Certmgr.

Аннотация.

Данный документ содержит общую информацию о программном продукте «certmgr», входящем в состав Крипто-Про CSP 3.6 (для UNIX-платформ): требования к системе, руководство по использованию приложения.

Общие сведения.

Данный программный продукт представляет собой приложение командной строки для работы с сертификатами и списками отзыва, их установки, удаления, декодирования, экспорта и просмотра сертификатов в хранилище или в ключевом контейнере.

Системные требования.

Приложение работает в операционных системах:

- Linux Standard Base ISO/IEC 23360 (платформа ia32/x64);
- Solaris 10(платформа sparc/ia32/x64);
- FreeBSD 5 (платформа ia32).

Вызов приложения.

Исполняемый файл после установки КриптоПро CSP 3.6 находится в директории /usr/CPROcsp/bin/ (/opt/CPROcsp/bin/ - Solaris). Для запуска приложения необходимо в этой директории выполнить следующую команду:

```
# ./certmgr <команда> [<опции>]
```

При каждом вызове приложения может быть выполнена только одна команда. Порядок следования команды и опций может быть произвольным.

Использование приложения.

```
-inst [-store <название хранилища>] [-file <название файла>]
[-cont <имя контейнера> [-pin <пин-код>] [-at_signature]] [-crl]
```

Установка сертификата или списка отозванных сертификатов в хранилище.

-store Имя хранилища сертификатов. По умолчанию в системе используются хранилища: My – для личных сертификатов, Root – для корневых сертификатов Удостоверяющих Центров, CA – для сертификатов промежуточных Удостоверяющих Центров и списков отозванных сертификатов, AddressBook – для сертификатов других пользователей.
Перед названием хранилища может стоять буква u или m, указывающая, что работа будет вестись с хранилищем пользователя или компьютера соответственно. Хранилище, используемое по умолчанию: uMy.

-file Путь к файлу с сертификатом или списком отозванных сертификатов.

-cont Название контейнера закрытого ключа. Название должно иметь формат \\.\<имя_считывателя>\<имя_контейнера>. Название контейнера необходимо заключить в апострофы (‘) или кавычки (“ – в этом случае все «слэши» удваиваются: “\\\\.\\<имя_считывателя>\\<имя_контейнера>”). Вместо названия контейнера можно указать флаг skip, тогда при установке сертификата привязка к закрытому ключу делаться не будет. Если опция –cont не указана – пользователю будет предложено выбрать контейнер из списка доступных.

-pin Пин-код на контейнер закрытого ключа.

-at_signature Закрытый ключ имеет тип «ключ подписи», а не «ключ обмена», как предполагается по умолчанию.

-crl Работа со списком отзыва сертификатов, а не с сертификатом, как предполагается по умолчанию.

Примечание: При указании вместе опций –file и –cont будет произведена попытка привязать сертификат из файла к ключу в контейнере. При отсутствии опции –file – сертификат будет взят из контейнера, при его отсутствии в контейнере будет возвращена ошибка.

При указании опции –crl опция –cont будет игнорироваться.

Примеры:

```
./certmgr -inst -store uMy -file /media/floppy/testuser.cer -cont
'\\.\FAT12_0\31cc730c-e57e-4b56-8014-9b8f2ab79d6d' -pin 12345
```

Установка сертификата из файла testuser.cer в личное хранилище текущего пользователя с привязкой к закрытому ключу на дискете. Контейнер защищен пин-кодом.

```
./certmgr -inst -crl -store mCA -file /media/floppy/revocationlist.crl
```

Установка списка отозванных сертификатов из файла в хранилище «CA» локального компьютера.

```
./certmgr -inst -store uAddressBook -file /media/floppy/usercert.cer
-cont skip
```

Установка сертификата из файла usercert.cer в пользовательское хранилище «AddressBook» без привязывания к контейнеру закрытого ключа.

```
-list [-store <название хранилища> | -file <название файла> |
-cont <имя контейнера>] [-dn <критерий поиска сертификатов>]
[-crl]
```

Вывод перечня сертификатов или списков отозванных сертификатов, содержащихся в хранилище, файле или контейнере закрытого ключа и удовлетворяющих заданному критерию.

-store Имя хранилища сертификатов. По умолчанию в системе используются хранилища: My – для личных сертификатов, Root – для корневых сертификатов Удостоверяющих Центров, CA – для сертификатов промежуточных Удостоверяющих Центров и списков отозванных сертификатов, AddressBook – для сертификатов других пользователей.
Перед названием хранилища может стоять буква u или m, указывающая, что работа будет вестись с хранилищем пользователя или компьютера соответственно. Хранилище, используемое по умолчанию: uMy.

-file Путь к файлу с сертификатом или списком отозванных сертификатов.

-cont Название контейнера закрытого ключа, сертификаты из которого необходимо перечислить. Название должно иметь формат \\.\<имя_считывателя>\<имя_контейнера>. Название контейнера необходимо заключить в апострофы (‘) или кавычки (“ – в этом случае все «слэши» удваиваются: “\\\\.\\<имя_считывателя>\\<имя_контейнера>”).

-dn Критерий поиска сертификатов. Возможен поиск по любому компоненту имени, либо по нескольким компонентам одновременно. Формат задания критерия для поиска: field1=value1,field2=value2,….

