ПАО «МОСКОВСКАЯ БИРЖА»

УТВЕРЖДЕН
ВАМБ.00075-02 34 02–ЛУ

# АППАРАТНО-ПРОГРАММНЫЙ КОМПЛЕКС «КЛИЕНТ МБ» ВЕРСИЯ 2.0

# УТИЛИТА КОМАНДНОЙ СТРОКИ

РУКОВОДСТВО ОПЕРАТОРА

ВАМБ.00075-02 34 02

2015

# Аннотация

Данный документ содержит описание утилиты командной строки для работы с Библиотекой упрощенного прикладного программного интерфейса для работы с сертификатами, входящей в состав АПК «Клиент МБ».

Утилита командной строки предназначена для вызова криптографических функций, из режима командной строки ОС Windows и позволяет осуществлять шифрование/расшифрование информации, формирование/проверку подлинности электронной подписи (ЭП). Документ предназначен для операторов как руководство по эксплуатации утилиты.

# Содержание

# 1 НАЗНАЧЕНИЕ

Утилита командной строки предназначена для осуществления доступа пользователей к криптографическим функциям из режима командной строки ОС Microsoft Windows. Утилита командной строки позволяет осуществлять шифрование/расшифрование информации и формирование/проверку подлинности электронной подписи (ЭП). Комплекс использует «Справочник Сертификатов» для управления справочниками сертификатов и взаимодействия с Центром Регистрации.

Доступ пользователей к криптографическим функциям осуществляется через вызов утилиты с заданием параметров выполнения из режима командной строки.

Утилита предназначена для работы в следующих локализованных операционных системах:

- Microsoft Windows Vista с пакетом обновлений 1 и выше;
- Microsoft Windows Server 2008 с пакетом обновлений 1 и выше;
- Microsoft Windows 7;
- Microsoft Windows Server 2008 R2;
- Microsoft Windows 8/8.1;
- Microsoft Windows Server 2012/2012 R2;
- Windows 10.

Перед началом работы с утилитой необходимо установить и настроить СКЗИ и ПК «Справочник сертификатов».

# 2 РАБОТА С КОМПЛЕКСОМ

## 2.1 Инициализация криптографического модуля

Инициализация криптографического модуля и загрузка ключа ЭП происходит при первом вызове криптографической операции в утилите.

При инициализации ПО проверяет наличие и целостность персонального справочника пользователя (ПСП). Для этого производится проверка ЭП персонального справочника сертификатов и загрузка с использованием выбранного устройства считывания ключа ЭП[1] с определенным идентификатором, соответствующим сертификату, на котором подписан ПСП. Идентификатор ключа представляет собой последовательность цифр и латинских букв длиной 16 символов и соответствует идентификатору ключа, содержащемуся в сертификате.

После проверки ЭП ПСП и проверки сертификата пользователя[2] завершается инициализация криптографического модуля.

## 2.2 Параметры вызова утилиты

Доступ к криптографическим функциям при работе с утилитой осуществляется при вызове исполняемого модуля xpki1utl.exe с заданием параметров вызова в командной строке.

```
xpki1utl.exe [операции] [параметры] {опции}
```

В квадратных скобках указаны обязательные параметры командной строки, в фигурных - необязательные. Разделителем операций, параметров, значений параметров, опций и значений опций является как минимум один пробел. Использование разделителя является обязательным. Максимальная длина командной строки 256 символов. После окончания работы модуля закрытый ключ не сохраняется, т.е. ключ нужно вводить при каждом следующем выполнении модуля.

Выполняемые операции:

- `sign` – выполнить ЭП (можно вместе с заданием шифрования);
- `verify` – выполнить проверку ЭП;
- `encrypt` – выполнить зашифрование;
- `decrypt` – выполнить расшифрование (можно вместе с проверкой ЭП);
- `help` – показать справку.

*Примечания*

*1 При выполнении операций производится проверка времени действия и параметра "дата отзыва" актуального списка отозванных сертификатов.*

*2 В первую очередь всегда производится подписание, а затем шифрование и наоборот, сначала расшифрование, а затем проверка подписи. При совместном использование операций encrypt и sign, а также decrypt и verify, порядок операций при задании в командной строке значения не имеет. Количество заданных операций одного типа на результат работы модуля влияния не оказывает, т.е. если в командной строке будет указано несколько операций sign, файл все равно будет подписан только один раз.*

*3 Следует иметь в виду, что использование только операции encrypt не обеспечивает контроля целостности данных и аутентификацию их источника. При необходимости контроля*

[1] Для операции проверки ЭП загрузка ключа ЭП не производится

[2] Необходимо следить за временем действия сертификата и актуальностью списка отозванных сертификатов. Для этого необходимо периодически запускать ПК «Справочник Сертификатов».

