УТВЕРЖДЕН

РБ.ЮСКИ.13008-02 34 01-ЛУ

УТИЛИТА КОМАНДНОЙ СТРОКИ AVCMUT

Подп. и дата	
Инв.№ дубл	
Взам. инв.№	
Подп. и	
Инв.№	

Руководство оператора

РБ.ЮСКИ. 13008-02 34 01

Листов 59

2023

АННОТАЦИЯ

Данный документ содержит руководство оператора программного продукта РБ.ЮСКИ.13008-02 «Утилита командной строки AvCmUt» (далее – AvCmUt). В документе содержится информация по использованию AvCmUt.

Утилита командной строки AvCmUt предназначена для проведения вспомогательных, а также тестовых (контрольных) криптографических процедур, включающих в себя выработку/проверку электронно-цифровой подписи (далее – ЭЦП), зашифрование/расшифрование, вычисление значения функции хэширования, проверку статуса сертификата по протоколу OCSP, выработку и проверку контрподписи (контрподпись (countersignature) - электронно-цифровая подпись, удостоверяющая другую электронно-цифровую подпись) и т.д.

Утилита командной строки AvCmUt предназначена для применения в среде ОС Windows совместно с ПО «Программный комплекс «Комплект Абонента АВЕСТ» AvUCK» и распространяется в его составе (в составе Программного комплекса «Персональный менеджер сертификатов АВЕСТ» (AvPCM)).

Утилита командной строки AvCmUt поставляется в виде исполняемого файла AvCmUtX.exe, где X – версия утилиты. В настоящее время распространяется версия 4.

Изготовителем AvCmUt является белорусское предприятие «Закрытое акционерное общество «АВЕСТ» (ЗАО «АВЕСТ»).

Адрес предприятия: 220116, Республика Беларусь, г. Минск, пр. газеты «Правда», д. 5, пом. 3Н, каб. 7.

Тел.: (+375 17) 257-99-74, 318-92-34, факс: (+375 17) 303-91-49.

Интернет-страница: https://www.avest.by.

Электронная почта: welcome@avest.by.

СОДЕРЖАНИЕ

1. УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

AvCmUt предназначен для работы на персональном компьютере общего назначения, функционирующим под управлением одной из следующих ОС:

- Windows 2008 R1 Server (x32, x64);
- Windows 2008 R2 Server (x64);
- Windows 2012 Server (x64);
- Windows 2012 R2 Server (x64);
- Windows 10 (x32, x64);
- Windows 2016 Server (x64);
- Windows 2019 Server (x64).

Примечание. Допускается работа AvCmUt в среде следующих ОС Windows, которые сняты с поддержки компании Microsoft:

- Windows 2003 Server (x32, x64) SP2;
- Windows XP SP3 (x32);
- Windows 7 (x32, x64);
- Windows 8 (x32, x64);
- Windows 8.1 (x32, x64).

В случае использования вышеуказанных ОС, снятых с поддержки компании Microsoft, устойчивая работа AvCmUt не гарантируется.

Для использования AvCmUt пользователь должен иметь права «Administrator (Администратор)» либо «Power User (Опытный пользователь)».

Необходимо установить поддержку русского языка для программ, не поддерживающих Юникод. Для этого:

В ОС Windows XP, Windows 2003 Server:

1. Перейти в меню «Start» - «Control Panel» («Пуск» - «Панель управления»), в зависимости от параметров просмотра элементов в панели управления (классический вид или по категориям) выбрать «Regional and Language Options» («Язык и региональные стандарты») или «Date, Time, Language and Regional Options» - «Regional and Language Options» («Дата, время, язык и региональные стандарты» - «Язык и региональные стандарты»).
2. На вкладке «Regional options» («Региональные параметры») в поле «Standards and formats» («Языковые стандарты и форматы») выбрать русский язык, в поле «Location» («Расположение») указать Беларусь, на вкладке «Advanced» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») выбрать русский язык.
3. Выполнить перезагрузку.
4. Проверить отображение кодировки.

В ОС Windows 7, Windows 2008 Server:

1. Перейти в меню «Start» - «Control Panel» («Пуск» - «Панель управления»), в зависимости от параметров отображения элементов в панели управления (категория или значки) выбрать «Clock, Language and Region» - «Region and Language» («Часы, язык и регион» - «Язык и региональные стандарты») или «Region and Language» («Язык и региональные стандарты»).

2. На вкладке «Formats» («Форматы») выбрать русский язык, на вкладке «Location» («Расположение») выбрать «Беларусь», на вкладке «Administrative» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») нажать кнопку «Change system locale...» («Изменить язык системы…»), в окне «Region and Language settings» («Язык и региональные стандарты») выбрать русский язык.

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

В ОС Windows 8, Windows 8.1, Windows 2012 Server:

1. Перейти в «Control Panel» («Панель управления») одним из способов, предусмотренных для данных ОС. Например, навести курсор мыши на правый верхний или нижний угол рабочего стола. В открывшейся боковой панели выбрать пункт «Settings» («Параметры»). В списке параметров выбрать пункт «Control Panel» («Панель управления»). Другой способ – нажать правой клавишей мыши по кнопке «Start» («Пуск»), выбрать пункт «Control Panel» («Панель управления»). При этом нужно учитывать, что в ОС Windows 8 данная кнопка не отображается, для ее отображения нужно на рабочем столе переместить курсор в нижний левый угол экрана. Далее, в зависимости от параметров просмотра элементов, в панели управления (категория или значки) выбрать «Clock, Language and Region» - «Region» («Часы, язык и регион» - «Региональные стандарты») или «Region» («Региональные стандарты»).

2. На вкладке «Formats» («Форматы») выбрать русский язык, на вкладке «Location» («Местоположение») выбрать «Беларусь», на вкладке «Administrative» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») нажать кнопку «Change system locale...» («Изменить язык системы…»), в окне «Region and Language settings» («Региональные стандарты») выбрать русский язык.

3. Выполнить перезагрузку.

4. Проверить отображение кодировки.

В ОС Windows 10, Windows 2016 Server, Windows 2019 Server:

1. Перейти в «Control Panel» («Панель управления») одним из способов, предусмотренных для данных ОС. Например, в строке поиска ввести «Control». Другой способ – нажать «Start» («Пуск»), в списке приложений найти «Windows System» («Служебные Windows»), выбрать «Control Panel» («Панель управления»). Далее, в зависимости от параметров просмотра элементов в панели управления (категория или значки) выбрать «Clock and Region» - «Region» («Часы и регион» - «Региональные стандарты») или «Region» («Региональные стандарты»).

2. На вкладке «Formats» («Форматы») выбрать русский язык, на вкладке «Administrative» («Дополнительно») в поле «Language for non-Unicode programs» («Язык для программ, не поддерживающих Юникод») нажать кнопку «Change system locale...» («Изменить язык системы…»), в окне «Region settings» («Региональные стандарты») выбрать русский язык. Галочку на пункте «Beta: Use Unicode UTF-8 for worldwide language support» («Бета-версия:

Использовать Юникод (UTF-8) для поддержки языка во всем мире») не устанавливать.

3. Выполнить перезагрузку.
4. Проверить отображение кодировки.

ВНИМАНИЕ!!!

Для правильного отображение всех символов в командной строке при работе с утилитой нужно использовать кодировку chcp 1251 (кодировка русского текста Windows) или chcp 65001 (UTF-8), шрифт Lucida Console или Consolas.

AvCmUt предназначен для работы на компьютере (сервере), имеющем следующие минимальные технические характеристики:

- процессор x86 (x64) с тактовой частотой - не менее 2,5 ГГц;
- объем ОЗУ - не менее 4 Гб;
- жесткий диск, содержащий не менее 8 Гб свободного пространства для стандартной установки ОС;
- монитор с поддержкой VGA или более высокого разрешения;
- манипулятор «мышь» Microsoft или совместимое указывающее устройство,
- свободный USB-порт.

Для хранения личных ключей пользователя ИОК AvCmUt использует отчуждаемые носители ключевой информации (далее - НКИ).

Для работы AvCmUt необходимо наличие на компьютере пользователя установленного одного из следующих криптопровайдеров или специализированных программно-аппаратных СКЗИ:

- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP» AvCSP (РБ.ЮСКИ.08000-03) (далее – криптопровайдер AvCSP): 32- разрядная версия AvCSP в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSP в 64-разрядных версиях ОС;
- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BEL» AvCSPBEL (РБ.ЮСКИ.12004-02) (далее – криптопровайдер AvCSPBEL): 32-разрядная версия AvCSPBEL в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSPBEL в 64-разрядных версиях ОС;
- программное средство криптографической защиты информации «Криптопровайдер AVEST CSP BIGN» AvCSPBIGN (РБ.ЮСКИ.12005-02) (далее – криптопровайдер AvCSPBIGN) (32-разрядная версия AvCSPBIGN в 32-разрядных версиях ОС; 32- и 64-разрядные версии AvCSPBIGN в 64-разрядных версиях ОС), использующий криптографические сервисы изделия Устройства программно-аппаратные электронной цифровой подписи и шифрования «AvBign» (ИЯТА.467532.003);
- устройство программно-аппаратное криптографическое «AvHSM-Bign» (ИЯТА.466217.003) (далее – устройство «AvHSM-Bign»);
- устройство программно-аппаратное электронной цифровой подписи и шифрования «AvBign» (ИЯТА.467532.003) (далее – устройство «AvBign»).

Утилита AvCmUt обеспечивает выполнение криптографических сервисов ЭЦП, шифрования, управления ключами, контроля целостности, управления СОК и СОС абонента ИОК, включая атрибутные сертификаты, в соответствии со следующими нормативными актами и документами:

1) ГОСТ 28147-89 «Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования»;

2) СТБ 1176.1-99 «Информационная технология. Защита информации. Функция хэширования»;

3) СТБ 1176.2-99 «Информационная технология. Защита информации. Процедуры выработки и проверки электронной цифровой подписи»;

4) СТБ 34.101.17-2012 «Информационные технологии и безопасность. Синтаксис запроса на получение сертификата»;

5) СТБ 34.101.19-2012 «Информационные технологии и безопасность. Форматы сертификатов и списков отозванных сертификатов инфраструктуры открытых ключей»

6) СТБ 34.101.23-2012 «Информационные технологии и безопасность. Синтаксис криптографических сообщений»;

7) СТБ 34.101.26-2012 «Информационные технологии и безопасность. Онлайновый протокол проверки статуса сертификата (OCSP)»;

9) СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности»;

10) СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых»;

11) СТБ 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел»;

14) СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых»;

15) СТБ 34.101.67-2014 «Информационные технологии и безопасность. Инфраструктура атрибутных сертификатов»;

16) СТБ 34.101.78-2019 «Информационные технологии и безопасность. Профиль инфраструктуры открытых ключей»;

17) Проект Руководящего документа Республики Беларусь «Банковские технологии. Протоколы формирования общего ключа» (ПФОК);

18) ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность».

