. Other Required Software .....	8
4. Optional Server Hardware .....	9
5. Optional Client Hardware .....	9
4. Obtaining Packages .....	11
5. Important Notes .....	13
1. Installation Notes .....	13
2. Required JRE .....	13
3. Required JDK .....	14
4. TPS Subsystem Considerations .....	14
5. Directory Server Information .....	14
6. Source RPMs .....	14
6. Documentation .....	17
7. Known Issues .....	19
1. Manually Adding a New Port to the RA .....	19
2. Viewing ESC Logs on MacOS .....	20
3. Other Known Issues .....	21
8. Copyright and Third-Party Acknowledgments .....	25



# Introduction

These release notes contain important information related to Red Hat Certificate System 7.3 that may not be currently available in the Product Manuals. New features, system requirements, installation notes, known problems, resources, and other current issues are addressed here. You should read these Release Notes in their entirety before deploying Red Hat Certificate System 7.3.



# New Features in Red Hat Certificate System 7.3

## 1. Registration Authority

Red Hat Certificate System 7.3 supports a stand-alone Registration Authority (RA), which supports the automatic issue of certificates to devices and servers.

The RA subsystem is a front-end subsystem to the Certificate Authority (CA), and it performs local authentication, requestor information gathering and request validation. It is responsible for forwarding requests to the CA for signing.

The RA can be configured to authenticate incoming requests, or to route the request to appropriate personnel for approval before forwarding the request to the CA for certificate creation. The RA is typically set up outside of the firewall, while the CA is behind the firewall.

### 1.1. Enrollment Types

The RA currently provides the following enrollment types:

- SCEP enrollment
- Server certificate enrollment
- User certificate enrollment and renewal
- RA Agent enrollment

The RA also supports:

- Status checks of Certificate Requests
- Certificate retrieval
- Email notification on Certificate Request creation and approval

### 1.2. RA Roles

The RA supports the following roles:

- End Users - people who submit enrollment requests
- RA Agents - privileged RA users who are responsible for daily operation such as request approval

- Administrators - people responsible for installing and configuring the RA. Administrators can also create new users and assign them as Agents.

## 2. SCEP

SCEP (Simple Certificate Enrollment Protocol) is a protocol designed by Cisco. It specifies a way for a router to communicate with RAs and CAs for enrollment. Red Hat Certificate System 7.3 enables routers to enroll for a certificate from an RA using this protocol.

Routers can communicate with the RA using the SCEP protocol to:

- Retrieve CA certificates
- Submit a Certificate Request
- Retrieve the issued certificate
- Submit a status request if the Certificate Request is pending

SCEP specifies two modes of operation: RA mode; and CA mode.

In RA mode, the enrollment request is encrypted with the RA signing certificate. In CA mode, the request is encrypted with the CA signing certificate. The current implementation of RA and CA only supports CA mode.

## 3. Auto-enrollment Proxy

Red Hat Certificate System 7.3 supports an Auto-enrollment proxy (AEP) for Windows®, which allows users and computers in a Microsoft Windows® domain to automatically enroll for certificates issued from Red Hat Certificate System.

Designed to integrate seamlessly with an existing Windows® infrastructure, the AEP module minimizes administration overhead:

- Users and computers registered in a Windows® domain can automatically discover the location of the proxy on their network
- Computers in a domain can automatically compose a certificate request, and submit it to a Red Hat Certificate System CA via the proxy
- The Kerberos authentication mechanism built into Windows® authenticates these certificate requests
- When the CA issues a certificate, it is automatically installed into the requesting application

The AEP solution can issue certificates for domain controllers (including backup controllers),

web servers, computers, and users.

For more information about this feature, refer to  
[http://directory.fedoraproject.org/wiki/Auto\\_Enroll\\_Documentation](http://directory.fedoraproject.org/wiki/Auto_Enroll_Documentation)



# Deployment Notes

This section contains information related to installing Red Hat Certificate System 7.3, including hardware and platform requirements and prerequisites.