*целостности и аутентификации следует использовать совместно операции encrypt и sign, а при расшифровании и проверке ЭП – операции decrypt и verify.*

Параметры:

– `profile [PROFILE]` – установить профиль (настройки справочников сертификатов) в соответствии с файлом PROFILE на время работы программного модуля. Без использования параметра –profile по умолчанию используются настройки ПК Справочника Сертификатов. Может использоваться для выполнения операций с использованием различных закрытых ключей.

– `in [INFILE]` – установить имя входного файла в [INFILE];

– `out [OUTFILE]` – установить имя выходного файла в [OUTFILE];

– `data [DATAFILE]` – установить имя файла данных в [DATAFILE] для выполнения ЭП или проверки ЭП с отделенными (detached) данными.

Опции выполнения:

– `silent {ERRFILE}` – режим без показа сообщений (для использования в автоматизированных системах) с записью протокола в ERRFILE;

– `sendcert` – добавлять собственный сертификат при выполнении ЭП

– `crlupdate {FILE}` – опция обновления СОС, в качестве параметра передается файл в DER-кодировке. Опция обновления СОС может использоваться при выполнении любых операций. Данная функция не предназначена для добавления СОС Центра Регистрации в Локальный Справочник. В случае если операция выполнена успешно (без ошибок), то СОС будет добавлен в используемый локальный справочник.

Опции проверки ЭП:

– `detached` – отделенная ЭП

– `eku [EKU]` – добавить oid [EKU] расширенного использования ключа при проверке сертификата отправителя;

– `policy [POLICY]` – добавить oid [POLICY] политики использования сертификата при проверке сертификата отправителя;

– `delete [КОЛ]` – удалить [КОЛ] подписей после проверки (-1 для удаления всех ЭП);

– `ldap` – использовать LDAP для поиска сертификатов;

– `info [FIELDS]` – использование этой опции проверки ЭП позволяет задать поля сертификата подписавшего, которые будут отображены (по умолчанию: владелец, хеш). Возможные значения: subject, hash, altname, serial, notbefore, notafter.

Опции шифрования:

– `recsubj [SUBJ]` - добавить сертификат с именем владельца (DN) равного [SUBJ] в список получателей зашифрованного файла, например, «cn=0010400001»;

*Примечания*
*1 Для указания нескольких получателей зашифрованного файла необходимо несколько раз задать опцию recsubj (например, –recsubj cn=user1 –recsubj user2).*
*2 В поле [SUBJ] имя владельца сертификата указывается полностью.*

– `rechash [HASH]` – добавить сертификат с отпечатком в шестнадцатеричном представлении равным [HASH] в список получателей зашифрованного файла, например, «E2FFCC7FB347E41B4E220F96D23A4CC2596DB0E».

– `reclist [FILE]` – считать список получателей зашифрованного файла из заданного формализованного файла. Ели не задан полный путь к файлу (например, .\reclist.txt), файл считывается из системного каталога ОС Windows (например, C:\Windows\reclist.txt).

Если не задан режим без показа сообщений, то при выполнении операций на экране будут отображаться выполняемые операции и результат выполнения.

## 2.3 Примеры использования утилиты

### 2.3.1 Выполнение ЭП

Следующая команда выполняет ЭП файла 1.txt и сохраняет результат в файл 1.s:

```
xpki1utl.exe -sign -data 1.txt -out 1.s
```

### 2.3.2 Выполнение проверки ЭП

Следующая команда выполняет проверку ЭП файла 1.s и проверку сертификата для применения как клиента системы клиент-банк без показа сообщений:

```
xpki1utl.exe -verify -in 1.s -eku 1.3.6.1.4.1.15477.4.2.2 -silent
```

### 2.3.3 Выполнения зашифрования

Следующая команда выполняет зашифрование файла 1.txt для всех сертификатов с действующим сроком действия с именем владельца cn=ivanov,o=x509,c=ru с сохранением результата в файл 1.e:

```
xpki1utl.exe -encrypt -in 1.txt -out 1.e -recsubj ‘‘cn=ivanov,o=x509,c=ru’’
```