AvCmUt поддерживает криптографические алгоритмы в зависимости от установленного типа криптопровайдера, сведения о поддержке криптографических алгоритмов каждым типом криптопровайдера в отдельности содержатся в ПРИЛОЖЕНИЕ 1.

Обращаем ваше внимание, что в 2020 г. в связи с приказом ОАЦ №77 от 12 марта 2020 г. https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020-77.pdf было принято решение о прекращении использования криптопровайдера Avest CSP тип 421 base (независимо от версии), реализующего алгоритм СТБ 1176.2-99. Согласно приказу, этот алгоритм может использоваться только для проверки ЭЦП.

2. УСТАНОВКА И ИСПОЛЬЗОВАНИЕ

Утилита входит в состав программного комплекса «Персональный менеджер сертификатов АВЕСТ» AvPCM (далее – ПК AvPCM) и не требует дополнительных процедур по установке. Исполняемый файл утилиты находится в одной папке с установленным ПК AvPCM.

Для выполнения отдельных процедур утилиты необходимо наличие корректно проимпортированных сертификатов в хранилище, на которое настроена ПК AvPCM, и НКИ, на котором хранится соответствующий ключ выработки ЭЦП пользователя.

Общий синтаксис команды запуска утилиты выглядит следующим образом:

AvCmUt4 <Операция> <Входной файл> <Параметры>

При запуске утилиты в командной строке отображается версия утилиты и версия библиотеки AvCryptMail.dll:

```
Утилита Avest CryptMail. Версия X.X.X.XXX
        AvCryptMail.dll. Версия X.X.X.XXXX
```

Большие и маленькие буквы в параметрах различаются. То есть, ключи «**-s**» и «**-S**» означают различные операции.

В качестве разделителя между операцией и входным файлом используется пробел, также в качестве разделителя допустимо использовать знак «=». Т.е операция выработки ЭЦП для файла test с указанием параметров аутентификации

```
AvCmUt4.exe –s test -l 4B5CAFE0235786E28FB55744A756C9B91E822E66
–p 12345678
```

будет аналогична

```
AvCmUt4.exe –s=test –l=4B5CAFE0235786E28FB55744A756C9B91E822E66
–p=12345678
```

Если в атрибутах параметров есть пробелы или специальные символы («>», «^» и т.д.), то атрибут следует брать в двойные кавычки, например:

```
-c "ALEXEY IVANOV"
```

Если в атрибутах параметров есть кавычки, то их нужно удваивать, например:

```
-X 2.5.4.10="ЗАО ""Организация"""
```

Если предназначенный для обработки файл находится не в одной папке с утилитой AvCmUt, нужно прописать его полный путь.

3. ОСНОВНЫЕ ОПЕРАЦИИ

Обязательно нужно указать одну из операций.

Входной файл обязательно указывается после указания требуемой операции (за исключением опции вывода справки о программе -?).

3.1. Вывод справки о программе (-?)

AvCmUt4.exe -?

Отобразить на экране список поддерживаемых операций и параметров.

3.2. Функции выработки ЭЦП

3.2.1. Выработка ЭЦП входного файла (-s)

AvCmUt4.exe -s <подписываемый файл>

Если параметр «выходной файл» (см. **п. 4.2.1. Указание выходного файла (-o))** не указан, подписанный документ будет записан в файл с расширением «**.p7s**».

Пример:

```
AvCmUt4.exe –s test.txt
```

3.2.2. Выработка дополнительной ЭЦП (–S)

AvCmUt4.exe -S <подписываемый файл>

Входной файл должен содержать подписанный документ, операция добавит новую ЭЦП. Если параметр «выходной файл» не указан (см. **п. 4.2.1. Указание выходного файла (-o)**), подписанный документ будет записан в файл с расширением «**.p7s**». Если дополнительная ЭЦП вырабатывается к файлу с расширением «.p7s», то при выполнении операции данный файл будет перезаписан, поэтому надо или добавлять флаг –R (см. **п. 4.5.1. Заменить существующий файл (-R)**), или указывать параметр «выходной файл».

Если дополнительная ЭЦП вырабатывается к файлу с раздельной ЭЦП (как выработать раздельную ЭЦП см. в **п. 4.4.4. Не включать исходный документ в подписываемое сообщение (-T)**), нужно указать файл документа для проверки раздельной ЭЦП (см. **п. 4.2.3. Указание файла документа для проверки раздельной ЭЦП (-F)**).

Пример:

```
AvCmUt4.exe –S test.txt.p7s -R
```

3.2.3. Проверка ЭЦП (-v)

AvCmUt4.exe -v <проверяемый файл>

При проверке ЭЦП в лог будут выводиться результат проверки ЭЦП, дата и время выработки ЭЦП, информация о субъекте-подписанте из его сертификата, информация о

действительности сертификата подписанта. Входной файл должен содержать подписанный документ. Если параметры указания сертификата проверяемой подписи не заданы (см. п. **4.3. Дополнительные параметры для выбора сертификатов при проверке ЭЦП и зашифровании**), будут проверены **все** ЭЦП в документе. Если параметр «выходной файл» не указан, выходной файл будет записан в файл с исходным расширением.

Примечание. Если при проверке ЭЦП использовались недействительные сертификаты (например, с истекшим сроком действия), то результаты выполнения функции будут содержать ошибку с указанием сертификата, который был недействителен. При этом в результате проверки ЭЦП выводится сообщение «ЭЦП сообщения верна», что означает отсутствие ошибки в работе алгоритма проверки ЭЦП, т.е. целостность сообщения не нарушена, но при этом ЭЦП сообщения является «недействительной» в юридическом смысле.

Пример:

```
AvCmUt4.exe –v test.txt.p7s
```

3.2.4. Проверка ЭЦП без записи исходного файла (-V)

AvCmUt4.exe -V <проверяемый файл>

При проверке ЭЦП в лог будут выводиться результат проверки ЭЦП, дата и время выработки ЭЦП, информация о субъекте-подписанте из его сертификата, информация о действительности сертификата подписанта. Входной файл должен содержать подписанный документ. Если параметры указания сертификата проверяемой подписи не заданы, будут проверены **все** ЭЦП в документе.

Примечание. Если при проверке ЭЦП использовались недействительные сертификаты (например, с истекшим сроком действия), то результаты выполнения функции будут содержать ошибку с указанием сертификата, который был недействителен. При этом в результате проверки ЭЦП выводится сообщение «ЭЦП сообщения верна», что означает отсутствие ошибки в работе алгоритма проверки ЭЦП, т.е. целостность сообщения не нарушена, но при этом ЭЦП сообщения является «недействительной» в юридическом смысле.

Пример:

```
AvCmUt4.exe –V test.txt.p7s
```

Также используется (и выходной файл будет создаваться):

- при добавлении в сообщение ответа OCSP сервера проверки статуса сертификата, атрибутного сертификата **(**см. **п. 5. Проверка статуса сертификата по протоколу OCSP**),
- при удостоверении ЭЦП сообщения, при удостоверении контрподписи (см. **п. 6. Выработка контрподписи**).

3.3. Функции шифрования

3.3.1. Зашифрование входного файла (-e)

AvCmUt4.exe -e <зашифровываемый файл>

Нужно указать атрибуты сертификата получателя зашифрованного файла, для которого будет произведено зашифрование, если получатели не определены, зашифрование будет произведено на себя. Если параметр «выходной файл» не указан, зашифрованный документ будет записан в файл с расширением «**.p7e**».

Сертификат получателя зашифрованного сообщения должен находится в сетевом справочнике сертификатов и быть действительным на момент зашифрования.

Максимальное количество получателей зашифрованного сообщения указано в файле AvCmUt4.ini в секции [ENCRYPT] (100 по умолчанию):

```
[ENCRYPT]
MaxRecipient=100
```

Если количество получателей зашифрованного сообщения больше 100, надо отредактировать файл AvCmUt4.ini, указав нужное количество.

Пример:

```
AvCmUt4.exe –e test.txt
```

3.3.2. Расшифрование входного файла (-d)

AvCmUt4.exe -d <расшифровываемый файл>

Входной файл должен содержать зашифрованный документ, получателем которого является владелец личного ключа. Если параметр «выходной файл» не указан, расшифрованный документ будет записан в файл с исходным расширением.

Пример:

```
AvCmUt4.exe –d test.txt.p7e
```

3.4. Функции выработки ЭЦП и зашифрования

3.4.1. Выработка ЭЦП и зашифрование входного файла (-E)

AvCmUt4.exe -E <подписываемый и зашифровываемый файл>

Обязательно нужно указать атрибуты сертификата получателя зашифрованного файла, для которого будет произведено зашифрование, если получатели не определены – зашифрование будет произведено на себя. Если параметр «выходной файл» не указан, подписанный и зашифрованный документ будет записан в файл с расширением «**p7s.p7e**».

Максимальное количество получателей зашифрованного сообщения указано в файле AvCmUt4.ini в секции [ENCRYPT] (100 по умолчанию):

```
[ENCRYPT]
MaxRecipient=100
```

Если количество получателей зашифрованного сообщения больше 100, нужно отредактировать файл AvCmUt4.ini, указав нужное количество.
Пример:

```
AvCmUt4.exe –E test.txt
```

3.4.2. Выработка дополнительной ЭЦП и зашифрование входного файла (-G)

AvCmUt4.exe -G <подписываемый и зашифровываемый файл>

Входной файл должен содержать подписанный документ, операция добавит новую ЭЦП. Обязательно надо указать атрибуты сертификата получателя зашифрованного файла, для которого будет произведено зашифрование (см. **п. 4.3. Дополнительные параметры для выбора сертификатов при проверке ЭЦП и зашифровании)**, если получатели не определены – зашифрование будет произведено на себя. Если параметр «выходной файл» не указан, подписанный и зашифрованный документ будет записан в файл с расширением «**p7s.p7e**».
Пример:

```
AvCmUt4.exe –G test.txt.p7s
```

3.4.3. Расшифрование и проверка ЭЦП (-D)

AvCmUt4.exe -D <расшифровываемый и проверяемый файл>

При проверке ЭЦП в лог будет выводиться информация о субъекте-подписанте, а также дата и время подписи. Входной файл должен содержать подписанный и зашифрованный документ, получателем которого является владелец личного ключа. Если параметры для определения сертификата проверяемой подписи не заданы, будут проверены **все** ЭЦП в документе. Если параметр «выходной файл» не указан, расшифрованный файл без ЭЦП будет записан в файл с исходным расширением.
Пример:

```
AvCmUt4.exe –D test.txt.p7s.p7e
```

3.5. Функции вычисления значений хэширования

3.5.1. Вычисление значения функции хэширования по алгоритму СТБ 34.101.31-2020 Belt (-H)

AvCmUt4.exe -H <исходный файл>

Пример:

```
AvCmUt4.exe –H avc.dll
```

3.5.2. Вычисление значения функции хэширования по алгоритму СТБ 1176.1-99 BHF (-h)

AvCmUt4.exe -h <исходный файл>

Пример:

```
AvCmUt4.exe –h avc.dll
```

3.6. Функции работы с сертификатами

3.6.1. Запуск мастера импорта сертификатов и СОС из файла *.p7b (-i)

AvCmUt4.exe -i <файл PKCS#7 (*.p7b)>

Пример:

```
AvCmUt4.exe –i certificate.p7b
```

3.6.2. Импорт СОС из файла *.crl (-C)

AvCmUt4.exe -C <файл с СОС (*.crl)>

Пример:

```
AvCmUt4.exe –C CRL.crl
```

3.6.3. Обновление СОС и сертификатов УЦ онлайн (-CDP)

AvCmUt4.exe -CDP <файл точек распространения СОС>

Пример:

```
AvCmUt4.exe –CDP CrlDPExt.txt
```

3.6.4. Запуск мастера генерации запроса на сертификат (-r)

AvCmUt4.exe -r <выходной файл (*.req)>

Запуск мастера генерации запроса на сертификат.
После создания запроса он будет сохранен в указанный файл. Для генерации запроса на основе предопределенного шаблона на сертификат, используйте опцию **–t** (см. **п. 4.2.4. Указание файла шаблона на сертификат (-t)**).
Пример:

```
AvCmUt4.exe –r request.req –t face.tpl
```

4. ПАРАМЕТРЫ

4.1. Параметры аутентификации пользователя

Параметры аутентификации пользователя не являются обязательными.

