127 018, Москва, Сущевский вал, д.18
Телефон: (495) 995 4820
Факс: (495) 995 4820
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

КРИПТОПРО

Средство Криптографической Защиты Информации

# КриптоПро CSP

Версия 4.0 R4 KC1

## Приложение командной строки для работы с сертификатами

ЖТЯИ.00087-03 93 02

Листов 8

2018 г.

# Содержание

# Аннотация

Данный документ содержит общую информацию по использованию программного продукта «ЖТЯИ.00087-03 93 01. КриптоПро CSP. Приложение командной строки», предназначенного для работы с сертификатами с использованием инфраструктуры открытых ключей, шифрования/расшифрования сообщений, содержащихся в файлах, создания/проверки электронных подписей и хэширования сообщений, содержащихся в файле или группе файлов.

# 1. Системные требования

Windows

Включает программно-аппаратные среды:

Windows XP[1] (x86);
Windows 7/8/8.1/10/Server 2003/2008 (x86, x64);
Windows Server 2008 R2/2012/2012 R2/2016 (x64).

LSB Linux

Включает дистрибутивы Linux, удовлетворяющие стандарту Linux Standard Base ISO/IEC 23360 версии LSB 4.x:

CentOS 4/5/6 (x86, x64);
CentOS 7 (x86, x64, POWER, ARM, ARM64);
ОСь (OS-RT) (x64);
ТД ОС АИС ФССП России (GosLinux) (x86, x64);
Red OS (x86, x64);
Fedora 27/28/29 (x86, x64, ARM);
Oracle Linux 4/5/6 (x86, x64);
Oracle Linux 7 (x64);
OpenSUSE Leap 42, 15 (x86, x64, ARM, ARM64);
AlterOS (x64);
SUSE Linux Enterprise Server 11SP4 (x86, x64);
SUSE Linux Enterprise Server 12/15, Desktop 12/15 (x64, POWER, ARM64);
Red Hat Enterprise Linux 4/5/6 (x86, x64);
Red Hat Enterprise Linux 7 (x64, POWER, ARM64);
Синтез-ОС.РС (x86, x64);
ПК «СинтезМ-Клиент» в составе КП «ЗОС «СинтезМ» (x64);
ПК «СинтезМ-Сервер» в составе КП «ЗОС «СинтезМ» (x64);
КП «ОС «СинтезМ-К» (x64);
Ubuntu 14.04/16.04 (x86, x64, POWER, ARM, ARM64);
Ubuntu 18.04/18.10 (x86, x64);
Linux Mint 17/18/19 (x86, x64);
Debian 7/8/9 (x86, x64, POWER, ARM, ARM64, MIPS);
ОС Лотос (x86, x64);
Astra Linux Special Edition, Common Edition (x64, MIPS, Эльбрус);
МСВСфера 6.3 Сервер (x64, ARM64).

Unix

Включает программно-аппаратные среды:

ОС Эльбрус версия 3 (Эльбрус);
ALT Linux 6/7 (x86, x64, ARM);
Альт Сервер 8, Альт 8 СП Сервер (x86, x64, ARM, ARM64);
Альт Рабочая станция 8, Альт Рабочая станция К 8, Альт 8 СП Рабочая станция (x86, x64, ARM, ARM64);
ROSA Fresh, Enterprise Desktop, Enterprise Linux Server (x86, x64);
РОСА ХРОМ/КОБАЛЬТ/НИКЕЛЬ (x86, x64);

FreeBSD 11, pfSense 2.x (x86, x64);
AIX 6/7 (POWER);
Mac OS X 10.9/10.10/10.11/10.12/10.13/10.14 (x64).

Solaris

Включает программно-аппаратные среды:

Solaris 10 (sparc, x86, x64);
Solaris 11 (sparc, x64).

Sailfish

Включает программно-аппаратную среду:

SailfishOS 2.1.1.12 (ARMv7).

iOS

Включает программно-аппаратные среды:

Apple iOS 8.0/8.0.1/8.0.2/8.1/8.1.1/8.1.2/8.1.3/8.2/8.3/8.4/8.4.1/9/9.0.1/9.0.2/9.1/9.2/9.2.1/9.3/9.3.1/9.3.2/9.3.3/9.3.4/9.3.5/10/11/12 (ARMv7, ARM64).

