

**NAME**

cmsutil – Performs basic cryptographic operations, such as encryption and decryption, on Cryptographic Message Syntax (CMS) messages.

**SYNOPSIS**

**cmsutil** [*options*] [[*arguments*]]

**STATUS**

This documentation is still work in progress. Please contribute to the initial review in **Mozilla NSS bug 836477**<sup>[1]</sup>

**DESCRIPTION**

The **cmsutil** command-line uses the S/MIME Toolkit to perform basic operations, such as encryption and decryption, on Cryptographic Message Syntax (CMS) messages.

To run cmsutil, type the command cmsutil option [arguments] where option and arguments are combinations of the options and arguments listed in the following section. Each command takes one option. Each option may take zero or more arguments. To see a usage string, issue the command without options.

**OPTIONS AND ARGUMENTS****Options**

Options specify an action. Option arguments modify an action. The options and arguments for the cmsutil command are defined as follows:

- C  
Encrypt a message.
- D  
Decode a message.
- E  
Envelope a message.
- O  
Create a certificates-only message.
- S  
Sign a message.

**Arguments**

Option arguments modify an action.

- b  
Decode a batch of files named in infile.
- c content  
Use this detached content (decode only).
- d dbdir  
Specify the key/certificate database directory (default is ".")
- e envfile  
Specify a file containing an enveloped message for a set of recipients to which you would like to send an encrypted message. If this is the first encrypted message for that set of recipients, a new enveloped message will be created that you can then use for future messages (encrypt only).
- f pwfile  
Use password file to set password on all PKCS#11 tokens.
- G  
Include a signing time attribute (sign only).
- H hash

- Use specified hash algorithm (default:SHA1).
- h num  
Generate email headers with info about CMS message (decode only).
- i infile  
Use infile as a source of data (default is stdin).
- k  
Keep decoded encryption certs in permanent cert db.
- N nickname  
Specify nickname of certificate to sign with (sign only).
- n  
Suppress output of contents (decode only).
- o outfile  
Use outfile as a destination of data (default is stdout).
- P  
Include an S/MIME capabilities attribute.
- p password  
Use password as key database password.
- r recipient1,recipient2, ...  
Specify list of recipients (email addresses) for an encrypted or enveloped message. For certificates-only message, list of certificates to send.
- T  
Suppress content in CMS message (sign only).
- u certusage  
Set type of cert usage (default is certUsageEmailSigner).
- v  
Print debugging information.
- Y ekprefnick  
Specify an encryption key preference by nickname.

## USAGE

### Encrypt Example

```
cmsutil -C [-i infile] [-o outfile] [-d dbdir] [-p password] -r "recipient1,recipient2, ..." -e envfile
```

### Decode Example

```
cmsutil -D [-i infile] [-o outfile] [-d dbdir] [-p password] [-c content] [-n] [-h num]
```

### Envelope Example

```
cmsutil -E [-i infile] [-o outfile] [-d dbdir] [-p password] -r "recipient1,recipient2, ..."
```

### Certificate-only Example

```
cmsutil -O [-i infile] [-o outfile] [-d dbdir] [-p password] -r "cert1,cert2, ..."
```

### Sign Message Example

`cmsutil -S [-i infile] [-o outfile] [-d dbdir] [-p password] -N nickname[-TGP] [-Y ekprefnick]`

## SEE ALSO

`certutil(1)`

## ADDITIONAL RESOURCES

For information about NSS and other tools related to NSS (like JSS), check out the NSS project wiki at <http://www.mozilla.org/projects/security/pki/nss/>. The NSS site relates directly to NSS code changes and releases.

Mailing lists: <https://lists.mozilla.org/listinfo/dev-tech-crypto>

IRC: Freenode at #dogtag-pki

## AUTHORS

The NSS tools were written and maintained by developers with Netscape, Red Hat, Sun, Oracle, Mozilla, and Google.

Authors: Elio Maldonado <[emaldona@redhat.com](mailto:emaldona@redhat.com)>, Deon Lackey <[dlackey@redhat.com](mailto:dlackey@redhat.com)>.

## LICENSE

Licensed under the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at <http://mozilla.org/MPL/2.0/>.

## NOTES

1. Mozilla NSS bug 836477  
[https://bugzilla.mozilla.org/show\\_bug.cgi?id=836477](https://bugzilla.mozilla.org/show_bug.cgi?id=836477)