## 1. Server Support

The Certificate System subsystems are supported on the following platforms:

- Red Hat Enterprise Linux AS 4 for i386
- Red Hat Enterprise Linux ES 4 for i386
- Red Hat Enterprise Linux AS 4 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux ES 4 for AMD64 and Intel EM64T
- 64-bit Solaris 9 for SPARC

### 1.1. Server Requirements

Component	Details
CPU	Intel — 2.0 GHz Pentium 4 or faster
RAM	1 GB (required)
Hard disk storage space	<p>Total is approximately 5 GB</p> <ul style="list-style-type: none"><li>• Total transient space required during installation: 1 GB</li><li>• Hard disk storage space required for installation:<ul style="list-style-type: none"><li>• Space required to set up, configure, and run the server: approximately 2 GB</li><li>• Additional space for database growth in pilot deployment: approximately 1 GB</li><li>• Total disk storage space for installation: approximately 1 GB</li></ul></li></ul>

**Table 3.1. Red Hat Enterprise Linux Server Requirements**

### 1.2. Red Hat Enterprise Linux Considerations

Before installing the Certificate System packages, ensure that the proper dependencies are installed on the Red Hat Enterprise Linux system.

The following package groups and packages must be installed on all Red Hat Enterprise Linux systems:

- dialup (package group)
- gnome-desktop (package group)
- compat-arch-support (package group)
- web-server (package group)
- kernel-smp (package)
- e2fsprogs (package)
- firefox (package)

On 64-bit Red Hat Enterprise Linux platforms, ensure that the 64-bit (x86\_64) `compat-libstdc++` libraries are installed, and not only the 32-bit (i386) libraries. To confirm this, run the following command as `root`:

```
rpm -qa --queryformat '%{VERSION}-%{RELEASE} .%{ARCH}.rpm |  
grep x86_64
```

Numerous libraries should be displayed.

## 2. Client Support

The Enterprise Security Client is supported on the following platforms:

- Apple Macintosh OS X 10.4.x (Tiger) (Power PC, Intel)
- Microsoft Windows XP Professional (i386)
- Red Hat Enterprise Linux AS 4 (i386)
- Red Hat Enterprise Linux ES 4 (i386)
- Red Hat Enterprise Linux AS 4 for AMD64 and Intel EM64T
- Red Hat Enterprise Linux ES 4 for AMD64 and Intel EM64T

## 3. Other Required Software

- Red Hat Directory Server 7.1; the source code and binaries for this component are available at <https://rhn.redhat.com>), through the Red Hat Directory Server 7.1 channel.
- Web browser software that supports SSL. It is strongly recommended that users such as agents or administrators use Mozilla Firefox. End-entities should use Mozilla Firefox or Microsoft Internet Explorer.

The only browser that is fully-supported for the HTML-based instance configuration wizard is Mozilla Firefox.

## 4. Optional Server Hardware

- Chrysalis-ITS LunaSA Hardware Security Module (HSM)
  - Firmware: 4.5.2
  - Appliance Software: 3.2.4
  - Client Software: 3.2.4
- nCipher netHSM
  - Firmware: 2.12
  - Software: 9.01

## 5. Optional Client Hardware

- Axalto Global Platform compatible Cyberflex eGate token



## Obtaining Packages

Red Hat Network (<http://rhn.redhat.com>) is the software distribution mechanism for most Red Hat customers. Account login information for Red Hat Network, including entitlements for the Red Hat Certificate System 7.3 release, is required to download this software from Red Hat Network. After logging into Red Hat Network, go to the appropriate Red Hat Certificate System 7.3 channel to download the packages for the selected Red Hat Enterprise Linux platform.



### NOTE

The source code for Red Hat Directory Server 7.1 is included with the ISO image downloaded for the 32-bit Red Hat Enterprise Linux version. Red Hat Certificate System itself is not yet open source.

Red Hat Enterprise Linux systems can upgrade or download Red Hat Certificate System using `up2date`.



# Important Notes

The following sections contain important installation, configuration, and deployment information for Red Hat Certificate System 7.3.