-crl Работа со списком отзыва сертификатов, а не с сертификатом, как предполагается по умолчанию.

Пример:

```
./certmgr -list -store uRoot -dn CN=MyCA
```

Поиск в хранилище «Root» текущего пользователя сертификатов, общее имя которых содержит строчку MyCA.

```
-decode [-src_file <название файла>] [-dest <название файла>]
[-der | -base64]
```

Декодирование сертификата или списка отозванных сертификатов из der-кодировки в base64 или наоборот.

-src Файл, содержащий сертификат или список отозванных сертификатов для декодирования.

-dest Файл, в который будет помещен декодированный сертификат или список отозванных сертификатов.

-der Декодировать сертификат или список отозванных сертификатов в der.

-base64 Декодировать сертификат или список отозванных сертификатов в base64.

Пример:

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

Декодирование сертификата testuser.cer из der-кодировки в base64. Результат будет помещен в файл testuser_base64.cer.

```
-export [-cont <имя контейнера> | -store <название хранилища>]
[-dest <название файла>] [-dn <критерий поиска сертификатов>]
[-base64] [-crl]
```

Экспортирует сертификат или список отозванных сертификатов, удовлетворяющий заданному критерию, из хранилища или контейнера закрытого ключа в файл.

-cont Название контейнера закрытого ключа. Название должно иметь формат \\.\<имя_считывателя>\<имя_контейнера>. Название контейнера необходимо заключить в апострофы (‘) или кавычки (“ – в этом случае все «слэши» удваиваются: “\\\\.\\<имя_считывателя>\\<имя_контейнера>”).

-store Имя хранилища сертификатов. По умолчанию в системе используются хранилища: My – для личных сертификатов, Root – для корневых сертификатов Удостоверяющих Центров, CA – для сертификатов промежуточных Удостоверяющих Центров и списков отозванных сертификатов, AddressBook – для сертификатов других пользователей.

Перед названием хранилища может стоять буква u или m, указывающая, что работа будет вестись с хранилищем пользователя или компьютера соответственно. Хранилище, используемое по умолчанию: uMy.

-dest Файл, в который будет помещен сертификат или список отозванных сертификатов.

-dn Критерий поиска сертификатов. Возможен поиск по любому компоненту имени, либо по нескольким компонентам одновременно. Формат задания критерия для поиска: field1=value1,field2=value2,….

Если указанному критерию будет удовлетворять несколько сертификатов – пользователю будет предложено выбрать один из них.

-base64 Экспортировать сертификат или список отозванных сертификатов в base64, а не в der, как предполагается по умолчанию.

-crl Работа со списком отзыва сертификатов, а не с сертификатом, как предполагается по умолчанию.

Пример:

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

Экспорт списка отозванных сертификатов из хранилища «Промежуточные Центры Сертификации» локального компьютера в файл root.crl.

`-delete [[-store <название хранилища>] [-dn <критерий поиска сертификатов>] [-crl]] | [-cont <имя контейнера>]`

Удаляет сертификат или список отозванных сертификатов, удовлетворяющий заданному критерию, из хранилища или контейнер закрытого ключа с носителя.

-store Имя хранилища сертификатов. По умолчанию в системе используются хранилища: My – для личных сертификатов, Root – для корневых сертификатов Удостоверяющих Центров, CA – для сертификатов промежуточных Удостоверяющих Центров и списков отозванных сертификатов, AddressBook – для сертификатов других пользователей.

Перед названием хранилища может стоять буква u или m, указывающая, что работа будет вестись с хранилищем пользователя или компьютера соответственно. Хранилище, используемое по умолчанию: uMy.

-dn Критерий поиска сертификатов. Возможен поиск по любому компоненту имени, либо по нескольким компонентам одновременно. Формат задания критерия для поиска: field1=value1,field2=value2,….

Если указанному критерию будет удовлетворять несколько сертификатов – пользователю будет предложено выбрать один из них.

-crl Работа со списком отзыва сертификатов, а не с сертификатом, как предполагается по умолчанию.

-cont Название контейнера закрытого ключа. Название должно иметь формат \\.\<имя_считывателя>\<имя_контейнера>. Название контейнера необходимо заключить в апострофы (‘) или кавычки (“ – в этом случае все «слэши» удваиваются: “\\\\.\\<имя_считывателя>\\<имя_контейнера>”).

Пример:

`./certmgr –delete –store mMy –dn CN=localcomputer`

Удаление из личного хранилища локального компьютера сертификата, общее имя в котором содержит строчку localcomputer.

`./certmgr –delete –cont “\\\\.\\HDIMAGE\\testcontainer”`

Удаление контейнера.

`-help`

Выводит на экран информацию обо всех командах, либо, при указании конкретной команды – о доступных опциях.

Дополнительная информация.

Дополнительную информацию о работе с приложением можно получить из встроенного man-файла вызовом команды

```
# man certmgr
```

Типичные ошибки.

Все ошибки возвращаются в stderr. Если работа завершена успешно – возвращается нулевой код, иначе – код ошибки.
Также некоторую информацию о работе утилиты можно узнать из файла /var/log/messages.