4.1.1. Указание идентификатора открытого ключа сертификата пользователя (-l)

AvCmUt4.exe <операция> <входной файл> -l <идентификатор>

Идентификатор открытого ключа сертификата пользователя указывается в шестнадцатеричном виде. В случае, если данный параметр не указан, программой будет выдан диалог для выбора личного сертификата.

Если при этом также указано значение пароля (параметр **–p**), то утилита не будет выводить никаких диалоговых окон, а если параметр **–p** не указан, то будет выведен диалог для ввода значения пароля.

Пример:

```
AvCmUt4.exe –s test.txt -l
4B5CAFE0235786E28FB55744A756C9B91E822E66
```

- выработка ЭЦП к файлу test.txt с указанием идентификатора открытого ключа сертификата пользователя, выполняющего операцию.

4.1.2. Указание значения пароля к контейнеру с личным ключом (-p)

AvCmUt4.exe <операция> <входной файл>-p <пароль>

Пример:

```
AvCmUt4.exe –s test.txt -p password
```

- выработка ЭЦП к файлу test.txt с указанием значения пароля на доступ к контейнеру с личным ключом.

4.1.3. Без аутентификации (-NA)

AvCmUt4.exe <операция> <входной файл> -NA

При использовании данного параметра хранилище сертификатов должно быть **в реестре или LDAP**

Может использоваться:

1. при проверке ЭЦП

Пример:

```
AvCmUt4.exe –v test.txt.p7s -NA
```

2. зашифровании (при выборе получателей зашифрованного сообщения, см. **п. 4.3. Дополнительные параметры для выбора сертификатов при проверке ЭЦП и зашифровании)**.

Пример:

```
AvCmUt4.exe –e test.txt -c "Иванов И. И." -NA
```

4.2. Дополнительные параметры

4.2.1. Указание выходного файла (-o)

AvCmUt4.exe <операция> <входной файл> -o <выходной файл>

В случае, если данный параметр опущен, файл будет создан с расширением по умолчанию для выбранной операции.

Пример:

```
AvCmUt4.exe –s test.txt -o test
```

4.2.2. Указание файла для записи результатов выполнения операций (-O)

AvCmUt4.exe <операция> <входной файл> -O <файл для записи>

Использование:

- при проверке ЭЦП: в данный файл будет записано значение идентификаторов открытых ключей, проверка ЭЦП которых прошла успешно (см. **пп. 3.2.3. Проверка ЭЦП (-v)** и **3.2.4. Проверка ЭЦП без записи исходного файла (-V))**;

Пример:

```
AvCmUt4.exe –v test.txt.p7s -O ip.txt
```

- при вычислении значений функций хэширования Belt и Bhf **(см. п. 3.5. Функции вычисления значений хэширования);**

Пример:

```
AvCmUt4.exe –v test.txt.p7s -O ip.txt
```

- при выполнении операции Обновление СОС и сертификатов УЦ (**см. п. 3.6.3. Обновление СОС и сертификатов УЦ онлайн (-CDP)).**

Пример:

```
AvCmUt4.exe –CDP CrlDPExt.txt -O result.txt
```

4.2.3. Указание файла документа для проверки раздельной ЭЦП (-F)

AvCmUt4.exe <операция> <входной файл> -F <файл с исходным документом>

Используется при проверке ЭЦП, в случае, если при выработке ЭЦП исходный документ не был включен в подписываемое сообщение (см. **п. 4.4.4. Не включать исходный документ в подписываемое сообщение (-T)**). При проверке отделенной ЭЦП запись выходного файла не производится.

Пример:

```
AvCmUt4.exe -v test.txt.p7s -F test.txt
```

Также параметр –F используется при выработке дополнительной ЭЦП к файлу с раздельной ЭЦП (как выработать дополнительную ЭЦП см. в **п. 3.2.2. Выработка дополнительной ЭЦП (–S)).**

Пример:

```
AvCmUt4.exe -S test.txt.p7s -o out.txt.p7s -F test.txt
```

4.2.4. Указание файла шаблона на сертификат (-t)

AvCmUt4.exe <операция> <входной файл> -t <файл шаблона>

Необязательный параметр. Используется при генерации запроса на сертификат (см. **п.3.6.4. Запуск мастера генерации запроса на сертификат (-r)**).

Параметр указывает имя файла, в котором находится шаблон запроса на сертификат, для генерации запроса на сертификат с использованием данного шаблона.

Пример:

```
AvCmUt4.exe -r request.req –t face.tpl
```

4.2.5. Указание папки для помещения выходных файлов (-P)

AvCmUt4.exe <операция> <входной файл> -P <имя папки>

Пример:

```
AvCmUt4.exe –s test.txt -P "c:\out"
```

- выработка ЭЦП для файла test.txt с указанием папки c:\out для помещения выходного файла test.txt.p7s.

4.2.6. Указание файла лога для выводов результатов выполнения операций (-LOG)

AvCmUt4.exe <операция> <входной файл> -LOG <файл лога>

Если данный параметр не задан, то по умолчанию файл лога AvCmUt4.log создается в текущей папке (в папке, из которой была запущена командная строка).

Пример:

```
AvCmUt4.exe –s test.txt -LOG "c:\LOG_FOLDER\AvCmUt4.log"
```

- выработка ЭЦП для файла test.txt с указанием файла c:\LOG_FOLDER\AvCmUt4.log для записи результатов выполнения операции.

4.2.7. Запрет на запись лога (-LOG NUL)

AvCmUt4.exe <операция> <входной файл> -LOG NUL

Пример:

```
AvCmUt4.exe –s test.txt -LOG NUL
```

4.3. Дополнительные параметры для выбора сертификатов при проверке ЭЦП и зашифровании

Данные параметры могут быть указаны при зашифровании для выбора получателя зашифрованного сообщения и при проверке ЭЦП для выбора тех ЭЦП, которые надо проверить.

4.3.1. Указание Common Name (-c)

AvCmUt4.exe <операция> <входной файл> -c <Common Name>

Параметр используется для указания общих данных (наименование организации, Ф. И. О. владельца сертификата открытого ключа и т.д.).

Пример:

```
AvCmUt4.exe –v test.p7s -c "ALEXEY IVANOV"
```

– проверка ЭЦП в файле test.p7s с отбором сертификатов, владельцем которых является ALEXEY IVANOV.

4.3.2. Указание атрибута субъекта (-X)

AvCmUt4.exe <операция> <входной файл> -X <OID>=<значение>

Таких параметров в командной строке может быть указано несколько, при этом будет производится отбор сертификатов, в которых установлены **все** указанные атрибута субъекта.

Пример:

```
AvCmUt4.exe –v test.p7s -X 2.5.4.10="ЗАО ""Организация"""
```

– проверка ЭЦП в файле test.p7s с отбором сертификатов, выпущенных на организацию ЗАО "Организация"

4.3.3. Указание дополнения, имеющегося в сертификате в текстовом виде (-x)

AvCmUt4.exe <операция> <входной файл> -x <OID>=<значение>

Таких параметров в командной строке может быть указано несколько, при этом будет производится отбор сертификатов, в которых установлены **все** указанные дополнения.

Пример:

```
AvCmUt4.exe –e test.txt -x rfc822Name=test@email.org
```

– зашифрование файла test.txt на пользователей, в сертификатах которых указан адрес электронной почты test@email.org.

4.3.4. Указание OID расширенного применения ключа (–u)

AvCmUt4.exe <операция> <входной файл> -u <OID>

Таких параметров в командной строке может быть указано несколько, при этом будет производится отбор сертификатов, в которых установлены **все** указанные расширенные применения ключа.

Пример:

```
AvCmUt4.exe –e test.txt -u 1.3.6.1.4.1.12656.101.1.1
```

– зашифрование файла test.txt на пользователей, в сертификатах которых установлено расширенное применение ключа с OID 1.3.6.1.4.1.12656.101.1.1. В данном примере производится отбор сертификатов, имеющих расширенное применение ключа “Подпись документов на банк”.

Данные параметры отбора сертификатов (**-c, -x, -X, -u**) могут использоваться совместно, при этом производится отбор сертификатов, удовлетворяющих **всем** указанным условиям.

4.3.5. Указание идентификатора открытого ключа сертификата (-k)

AvCmUt4.exe <операция> <входной файл> -k <идентификатор>

Таких параметров в командной строке может быть указано несколько, будут отобраны сертификаты с указанными идентификаторами.

Идентификатор открытого ключа является уникальным параметром. При его указании задавать остальные параметры не следует.

Пример:

```
AvCmUt4.exe –e test.txt -k
4B5CAFE0235786E28FB55744A756C9B91E822E66 –k
462D8D14A47BA35B3DB7DDF5BE51CD06D9EDD337
```

– зашифрование файла test.txt на два сертификата с идентификаторами открытого ключа 4B5CAFE0235786E28FB55744A756C9B91E822E66 для одного и 462D8D14A47BA35B3DB7DDF5BE51CD06D9EDD337 для другого.

4.3.6. Контроль атрибутов атрибутного сертификата (сертификатов) при выработке и проверке ЭЦП (-A)

AvCmUt4.exe <операция> <входной файл> -A <OID>=<значение>

Таких параметров в командной строке может быть указано несколько, при этом будет производится отбор атрибутных сертификатов, в которых установлены **все** указанные атрибуты.

При выработке ЭЦП (см. пп. 3.2.1. Выработка ЭЦП входного файла (-s) и 3.2.2. Выработка дополнительной ЭЦП (–S)), производится поиск атрибутного сертификата удовлетворяющего параметром контроля, найденный сертификат помещается в подписанное сообщение.

При проверке ЭЦП (см. **пп. 3.2.3. Проверка ЭЦП (-v)** и **3.2.4. Проверка ЭЦП без записи исходного файла (-V)**), проверяется соответствие сертификата параметрам контроля, если сертификат не удовлетворяет параметрам контроля, производится поиск атрибутных сертификатов в сообщении и хранилище сертификатов и проверяется

соответствие параметрам контроля, а также действительность атрибутного сертификата. Если требуемый атрибутный сертификат не найден, ЭЦП считается недействительной.

Примеры:

```
AvCmUt4.exe -s input.txt –A 1.2.112.1.2.1.1.1.1.2=123456789
```

- добавление атрибутного сертификата в подписанное сообщение (атрибут: УНП=123456789):

```
AvCmUt4.exe -v output.p7s –A 1.2.112.1.2.1.1.1.1.2=123456789
```

- проверка ЭЦП для организации с УНП 123456789

4.4. Флаги, позволяющие не включать сертификаты, СОС, исходный документ в подписанное сообщение

4.4.1. Не включать сертификаты в подписанное сообщение (-m)

AvCmUt4.exe <операция> <входной файл> -m

По умолчанию в подписываемое сообщение включаются вся цепочка сертификатов от сертификатов корневого и подчиненного удостоверяющих центров до сертификата подписывающего и все соответствующие списки отозванных сертификатов. При указании данного флага цепочка сертификатов в подписанное сообщение включаться не будет. Используются для операций выработки ЭЦП/дополнительной ЭЦП (см. **пп. 3.2.1. Выработка ЭЦП входного файла (-s)** и **3.2.2. Выработка дополнительной ЭЦП (–S)**).

Пример:

```
AvCmUt4.exe –s test.txt -m
```

4.4.2. Не включать сертификаты издателей в подписанное сообщение (-m1)

AvCmUt4.exe <операция> <входной файл> -m1

При указание данного флага в подписанное сообщение будет включаться только личный сертификат подписанта без сертификатов удостоверяющих центров и списков отозванных сертификатов.
Используются для операций выработки ЭЦП/дополнительной ЭЦП (см. **пп. 3.2.1. Выработка ЭЦП входного файла (-s)** и **3.2.2. Выработка дополнительной ЭЦП (–S)**).

Пример:

```
AvCmUt4.exe –s test.txt –m1
```

4.4.3. Не включать СОС в подписанное сообщение (-M)

AvCmUt4.exe <операция> <входной файл> -M

При указание данного флага в подписанное сообщение будет включаться только личный сертификат подписанта и сертификаты издателей без списков отозванных сертификатов.

Используются для операций выработки ЭЦП/дополнительной ЭЦП (см. **пп. 3.2.1. Выработка ЭЦП входного файла (-s)** и **3.2.2. Выработка дополнительной ЭЦП (–S)**).

Пример:

```
AvCmUt4.exe –s test.txt –M
```

4.4.4. Не включать исходный документ в подписываемое сообщение (-T)

AvCmUt4.exe <операция> <входной файл> -T

Данный флаг указывается при необходимости выработки раздельной ЭЦП, т.е. подписи файла без сохранения исходного документа в выходном файле.
Используются для операций выработки ЭЦП/дополнительной ЭЦП (см. **пп. 3.2.1. Выработка ЭЦП входного файла (-s)** и **3.2.2. Выработка дополнительной ЭЦП (–S)**).

Пример:

```
AvCmUt4.exe –s test.txt –T
```

При проверке отделенной ЭЦП нужно указать файл с исходным документом с использованием параметра **–F** (см. **п. 4.2.3. Указание файла документа для проверки раздельной ЭЦП (-F)**), запись выходного файла при этом производиться не будет.
Для выработки дополнительной ЭЦП к файлу с отделенной ЭЦП параметр –T не применяется, указывается файл с исходным документом с использованием параметра **–F**, (см. **п. 4.2.3. Указание файла документа для проверки раздельной ЭЦП (-F)**).

4.5. Дополнительные флаги

4.5.1. Заменить существующий файл (-R)

AvCmUt4.exe <операция> <входной файл> -R

Используется в случае, если имя выходного файла совпадает с именем файла, уже существующего в указанной папке, и надо его перезаписать.

Пример:

```
AvCmUt4.exe –V test.txt.p7s –R
```

4.5.2. Установить дату и время выходного файла равной дате и времени входного файла (-a)

AvCmUt4.exe <операция> <входной файл> -a

Пример:

```
AvCmUt4.exe –V test.txt.p7s –a
```

4.5.3. Операцию выполнять, если хотя бы один из сертификатов удовлетворяет условию (-n)

AvCmUt4.exe <операция> <входной файл> -n

Используется:

1. при проверке ЭЦП (см. **пп. 3.2.3. Проверка ЭЦП (-v)** и **3.2.4. Проверка ЭЦП без записи исходного файла (-V);**

Пример:

```
AvCmUt4.exe –v test.txt.p7s –n
```

2. при проверке ответа OCSP сервера проверки статуса сертификата/атрибутного сертификата (см. **п. 5. Проверка статуса сертификата по протоколу OCSP**);

Пример:

```
AvCmUt4.exe –v out.p7s.p7s –o result.txt –VERIFYTIME SIGNTIME –n
```

- проверяется файл с дополнительной ЭЦП, ответ OCSP был добавлен при выработке только дополнительной ЭЦП, если бы параметр –n не был указан, то была бы ошибка **Ошибка: OCSP ответ для данного сертификата отсутствует в сообщении;**

3. при зашифровании на получателя (см. **п. 4.3. Дополнительные параметры для выбора сертификатов при проверке ЭЦП и зашифровании**).

Пример:

```
AvCmUt4.exe –e test.txt -k
4B5CAFE0235786E28FB55744A756C9B91E822E66 –k
462D8D14A47BA35B3DB7DDF5BE51CD06D9EDD337 –n
```

4.5.4. Просмотр ЭЦП сообщений (-VIEWMSG)

AvCmUt4.exe <операция> <входной файл> -VIEWMSG

Использование:

- при проверке ЭЦП (см. **пп. 3.2.3. Проверка ЭЦП (-v)** и **3.2.4. Проверка ЭЦП без записи исходного файла (-V);**
- при выработке дополнительной ЭЦП (см. **п. 3.2.2. Выработка дополнительной ЭЦП (–S)**);
- при ONLINE проверке статуса сертификата/атрибутного сертификата (см. **пп. 5.1. ONLINE проверка статуса сертификата (-L) и 5.2. ONLINE проверка статуса атрибутного сертификата (-LA)**);
- при проверке ЭЦП сообщений, содержащих ответ OCSP сервера проверки статуса сертификата/атрибутного сертификата, в том числе с использованием параметра **–VERIFYTIME** (см. **п. 5.5. Проверять статус сертификата на указанное время (-VERIFYTIME));**
- при выработке/проверке контрподписи (см. **п. 6. Выработка контрподписи**).

Данный параметр открывает окно просмотра ЭЦП в графическом интерфейсе.

Окно просмотра ЭЦП состоит из четырех закладок (открываются в левой части окна):

- Общие (сведения о цифровой подписи),

- Атрибуты подписи,
- Атрибуты сертификата,
- Путь проверки (показана вся цепочка сертификатов, удостоверяющих данный сертификат, до корневого).

Правая часть окна состоит из трех полей:

- ЭЦП сообщения,
- Контент (отображается содержимое сообщения),
- Сертификаты/СОС, добавленные в сообщение.

Закладка «Общие».

Отображается информация о субъекте-подписанте, а также дата и время подписи (см. Рисунок 1. Закладка «Общие»).

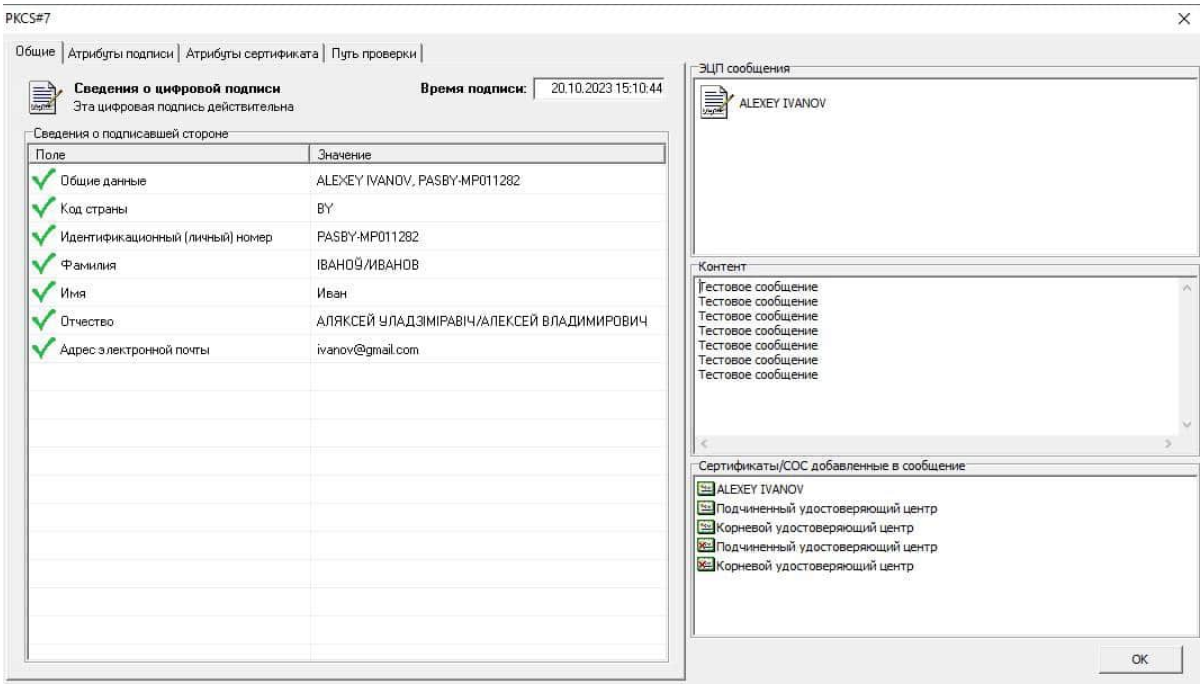

Рисунок 1. Закладка «Общие»

Закладка «Атрибуты подписи».

Отображается информация об атрибутах подписи (версия, поставщик сертификата-подписанта, алгоритм выработки и т.д.). При выборе одного из полей внизу панели будет отображена информация о его составе (см. Рисунок 2. Закладка «Атрибуты подписи»).

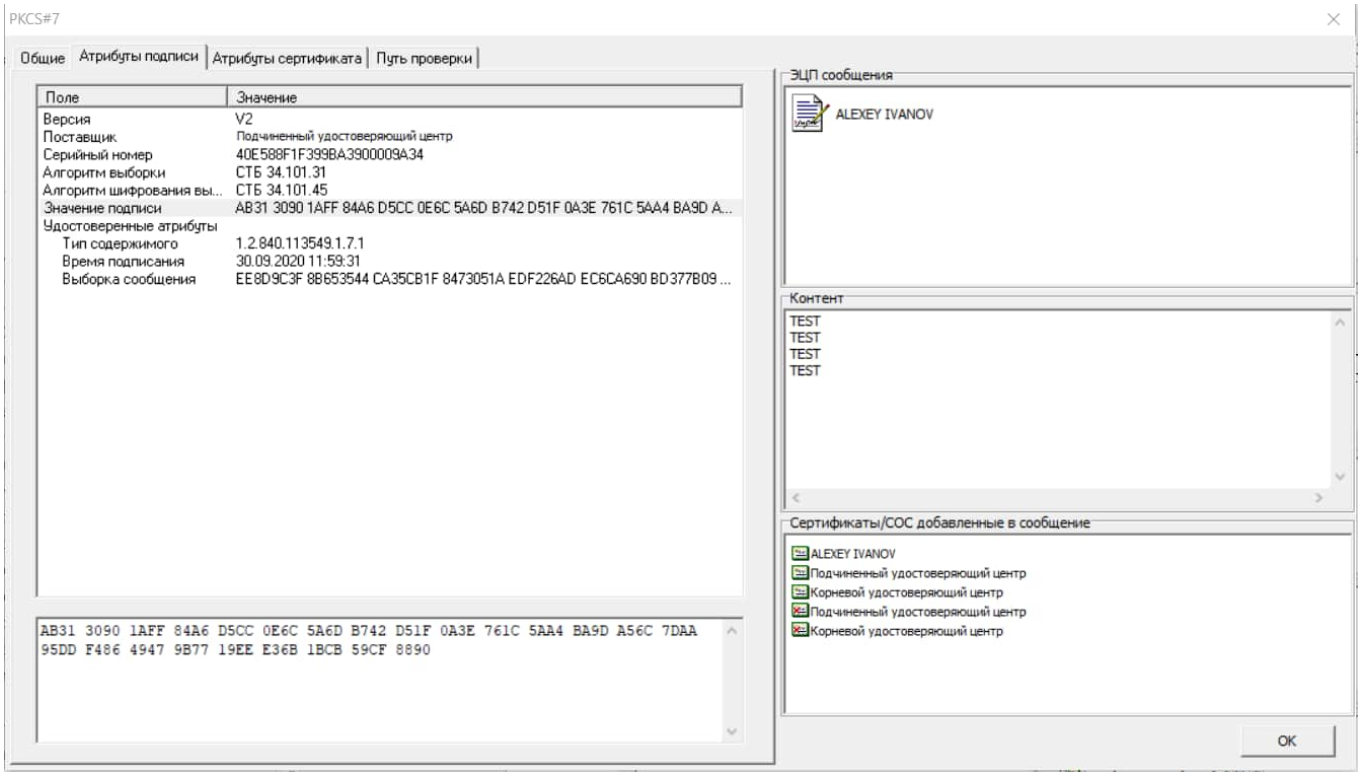

Рисунок 2. Закладка «Атрибуты подписи»

Закладка «Атрибуты сертификата».

В данной панели можно увидеть точный состав сертификата, в том числе его серийный номер, алгоритм подписи, открытый ключ сертификата и т.д. (см. Рисунок 3. Закладка «Атрибуты сертификата»).

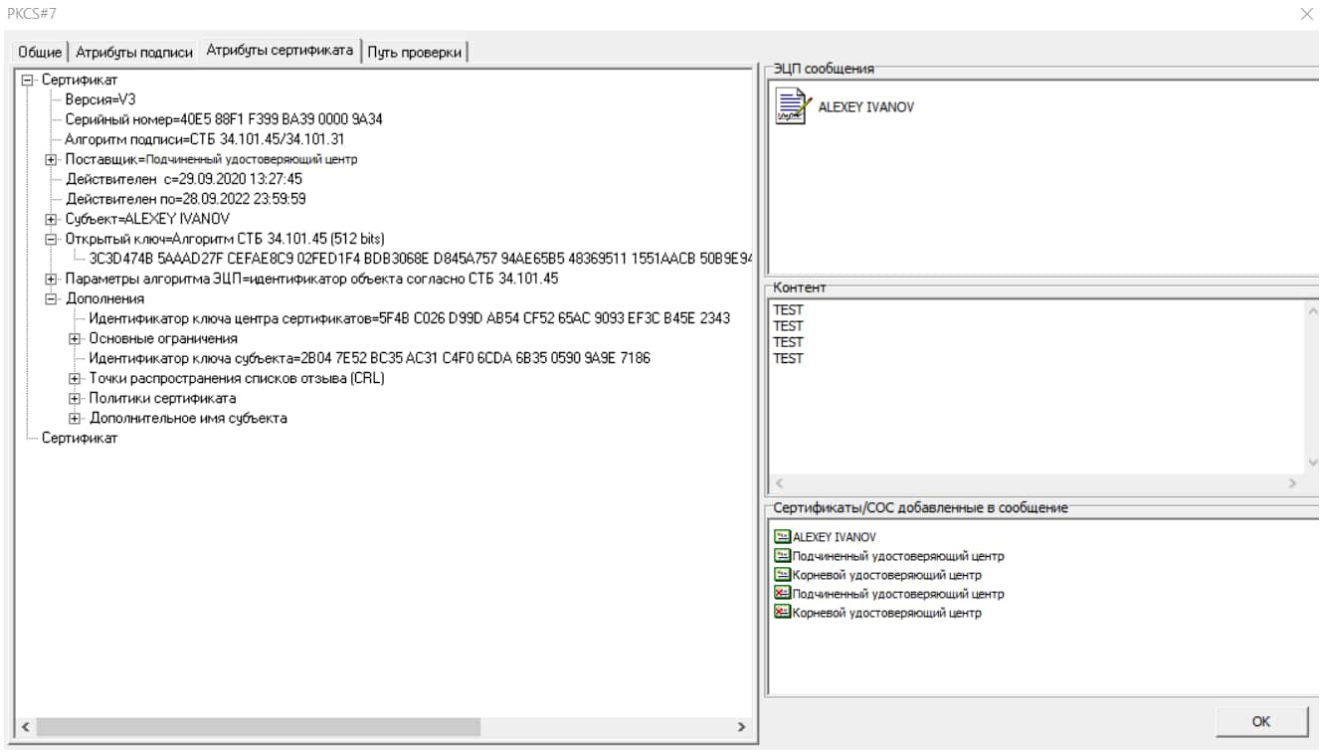

Рисунок 3. Закладка «Атрибуты сертификата»

Закладка «Путь проверки».

В данной панели можно увидеть, каким сертификатом был выдан сертификат подписанта, и в каком списке отозванных сертификатов он был проверен (см. Рисунок 4. Закладка «Путь проверки»).

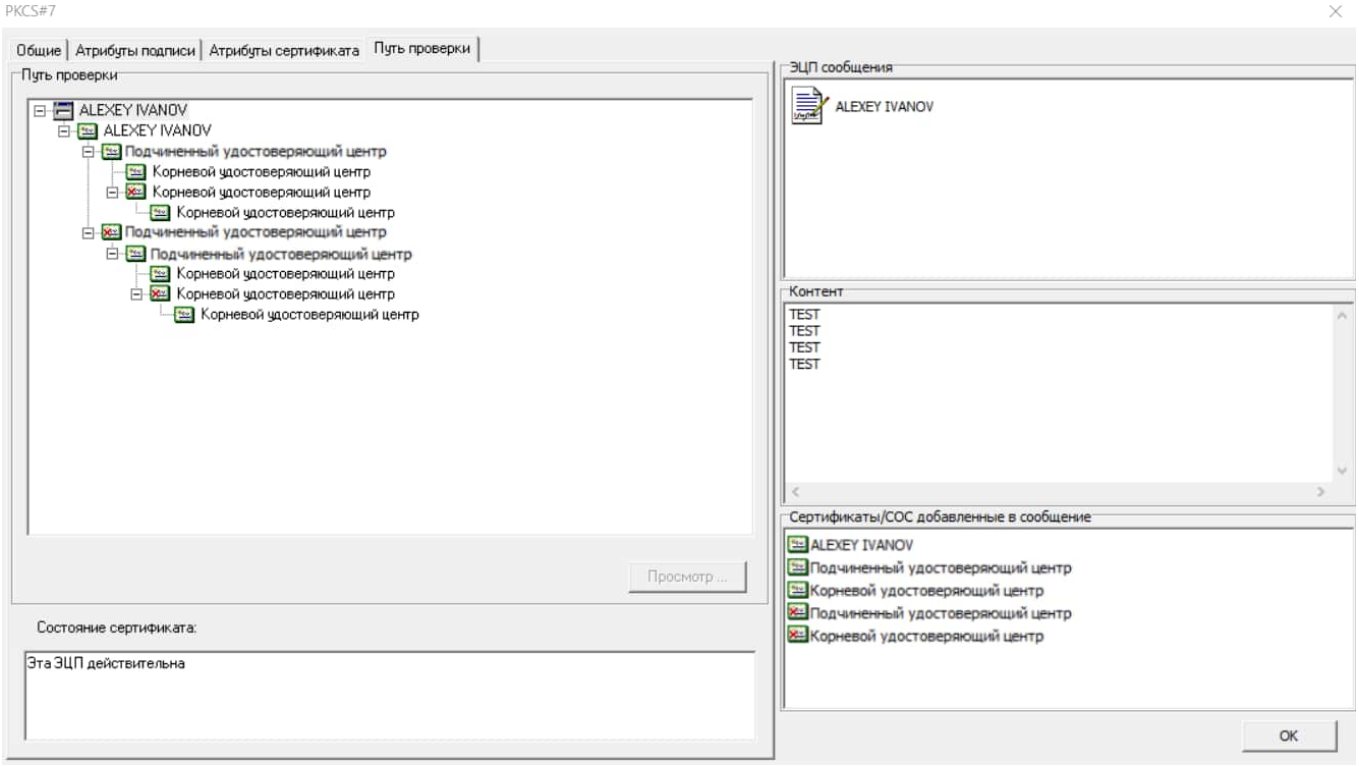

Рисунок 4. Закладка «Путь проверки»

Если при проверке какого-либо из показанных сертификатов или при проверке СОС возникла какая-либо ошибка, например, неверная подпись, сертификат будет отображен с крестиком в красном круге. Внизу панели будет отображена информация о результате проверки цепочки сертификатов и СОС.

Также в окне Путь проверки будет отображаться сведения о контрподписи (в случае ее наличия в сообщении) и ответ OCSP сервера (если в сообщение добавлен такой ответ или если в менеджере сертификатов прописаны настройки подключения к OCSP).