### 2.3.4 Выполнение расшифрования

Следующая команда выполняет расшифрование файла crypt.e с сохранением результата в файл plaint.txt:

```
xpki1utl.exe -decrypt -in crypt.e -out plain.txt
```

# 3 ПРИМЕР ФАЙЛА ДЛЯ ЗАШИФРОВАНИЯ

## 3.1 Пример файла

При работе с утилитой командной строки есть возможность использования подготовленного формализованного файла для выбора группы получателей для шифрования (с использованием опции `-reclist` зашифрования).

Ниже приведён пример такого файла для задания списка получателей

```
; encryption recipients configuration file
[General]
Number=2

[Recipient1]
;Type could be one of the following:
;KeyId, Subject, Hash, Mail
Type=KeyId
Value=1209ABSCDI01

[Recipient2]
Type=Subject
Value=cn=ivanov,o=cbr,c=ru
```

## 3.2 Описание параметров

Комментарий задаётся после знака «;».

Параметр Number в секции General задаётся количество получателей зашифрованного файла.

Для каждого из получателей задана секция [RecipientN], где N – номер получателя.

В каждой из секций необходимо задать параметр Type – тип идентификации получателя, поддерживаются следующие типы:

– KeyId – идентификатор ключа ЭП;

– Subject – полное X.500 имя владельца (DN, например, `cn=user,o=x509,c=ru`);

– Hash – отпечаток (хэш издателя и серийного номера сертификата, который отображается в нижней части диалога отображения сертификата в ПК Справочник Сертификатов) в шестнадцатеричном представлении, разделенный двоеточием, например, “`E2:FF:CC:7F:B3:47:E4:1B:4E:22:0F:96:D2:3A:4C:C2:59`”;

– Mail – адрес электронной почты получателя.

В соответствии с заданным типом необходимо задать значение для поиска сертификата при зашифровании в параметре Value.

*Примечание - Наиболее быстрый поиск происходит при задании отпечатка сертификата. Задание X.500 имени или адреса электронной почты может привести к нахождению нескольких сертификатов для зашифрования.*

# 4 ПРИМЕР КОНФИГУРАЦИОННОГО ФАЙЛА

## 4.1 Пример конфигурационного файла

При работе с утилитой командной строки есть возможность использования подготовленного конфигурационного файла и заранее сформированных баз сертификатов, (то есть без необходимости запускать ПК «Справочник Сертификатов»). Для этого необходимо запустить модуль с параметром -profile <имя>, указывающий имя настройки в конфигурационном файле pki1.conf.

Ниже приведён пример конфигурационного файла pki1.conf для настроек профилей справочников для библиотеки

```
# pki1 configuration file

default: ivanov

local: ivanov
pse: pse://signed/c:\ivanov\local.pse
localstore: file://c:\ivanov\local.gdbm
ldap: ldap://ldap.x509.ru/o=x509,c=ru
```

## 4.2 Описание параметров

Комментарий задается после знака #.

Параметр **default** задает название одного из профилей настройки подключения конфигурационного файла «по умолчанию».

В случае использования параметра **profile** без аргумента, используется профиль, указанный в параметре default в конфигурационном файле.

Параметр **local** задает название профиля настройки для использования этого названия в качестве аргумента параметра **profile**.

Параметр **pse** задает URI доступа к персональному справочнику пользователя (ПСП)

Параметр **localstore** задает URI доступа к локальному справочнику пользователя

Параметр **ldap** задает URI доступа к сетевому справочнику сертификатов.

# 5 КОДЫ ВОЗВРАТА

Коды возврата, возвращаемые утилитой командной строки.

| Код возврата | Описание |
|---|---|
| 0 | Нет ошибки. Программа выполнена успешно |
| Другой код | Код ошибки прикладной библиотеки |

# Лист регистрации изменений

| Номера листов (страниц) | | | | | Всего листов (страниц) в докум | № документа | Входящий № сопроводительного докум и дата | Подп | Дата |
|---|---|---|---|---|---|---|---|---|---|
| Изм | изменённых | заменённых | новых | аннулированных | | | | | |
| 1 | | Все | | | | ВАМБ.00075-02.001 | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |