Red Hat Certificate System 10

Release Notes

Highlighted features and updates related to Red Hat Certificate System 10

Last Updated: 2022-02-02

Red Hat Certificate System 10 Release Notes

Highlighted features and updates related to Red Hat Certificate System 10

Legal Notice

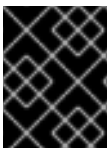
Abstract

These release notes contain important information related to Red Hat Certificate System 10, such as system requirements, installation notes, significant changes and current issues. You should read these Release Notes in their entirety before deploying Red Hat Certificate System 10.

Table of Contents

CHAPTER 1. RED HAT CERTIFICATE SYSTEM 10

This section contains general information about Red Hat Certificate System 10, such as the supported platforms and system requirements, installation notes, and deprecations.



IMPORTANT

Red Hat Certificate System 10 packages and their dependencies are provided on Red Hat Enterprise Linux 8 via the **redhat-pki** module.

1.1. PREREQUISITES

Installing Red Hat Certificate System 10 requires Red Hat Enterprise Linux 8. For details on how to install Red Hat Enterprise Linux 8, see Performing a standard RHEL installation .

1.2. HARDWARE REQUIREMENTS

This section describes the minimal and recommended hardware for Red Hat Certificate System 10. Note that, depending on your environment, more resources might be required.

1.2.1. Minimal Requirements

- CPU: 2 threads
- RAM: 2 GB
- Disk space: 20 GB

The minimal requirements are based on the Red Hat Enterprise Linux 8 minimal requirements. For details, see Red Hat Enterprise Linux technology capabilities and limits .

1.2.2. Recommended Requirements

- CPU: 4 or more threads, AES-NI support
- RAM: 4 GB or more
- Disk space: 80 GB or more

1.3. SUPPORTED PLATFORMS

This section describes the different server platforms, hardware, tokens, and software supported by Red Hat Certificate System 10.

1.3.1. Server Support

Running the Certificate Authority (CA), Key Recovery Authority (KRA), Online Certificate Status Protocol (OCSP), Token Key Service (TKS), and Token Processing System (TPS) subsystems of {RHCS }10 is supported on Red Hat Enterprise Linux 8 and later. The supported Red Hat Directory Server version is 11 and later.

NOTE

Red Hat Certificate System 10 is supported running on a Red Hat Enterprise Linux 8 virtual guest on a certified hypervisor. For details, see the Which hypervisors are certified to run RHEL? solution article.

1.3.2. Client Support

The Enterprise Security Client (ESC) is supported on:

- Red Hat Enterprise Linux 8.
- The latest versions of Red Hat Enterprise Linux 6 and 7.
  Although these platforms do not support Red Hat Certificate System 10, those clients can be used with the Token Management System (TMS) system in Red Hat Certificate System 10.

1.3.3. Supported Web Browsers

Red Hat Certificate System 10 supports the following browsers:

Table 1.1. Supported Web Browsers by Platform

Platform	Agent Services	End User Pages
Red Hat Enterprise Linux	Firefox 60 and later[a]	Firefox 60 and later
Windows 7	Firefox 60 and later	Firefox 60 and later Internet Explorer 10 [b]

[a] This Firefox version no longer supports the crypto web object used to generate and archive keys from the browser. As a result, expect limited functionality in this area.

[b] Internet Explorer 11 is currently not supported by Red Hat Certificate System 10 because the enrollment code for this web browser depends upon Visual Basic Script, which has been deprecated in Internet Explorer 11.

NOTE

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

1.3.4. Supported Smart Cards

The Enterprise Security Client (ESC) supports Global Platform 2.01-compliant smart cards and JavaCard 2.1 or higher.

The Certificate System subsystems have been tested using the following tokens:

- Gemalto TOP IM FIPS CY2 64K token (SCP01)
- Giesecke & Devrient (G&D) SmartCafe Expert 7.0 (SCP03)
- SafeNet Assured Technologies SC-650 (SCP01)

The only card manager applet supported with Certificate System is the **CoolKey** applet, which is part of the pki-tps package in Red Hat Certificate System.

1.3.5. Supported Hardware Security Modules

The following table lists Hardware Security Modules (HSM) supported by Red Hat Certificate System.

HSM	Firmware	Appliance Software	Client Software
nCipher nShield Connect 6000	2.61.2	CipherTools-linux64-dev-12.30.00	CipherTools-linux64-dev-12.30.00
Gemalto SafeNet Luna SA 1700 / 7000 (limited) (Limited support: see details below)	6.24.0	6.2.0-15	libcryptoki-6.2.x86_64

1.3.5.1. Gemalto SafeNet Luna SA 1700 / 7000 (limited)

This section provides information on supported features when using the Gemalto SafeNet Luna SA 1700 / 7000 HSM.

Gemalto SafeNet Luna SA only supports PKI private key extraction in its CKE - Key Export model, and only in non-FIPS mode. The Luna SA Cloning model and the CKE model in FIPS mode do not support PKI private key extraction. Then Luna SA CKE – Key Export Model is in FIPS mode, PKI private keys cannot be extracted.

CL - Cloning Model

- Cloning of symmetric keys and objects: Possible to other Luna SAs/G5 or Luna Backup HSM
- Cloning of asymmetric (private) keys and objects: Possible to other Luna SAs/G5 or Luna Backup HSM
- Replication of symmetric keys and objects: All symmetric keys and objects are replicated when configured in an HA group
- Replication of asymmetric keys and objects: All asymmetric keys and objects are replicated when configured in an HA group
- Wrapping private (asymmetric) keys off the HSM: Not possible

.Example of a Cloning Model image::images/lunasa-cloning.png[]

CKE - Key Export Model

- Cloning of symmetric keys and objects: Possible to other Luna SAs/G5 or Luna Backup HSM
- Cloning of asymmetric (private) keys and objects: Not possible
- Replication of symmetric keys and objects: All symmetric keys and objects are replicated when configured in an HA group

- Replication of asymmetric keys and objects: Not possible
- Wrapping private (asymmetric) keys off the HSM: Possible

.Example of a Key Export Model image::images/lunasa-CKE.png[]

1.4. QUICKSTART FOR INSTALLING RHCS SUBSYSTEMS

The following procedure describes the prerequisites and the basic installation process for {RHCS} 10.

Prerequisites

- The latest Red Hat Enterprise Linux 8 version is installed with an active network connexion. For the latest iso image, see Download Red Hat Enterprise Linux .

Procedure

1. Register the system to a Customer Portal account using Red Hat Subscription Manager (RHSM), then list the subscriptions available on this account for the system you registered:

```
$ subscription-manager register
$ subscription-manager list --available --all
```

2. Attach the required subscriptions for Red Hat Enterprise Linux Server and Red Hat Certificate System using the corresponding pool IDs obtained in the previous step:

```
$ subscription-manager attach --pool=POOL_ID_RHEL_SERVER
$ subscription-manager attach --pool=POOL_ID_CERT_SYSTEM
```

3. Make sure Red Hat Enterprise Linux has the latest updates:

```
$ dnf update
```

4. Install the Directory Server module:

```
& dnf module enable 389-ds:1.4 && dnf install 389-ds-base
```

5. Ensure that a real domain name is specified is **/etc/resolv.conf** a host name is set within **/etc/hosts**.

6. Run the Directory Server interactive installer and customize as required.

```
$ dscreate interactive
```

   For more information or for other installation methods, refer to the Red Hat Directory Server installation guide.

7. Install Certificate System packages and dependencies:

```
$ dnf module enable redhat-pki:10 && dnf install redhat-pki
```

8. Run the **pkispawn** script to create and configure the subsystem instances. You must install and fully configure at least one CA subsystem before you can configure any other type of subsystem. For details, see the **pkispawn** manpage. Without options, pkispawn runs in interactive mode, prompting the user for basic information required for installation.

```
$ pkispawn
```

9. Access the agent interface of various Red Hat Certificate System subsystems by using a properly configured local or remote Mozilla Firefox web browser.

Installing and configuring Red Hat Certificate System subsystems is described in more detail in the Planning, Installation, and Deployment Guide.

Additional resources

- Download Red Hat Enterprise Linux.
- Performing a standard RHEL installation.
- Red Hat Directory Server installation guide.
- Planning, Installation, and Deployment Guide

1.5. DEPRECATED FUNCTIONALITY

This section describes deprecated functionality in Red Hat Certificate System 10.

SCP01 support in Certificate System is deprecated

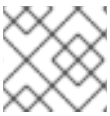
Support for Secure Channel Protocol 01 (SCP01) is deprecated in Certificate System 10 and may be removed. Red Hat recommends using smart cards that support SCP03.

The pkiconsole tool is being deprecated

In Certificate System 10, the **pkiconsole** tool will be deprecated.

CHAPTER 2. RED HAT CERTIFICATE SYSTEM 10.3

This section describes significant changes in Red Hat Certificate System 10.3, such as highlighted updates and new features, important bug fixes, and current known issues users should be aware of.



NOTE

Downgrading Red Hat Certificate System to a previous minor version is not supported.

2.1. UPDATES AND NEW FEATURES IN CS 10.3

This section documents new features and important updates in Red Hat Certificate System 10.3:

Updates and new features in the **pki-core** package:

Certificate System packages rebased to version 10.12.4

The **pki-core**, **redhat-pki**, **redhat-pki-theme**, and **pki-console** packages have been upgraded to upstream version 10.12.4, which provides a number of bug fixes and enhancements over the previous version.

2.2. BUG FIXES IN CS 10.3

This part describes bugs fixed in Red Hat Certificate System 10.3 that have a significant impact on users.

Bug fixes in the **pki-core** package:

Completing a secure channel with certain SCP03 and SCP01 tokens no longer fails due to **pcsc-lite**, **pcsc-lite-ccid**, and **esc**

As of the release of Red Hat Certificate System 10.2, an issue with **pcsc-lite**, **pcsc-lite-ccid**, and **esc** packages led to failures to complete a secure channel with certain SCP03 and SCP01 tokens. This has been fixed by a subsequent batch update.

SubCA two-step installation no longer fails while validating the SubCA signing certificate

Previously, installing a SubCA using the two-step method failed in an HSM environment with FIPS enabled: with either of the RSA or ECC options, attempting to validate the SubCA signing certificate returned an error. This fix changes the pki cli command from **nss-import-cert** to **client-import-cert** and **--cert `to `--ca-cert**. As a result, the CA signing cert is imported properly into the nssdb with trust. In addition, if pkispawn fails the **pki-server subsystem-cert-validate** call, this patch allows to provide more details on the failure while allowing **pkispawn** to complete. This would allow admins to manually add the CA signing certificate, although the aforementioned fix should now prevent the issue from happening.

2.3. KNOWN ISSUES IN CS 10.3

This part describes known problems users should be aware of in Red Hat Certificate System 10.3, and, if applicable, workarounds.

TPS requires adding anonymous bind ACI access

In previous versions, the anonymous bind ACI was allowed by default, but it is now disabled in LDAP. Consequently, this prevents enrolling or formatting TPS smart cards.

To work around this problem until a fix, you need to add the anonymous bind ACI in Directory Server manually:

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

Known issues in the pki-core package:

Cloning KRA with HSM fails due to missing attribute in auditSigningCert

When cloning a KRA with HSM, the **auditSigningCert** trust attribute **u,u,Pu** should get synced implicitly in the alias DB between the master and the clone. However, it now fails to replicate in the clone's alias DB. As a consequence, cloning a KRA with HSM fails with the error **auditSigningCert cert-topology-02-KRA KRA is invalid: Invalid certificate: (-8101) Certificate type not approved for application**.

To work around this problem, you must add the **u,u,Pu** trust attribute for **auditSigningCert** explicitly in the alias DB of the clone KRA and restart the instance. For example:

- Before the workaround:

```
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-
topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is invalid: Certificate type not approved for application.
```

- After the workaround:

```
# certutil -M -d /var/lib/pki/clone-KRA/alias/ -n 'token:auditSigningCert cert-topology-
02-KRA KRA' -t u,u,Pu
# certutil -vv -V -d /var/lib/pki/clone-KRA/alias/ -h nfast -n 'token:auditSigningCert cert-
topology-02-KRA KRA' -u J
  Enter Password or Pin for "token":
  certutil: certificate is valid
```

Tokens are not visible on the TPS Web UI

When formatting and enrolling a token via the **tpsclient** tool or adding a token via the Web UI, none of the tokens are visible on the TPS Web UI, although debug logs show the entries getting recorded successfully.

To work around this issue until a fix, you can list the tokens using the **tps-token-find** command, for example:

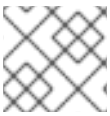
```
# pki -d /opt/pki/certdb/ -c SECret.123 -p 25443 -n 'PKI TPS Administrator for Example.Org'
tps-token-find
```

Using the cert-fix utility with the --agent-uid pkidbuser option breaks Certificate System

Using the **cert-fix** utility with the **--agent-uid pkidbuser** option corrupts the LDAP configuration of Certificate System. As a consequence, Certificate System might become unstable and manual steps are required to recover the system.

CHAPTER 3. RED HAT CERTIFICATE SYSTEM 10.2

This section describes significant changes in Red Hat Certificate System 10.2, such as highlighted updates and new features, important bug fixes, and current known issues users should be aware of.



NOTE

Downgrading Red Hat Certificate System to a previous minor version is not supported.

3.1. UPDATES AND NEW FEATURES IN CS 10.2

This section documents new features and important updates in Red Hat Certificate System 10.2:

Updates and new features in the **pki-core** package:

Certificate System packages rebased to version 10.10.5

The **pki-core**, **redhat-pki**, **redhat-pki-theme**, and **pki-console** packages have been upgraded to upstream version 10.10.5, which provides a number of bug fixes and enhancements over the previous version.

3.2. BUG FIXES IN CS 10.2

This part describes bugs fixed in Red Hat Certificate System 10.2 that have a significant impact on users.

Bug fixes in the **pki-core** package:

Certificates issued by PKI ACME Responder connected to PKI CA no longer fail OCSP validation

Previously, the default ACME certificate profile provided by PKI CA contained a sample OCSP URL that did not point to an actual OCSP service. As a consequence, if PKI ACME Responder was configured to use a PKI CA issuer, the certificates issued by the responder could fail OCSP validation. This update removes hard-coded URLs in the ACME certificate profile and adds an upgrade script to fix the profile configuration file in case you did not customize it.

pki-tools files are now in a single folder

The following files from the **pki-tools** package were in separate *java-tools* and *native-tools* folders:

- */usr/share/pki/java-tools/DRMTool.cfg*
- */usr/share/pki/java-tools/KRATool.cfg*
- */usr/share/pki/native-tools/setpin.conf*

For consistency, they are now merged into a single folder:

- */usr/share/pki/tools/DRMTool.cfg*
- */usr/share/pki/tools/KRATool.cfg*
- */usr/share/pki/tools/setpin.conf*

3.3. KNOWN ISSUES IN CS 10.2

This part describes known problems users should be aware of in Red Hat Certificate System 10.2, and, if applicable, workarounds.

Known issue with pcsc-lite, pcsc-lite-ccid, and esc

As of the release date of Red Hat Certificate System 10.2, a known issue with the versions of the **pcsc-lite**, **pcsc-lite-ccid**, and **esc** packages that are currently available may lead to failures to complete a secure channel with certain SCP03 and SCP01 tokens. The forthcoming batch update for RHEL 8.4 will provide corrected versions of these packages.

Cloning KRA with HSM is failing

Cloning KRA with HSM is failing with the error *auditSigningCert cert-topology-02-KRA KRA is invalid: Invalid certificate: (-8101) Certificate type not approved for application* in the debug log of the clone.

SubCA two-step installation fails while validating the SubCA signing certificate

Installing a SubCA using the two-step method fails in an HSM environment with FIPS enabled. With either of the RSA or ECC options, validating the SubCA signing certificate returns an error.

TPS requires adding anonymous bind ACI access

In previous versions, the anonymous bind ACI was allowed by default, but it is now disabled in LDAP. Consequently, this prevents enrolling or formatting TPS smart cards.

To work around this problem until a fix, you need to add the anonymous bind ACI in Directory Server manually:

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

Known issues in the pki-core package:

Using the cert-fix utility with the --agent-uid pkidbuser option breaks Certificate System

Using the **cert-fix** utility with the **--agent-uid pkidbuser** option corrupts the LDAP configuration of Certificate System. As a consequence, Certificate System might become unstable and manual steps are required to recover the system.

CHAPTER 4. RED HAT CERTIFICATE SYSTEM 10.1

This section describes significant changes in Red Hat Certificate System 10.1, such as highlighted updates and new features, important bug fixes, and current known issues users should be aware of.

NOTE

Downgrading Red Hat Certificate System to a previous minor version is not supported.

4.1. UPDATES AND NEW FEATURES IN CS 10.1

This section documents new features and important updates in Red Hat Certificate System 10.1:

Certificate System packages rebased to version 10.9.0

The **pki-core**, **redhat-pki**, **redhat-pki-theme**, and **pki-console** packages have been upgraded to upstream version 10.9.0, which provides a number of bug fixes and enhancements over the previous version.

ACME support in RHCS

Server certificate issuance via an Automated Certificate Management Environment (ACME) responder is available for Red Hat Certificate System (RHCS). The ACME responder supports the ACME v2 protocol (RFC 8555).

Previously, users had to use the Certificate Authority (CA)'s proprietary certificate signing request (CSR) submission routines. The routines sometimes required certificate authority (CA) agents to manually review the requests and issue the certificates.

The RHCS ACME responder now provides a standard mechanism for automatic server certificate issuance and life cycle management without involving CA agents. The feature allows the RHCS CA to integrate with existing certificate issuance infrastructure to target public CAs for deployment and internal CAs for development.

Be aware that future RHEL updates can potentially break ACME installations.

For more information, see the IETF definition of ACME .

JSS now provides a FIPS-compliant SSLContext

Previously, Tomcat used the SSLEngine directive from the Java Cryptography Architecture (JCA) SSLContext class. The default SunJSSE implementation is not compliant with the Federal Information Processing Standard (FIPS), therefore PKI now provides a FIPS-compliant implementation via JSS.

Server-Side keygen Enrollment

Many newer versions of browsers have removed the functionality to generate PKI keys and CRMF support for key archival. To resolve this deficiency, Red Hat Certificate System 10.1 introduces a Server-Side Keygen enrollment mechanism: keys are generated on the KRA server and then transferred securely back to the client in PKCS#12.

NOTE

It is highly recommended to employ the Server-Side Keygen mechanism only for encryption certificates.

Functionality Highlights:

- Certificate request keys are generated on the KRA (Note: a KRA must be installed to work with the CA)
- The profile default plugin, *serverKeygenUserKeyDefaultImpl*, provides selection to enable or disable key archival (i.e. the **enableArchival**)
- Support for both RSA and EC keys
- Support for both manual (agent) approval and automatic approval (e.g. directory password-based)

CA Certificate Transparency with Embedded Signed Certificate Time stamp

Red Hat Certificate System now offers a basic version of Certificate Transparency (CT) V1 support (rfc 6962). It has the capability of issuing certificates with embedded Signed Certificate Time stamps (SCTs) from any trusted log where each deployment site chooses to have its root CA certificate included. The system can be configured to support multiple CT logs. For this feature to work, a minimum of one trusted CT log is required.

IMPORTANT

It is the responsibility of the deployment site to establish its trust relationship with a trusted CT log server.

Updates and new features in the pki-core package:

Checking the overall health of your public key infrastructure is now available

The **pki-healthcheck** tool provides several checks that help you find and report error conditions that may impact the health of your public key infrastructure (PKI) environment.

PKI now supports the RSA PSS (Probabilistic Signature Scheme) signing algorithm

With this enhancement, PKI now supports the RSA PSS (Probabilistic Signature Scheme) signing algorithm. To enable this feature, set the following line in the **pkispawn** script file for a given subsystem: **pki_use_pss_rsa_signing_algorithm=True**

4.2. BUG FIXES IN CS 10.1

This part describes bugs fixed in Red Hat Certificate System 10.1 that have a significant impact on users.

Bug fixes in the pki-core package:

Auditors group now available for TPS installations

Previously, LDAP lacked a group entry for TPS-specific Auditors. New installations now feature a default TPS *Auditors* group. Existing instances require a manual LDAP procedure in order to use this group.

1. To correct this, run the **ldapmodify** utility to connect to the LDAP server in question and add the missing object:

```
$ ldapmodify -x -D "cn=Directory Manager" -w $PASSWORD << EOF
dn: cn=Auditors,ou=Groups,{rootSuffix}
changeType: add
```

```
objectClass: top
objectClass: groupOfUniqueNames
cn: Auditors
description: People who can read the signed audit logs for TPS
EOF
```

Replace **{rootSuffix}** with the base DN (**pki_ds_base_dn**) from the TPS configuration file. For example **dc=tks,dc=pki,dc={DOMAIN…},dc={TLD}**.

As a result, existing TPS installations can use the *Auditors* group along with new TPS installations.

4.3. KNOWN ISSUES IN CS 10.1

This part describes known problems users should be aware of in Red Hat Certificate System 10.1, and, if applicable, workarounds.

TPS requires adding anonymous bind ACI access

In previous versions, the anonymous bind ACI was allowed by default, but it is now disabled in LDAP. Consequently, this prevents enrolling or formatting TPS smart cards.

To work around this problem until a fix, you need to add the anonymous bind ACI in Directory Server manually:

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

Known issues in the pki-core package:

Certificates issued by PKI ACME Responder connected to PKI CA may fail OCSP validation

The default ACME certificate profile provided by PKI CA contains a sample OCSP URL that does notpoint to an actual OCSP service. As a consequence, if PKI ACME Responder is configured to use a PKI CA issuer, the certificates issued by the responder may fail OCSP validation

To work around this problem, you need to set the **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0** property to a blank value in the */usr/share/pki/ca/profiles/ca/acmeServerCert.cfg* configuration file:

1. In the ACME Responder configuration file, change the line **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=http://ocsp.example.com** to **policyset.serverCertSet.5.default.params.authInfoAccessADLocation_0=**
2. Restart the service and regenerate the certificate

As a result, PKI CA will generate ACME certificates with an autogenerated OCSP URL that points to an actual OCSP service.

Using the cert-fix utility with the --agent-uid pkidbuser option breaks Certificate System

Using the **cert-fix** utility with the **--agent-uid pkidbuser** option corrupts the LDAP configuration of Certificate System. As a consequence, Certificate System might become unstable and manual steps are required to recover the system.

CHAPTER 5. RED HAT CERTIFICATE SYSTEM 10.0

This section describes significant changes in Red Hat Certificate System 10.0, such as highlighted updates and new features, important bug fixes, and current known issues users should be aware of.

5.1. UPDATES AND NEW FEATURES IN CS 10.0

This section documents new features and important updates in Red Hat Certificate System 10.0:

Certificate System packages rebased to version 10.8.3

The **pki-core**, **redhat-pki**, **redhat-pki-theme**, and **pki-console** packages have been upgraded to upstream version 10.8.3, which provides a number of bug fixes and enhancements over the previous version.

ACME support in RHCS available as Technology Preview

Server certificate issuance via an Automated Certificate Management Environment (ACME) responder is available for Red Hat Certificate System (RHCS). The ACME responder supports the ACME v2 protocol (RFC 8555).

Previously, users had to use the Certificate Authority (CA)'s proprietary certificate signing request (CSR) submission routines. The routines sometimes required certificate authority (CA) agents to manually review the requests and issue the certificates.

The RHCS ACME responder now provides a standard mechanism for automatic server certificate issuance and life cycle management without involving CA agents. The feature allows the RHCS CA to integrate with existing certificate issuance infrastructure to target public CAs for deployment and internal CAs for development.

Note that this Technology Preview only includes an ACME server support. No ACME client is shipped as part of this release. Additionally, this ACME preview does not retain issuance data or handle user registration.

Be aware that future Red Hat Enterprise Linux updates can potentially break ACME installations.

For more information, see the IETF definition of ACME .

NOTE

Note that this feature is offered as a technology preview, provides early access to upcoming product functionality, and is not yet fully supported under subscription agreements.

Updates and new features in the **pki-core** package:

Checking the overall health of your public key infrastructure is now available as a Technology Preview

The **pki-healthcheck** tool provides several checks that help you find and report error conditions that may impact the health of your public key infrastructure (PKI) environment.

NOTE

Note that this feature is offered as a technology preview, provides early access to upcoming product functionality, and is not yet fully supported under subscription agreements.

The pki subsystem-cert-find and pki subsystem-cert-show commands now show the serial number of certificates

With this enhancement, the **pki subsystem-cert-find** and **pki subsystem-cert-show** commands in Certificate System show the serial number of certificates in their output. The serial number is an important piece of information and often required by multiple other commands. As a result, identifying the serial number of a certificate is now easier.

The pki user and pki group commands have been deprecated in Certificate System

With this update, the new **pki <subsystem>-user** and **pki <subsystem>-group** commands replace the **pki user** and **pki group** commands in Certificate System. The replaced commands still work, but they display a message that the command is deprecated and refer to the new commands.

Certificate System now supports offline renewal of system certificates

With this enhancement, administrators can use the offline renewal feature to renew system certificates configured in Certificate System. When a system certificate expires, Certificate System fails to start. As a result of the enhancement, administrators no longer need workarounds to replace an expired system certificate.

Certificate System can now create CSRs with SKI extension for external CA signing

With this enhancement, Certificate System supports creating a certificate signing request (CSR) with the Subject Key Identifier (SKI) extension for external certificate authority (CA) signing. Certain CAs require this extension either with a particular value or derived from the CA public key. As a result, administrators can now use the ***pki_req_ski*** parameter in the configuration file passed to the **pkispawn** utility to create a CSR with SKI extension.

5.2. BUG FIXES IN CS 10.0

This part describes bugs fixed in Red Hat Certificate System 10.0 that have a significant impact on users.

Bug fixes in the pki-core package:

The pkidestroy utility now picks the correct instance

Previously, the **pkidestroy --force** command executed on a half-removed instance picked the *pki-tomcat* instance by default, regardless of the instance name specified with the **-i *instance*** option. As a consequence, this removed the *pki-tomcat* instance instead of the intended instance, and the **--remove-logs** option did not remove the intended instance's logs. **pkidestroy** now applies the right instance name, removing only the intended instance's leftovers.

The Nuxwdog service no longer fails to start the PKI server in HSM environments

Previously, due to bugs, the **keyutils** package was not installed as a dependency of the **pki-core** package. Additionally, the **Nuxwdog** watchdog service failed to start the public key infrastructure (PKI) server in environments that use a hardware security module (HSM). These problems have been fixed. As a result, the required **keyutils** package is now installed automatically as a dependency, and **Nuxwdog** starts the PKI server as expected in environments with HSM.

Certificate System no longer logs SetAllPropertiesRule operation warnings when the service starts

Previously, Certificate System logged warnings on the **SetAllPropertiesRule** operation in the */var/log/messages* log file when the service started. The problem has been fixed, and the mentioned warnings are no longer logged.

Certificate System now supports rotating debug logs

Previously, Certificate System used a custom logging framework, which did not support log rotation. As a consequence, debug logs such as **/var/log/pki/instance_name/ca/debug** grew indefinitely. With this update, Certificate System uses the java.logging.util framework, which supports log rotation. As a result, you can configure log rotation in the **/var/lib/pki/instance_name/conf/logging.properties** file.

The Certificate System KRA client parses Key Request responses correctly

Certificate System switched to a new JSON library. As a consequence, serialization for certain objects differed, and the Python key recovery authority (KRA) client failed to parse **Key Request** responses. The client has been modified to support responses using both the old and the new JSON library. As a result, the Python KRA client parses **Key Request** responses correctly.

5.3. KNOWN ISSUES IN CS 10.0

This part describes known problems users should be aware of in Red Hat Certificate System 10.0, and, if applicable, workarounds.

TPS requires adding anonymous bind ACI access

In previous versions, the anonymous bind ACI was allowed by default, but it is now disabled in LDAP. Consequently, this prevents enrolling or formatting TPS smart cards.

To work around this problem until a fix, you need to add the anonymous bind ACI in Directory Server manually:

```
$ ldapmodify -D "cn=Directory Manager" -W -x -p 3389 -h hostname -x <<EOF
dn: dc=example,dc=org
changetype: modify
add: aci
aci: (targetattr!="userPassword || aci")(version 3.0; acl "Enable anonymous access"; allow (read,
search, compare) userdn="ldap:///anyone";)
EOF
```

Known issues in the pki-core package:

Using the cert-fix utility with the --agent-uid pkidbuser option breaks Certificate System

Using the **cert-fix** utility with the **--agent-uid pkidbuser** option corrupts the LDAP configuration of Certificate System. As a consequence, Certificate System might become unstable and manual steps are required to recover the system.