## 1. Installation Notes

- Packages are non-relocatable. The Red Hat Certificate System base packages can not be installed to a user-designated location.
- Do not use the Autorun feature of the CD drive. If you use the Autorun feature with a CD created from the ISO image, all subsystems (CA, DRM, OCSP, TKS, and TPS) as well as the Enterprise Security Client are installed on the system by default.

The preferred alternative is to run the installation scripts provided for the server, or to follow the installation instructions in the *Red Hat Certificate System 7.3 Administration Guide*.

- Ensure that you remove any existing installations of \*sqlite\* RPM files for RA, specifically `libssqlite`. The `sqlite-<XX>` RPM files that ship with RA will cause conflicts with those files.

## 2. Required JRE

*Java™ 1.5.0 Java Runtime Environment (JRE)*. Certificate System does not support earlier versions of the JRE. This JRE is required for running Tomcat, among other applications for the Certificate System.

On 32-bit Red Hat Enterprise Linux 4 platforms, Certificate System 7.3 requires the 32-bit version of the IBM JRE 1.5.0. A pre-packaged binary distribution of this package, the `java-1.5.0-ibm` rpm package, is available through either the **Red Hat Enterprise Linux AS (v. 4 for x86) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for x86) Extras** Red Hat Network channel.

A similar package is available for 64-bit Red Hat Enterprise Linux 4 platforms. This package is available through either the **Red Hat Enterprise Linux AS (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel.

As root, run `/usr/sbin/alternatives --config java` to ensure that the IBM Java™ 1.5.0 JRE is selected.



### Warning

Both the 32-bit xSeries (Intel-compatible) and 64-bit AMD/Opteron/EM64T versions of the IBM J2SE JRE 5.0 RPM packages available through the IBM

download site are packaged in a format which is incompatible with Certificate System 7.3.

### 3. Required JDK

A JDK must be present on Red Hat Enterprise Linux systems. See [http://kbase.redhat.com/faq/FAQ\\_54\\_4667.shtml](http://kbase.redhat.com/faq/FAQ_54_4667.shtml) for more information. While almost any JDK is sufficient, installing one of these JDKs is recommended:

- For 32-bit Red Hat Enterprise Linux 4 platforms, a pre-packaged binary distribution of the 32-bit version of the IBM JDK 1.5.0, the `java-1.5.0-ibm-devel` rpm package, is available through either the **Red Hat Enterprise Linux AS (v. 4 for x86) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for x86) Extras** Red Hat Network channel.
- A similar package is available for 64-bit Red Hat Enterprise Linux 4 platforms. This package is available through either the **Red Hat Enterprise Linux AS (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel or the **Red Hat Enterprise Linux ES (v. 4 for AMD64/EM64T) Extras** Red Hat Network channel.

After installing the JDK, run `/usr/sbin/alternatives --config javac` as root to ensure that a JDK is available.

### 4. TPS Subsystem Considerations

- TPS subsystems installed on a Red Hat Enterprise Linux system require a local installation of the Apache 2.0.x web server.
- The TPS subsystem cannot be cloned.

### 5. Directory Server Information

All subsystems require access to Red Hat Directory Server 7.1 on either the local machine (if it is also a 32-bit Red Hat Enterprise Linux platform) or a remote machine (acceptable platforms are 32-bit Red Hat Enterprise Linux 4, 32-bit Solaris 9 for SPARC, or 64-bit Solaris 9 for SPARC).

### 6. Source RPMs

Red Hat Certificate System 7.3 is not an open-source product. Consequently, source RPMs are only available for third-party packages.



**NOTE**

Several of these third-party packages may issue warnings when they are installed because they may contain the UID and GID of their original packager.



## Documentation

The Red Hat Certificate System 7.3 documentation includes the following manuals:

- *Certificate System Administrator's Guide* explains all administrative functions for the Certificate System, such as adding users, creating and renewing certificates, managing smart cards, publishing CRLs, and modifying subsystem settings like port numbers.
- *Certificate System Agent's Guide* details how to perform agent operations for the CA, DRM, OCSP, and TPS subsystems through the Certificate System agent services interfaces.
- *Certificate System Enterprise Security Client Guide* explains how to install, configure, and use the Enterprise Security Client, the user client application for managing smart cards, user certificates, and user keys.



# Known Issues

## 1. Manually Adding a New Port to the RA

Bugzilla Bug: 229246

The following section documents how to manually add a new port to the RA.

The default RA server has an "optional" port for performing SSL client authentication. It is expected that the agent/administration users will select the appropriate certificate to perform SSL authentication when asked, while EE users will just "Cancel" out of the certificate selection process, if asked. The problem with this approach is that if an EE user cancels out of the certificate selection process, and chooses to renew a certificate (Bugzilla Bug# 233274), then the certificate selection process is automatically skipped, thus causing an error during certificate renewal.

This forces an EE user who wishes to renew a certificate to select the certificate to be renewed the first time they are asked to authenticate. This is awkward. To circumvent this situation, the following steps should be taken by the administrator to provide a second port purely to handle EE operations.

After performing the recommended installation procedure:

1. Change to the configuration directory: `cd /var/lib/rhpmi-ra/conf`
2. Edit the `nss.conf` file:
  - a. At the top, add another "Listen" line with a different port. For example, `Listen 0.0.0.0:12889`
  - b. Search for an existing `<VirtualHost ...> ... </VirtualHost>` container, copy the entire container and paste it at the end. Change the new container's port number to the new port: for example, `<VirtualHost _default_:12891>`
  - c. Go to the original `<VirtualHost ...>` container, and change the value of "NSSVerifyClient" from "optional" to "require."
  - d. Go to the new `<VirtualHost ...>` container, and change the value of "NSSVerifyClient" from "optional" to "none."
  - e. Save and exit.
3. Edit the `cs.cfg` file:
  - a. Search for "service.securePort" and add the following line below it:  
`service.secureEePort=12891`

- b. Save and exit.
4. Change to the document root directory: `cd /var/lib/rhpk-ra/docroot`
  - a. Edit the `index.cgi` file. Search for "securePort" and make a similar line with `secureEePort`: for example, `::symbol{secureEePort} = $cfg->get("service.secureEePort");`
  - b. Edit the `index.vm` file. Search for "SSL End Users" and change the href line to use `secureEePort`: for example: `<a href="https://$machineName:$secureEePort/ee/index.cgi">SSL End Users Services</a>`
  - c. Save both files and exit.
5. Restart the RA system.

## 2. Viewing ESC Logs on MacOS

Bugzilla Bug: 234887

The following is a workaround for the Mac ESC should one want to view the logs either within the diagnostics window or with a text editor.

1. Navigate to `/Applications/ESC.app/Contents/MacOS`
2. Create an `esc.sh` file, as follows:

```
#!/bin/sh
NSPR_LOG_FILE=~/.Library/"Application Support"/ESC/Profiles/esc.log
NSPR_LOG_MODULES=tray:2,coolKeyLib:2,coolKey:2,coolKeyNSS:2,coolKeySmart:2,coolKeyHandler:2
BASE_DIR=`dirname $0`
$BASE_DIR/xulrunner &
```

3. Navigate to `/Applications/ESC.app/Contents/MacOS`
4. Execute `./esc.sh`
5. View the logs in the ESC client or in the user's profile directory.

This method also works for the Windows ESC.

1. Navigate to the `C:\Program Files\RedHat\ESC` directory
2. Create an `esc.bat` file, as follows:

```
@echo off
SET
NSPR_LOG_MODULES=tray:2,coolKeyLib:2,coolKey:2,coolKeyNSS:2,coolKeySmart:2,coolKeyHandler:2
set NSPR_LOG_FILE=%USERPROFILE%\Application Data\RedHat\ESC\esc.log esc.exe
```

### 3. Other Known Issues

#### **Bugzilla Bug 228932: Router Prints Abort Message when Downloading Certificate Chain.**

The Cisco router may sometimes print an "abort" message when trying to download the CA certificate chain from a sub-ordinate. This is only a warning message, and can be ignored.

#### **Bugzilla Bug 236795.**

ESC : Security officer mode does not work on MAC OS X

#### **Bugzilla Bug 236857.**

In the RA agent page, the RA attempts to retrieve revocation information for a certificate that the agent does not have the rights to see. This is not an issue at present and can be ignored.

#### **Bugzilla Bug 224612: RA SQLite dependency errors on 64bit .**

It was determined that this bug was caused by a configuration issue on the machine that the 64-bit RA was being installed on. The "sqlite-devel-3.3.5-1" and "libsquite-3.2.1-1" packages must be removed prior to installation of this component.

#### **Bugzilla Bug 237042: Cannot enroll new token.**

This situation can arise if there are multiple token entries for the same user. You can resolve this situation by using the TPS agent page to delete one of the duplicate tokens.

#### **Bugzilla Bug 237050: "File does not exist" errors.**

The administrator can safely ignore these error messages.

#### **Bugzilla Bug 237251: No option to add comments to the revocation request.**

This is useful for agents if they are temporarily putting certificates on hold. This facility is currently only provided in the CA. It will be added to the RA in the next release.

### **Bugzilla Bug 237250: No way to cancel certificate revocation.**

There is currently no facility for canceling certificate revocation. This will be added in the next release.

### **Bugzilla Bug 236982: Serial number is listed as unavailable during certificate approval.**

This problem only occurs on the approval page. If the user views the request again, the correct serial number will be shown. This will be fixed in the next release.

### **Bugzilla Bug 235150: The start/stop scripts should check for subsystem presence.**

The TKS sub-system start/stop script currently does not check that the package is installed before attempting to execute.

### **Bugzilla Bug 237056: List certificates page should show the total number of certificates.**

On the Agent Interface of the RA, the List Requests page indicates the total number of certificate requests. On the List Certificates page, the corresponding information is missing. This will be fixed in the next release.

### **Bugzilla Bug 230914: AEP support in CS 7.3.**

AEP is supported in Certificate System 7.3, although it is currently not documented as such.

### **Bugzilla Bug 237305: SCEP: Fingerprint does not match for old request.**

The CA component in Certificate System 7.3 does not process SCEP requests that have been previously submitted. This can result in an error message similar to the following:

```
1706.http-9080-Processor24 - [20/Apr/2007:05:47:23 PDT] [20] [3] CEP
Enrollment: Enrollment failed: user used
duplicate transaction ID.
```

To circumvent this situation, ensure that the Cisco router generates fresh sets of keys for SCEP enrollments.

### **Bugzilla Bug 234884: Phone Home UI pops up for both enrolled and un-initialized tokens on RHEL4 and MAC OS X.**

The Phone Home UI pops up for both enrolled and un-initialized tokens on RHEL4 and MAC OS X, even though the tokens contain phoneHome URLs. If and when the problem occurs, type in the phoneHome URL and proceed.

**Bugzilla Bug 237353: RA: SSL connection aborts during List Requests and List Certificates.**

If the user clicks a link in the agent interface too fast and too many times, the server may return "Broken pipe: core\_output\_filter: writing data to the network" and terminate the SSL connection. Further access to the agent interface will require re-authentication.

**Bugzilla Bug 233024: AEP configuration not added to everyone's profile.**

The auto enrollment proxy configuration is not added to everyone's profile. This is typically found to be a problem when configuring the AEP proxy on Windows child domains where the local administrator does not have permission to modify the *cn=configuration* tree in AD. The simplest workaround is to use the `Run as ..` option to authenticate as the "Primary domain controller's administrator" and to then try to modify the *cn=configuration*. This relates to the "Populate AD" option in AEP.

**Bugzilla Bug 224994: CEP Authentication failures are not audited to the Audit Log.**

CEP currently logs any authentication failures during enrollment to the system log. These should log to the audit log.

**Bug 238039: caDirUserCert profile incorrectly processes subject altname extension.**

The Subject Alt name extension in certificates that are issued using the `caDirUserCert` profile will contain variables in un-substituted fashion (for example, `$request.requestor_email$`), if the profile request does not contain values available for substitution. There is currently no known workaround.