Виртуальные среды

Microsoft Hyper-V Server 2008/2008R2/2012/2012R2/2016 (x64);
Microsoft Hyper-V 8/8.1/10 (x64);
Citrix XenServer 7 (x64);
VMWare WorkStation 11/12/14/15 (x86, x64);
VMWare WorkStation Player 12/14/15 (x86, x64);
VMWare vSphere ESXi/Hypervisor 5.5/6.0/6.5/6.7 (x64);
Oracle VirtualBox 5.2 (x86, x64);
RHEV 4 (x64).

Примечания:

1. Версия POSReady.

## 2. Использование 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.

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

<certmgr> <-команда> [<-options> ]

<certmgr> <-inst> [<-store>] | [<-file>] | [<-cont>] |
[<-pin>] | [<-crl>] | [<-at_signature>] | [<-provname>] | [<-provtype>]

<certmgr> <-list> [<-store>] | [<-file>] | [<-cont>] | [<-dn>] | [<-crl>]
| [<-thumbprint>] | [<-verbose>]

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

<certmgr> <-export> [<-cont>] | [<-store>] | [<-dest>] | [<-dn>] | [<-base64>] | [<-crl>]
| [<-provname>] | [<-provtype>] | [<-thumbprint>] | [<-at_signature>] | [<-silent>]

<certmgr> <-delete> [<-store>] | [<-dn>] | [<-crl>] | [<-cont>] | [<-thumbprint>]
| [<-provname>] | [<-provtype>] | [<-all>] | [<-silent>]

-inst

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

Перекодировать сертификат или CRL из DER в base64 или обратно.

-export

Экспортировать сертификат или CRL из хранилища или контейнера в файл.

-delete

Удалить сертификат или CRL из хранилища.

-help

Вывести справку.

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

-at_signature

Использовать закрытый ключ AT_SIGNATURE вместо AT_KEYEXCHANGE.

-ask-cont

Попросить пользователя указать контейнер из списка доступных контейнеров.

-base64

Закодировать сертификат или CRL в base64 кодировку.

-cont <container>

Указать имя контейнера с сертификатом или закрытым ключом. Имя имеет формат, например, \\.\reader\name. Если опция B<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.

-cert

Работать с сертификатом (значение по умолчанию).

-crl

Работать со списком отзыва сертификатов вместо сертификата.

-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.

-all

Использовать все подходящие сертификаты(CRL).

-der

Закодировать сертификат или CRL в DER-кодировку (значение по умолчанию).

-dest <path>

Файл для раскодированного 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).

-provname <name>

Имя провайдера.

-provtype <type>

Тип провайдера (значение по умолчанию 75).

-help

Вывести справку о заданной команде.

-pin <pincode>

Пин-код контейнера.

-src_file <path>

Файл с сертификатом или CRL для раскодирования.

-thumbprint <hash>

Цифровой отпечаток сертификата для фильтрации.

-verbose

Выводить подробную информацию о сертификате.

-store <name>

Имя хранилища. Первая буква указывает тип хранилища - 'u' для пользовательского хранилища, 'm' для хранилища машины, 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.

certmgr возвращает ноль при успехе и ненулевой код ошибки при ошибке.

## 3. Примеры использования

certmgr -inst -store uMy -file /media/floppy/testuser.cer -cont '\\.\FAT12_0\31cc730c-e57e-4b56-8014-9b8f2ab79d6d'
Установить сертификат из файла testuser.cer в пользовательское хранилище My с ссылкой на закрытый ключ.

certmgr -decode -src /media/floppy/testuser.cer -dest /media/floppy/testuser_base64.cer -base64
Раскодировать сертификат из файла testuser.cer в base64 кодировку и положить его в testuser_base64.cer.

certmgr -export -crl -store mCA -dest /media/floppy/root.crl
Экспортировать CRL из машинного хранилища CA в файл root.crl