NAME

certmonger.conf - configuration file for certmonger

DESCRIPTION

The *certmonger.conf* file contains default settings used by certmonger. Its format is more or less that of a typical INI-style file. The only sections currently of note are named *defaults* and *selfsign*.

DEFAULTS

Within the *defaults* section, these variables and values are recognized:

notify_ttls

This is the list of times, given in seconds, before a certificate's not-after validity date (often referred to as its expiration time) when *certmonger* should warn that the certificate will soon no longer be valid. If this value is not specified, *certmonger* will attempt to use the value of the *ttls* setting. The default list of values is "2419200, 604800, 259200, 172800, 86400".

enroll_ttls

This is the list of times, given in seconds, before a certificate's not-after validity date (often referred to as its expiration time) when *certmonger* should attempt to automatically renew the certificate, if it is configured to do so. If this value is not specified, *certmonger* will attempt to use the value of the *ttls* setting. The default list of values is "2419200, 604800, 259200, 172800, 86400".

notification_method

This is the method by which *certmonger* will notify the system administrator that a certificate will soon become invalid. The recognized values are *syslog*, *mail*, and *command*. The default is *syslog*. When sending mail, the notification message will be the mail message subject. When invoking a command, the notification message will be available in the "CERTMONGER_NOTIFICATION" environment variable.

notification_destination

This is the destination to which *certmonger* will send notifications. It can be a syslog priority and/or facility, separated by a period, it can be an email address, or it can be a command to run. The default value is *daemon.notice*.

key_type

This is the type of key pair which will be generated, used in certificate signing requests, and used when self-signing certificates. *RSA* and *DSA* are supported. *EC* (also known as *ECDSA*) is also supported. The default is *RSA*.

symmetric_cipher

This is the symmetric cipher which will be used to encrypt private keys stored in OpenSSL's PEM format. Recognized values include *aes128* and *aes256*. The default is *aes128*. It is not recommended that this value be changed except in cases where the default is incompatible with other software.

digest This is the digest algorithm which will be used when signing certificate signing requests and self-signed certificates. Recognized values include *sha1*, *sha256*, *sha384*, and *sha512*. The default is *sha256*. It is not recommended that this value be changed except in cases where the default is incompatible with other software.

nss_ca_trust
: These are the trust attributes which are applied to CA certificates which should be trusted, when they are saved to NSS databases. The default is *CT,C,C*.

nss_other_trust
: These are the trust attributes which are applied to certificates which are not necessarily to be trusted, when they are saved to NSS databases. The default is ,,.

SELFSIGN

Within the *selfsign* section, these variables and values are recognized:

validity_period
: This is the validity period given to self-signed certificates. The value is specified as a combination of years (y), months (M), weeks (w), days (d), hours (h), minutes (m), and/or seconds (s). If no unit of time is specified, seconds are assumed. The default value is *1y*.

populate_unique_id
: This controls whether or not self-signed certificates will have their subjectUniqueID and issuerUniqueID fields populated. While RFC5280 prohibits their use, they may be needed and/or used by older applications. The default value is *no*.

LOCAL

Within the *local* section, these variables and values are recognized:

validity_period
: This is the validity period given to the locally-signed CA's certificate when it is generated. The value is specified as a combination of years (y), months (M), weeks (w), days (d), hours (h), minutes (m), and/or seconds (s). If no unit of time is specified, seconds are assumed. If not set, the value of the *validity_period* setting from the *selfsign* section, if one is set there, will be used. The default value is *1y*.

BUGS

Please file tickets for any that you find at https://fedorahosted.org/certmonger/

SEE ALSO

certmonger(8) **certmonger_selinux**(8)