**Bugzilla Bug 238203: TPS: rhpki-tps instance name is hardcoded in cfg.pl.**

Because the instance name is hard-coded, the TPS looks for the configuration file in

```
/var/lib/rhpki-tps/conf/CS.cfg
```

Workaround: if you create an instance name that differs from `rhpki-tps`, you need to modify the `/var/lib/<tps-instance-name>/cgi-bin/sow/cfg.pl` to remove the above-mentioned hardcoding.



# Copyright and Third-Party Acknowledgments

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.3 servers include the following:

## Apache Software Foundation

Red Hat Certificate System TPS subsystems require a locally-installed Apache 2.0.x HTTP server. Although a local copy of this server is generally installed as part of the operating system (with its corresponding license located in `/usr/share/doc/httpd-version/LICENSE`, the latest version of this server is available at the following URL:

<http://httpd.apache.org>

Red Hat Certificate System CA, DRM, OCSP, and TKS subsystems use a locally-installed Tomcat 5.5 web server. Although an appropriate server is installed when any of these subsystems are installed, the latest version of this server is available at the following URL:

<http://tomcat.apache.org>

Red Hat Certificate System uses many components made available from Apache.

- The XML project jars are `crimson.jar` and `xalan.jar`. These are available at the following URL:

<http://xml.apache.org><sup>1</sup>

- The Tomcat project jar files are `servlet.jar` and `jakarta-naming.jar`. These are available at the following URL:

<http://jakarta.apache.org/tomcat/index.html><sup>2</sup>

## Mozilla Foundation

Red Hat Certificate System uses version 4.2 of the Java™ Security Services (JSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of and, potentially, the binary images for newer versions are available at the following URL:

<http://www.mozilla.org/projects/security/pki/jss/index.html><sup>3</sup>

Red Hat Certificate System also uses version 4.6 of the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

---

<sup>1</sup> <http://xml.apache.org>

<sup>2</sup> <http://jakarta.apache.org/tomcat/index.html>

<sup>3</sup> <http://www.mozilla.org/projects/security/pki/jss/index.html>

<sup>4</sup> <http://www.mozilla.org/projects/nspr/index.html>

Additionally, Red Hat Certificate System uses version 3.11 of the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, the binary images for newer versions are available at the following URL:

<http://www.mozilla.org/projects/security/pki/nss/index.html>

Red Hat Certificate System includes a set of compiled binaries (from NSS 3.11) of several tools from the Mozilla Project provided for the convenience of the user. This includes `certutil`, `cmsutil`, `modutil`, `pk12util`, `signtool`, `signver`, and `ssltap`. If any problems are found in these specific tools, the source code and build instructions for the latest version of this tool and, potentially, a binary image for other newer tools are available at the following URL:

<http://www.mozilla.org/projects/security/pki/nss/tools/index.html><sup>5</sup>

Red Hat Certificate System includes version 1.5 R3 of Rhino JavaScript for Java™. If any problems are found in this specific distribution, the source code and build instructions for the latest version and, potentially, a binary image are available at the following URL:

<http://www.mozilla.org/rhino/index.html><sup>6</sup>

### Red Hat

Red Hat Certificate System requires a complete Red Hat Directory Server 7.1 binary, and the open source portion of Certificate System is available at the following URL:

<https://rhn.redhat.com><sup>7</sup>

Copyrights and third-party acknowledgments for portions of Red Hat Certificate System 7.3 clients include the following:

### Mozilla Foundation

USE AND AVAILABILITY OF OPEN SOURCE CODE. Portions of the Product were created using source code governed by the Mozilla Public License (MPL). The source code for the portions of the Product governed by the MPL is available from <http://www.mozilla.org> under those licenses.

Red Hat Enterprise Security Client uses the latest version of the XULRunner cross-platform package. XULRunner is a Mozilla runtime package that can be used to bootstrap XUL+XPCOM applications that are as rich as Firefox and Thunderbird. If any problems are found in this specific distribution, the source code and build instructions for the latest

---

<sup>5</sup> <http://www.mozilla.org/projects/security/pki/nss/tools/index.html>

<sup>6</sup> <http://www.mozilla.org/rhino/index.html>

<sup>7</sup> <https://rhn.redhat.com>

---

versions and, potentially, a binary image are available at the following URL:

[http://developer.mozilla.org/en/docs/XULRunner\\_1.8.0.1\\_Release\\_Notes](http://developer.mozilla.org/en/docs/XULRunner_1.8.0.1_Release_Notes)<sup>8</sup>

Red Hat Enterprise Security Client also uses the Netscape Portable Runtime (NSPR) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

<http://www.mozilla.org/projects/nspr/index.html><sup>9</sup>

Red Hat Enterprise Security Client also uses the Network Security Services (NSS) libraries from the Mozilla Project. If any problems are found in these specific libraries, the source code and build instructions for the latest version of these libraries and, potentially, binary images for newer versions are available at the following URL:

<http://www.mozilla.org/projects/security/pki/nss/index.html>

Additional Red Hat Enterprise Security Client smart card libraries and modules:

- e-gate Smart Card Drivers for Windows 2000/XP Copyright 2002-2003 Schlumberger. All rights reserved.
- e-gate Smart Card Driver for Mac OS X Copyright 2003 by Chaskiel Grundman.

Copyright 2003 by Philip Edelbrock.

Significantly based on the Alladin etoken driver (the T=1 code is not needed): Copyright 2002 by Andreas Jellinghaus.

Copyright 2002 by Olaf Kirch.

See license terms below for rights on both parts.

Some header files are from the pcsclite distribution: Copyright 1999 David Corcoran.

- MUSCLE smart card middleware and applets

Copyright 1999-2002 David Corcoran.

Copyright 2002 Schlumberger Network Solution.

All rights reserved.

---

<sup>8</sup> [http://developer.mozilla.org/en/docs/XULRunner\\_1.8.0.1\\_Release\\_Notes](http://developer.mozilla.org/en/docs/XULRunner_1.8.0.1_Release_Notes)

<sup>9</sup> <http://www.mozilla.org/projects/nspr/index.html>

The following license terms govern the identified modules and libraries:

- e-gate Smart Card Drivers for Windows 2000/XP:

Limited Warranty/ Exclusive Remedies. Schlumberger warrants to the benefit of Customer only, for a term of sixty (60) days from the date of acquisition of the e-gate Smart Card ("Warranty Term"), that if operated as directed under normal use and service, the Software will substantially perform the functions described in its applicable documentation. Schlumberger does not warrant that the Software will meet Customer's requirements or will operate in combinations that Customer may select for use, or that the operation of the Software will be uninterrupted or error-free, or that all Software errors will be corrected. Schlumberger's sole obligation and liability under this limited warranty shall be, at Schlumberger's option, to remedy any substantial non-performance of the Software to the functional descriptions set forth in its applicable documentation. If Schlumberger is unable to satisfy the foregoing limited warranty obligations during the Warranty Term, then Schlumberger shall, upon Customer's written request for termination of this Agreement, refund to Customer all sums paid to Schlumberger for the licensing of the Software hereunder. These are Customer's sole and exclusive remedies for any breach of warranty.

WARRANTY DISCLAIMER. EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH IN SECTION 5 ABOVE, THE SOFTWARE IS PROVIDED AS IS. SCHLUMBERGER AND ITS SUPPLIERS MAKE NO OTHER EXPRESS WARRANTIES. TO THE EXTENT AUTHORIZED BY APPLICABLE LAW, ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT, ARE SPECIFICALLY DISCLAIMED. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS AGREEMENT.

Limitation of Liability. Schlumberger's cumulative liability to Customer, or any third party, for loss or damages resulting from any claim, demand or action arising out of or relating to this Agreement or use of the Software ("Damages"), shall not exceed the net amount paid to Schlumberger for the licensing of the Software, in this case, the cost of the single e-gate Smart Card. In no event shall Schlumberger or any Supplier be liable for any indirect, incidental, special consequential or exemplary damages of any character, including, without limitation, damages for lost profits, goodwill, work stoppage, computer failure and all other commercial damages.

- e-gate Smart Card Driver for Mac OS X:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- 
- The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

- MUSCLE smart card middleware and applets:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

