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

Red Hat Enterprise Linux Release 9.2 Manual Pages on 'sscg.8' command

$ man sscg.8

SSCG(8) System Administration Utilities SSCG(8)

NAME

sscg - Tool for generating x.509 certificates

SYNOPSIS

sscg [OPTION...]

DESCRIPTION

-q, --quiet

Display no output unless there is an error.

-v, --verbose

Display progress messages.

-d, --debug

Enable logging of debug messages. Implies verbose. Warning!

This will print private key information to the screen!

-V, --version

Display the version number and exit.

-f, --force

Overwrite any pre-existing files in the requested locations

--lifetime=1-3650

Certificate lifetime (days). (default: 398)

--country=US, CZ, etc.

Certificate DN: Country (C). (default: "US")

--state=Massachusetts, British Columbia, etc.

Certificate DN: State or Province (ST).

--locality=Westford, Paris, etc.

Certificate DN: Locality (L).

--organization=My Company

Certificate DN: Organization (O). (default: "Unspecified")

--organizational-unit=Engineering, etc.

Certificate DN: Organizational Unit (OU).

--email=myname@example.com

Certificate DN: Email Address (Email).

--hostname=server.example.com

The valid hostname of the certificate. Must be an FQDN. (de?

fault: current system FQDN)

--subject-alt-name alt.example.com

Optional additional valid hostnames for the certificate. In ad?

dition to hostnames, this option also accepts explicit values

supported by RFC 5280 such as IP:xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy

May be specified multiple times.

--package=STRING

Unused. Retained for compatibility with earlier versions of

sscg.

--key-strength=2048 or larger

Strength of the certificate private keys in bits. (default:

2048)

--hash-alg={sha256,sha384,sha512}

Hashing algorithm to use for signing. (default: "sha256")

--cipher-alg={des-ede3-cbc,aes-256-cbc}

Cipher to use for encrypting key files. (default:

"aes-256-cbc")

--ca-file=STRING

Path where the public CA certificate will be stored. (default:

"./ca.crt")

--ca-mode=0644

File mode of the created CA certificate.

--ca-key-file=STRING

Path where the CA's private key will be stored. If unspecified, the key will be destroyed rather than written to the disk.

--ca-key-mode=0600

File mode of the created CA key.

--ca-key-password=STRING

Provide a password for the CA key file. Note that this will be visible in the process table for all users, so it should be used for testing purposes only. Use --ca-keypassfile or --ca-key-password-prompt for secure password entry.

--ca-key-passfile=STRING

A file containing the password to encrypt the CA key file.

-C, --ca-key-password-prompt

Prompt to enter a password for the CA key file.

--crl-file=STRING

Path where an (empty) Certificate Revocation List file will be created, for applications that expect such a file to exist. If unspecified, no such file will be created.

--crl-mode=0644

File mode of the created Certificate Revocation List.

--cert-file=STRING

Path where the public service certificate will be stored. (de? fault "./service.pem")

--cert-mode=0644

File mode of the created certificate.

--cert-key-file=STRING

Path where the service's private key will be stored. (default "service-key.pem")

--cert-key-mode=0600

File mode of the created certificate key.

-p, --cert-key-password=STRING

Provide a password for the service key file. Note that this will be visible in the process table for all users, so this flag should be used for testing purposes only. Use --cert-keypassfile

or --cert-key-password-prompt for secure password entry.

--cert-key-passfile=STRING

A file containing the password to encrypt the service key file.

-P, --cert-key-password-prompt

Prompt to enter a password for the service key file.

--client-file=STRING

Path where a client authentication certificate will be stored.

--client-mode=0644

File mode of the created certificate.

--client-key-file=STRING

Path where the client's private key will be stored. (default is the client-file)

--client-key-mode=0600

File mode of the created certificate key.

--client-key-password=STRING

Provide a password for the client key file. Note that this will be visible in the process table for all users, so this flag should be used for testing purposes only. Use --client-keypass? file or --client-key-password-prompt for secure password entry.

--client-key-passfile=STRING

A file containing the password to encrypt the client key file.

--client-key-password-prompt

Prompt to enter a password for the client key file.

--dhparams-file=STRING

A file to contain a set of Diffie-Hellman parameters. (Default: "./dhparams.pem")

--dhparams-named-group=STRING

Output well-known DH parameters. The available named groups are: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, modp_2048, modp_3072, modp_4096, modp_6144, modp_8192, modp_1536, dh_1024_160, dh_2048_224, dh_2048_256. (Default: "ffdhe4096")

--dhparams-prime-len=INT

The length of the prime number to generate for dhparams, in bits. If set to non-zero, the parameters will be generated rather than using a well-known group. (default: 0)

--dhparams-generator={2,3,5}

The generator value for dhparams. (default: 2)

Help options:

-?, --help

Show this help message

--usage

Display brief usage message