DoD Public Key Enablement (PKE) Reference Guide

CRLAutoCache for Linux User Guide

Contact: dodpke@mail.mil
URL: http://iase.disa.mil/pki/pke
URL: http://iase.disa.smil.mil/pki-pke

Enabling PKI Technology for DoD users

CRLAutoCache for Linux User Guide

3 June 2014

Version 2.2

DoD PKE Team

Revision History

Issue Date	Revision	Change Description
1/5/2012	1.0	Initial release
4/23/2012	1.1	OpennSSL Version Check
7/16/2012	2.0	Modifications to accommodate NSS Database Password requirement for CRL installation
11/28/2012	2.1	Contact Information Updates
6/3/2014	2.2	Updated "--external" and "--ECA" feature usage/ Added "--externalonly" and "--ECAonly" Added "—list" and "—listonly"

Contents

Overview

The CRLAutoCache utility provides the capability to download certificate revocation lists (CRLs) from the DoD PKI, National Security Systems (NSS) PKI and other PKIs to a Linux machine. The tool also has the ability to process downloaded CRLs for use with OpenSSL-based products such as Apache web server configured with mod_ssl and Mozilla Network Security Services (NSS).

The command utilities used in this guide are specific to Red Hat, Centos, and Fedora systems. If this guide is being implemented on different Linux distributions, equivalent commands will need to be used to accomplish each specific task in the guide.

Supplemental Information

The DoD PKE web site located at http://iase.disa.mil/pki-pke (NIPRNet) and http://iase.disa.smil.mil/pki-pke (SIPRNet) contains many informational documents and best practice guides related to PK-enablement and certificate validation implementation in the DoD. Guidance for the full configuration of Apache web server with both mod_ssl and mod_nss is available on the site.

System Requirements

Operating System

Any Linux distribution.

Required Packages

Please be sure the system has the latest versions of each of the following package:

- Curl
- BC (command-line calculator)
- OpenSSL

  NOTE: Security vulnerabilities are present in older versions of OpenSSL. Ensure the latest secure version is being used.

- NSS (only if the NSS feature will be used)

  NOTE: Installation of the CRLAutocache tool will vary depending on the version of NSS. See section Installing CRLAutoCache for Linux for details.

Storage and Memory

You will need sufficient disk space to store the CRLs you plan to download using the tool. At the time of writing, DoD's CRLs total about 55MB-compressed and 178MB-uncompressed.

User Privileges

You do not need administrative privileges in order to install and run CRLAutoCache for Linux; however, you must install it into a directory in which the user running the tool will have write permissions on that directory. Due to potential security issues, this script should be run as a non-privileged user (i.e. do not run as root). Adjust the permissions of the directories as needed.

Installing CRLAutoCache for Linux

The latest version of the CRLAutoCache tool can be downloaded from the DoD PKE web site at http://iase.disa.mil/pki-pke under *Tools* > *Certificate Validation*. There is a NIPRNet version of the tool and a SIPRNet version of the tool. The tool will be packaged in ".tar.gz" format. Save the file to a desired directory and extract the package with the following command:

```
$ tar -xvf CRLAutoCache_Linux-2.0X.tar.gz
```

The CRLAutoCache folder will be created. This folder will contain the `CRLAutoCache_Linux.sh` (NIPRNet) or `CRLAutoCache_Linux_S.sh` (SIPRNet) script.

NSS Database Password

NOTE: This only applies to those who will be leveraging the NSS feature of the tool. See the --nss description in the Optional Arguments section below for more information.

Verify the version of NSS installed on the system. If an rpm package was used for NSS, use the following command:

```
rpm -q nss
```

If the version is below 3.13.x, no additional configuration is required.

If the version is 3.13.x or above, the NSS database password must be entered when installing CRLs. This requirement cannot be overridden. Previous versions of NSS (3.12.x and below) do not have this requirement and thus when leveraging the CRLAutoCache tool to install the CRLs into the NSS database, the tool performs the installation without interruption. The only way to overcome this requirement is to specify an encrypted password file in the script. If a password file is not feasible, older versions of NSS (3.12.x or below) will have to be used. For those who will leverage the password file, perform the following steps:

1) Create a password file with the password in plain text on the first line and nothing else. Store the file in your desired file location. Create a new file to store the password; the following command may be used:

   ```
   vi /<some-directory>/pwdfile
   ```

2) Type the NSS database password on the first line and save the file by pressing `ESC` and then `:wq`.

3) Now, encrypt the password file using OpenSSL. Use the following command (the "." in front of the output file will make that file hidden in the directory):

   ```
   openssl aes-256-cbc -a -salt -in pwdfile -out .pwdfile.locked
   ```

   Set a "salt" password for the encryption. This password will be required to decrypt the file. The `pwdfile.locked` is now the encrypted pwdfile. **Delete/remove** the original plain text pwdfile from the system. The `pwdfile.locked` file and the "salt" password will be specified in the script.

4) Open the script in the *vi* text editor with the following command:

   ```
   vi CRLAutoCache_Linux.sh
   ```

5) Scroll down and find the `pFile` variable. Specify the encrypted password file similar to the format below:

   ```
   pFile="/<some-directory>/.pwdfile.locked"
   ```

6) Scroll down and find the `dPass` variable. Specify the "salt" password similar to the format below:

   ```
   dPass="someP@SSword"
   ```

7) Save the file by pressing `ESC` and then `:wq`.

CRLAutoCache for Linux Usage

NOTE: Due to potential security issues, this script should be run as a non-privileged user (i.e. do not run as root). Adjust the permissions of the directories as needed.

NOTE: The following examples pertain to the NIPRNet version of the tool. The syntax for the SIPRNet version of the tool will be identical with the exception of the _S on the end of the script name.

Running the Script

The script can be run using the `bash` command or the shell of choice. To run the script, in a terminal window first navigate to the directory containing the script and enter the following command:

```
$ bash CRLAutoCache_Linux.sh
```

To run the script as a service or different user than the currently logged-in user, use the `su` command. In the below commands, replace the `[target-username]` with the name of the user as whom you would like to run the script. If running the script as a different user, the applicable user should have read and write permissions of the directory in which the CRLAutoCache_Linux.sh resides. In addition, the applicable user should have read and execute permissions of the script itself. If running under a service account user, the applicable home directory of that service account should allow reading and writing for the service account user. For the "`apache`" user the home directory is usually `/var/www/`.

The quotes are **required** and this command should be on one line:

```
$ su [target-username] -s /bin/bash -c
"/[location_of_the_tool]/CRLAutoCache_Linux.sh"
```

Any desired tool options should be specified after the `CRLAutoCache_Linux.sh` (and within the same set of quotations, where they are used). For example, to view help the command would be:

```
$ bash CRLAutoCache_Linux.sh --help
```

Or for an alternative user:

```
$ su [target-username] -s /bin/bash -c
"/[location_of_the_tool]/CRLAutoCache_Linux.sh --help"
```

Default Behavior

By default (no options specified), the NIPRNet version of the tool will download the DoD CRLs from the Global Directory Service (GDS) and save them to the default download directory ($HOME/.CRLAutoCache/crls). The SIPRNet version of the tool

will by default attempt to download the NSS and legacy DoD SIPRNet PKI CRLs. To alter the download directory, download CRLs from different locations, or take advantage of additional functionality such as generating hashes for use by OpenSSL or importing CRLs into an NSS database, use the appropriate **Optional Arguments**.

Default Locations

The default save locations used by the tool are as follows:

DoD CRLs download directory: `$HOME/.CRLAutoCache/crls`

NOTE: $HOME is the home directory of the user running the script.

Overridden by using the `--dest` flag.

ECA CRLs download directory: `$HOME/.CRLAutoCache/eca`

NOTE: $HOME is the home directory of the user running the script.

Overridden by specifying an alternate directory following the `--ECA` flag.

DoD-approved External PKI CRL download directory:
`$HOME/.CRLAutoCache/ext_pki_crls`

NOTE: $HOME is the home directory of the user running the script.

Overridden by specifying an alternate directory following the `--external` or `--externalonly` flag.

List file PKI CRL download directory: `$HOME/.CRLAutoCache/list`

NOTE: $HOME is the home directory of the user running the script.

Overridden by specifying an alternate directory following the `--list` or `--listonly` flag.

Directory for CRLs and hash links for use with OpenSSL-based products:
`/etc/pki/tls/crls`

This is the default location when the `--openssl` flag is specified. The location is overridden by specifying an alternate directory following the `--openssl` flag.

NSS database directory: `/etc/httpd/alias`

This is the default location when the `--nss` flag is specified. The location is overridden by specifying an alternate directory following the `--nss` flag.