При проверке сообщений, содержащих ответ OCSP сервера, надо иметь в виду, что срок действия данного ответа ограничен настройками сервера (по умолчанию 2 часа с момента добавления), соответственно при истечении данного времени при просмотре ЭЦП в ответе OCSP будет ошибка: **Срок действия OCSP ответа истек.**

Примеры вывода окна просмотра ЭЦП в сообщения с ответами OCSP и контрподписью:

1. Проверка ЭЦП и ответа OCSP сервера в файле out.p7s (в файл добавлен ответ OCSP сервера проверки статуса личного и атрибутного сертификатов) с контролем атрибута атрибутного сертификата УНП=123456789:

```
AvCmUt4.exe -v out.p7s -o result.txt -A
1.2.112.1.2.1.1.1.1.2=123456789 -VERIFYTIME "2020-08-28 1:00:00"
-VIEWMSG
```

Результат выполнения в командной строке (ответ OCSP сервера: личный и атрибутный сертификаты **действительны**):

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result.txt
Проверка ЭЦП
Дата/время подписи: 28.08.2020 16:28:16
Найден атрибутный сертификат серийный номер:
40E584F5A10B9AF700008BD6
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 28.08.2020 16:28:13
Сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
Субъект:
<…>
Серийный номер сертификата: 40E584D7FB79CF190000CCFF
Идентификатор открытого ключа:
F234E2B84DFD55CA64E5DA375A06A313B3629E8D
ЭЦП сообщения верна
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 28.08.2020 16:28:14
Сертификат действителен
ЭЦП действительна
```

Окно просмотра ЭЦП, если с момента добавления ответа OCSP сервера прошло менее 2 часов (см. Рисунок 5. Вывод окна просмотра ЭЦП при проверке сообщения с добавленным ответом OCSP сервера, вкладка «Путь проверки»):

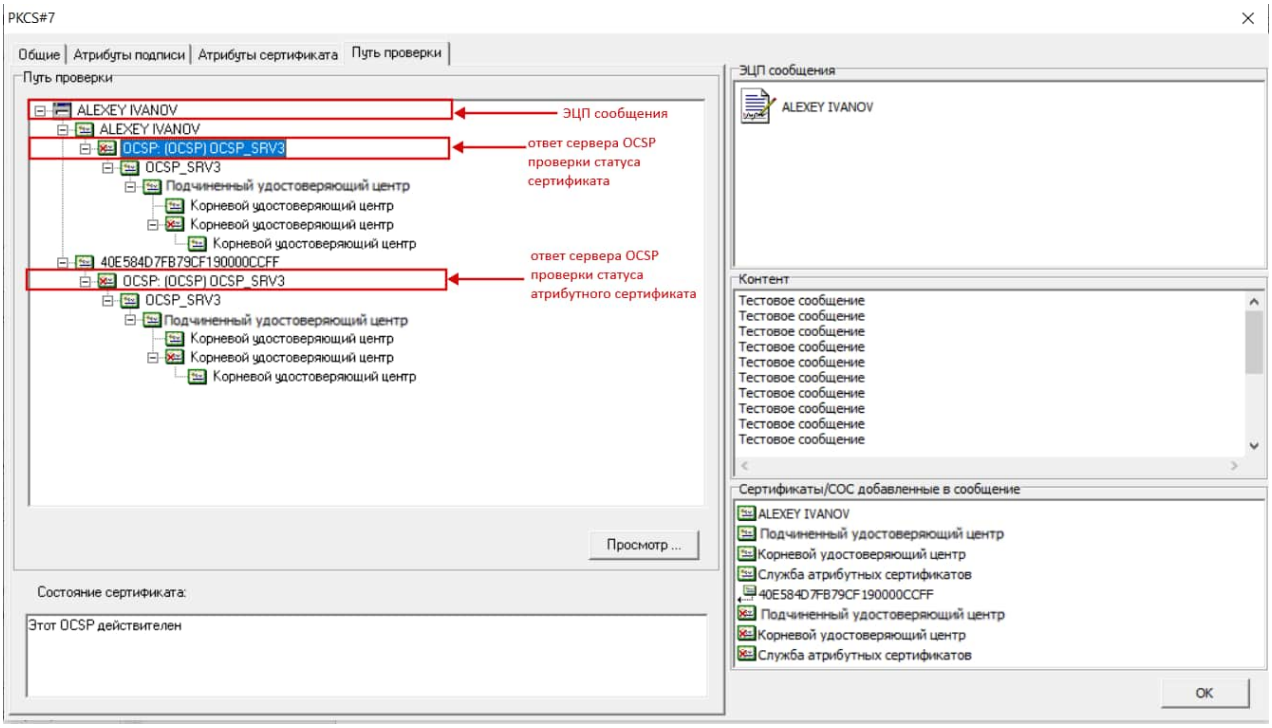

Рисунок 5. Вывод окна просмотра ЭЦП при проверке сообщения с добавленным ответом OCSP сервера, вкладка «Путь проверки»

Окно просмотра ЭЦП, если срок действия ответа OCSP сервера истек (см. Рисунок 6. Вывод окна просмотра ЭЦП при проверке сообщения с добавленным ответом OCSP сервера, вкладка «Путь проверки» (срок действия ответа OCSP сервера истек):

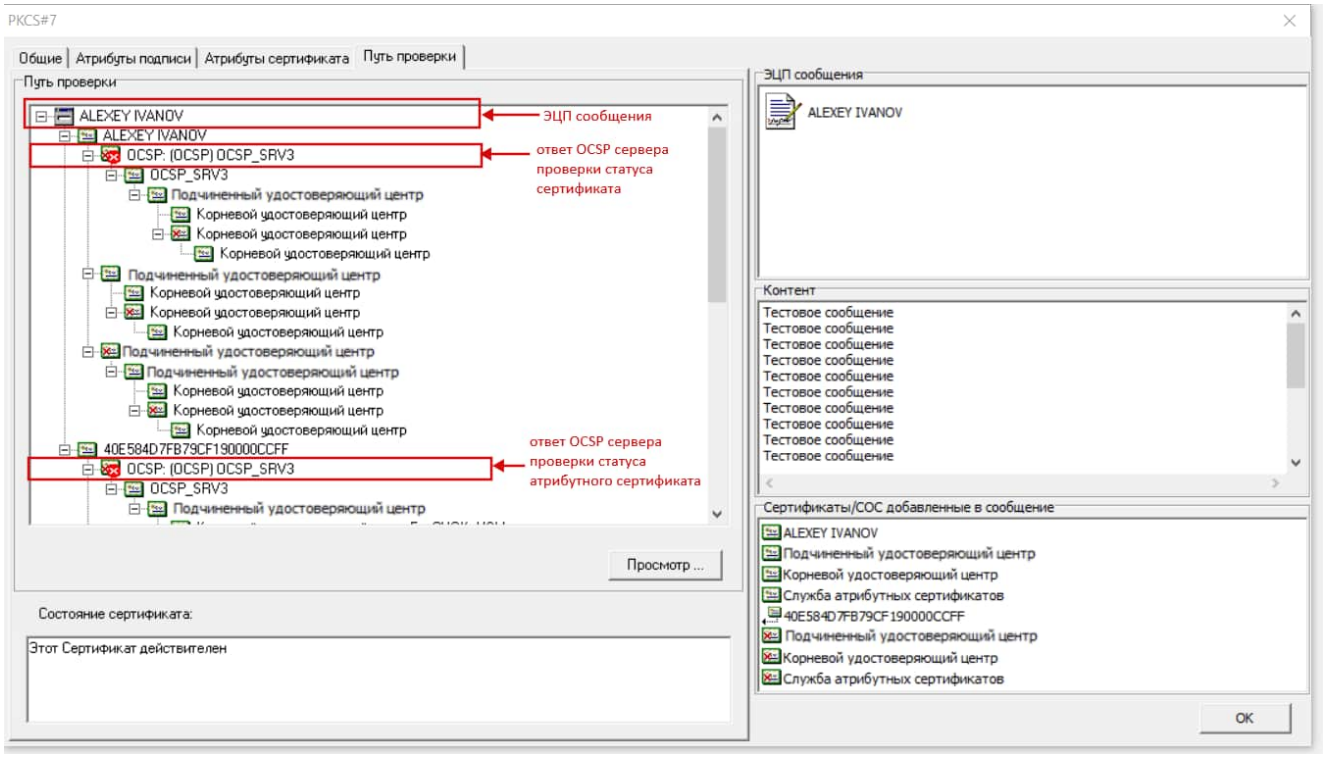

Рисунок 6. Вывод окна просмотра ЭЦП при проверке сообщения с добавленным ответом OCSP сервера, вкладка «Путь проверки» (срок действия ответа OCSP сервера истек)

2. Проверка ЭЦП, контрподписи и подписи, удостоверяющей контрподпись, в файле test.p7s.p7s.p7s без авторизации с выводом окна просмотра ЭЦП сообщения:

```
AvCmUt4.exe -v test.p7s.p7s.p7s –o result –NA -VIEWMSG
```

Результат выполнения в командной строке:

