Full credit is given to the above companies including the OS that this PDF file was generated!

Rocky Enterprise Linux 9.2 Manual Pages on command 'pkcs11.conf.5'

$ man pkcs11.conf.5

PKCS11.CONF(5)   System Files   PKCS11.CONF(5)

NAME

    pkcs11.conf - Configuration files for PKCS#11 modules

DESCRIPTION

    The pkcs11.conf configuration files are a standard way to configure

    PKCS#11 modules.

FILE FORMAT

    A complete configuration consists of several files. These files are

    text files. Since p11-kit is built to be used in all sorts of

    environments and at very low levels of the software stack, we cannot

    make use of high level configuration APIs that you may find on a modern

    desktop.

    Each setting in the config file is specified consists of a name and a

    value. The name is a simple string consisting of characters and dashes.

    The name consists of alpha numeric characters, dot, hyphen and

    underscore.

    The value is specified after the name on the same line, separated from

    it by a : (colon). White space between the name and value is ignored.

Blank lines are ignored. White space at the beginning or end of lines is stripped. Lines that begin with a # character are ignored as comments. Comments are not recognized when they come after a value on a line.

A fictitious module configuration file might look like:

    module: module.so

    # Here is a comment

    managed: true

    setting.2: A long value with text.

    x-custom : text

MODULE CONFIGURATION

Each configured PKCS#11 module has its own config file. These files can be placed in various locations.

The filename of the configuration file may consist of upper and lowercase letters underscore, comma, dash and dots. The first characters needs to be an alphanumeric, the filename should end with a .module extension.

Most importantly each config file specifies the path of the PKCS#11 module to load. A module config file has the following fields:

module:

    The filename of the PKCS#11 module to load. This should include an extension like .so

    If this value is blank, then the module will be ignored. This can be used in the user configs to override loading of a module specified in the system configuration.

    If this is a relative path, then the module will be loaded from the default module directory.

critical:

    Set to yes if the module is critical and required to load. If a critical module fails to load or initialize, then the loading process for all registered modules will abort and return an error code.

    This argument is optional and defaults to no.

enable-in:

A comma and/or space separated list of names of programs that this
module should only be loaded in. The module will not be loaded for
other programs using p11-kit. The base name of the process
executable should be used here, for example seahorse, ssh.
This option can also be used to control whether the module will be
loaded by the proxy module. To enable loading only from the proxy
module, specify p11-kit-proxy as the value.
This is not a security feature. The argument is optional. If not
present, then any process will load the module.

disable-in:

A comma and/or space separated list of names of programs that this
module should not be loaded in. The module will be loaded for any
other programs using p11-kit. The base name of the process
executable should be used here, for example firefox,
thunderbird-bin.
This option can also be used to control whether the module will be
loaded by the proxy module. To disable loading from the proxy
module, specify p11-kit-proxy as the value.
This is not a security feature. The argument is optional. If not
present, then any process will load the module.

managed:

Set to no if the module is not to be managed by p11-kit. Making a
module unmanaged is not recommended, and will cause problems if
multiple callers in a single process share a PKCS#11 module.
This argument is optional and defaults to yes.

priority:

The value should be an integer. When lists of modules are returned
to a caller of p11-kit, modules with a higher number are sorted
first. When applications search modules for certificates, keys and
trust policy information, this setting will affect what find first.
This argument is optional, and defaults to zero. Modules with the
same priority option will be sorted alphabetically.

remote:

    Instead of loading the PKCS#11 module locally, run the module

    remotely.

    Specify a command to run, prefixed with | a pipe. The command must

    speak the p11-kit remoting protocol on its standard in and standard

    out. For example:

        remote: |ssh user@remote p11-kit remote /path/to/module.so

    Other forms of remoting will appear in later p11-kit releases.

trust-policy:

    Set to yes to use use this module as a source of trust policy

    information such as certificate anchors and blocklists.

log-calls:

    Set to yes to write a log to stderr of all the calls into the

    module. This is only supported for managed modules.

    This argument is optional and defaults to no.

Do not specify both enable-in and disable-in for the same module.

Other fields may be present, but it is recommended that field names

that are not specified in this document start with a x- prefix.

GLOBAL CONFIGURATION

    A global configuration may also be present. This file contains settings

    that are not related to a single PKCS#11 module. The location(s) of the

    global configuration are described below. The global configuration file

    can contain the following fields:

    user-config:

        This will be equal to one of the following values: none, merge,

        only.

    managed:

        Set to yes or no to force all modules to be managed or unmanaged by

        p11-kit. Setting this setting in a global configuration file will

        override the managed setting in the individual module configuration

        files. Making modules unmanaged is not recommended, and will cause

        problems if multiple callers in a single process share a PKCS#11

        module.

This argument is optional.

log-calls:

Set to yes to write a log to stderr of all the calls into all

configured modules. This is only supported for managed modules.

This argument is optional.

Other fields may be present, but it is recommended that field names

that are not specified in this document start with a x- prefix.

CONFIGURATION FILES

Each configured PKCS#11 module has its own config file. These files are

placed in a directory. In addition a global config file exists. There

is a system configuration consisting of the various module config files

and a file for global configuration. Optionally each user can provide

additional configuration or override the system configuration.

The system global configuration file is usually in

/etc/pkcs11/pkcs11.conf and the user global configuration file is in

~/.config/pkcs11/pkcs11.conf in the user's home directory.

The module config files are usually located in the /etc/pkcs11/modules

directory, with one configuration file per module. In addition the

~/.config/pkcs11/modules directory can be used for modules installed by

the user.

Note that user configuration files are not loaded from the home

directory if running inside a setuid or setgid program.

The default system config file and module directory can be changed when

building p11-kit. Always lookup these paths using pkg-config.

SEE ALSO

p11-kit(8)

Further details available in the p11-kit online documentation at

https://p11-glue.github.io/p11-glue/p11-kit/manual/.

p11-kit   PKCS11.CONF(5)