Optional Arguments

--debug

This option will cause the tool to provide more detailed output when it runs. This option provides an advanced level of debugging.

```
--debug
```

Example:

```
$ bash CRLAutoCache_Linux.sh --debug
```

--dest

This option will override the standard DoD CRLs download directory (`$HOME/.CRLAutoCache/crls`). It will also override the download directory location for the CRLs downloaded with the --`url` flag. Replace the `[Directory Path]` with the appropriate value.

```
--dest [Directory Path]
```

Example:

```
$ bash CRLAutoCache_Linux.sh --dest /etc/pki/tls/newFolder
```

This option can be used with the following:

```
--ECA, --openssl, --nss, --external, --url, --verbose, --debug
```

NOTE: Each time the tool is run, the standard CRLs will be initially saved in the default save directory unless this option specifies a different location. A `temp` directory is created within this directory which is used to save the temporary files.

--ECA (ONLY available in NIPRNet version)

This option will download the ECA CRLs in addition to the DoD standard CRLs.

```
--ECA
```

Example:

```
$ bash CRLAutoCache_Linux.sh --ECA
```

This option can be used with the following:

```
--openssl, --nss, --external, --url, --verbose, --debug
```

NOTE: Some ECA CRLs are only valid for 18 hours, so when using this option (or relying on ECA CRLs in general) the script will need to be run multiple times a day. This option can be used in conjunction with the default behavior,

scheduling the tool to run once without the ECA option specified to download all DoD and ECA CRLs, and at a different time during the day with the ECA option specified to download only the new ECA CRLs, to minimize bandwidth demands generated by the download.

--ECAonly (ONLY available in NIPRNet version)

This option will download only the ECA CRLs. No DoD standard CRLs are downloaded when this option is used.

```
--ECAonly
```

Example:

```
$ bash CRLAutoCache_Linux.sh --ECAonly
```

This option can be used with the following:

```
--openssl, --nss, --verbose, --debug
```

--external (ONLY available in NIPRNet version)

This option causes the tool to download all the DoD-approved external PKI CRLs. The list of DoD-approved external PKI CRLs is specified on the DoD PKE Engineering IASE website (http://iase.disa.mil/pki-pke) on the *Interoperability* page. This tool pulls the download locations from the IASE CRL html page.

The standard DoD/NSS CRLs and the DoD-approved external PKI CRLs are downloaded in different locations by default. The default save directory for the DoD-approved external PKI CRLs is `$HOME/.CRLAutoCache/ext_pki_crls`. The default can be overridden by specifying a directory **directly (**with a space**)** after the `--external`.

```
--external
Or
--external [Directory]
```

Example:

```
$ bash CRLAutoCache_Linux.sh --external /etc/httpd/crls/external_crls
```

This option can be used with the following:

```
--ECA, --openssl, --url, --nss, --verbose, --debug
```

--externalonly (ONLY available in NIPRNet version)

This option causes the tool to download only the DoD-approved external PKI CRLs. The default save directory for the DoD-approved external PKI CRLs is `$HOME/.CRLAutoCache/ext_pki_crls`. The default can be overridden by specifying a directory **directly (**with a space**)** after the `--externalonly`.

```
--externalonly
```

```
Or
--externalonly [Directory]
```

Example:

```
$ bash CRLAutoCache_Linux.sh --externalonly
/etc/httpd/crls/external_crls
```

This option can be used with the following:

```
--openssl, --nss, --verbose, --debug
```

--help

To display the help screen use the `--help` option after the tool name:

```
$ bash CRLAutoCache_Linux.sh --help
```

--nss

This option processes the CRLs for use with NSS-based software by importing CRLs into the NSS database after download. The default NSS database (DB) directory location is `/etc/pki/nssdb`. You can override the default database path by specifying a directory following the flag. The CA certificates corresponding to the CRLs to be imported must be loaded into the trusted certificates portion of the NSS DB prior to running the script. If the `--external` command is used in addition to this command, both the standard and DoD-approved external PKI CRLs will be processed for NSS-based software. You may need to restart or reload the NSS-based service after the new CRLs are downloaded for them to take effect.

