127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

Средство
Криптографической
Защиты
Информации

КриптоПро CSP
Версия 5.0 КС1
1-Base
Приложение командной строки
для работы с сертификатами

ЖТЯИ.00101-01 93 02
Листов 8

2019 г

Содержание

Аннотация

Данный документ содержит общую информацию по использованию программного продукта «ЖТЯИ.00101-01 93 02. КриптоПро CSP. Приложение командной строки для работы с сертификатами», предназначенного для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами. Приложение позволяет устанавливать, удалять, раскодировать, экспортировать и отображать сертификаты или CRL из файлового хранилища или ключевого контейнера.

1 Системные требования

Приложение функционирует в программно-аппаратных средах, перечисленных в ЖТЯИ.00101-01 30 01. КриптоПро CSP. Формуляр, п. 3.2.

2 Описание программы

certmgr — утилита командной строки для управления сертификатами, списками отзыва сертификатов (CRL) и хранилищами.

Утилита может устанавливать, удалять, раскодировать, экспортировать и отображать сертификаты или CRL из файлового хранилища или ключевого контейнера.

3 Синтаксис

Во всех вызовах утилита certmgr должна быть единственной командой. Позиция команды и порядок опций не определены.

```
<certmgr> <-команда> [<-опции>]

<certmgr> <-install> [<-store>] | [<-file>] | [<-provname>] | [<-provtype>] | [<-container>] |
[<-ask-container>] | [<-certificate>] | [<-crl>] | [<-pfx>] | [<-pin>] | [<-at_signature>] |
[<-all>] | [<-silent>];

<certmgr> <-list> [<-store>] | [<-file>] | [<-container>] | [<-certificate>] | [<-crl>] |
[<-pkcs10>] | [<-dn>] | [<-thumbprint>] | [<-keyid>] | [<-verbose>] | [<-stdin>];

<certmgr> <-decode> [<-dest>] | [<-src>] | [<-der>] | [<-base64>];

<certmgr> <-export> [<-store>] | [<-dest>] | [<-provname>] | [<-provtype>] | [<-certificate>] |
[<-crl>] | [<-pfx>] | [<-container>] | [<-dn>] | [<-thumbprint>] | [<-keyid>] | [<-all>] |
[<-base64>] | [<-at_signature>] | [<-silent>];

<certmgr> <-delete> [<-store>] | [<-dn>] | [<-thumbprint>] | [<-keyid>] |  [<-certificate>] |
[<-provname>] | [<-provtype>] | [<-crl>] | [<-container>] | [<-all>] | [<-silent>];

<certmgr> <-enumstores> [<location>]
```

4 Команды и опции

В утилите certmgr поддерживается следующий перечень **команд**:

-help

Вывести справку об утилите.

-install

Установить сертификат или CRL в хранилище. Может создать ссылку из сертификата на закрытый ключ, если необходимо.

-list

Вывести в stdout сертификаты или CRL из хранилища, файла или контейнера.

-decode

Сменить кодировку сертификат или CRL с DER на base64 или обратно.

-export

Экспортировать сертификат или CRL из хранилища или контейнера в файл.

-delete

Удалить сертификат или CRL из хранилища.

-enumstores

Вывести в stdout перечень вложенных логических хранилищ выбранного хранилища сертификатов.

Примечание. Для утилиты `certmgr` нет разницы между длинными (--) и короткими (-) опциями. Порядок опций не определен.

В утилите `certmgr` используются следующие **опции**:

-all

Использовать все подходящие сертификаты (CRL).

-ask-container

Попросить пользователя указать контейнер из списка доступных контейнеров.

-at_signature

Использовать закрытый ключ AT_SIGNATURE вместо AT_KEYEXCHANGE.

-base64

Использовать для представления сертификата или CRL кодировку base64.

-certificate

Работать с сертификатом (*значение по умолчанию*).

-container <name>

Указать имя контейнера с сертификатом или закрытым ключом. Имя имеет формат вида `\\.\reader\name`. Если опция `-file` не была указана, закрытый ключ и сертификат будут взяты из указанного контейнера. Контейнер может быть указан в виде строки 'skip', в таком случае в сертификате не будет создана ссылка на закрытый ключ.

-crl

Работать со списком отозванных сертификатов (CRL).

-der

Использовать для представления сертификата или CRL кодировку DER (*значение по умолчанию*).

-dest <path>

Файл для декодированного сертификата или CRL.

-dn <field=value,...>

Критерии поиска для сертификата. Если более одного сертификата удовлетворяют заданным критериям, пользователю будет предложено выбрать один из найденных.

-file <path>

Путь к файлу с сертификатом или CRL (может быть DER или base64-закодированным или сериализованным хранилищем).

-help

Вывести справку о заданной команде.

-keyid <id>

Идентификатор ключа для фильтрации.

-pfx

Работать с PFX-файлом.

-pin <pincode>

Пин-код контейнера.

-pkcs10

Работать с PKCS#10-файлом.

-provname <name>

Имя провайдера.

-provtype <type>

Тип провайдера (*значение по умолчанию 75*).

-silent

Неинтерактивный режим. Возвращает ошибку в случае, если под заданные параметры подходит более одного сертификата (CRL), в таком случае требуется указать более строгие критерии поиска.

-src <path>

Файл с сертификатом или CRL для декодирования.

-stdin

Использовать для ввода данных стандартный поток ввода stdin.

-store <name>

Имя хранилища. Первая буква указывает тип хранилища — 'u' для хранилища Текущего пользователя, 'm' для хранилища Локального компьютера, остальная часть строки без первой буквы обозначает имя хранилища. Использование без 'u' или 'm' является устаревшим. Существует несколько предопределенных хранилищ:

- <My> — хранилище для пользовательских сертификатов,
- <Root> — для корневых CA сертификатов,
- <CA> — для промежуточных CA сертификатов или CRL,
- <AddressBook> — для других пользовательских сертификатов,
- <Cache> — хранилище кэша сертификатов/CRL (доступно только чтение и удаление).

<uMy> является значением по умолчанию.

-thumbprint <hash>

Цифровой отпечаток сертификата для фильтрации.

-verbose

Выводить подробную информацию о сертификате.

location

Тип хранилища сертификатов для просмотра вложенных хранилищ. Доступны следующие значения опции:

- user — показать хранилища Текущего пользователя,
- machine — показать хранилища Локального компьютера,
- all_locations — показать все хранилища.

5 Возвращаемые значения

В случае успешного выполнения команды certmgr возвращает 0. Ненулевое возвращаемое значение обозначает наличие ошибки.

Текстовые ошибки выводятся в стандартный поток ошибок stderr.

6 Примеры использования

Пример 1: Установка сертификата из файла

Установить сертификат из файла testuser.cer в хранилище текущего пользователя My с ссылкой на закрытый ключ:

```
certmgr -inst -store uMy -file /media/floppy/testuser.cer -cont '\\.\FAT12_0\31cc730c-e57e-4b56-8014-9b8f2ab79d6d'
```

Пример 2: Запись сертификата в указанной кодировке

Представить сертификат из файла testuser.cer в base64 кодировке и записать его в testuser_base64.cer:

```
certmgr -decode -src /media/floppy/testuser.cer -dest /media/floppy/testuser_base64.cer -base64
```

Пример 3: Экспорт сертификата / списка отозванных сертификатов (CRL)

Экспортировать CRL из хранилища локального компьютера CA в файл root.crl:

```
certmgr -export -crl -store mCA -dest /media/floppy/root.crl
```