NOTE: Be sure the user running the tool has permissions to read, write, and execute for the NSS database files.

```
--nss
```

Or

```
--nss [NSS DB Directory Path]
```

Example:

```
$ bash CRLAutoCache_Linux.sh --nss /etc/httpd/alias
```

NOTE: To verify CRLs have been installed into the NSS DB, use the following command:

```
$ crlutil -L -d [NSS DB Directory Path]
```

This option can be used with the following:

```
--ECA, --ECAonly, --openssl, --external, --externalonly, --url,
--verbose, --debug
```

--openssl

This option processes the CRLs for use with OpenSSL-based software by creating symbolic links (symlinks) to the CRLs named according to the CRLs' hashed values. The default location for both the downloaded CRLs and symlinks is `/etc/pki/tls/crls`. You can override the default directory by specifying a directory following the flag. If the `--external` command is used in addition to this command, both the standard and DoD-approved external PKI CRLs will be processed for OpenSSL-based software. You may need to restart or reload the OpenSSL-based service after the new CRLs are downloaded for the CRLs to take effect.

```
--openssl
```

Or

```
--openssl [Directory Path]
```

Example:

```
$ bash CRLAutoCache_Linux.sh --openssl /etc/pki/tls/alternate_directory
```

This option can be used with the following:

```
--ECA, --ECAonly, --nss, --external, --externalonly, --url,
--verbose, --debug
```

--url

This option allows use of an HTTP URL as an alternate CRL source. This will override the default NIPRNet or SIPRNet CRL source. You can specify a CRL source that uses the "getlist" format or a source that points to a single ".crl" file. The default location for the downloaded CRLs is `$HOME/.CRLAutoCache/crls/url`. You can override the default directory by specifying a directory following the `--dest` flag. A sub-directory of the directory specified will be created with the name `url`. The CRLs will be saved in the sub-directory. Replace the `[HTTP URL]` with the appropriate value.

```
--url [HTTP URL]
```

Example:

```
$ bash CRLAutoCache_Linux.sh --url https://crl.nit.disa.mil
```

This option can be used with the following:

```
--ECA, --ECAonly, --openssl, --external, --externalonly, --nss, --
verbose, --debug
```

--list

This option causes the tool to download PKI CRLs from the distribution points listed in the `pki-crldps.txt` file. Any CRL distribution point can be specified in

the file. The purpose of the file is to facilitate bulk downloads of CRLs that are not hosted on the GDS or external partner servers. The CRLs downloaded with this option would be downloaded in addition to the standard NIPRNet or SIPRNet CRLs. To skip download of the NIPRNet or SIPRNet CRLs and only download the listed CRLs then use the `--listonly` command described in the next option description. The `pki-crldps.txt` file by default is contained in the CRLAutoCache package along with the script.

The standard NIPRNet/SIPRNet CRLs and the listed PKI CRLs are downloaded in different locations by default. The default save directory for the listed CRLs is `$HOME/.CRLAutoCache/list` . The default can be overridden by specifying a directory **directly** after the `--listdest` command.

```
--list [path to pki-crldps.txt]

Or

--list [path to pki-crldps.txt] --listdest [Directory]
```

Format information for `pki-crldps.txt`:

- Each URL listed in the file must be a URL pointing to a .crl file.
- In order to comment out a URL, change the "http" or "https" to "#" signs. For example `https://crl.af.pki/root.crl` would be changed to `#####://crl.af.pki/root.crl`.

Example:

```
$ bash CRLAutoCache_Linux.sh --list /etc/httpd/crls/pki-crldps.txt
--listdest /etc/httpd/crls/list_newdir
```

This option can be used with the following:

`--ECA, --openssl, --url, --nss, --verbose, --debug, --external`

--listonly

This option will skip download of the NIPRNet or SIPRNet CRLs and only download the listed CRLs. The `pki-crldps.txt` file by default is contained in the CRLAutoCache package along with the script.

The standard NIPRNet/SIPRNet CRLs and the listed PKI CRLs are downloaded in different locations by default. The default save directory for the listed CRLs is `$HOME/.CRLAutoCache/list`. The default can be overridden by specifying a directory **directly** after the `--listdest` command.

```
--listonly [path to pki-crldps.txt]
```

```
Or

--listonly [path to pki-crldps.txt] --listdest [Directory]
```

Example:

```
$ bash CRLAutoCache_Linux.sh --list /etc/httpd/crls/pki-crldps.txt
--listdest /etc/httpd/crls/list_newdir/
```

This option can be used with the following:

```
--openssl, --nss, --verbose, --debug
```

--verbose

This option will cause the tool to provide more detailed output when it runs. This option provides an intermediate level of debugging.

```
--verbose
```

Example:

```
$ bash CRLAutoCache_Linux.sh --verbose
```

This option can be used with the following:

```
--dest, --ECA, --ECAonly, --openssl, --external, --externalonly, --nss,
--url, --debug
```

Sample Use Cases

Download the DoD CRLs to default save directory ($HOME/.CRLAutoCache/crls):

```
bash CRLAutoCache_Linux.sh
```

Download the DoD-approved external PKI CRLs and the DoD CRLs:

```
bash CRLAutoCache_Linux.sh --external
```

Download the DoD-approved external PKI CRLs only:

```
bash CRLAutoCache_Linux.sh --externalonly
```

Download the DoD-approved external PKI CRLs only and specifying an alternate save folder:

```
bash CRLAutoCache_Linux.sh --externalonly /etc/httpd/newfolder
```

Download the DoD CRLs to /var/www/html/crls AND convert them to PEM format with symlinks in /etc/pki/tls/crls for use with OpenSSL:

```
bash CRLAutoCache_Linux.sh --dest /var/www/html/crls --openssl
```

Download the DoD and ECA CRLs to default save directory ($HOME/.CRLAutoCache/crls) AND convert them to PEM format with symlinks in /var/crls:

```
bash CRLAutoCache_Linux.sh --ECA --openssl /var/crls
```

Download the CRLs to save directory ($HOME/.CRLAutoCache/crls) AND add them into a NSS database in /etc/httpd/nssdb:

```
bash CRLAutoCache_Linux.sh --nss /etc/httpd/nssdb
```

Download the CRLs from crls.localcache.local to default save directory ($HOME/.CRLAutoCache/crls):

```
bash CRLAutoCache_Linux.sh --url http://crls.localcache.local
```

Automated Execution

It is extremely important that CRLs are installed and maintained in a secure fashion. If valid CRLs are not present, some applications will "fail open," meaning that the application will skip revocation checking and allow users access without determining whether the certificate was revoked; others will "fail closed," meaning that users will be denied access because a revocation check could not be performed. To avoid both of these scenarios, CRLs should be installed and refreshed daily using an automated process. The CRLAutoCache script can be scheduled to run nightly via 'cronjob' to ensure fresh CRLs are always available locally.

This script should NOT be run more frequently than every 24 hours due to bandwidth constraints and the DoD CRL update frequency. Although DoD/NSS CRLs are valid for five (NSS)/seven (DoD) days, new CRLs are published daily and it is recommended to schedule this script to run nightly during "off" hours to obtain the freshest revocation data. If the script is being used to retrieve non-DoD CRLs, the frequency of script runs should be based on the frequency of publication and validity period of the CRLs being retrieved.

The cronjob should be set up under a non-root user or service account. Output of the cronjob should be directed to a log file. Use the following guidance:

1) Open the crontab list. Replace `[user]` with the user account under which you would like the cronjob to run:

   ```
   $ crontab -e -u [user]
   ```

2) Add the cronjob to the list using a format similar to the example below. The example will run the script with the `--openssl` option nightly at 3AM and direct the output to a log file located at `/var/log/CRLAutoCache.log`. It is important to log the output of the script for debugging purposes. The user running the cronjob must have permissions to write to the download directories and log file:

   ```
   0 3 * * * /bin/bash /path/to/CRLAutoCache/script/CRLAutoCache_Linux.sh
   --openssl >> /var/log/CRLAutoCache.log 2>&1
   ```

NOTE: If you are seeing ERRORs that curl or openssl does not exist on the system when running this script as a cronjob, curl or openssl is probably installed in a non-default path and you will need to include a path declaration in the front of your cron declarations. By default the cron path is `/usr/bin/`.

Appendix A: Support

Web Site

Please visit the URLs below for additional information.
NIPRNet: http://iase.disa.mil/pki-pke
SIPRNet: http://iase.disa.smil.mil/pki-pke

Technical Support

Contact technical support at the email address below.
dodpke@mail.mil

Acronyms

CA	Certificate Authority
CRL	Certificate Revocation List
DB	Database
ECA	External Certification Authority
GDS	Global Directory Service
HTTP	Hyper Text Transfer Protocol
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network
NSS (PKI)	National Security Systems
NSS (database)	Network Security Services
PEM	Privacy Enhanced Mail format (Base64-encoded file type)
PKE	Public Key Enablement
PKI	Public Key Infrastructure
SIPRNet	Secret Internet Protocol Router Network
URL	Uniform Resource Locator