```
Проверка ЭЦП
Обработка файла: test.txt.p7s.p7s.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 03.09.2020 12:41:21
Субъект: CN=ALEXEY IVANOV
<>
Серийный номер сертификата: 40E584D7FB79CF190000CCFF
Идентификатор открытого ключа:
F234E2B84DFD55CA64E5DA375A06A313B3629E8D
ЭЦП сообщения верна
Сертификат действителен
ЭЦП удостоверена. Проверка контрподписей
Подпись удостоверил:
   Субъект: CN="OAO ""Тестовая организация
<>
   Серийный номер сертификата: 40E584F7DC59308C0000CFFB
   Идентификатор открытого ключа:
0AA65A9D0F89FE37B315795AF464CECC40480757
   Дата/время подписи: 03.09.2020 12:41:52
ЭЦП удостоверяющей подписи верна
Удостоверяющая подпись удостоверена. Проверка
удостоверяющих подписей
Подпись удостоверил:
   Субъект: CN="Piotr Brouka
<>
   Серийный номер сертификата: 40E574104CBFCA36000000D6
   Идентификатор открытого ключа:
E6A3BE26A9B7D9AA31AD5B2479B56A0AC5DD9294
   Дата/время подписи: 03.09.2020 12:42:31
ЭЦП удостоверяющей подписи верна
Сертификат действителен
ЭЦП действительна
```

Окно просмотра ЭЦП, вкладка «Путь проверки» (см. Рисунок 7. Вывод окна просмотра ЭЦП с контрподписью и подписью, удостоверяющую контрподпись, вкладка «Путь проверки»):

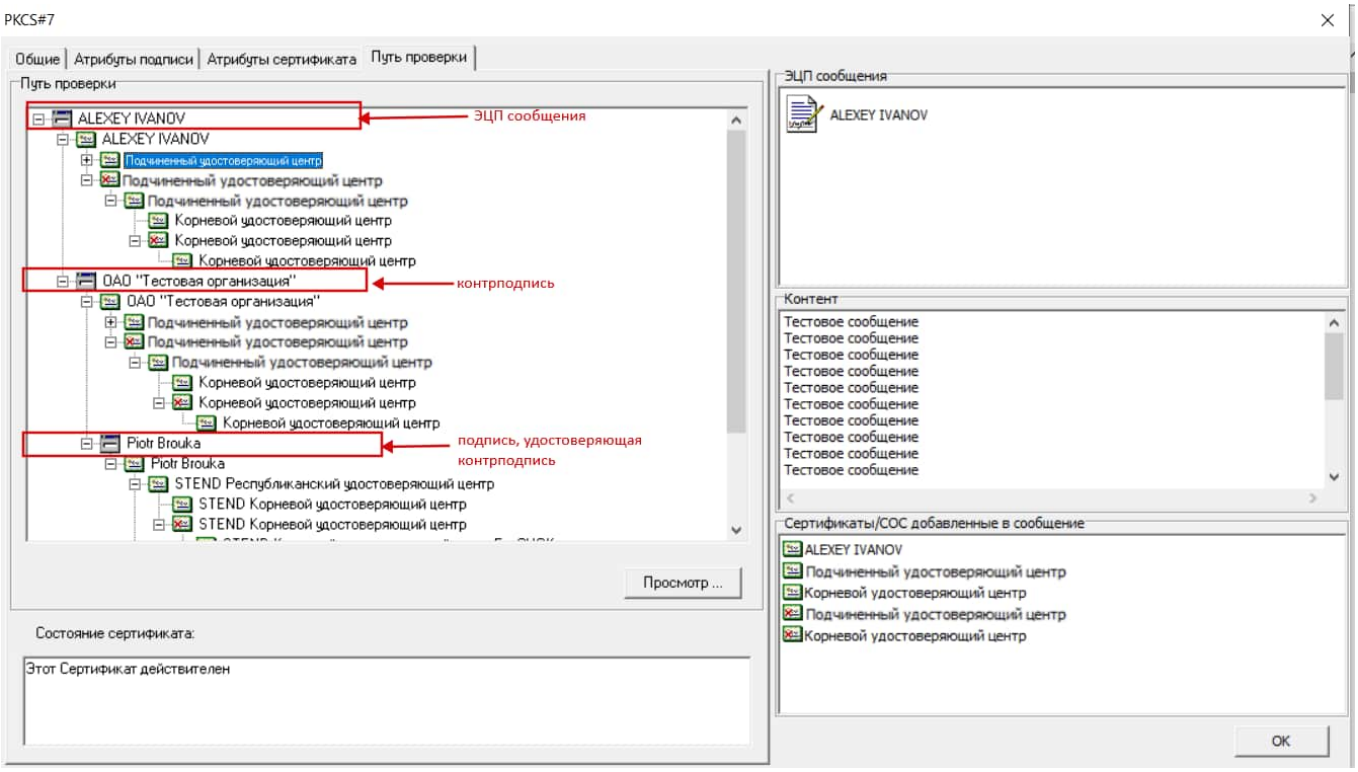

Рисунок 7. Вывод окна просмотра ЭЦП с контрподписью и подписью, удостоверяющую контрподпись, вкладка «Путь проверки»

5. ПРОВЕРКА СТАТУСА СЕРТИФИКАТА ПО ПРОТОКОЛУ OCSP

При проверке статуса сертификата по протоколу OCSP формируется запрос в службу OCSP и его отправка по адресу, прописанному в сертификате или указанному в настройках конфигурационного файла AvCmMsg.ini, который находится в папке с установленным ПК AvPCM (подробнее см. **Программный комплекс «Персональный менеджер сертификатов Авест» Руководство оператора, п. 6.14.3. Настройка автоматической проверки статуса сертификата (атрибутного сертификата) при помощи сервиса онлайн-проверки сертификата (OCSP-сервера)).**

Возможны 3 статуса действительности сертификатов:

- действителен:
  - выполняются все условия действительности сертификата;
- недействителен:
  - срок действия сертификата истек,
  - от OCSP сервера получен ответ "Сертификат отозван",
  - не строится цепочка сертификации,
  - сертификат имеет некорректную ЭЦП;
- неизвестен.

В случае отсутствия и в сертификате, и в настройках менеджера сертификатов адреса OCSP или указания несуществующего адреса, недоступности OCSP сервера, отсутствия Интернет подключения и т.д. при ONLINE проверке статуса сертификата будет возвращаться **Ошибка при обращении к OCSP серверу.**

5.1. ONLINE проверка статуса сертификата (-L)

AvCmUt4.exe <операция> <входной файл> -L

Используется при проверке ЭЦП (см. **пп. 3.2.3. Проверка ЭЦП (-v)** и **3.2.4. Проверка ЭЦП без записи исходного файла (-V)**).

Выходной файл будет записан вне зависимости от ответа OCSP сервера (если использовать команду –v).

Пример:

Проверка ЭЦП в файле out.p7s с проверкой статуса сертификата подписанта:

```
AvCmUt4.exe –v out.p7s –o result.txt –L
```

Результат выполнения в командной строке, **сертификат подписанта действителен:**

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result.txt
Дата/время подписи: 06.03.2017 11:15:19
Субъект:
<…>
Серийный номер сертификата: 40E427ECAB5910B40003E3F7
```

```
Идентификатор открытого ключа:
  40D0C8DA3AB10ED832810FB4337FFB73A7009E0C
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 11:16:59
Сертификат действителен
ЭЦП действительна
```

Результат выполнения в командной строке, **сертификат подписанта недействителен:**

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result.txt
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:51:02
Субъект:
<…>
Серийный номер сертификата: 40E427ECAB5910B40003E3F7
Идентификатор открытого ключа:
  40D0C8DA3AB10ED832810FB4337FFB73A7009E0C
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:51:01
Сертификат не действителен: Сертификат отозван.
Ошибка: Сертификат не действителен
```

Результат выполнения в командной строке, **статус сертификата подписанта неизвестен:**

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result.txt
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:58:34
Субъект:
<…>
Серийный номер сертификата: 40E427ECAB5910B40003E3F7
Идентификатор открытого ключа:
  40D0C8DA3AB10ED832810FB4337FFB73A7009E0C
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:01:37
Сертификат не действителен: OCSP-серверу не удалось
  определить статус сертификата
Ошибка: Сертификат не действителен
```

Результат выполнения в командной строке, **ошибка при обращении к OCSP серверу:**

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result.txt
Проверка ЭЦП
```

```
Дата/время подписи: 06.03.2017 11:22:06
Субъект:
<…>
Серийный номер сертификата: 40E427ECAB5910B40003E3F7
Идентификатор открытого ключа:
  40D0C8DA3AB10ED832810FB4337FFB73A7009E0C
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ошибка: Ошибка при обращении к OCSP серверу: OCSP сервис
  для данного сертификата не задан
```

5.2. ONLINE проверка статуса атрибутного сертификата (-LA)

AvCmUt4.exe <операция> <входной файл> -LA

Используется при выработке/проверке ЭЦП (см. **п. 3.2. Функции выработки ЭЦП**).

При выработке ЭЦП выходной файл будет записан, если статус атрибутного сертификата – действителен.

При проверке ЭЦП выходной файл будет записан вне зависимости от результатов проверки (если использовать команду –v).

При проверке ЭЦП одновременно с онлайн проверкой статуса атрибутного сертификата происходит проверка статуса личного сертификата подписанта.

Примеры:

1. Выработка ЭЦП с добавлением атрибутного сертификата с атрибутом Учетный номер плательщика=123456789 и проверкой его статуса:

```
AvCmUt4.exe -s test.txt -o out.p7s -A
1.2.112.1.2.1.1.1.1.2=789456123 –LA
```

Результат выполнения в командной строке, **атрибутный сертификат** с заданным параметром **действителен**:

```
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:36:48
Атрибутный сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
Выработка ЭЦП
Обработка файла: test.txt
Запись файла out.p7s
```

Результат выполнения в командной строке, **атрибутный сертификат** с заданным параметром **недействителен**:

```
Найден атрибутный сертификат серийный номер:
40E4E0D04624B7E70000001A
Получение статуса атрибутного сертификата от OCSP сервера
```

```
Ответ OCSP сервера от 06.03.2017 17:45:45
Атрибутный сертификат не действителен: Сертификат
отозван.
Ошибка: Не найден требуемый атрибутный сертификат
```

2. Проверка ЭЦП в файле out.p7s с атрибутным сертификатом (параметр контроля - атрибут Учетный номер плательщика=123456789) и проверкой его статуса:

```
AvCmUt4.exe -v out.p7s -o result -A
1.2.112.1.2.1.1.1.1.2=123456789 -LA
```

Результат выполнения в командной строке, **личный сертификат действителен, атрибутный сертификат** с заданным параметром **действителен**:

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:37:07
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:40:27
Атрибутный сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
Субъект:
<…>
Серийный номер сертификата: 40E4D9553E59321A0000419B
Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:40:27
Сертификат действителен
ЭЦП действительна
```

Результат выполнения в командной строке **личный сертификат недействителен, атрибутный сертификат** с заданным параметром **действителен**:

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:37:07
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:46:43
Атрибутный сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
```

```
Субъект:
<…>
Серийный номер сертификата: 40E4D9553E59321A0000419B
Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:46:43
Сертификат не действителен: Сертификат отозван.
Ошибка: Сертификат не действителен
```

Результат выполнения в командной строке **личный сертификат действителен, атрибутный сертификат** с заданным параметром **недействителен**:

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:37:07
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:44:53
Атрибутный сертификат не действителен: Сертификат
отозван.
Параметры отбора сертификата не подходят для проверки ЭЦП
№1
Ошибка: В сообщении нет подходящих подписей
```

Результат выполнения в командной строке **личный сертификат действителен, статус атрибутного сертификата** с заданным параметром **неизвестен**:

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 17:06:47
Найден атрибутный сертификат серийный номер:
40E4E0D04624B7E70000001A
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:07:27
Атрибутный сертификат не действителен: OCSP-серверу не
удалось определить статус сертификата
Параметры отбора сертификата не подходят для проверки ЭЦП
№1
Ошибка: В сообщении нет подходящих подписей
```

5.3. Добавить в сообщение ответы сервера OCSP проверки статуса сертификата (-ADDOCSP)

AvCmUt4.exe <операция> <входной файл> -ADDOCSP

Использование:

1. **При выработке ЭЦП (**см. **пп. 3.2.1. Выработка ЭЦП входного файла (-s)** и **3.2.2. Выработка дополнительной ЭЦП (–S)).**

   Добавляется при выработке ЭЦП/дополнительной ЭЦП (параметр -s/-S).

   Если параметр «выходной файл», не указан подписанный документ будет записан в файл с расширением «.p7s».

   При выработке ЭЦП выходной файл будет записан в случае, если ответ от OCSP сервера будет: статус сертификата **действителен** или **недействителен** и не будет записан в случае, если статус сертификата **неизвестен** или произошла **ошибка при обращении к OCSP серверу.**

2 **При проверке ЭЦП с использованием параметра -V (**см. **п. 3.2. Функции выработки ЭЦП)**

   При этом допускается задание выходного файла параметром –o (см. **п. 4.2.1**. **Указание выходного файла (-o)**). Если параметр «выходной файл» не был задан, выходной файл с ответом сервера будет записан в файл с расширением «.p7s».

   При проверке ЭЦП выходной файл с ответом OCSP сервера будет записан в случае отсутствия **ошибки при обращении к OCSP серверу.**

Примеры:

1. Выработка ЭЦП с добавлением ответа OCSP сервера:

```
AvCmUt4.exe -s test -o out.p7s -ADDOCSP
```

Результат выполнения в командной строке, **сертификат действителен**:

```
Выработка ЭЦП
Обработка файла: test.txt
Получение статуса личного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:30:41
Синхронизация времени с сервером OCSP, текущее время:
06.03.2017 17:30:40
Сертификат действителен
Ответ OCSP сервера добавлен в сообщение
Запись файла out.p7s
```

Результат выполнения в командной строке, **сертификат недействителен**:

```
Выработка ЭЦП
Обработка файла: test.txt
```

```
Получение статуса личного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:10:55
Сертификат не действителен
Ответ OCSP сервера добавлен в сообщение
Запись файла out.p7s
```

В обоих случаях будет записан выходной файл out.p7s, содержащий ЭЦП и ответ OCSP сервера проверки статуса сертификата.

2. Проверка ЭЦП в файле out.p7s с добавлением ответа OCSP сервера:

```
AvCmUt4.exe -V out.p7s -ADDOCSP
```

Результат выполнения в командной строке, **сертификат действителен**:

```
Проверка ЭЦП
Обработка файла: out.p7s
Проверка ЭЦП
Дата/время подписи: 06.03.2017 17:33:05
Субъект:
<…>
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:34:01
Сертификат действителен
Ответ OCSP сервера добавлен в сообщение
ЭЦП действительна
Запись файла out.p7s.p7s
```

Результат выполнения в командной строке, **сертификат недействителен**:
Инициализация приложения ...

```
Проверка ЭЦП
Обработка файла: out.p7s
Проверка ЭЦП
Дата/время подписи: 06.03.2017 17:36:25
Субъект:
<…>
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 18:14:36
Сертификат не действителен: Сертификат отозван.
Ответ OCSP сервера добавлен в сообщение
ЭЦП не действительна: Сертификат отозван.
Запись файла out.p7s.p7s
```

Результат выполнения в командной строке, статус **сертификата неизвестен**:

```
Проверка ЭЦП
Обработка файла: out.p7s
```

```
Проверка ЭЦП
Дата/время подписи: 06.03.2017 17:16:28
Субъект:
<…>
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 18:19:27
Сертификат не действителен: OCSP-серверу не удалось
определить статус сертификата
Ответ OCSP сервера добавлен в сообщение
ЭЦП не действительна: OCSP-серверу не удалось определить
статус сертификата
Запись файла out.p7s.p7s
```

Во всех случаях будет записан выходной файл out.p7s.p7s, содержащий ЭЦП и ответ OCSP сервера проверки статуса сертификата

Проверка добавленного ответа OCSP сервера в сообщении осуществляется с использованием параметра -VERIFITME (см. п. 5.5. Проверять статус сертификата на указанное время (-VERIFYTIME).

5.4. Добавить в сообщение ответы сервера OCSP проверки статуса атрибутного сертификата (-ADDAOCSP)

AvCmUt4.exe <операция> <входной файл> -ADDAOCSP

Использование:

1. **при выработке ЭЦП/дополнительной ЭЦП (**см. **пп. 3.2.1. Выработка ЭЦП входного файла (-s)** и **3.2.2. Выработка дополнительной ЭЦП (–S)).**
   Если параметр «выходной файл», не указан подписанный документ будет записан в файл с расширением «.p7s».
2. **при проверке ЭЦП с использованием параметра -V** (см. **п. 3.2.4. Проверка ЭЦП без записи исходного файла (-V))**
   При добавлении в сообщение ответа сервера OCSP допускается задание выходного файла параметром –o (см. **п. 4.2.1**. **Указание выходного файла (-o)**), если параметр «выходной файл» не был задан, выходной файл с ответом сервера будет записан в файл с расширением «.p7s»).

При добавлении в сообщение ответ OCSP сервера проверки статуса атрибутного сертификата выходной файл запишется только в случае, если статус атрибутного сертификата – **действителен.**

Примеры:

1. Выработка ЭЦП для файла test.txt с добавлением атрибутного сертификата с атрибутом Учётный номер плательщика (УНП) = 123456789 и добавлением ответов от OCSP сервера проверки статусов личного и атрибутного сертификатов:

```
AvCmUt4.exe -s test.txt -o output.p7s -A
1.2.112.1.2.1.1.1.1.2=123456789 -ADDOCSP -ADDAOCSP
```

Результат выполнения в командной строке (личный сертификат **действителен**, атрибутный сертификат с заданным параметром **действителен**):

```
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:58:47
Атрибутный сертификат действителен
Синхронизация времени с сервером OCSP, текущее время:
05.03.2017 19:58:46
Атрибутный сертификат подходит для удостоверения ЭЦП
Выработка ЭЦП
Обработка файла: test.txt
Ответ OCSP сервера для атрибутного сертификата добавлен в
сообщение
Получение статуса личного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:58:48
Сертификат действителен
Ответ OCSP сервера добавлен в сообщение
Запись файла out.p7s
```

Выходной файл out.p7s будет содержать ЭЦП и ответ OCSP сервера проверки статуса личного и атрибутного сертификатов.

Результат выполнения в командной строке (личный сертификат **действителен**, статус атрибутного сертификата с заданным параметром **недействителен**):

```
Найден атрибутный сертификат серийный номер:
40E4E0D04624B7E70000001A
Значение атрибута 1.2.112.1.2.1.1.1.1.2=364387654 не
соответствует заданному 123456789
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:39:06
Атрибутный сертификат не действителен: Сертификат
отозван.
Ошибка: Не найден требуемый атрибутный сертификат
```

Выходной файл записан не будет.

Результат выполнения в командной строке (личный сертификат **действителен**, атрибутный сертификат с заданным параметром **недействителен**):

```
Найден атрибутный сертификат серийный номер:
40E4E8172851059C00000006
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 17:27:00
Атрибутный сертификат не действителен: Сертификат
отозван.
Параметры отбора сертификата не подходят для проверки ЭЦП
№1
Ошибка: В сообщении нет подходящих подписей
```

Выходной файл записан не будет.

2. Проверка ЭЦП в файле out.p7s с атрибутным сертификатом с указанием параметра контроля атрибута Наименование организации "ОАО "Организация" и добавлением ответа от OCSP сервера проверки статусов личного и атрибутного сертификатов:

```
AvCmUt4.exe -V out.p7s -o result.p7s -R -A 2.5.4.10="ООО
""Организация""" -ADDOCSP -ADDAOCSP
```

Результат выполнения в командной строке (личный сертификат **недействителен**, атрибутный сертификат с заданным параметром **действителен**):

```
Вход в систему ...
Проверка ЭЦП
Обработка файла: out.p7s
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:31:40
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:37:14
Атрибутный сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
Ответ OCSP сервера атрибутных сертификатов добавлен в
сообщение
<…>
Серийный номер сертификата: 40E4D9553E59321A0000419B
Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
ЭЦП сообщения верна
Получение статуса сертификата от OCSP сервера
Ответ OCSP сервера от 06.03.2017 16:37:14
Сертификат не действителен: Сертификат отозван.
Ответ OCSP сервера добавлен в сообщение
ЭЦП не действительна: Сертификат отозван.
Запись файла result
```

Выходной файл result.p7s будет содержать ЭЦП и ответ OCSP сервера проверки статуса личного и атрибутного сертификатов.

Проверка добавленного ответа OCSP сервера в сообщении осуществляется с использованием параметра -VERIFITME (см. п. 5.5. Проверять статус сертификата на указанное время (-VERIFYTIME).

ВНИМАНИЕ!!!

При проверке сообщения с ответом сервера OCSP проверки статуса атрибутного сертификата по умолчанию будет также происходить проверка ответа OCSP статуса личного сертификата.

Поэтому надо добавлять ответ проверки статуса атрибутного сертификата или одновременно с добавлением ответа проверки статуса личного сертификата, или в сообщение с уже добавленным ответом, иначе при проверке такого сообщения будет ошибка:

```
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 06.03.2017 11:02:33
Сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
Субъект:
<…>
Серийный номер сертификата: 40E4D9553E59321A0000419B
Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
ЭЦП сообщения верна
Проверка ответов OCSP сервера добавленных в сообщение
Ошибка: OCSP ответ для данного сертификата отсутствует в
сообщении.
```

5.5. Проверять статус сертификата на указанное время (-VERIFYTIME)

AvCmUt4.exe <операция> <входной файл> -VERIFYTIME <[SIGNTIME]/[YYYY-MM-DD HH:MM:SS]>

Проверка добавленных ответов OCSP сервера в сообщении, используется при проверке ЭЦП (см. **пп. 3.2.3. Проверка ЭЦП (-v)** и **3.2.4. Проверка ЭЦП без записи исходного файла (-V)**).

Два способа задания времени:

1. **-VERIFYTIME SIGNTIME**
Используется, только если ответ OCSP сервера был добавлен во время выработки ЭЦП.

2. **-VERIFYTIME [YYYY-MM-DD HH:MM:SS]**
Используется как в случае, если ответ сервера был добавлен во время выработки ЭЦП, так и в случае, если ответ сервера добавлен во время проверки ЭЦП.

Диапазон допустимого времени начинается с момента добавления ответа OCSP сервера плюс 2 часа (в зависимости от настроек сервера).

Примеры:

1. Проверка ЭЦП и ответа OCSP сервера проверки статуса сертификата, добавленного во время выработки ЭЦП, в файле output.p7s:

```
AvCmUt4.exe -v output.p7s -o result -VERIFYTIME SIGNTIME
```

Результат выполнения в командной строке (ответ OCSP сервера – сертификат **действителен**):

```
Проверка ЭЦП
Обработка файла: output.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 11:11:37
Субъект:
<…>
ЭЦП сообщения верна
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 06.03.2017 11:11:36
Сертификат действителен
ЭЦП действительна
```

Результат выполнения в командной строке (ответ OCSP сервера – сертификат **недействителен**):

```
Проверка ЭЦП
Обработка файла: output.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 11:15:27
Субъект:
<…>
ЭЦП сообщения верна
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 06.03.2017 11:15:27
Сертификат не действителен: Сертификат отозван.
Ошибка: Сертификат отозван.
```

Выходной файл result будет представлять собой исходной документ до момента подписания и добавления в него ответа OCSP сервера.

2. Проверка ЭЦП и ответов OCSP сервера проверки статуса сертификата, добавленного во время проверки ЭЦП, в файле output.p7s:

```
AvCmUt4.exe -v out.p7s –o result -VERIFYTIME "2017-03-06
17:00:00"
```

Результат выполнения в командной строке (ответ OCSP сервера – сертификат **действителен**):

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:31:40
Субъект:
<…>
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 06.03.2017 16:37:14
Сертификат действителен
ЭЦП действительна
```

Результат выполнения в командной строке (ответ OCSP сервера – сертификат **недействителен**):

```
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 16:31:40
Субъект:
<…>
ЭЦП сообщения верна
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 06.03.2017 16:37:14
Сертификат не действителен: Сертификат отозван.
Ошибка: Сертификат отозван.
```

Выходной файл result будет представлять собой исходной документ до момента подписания и добавления в него ответа OCSP сервера.

3. Проверка в файле out.p7s ЭЦП и ответов OCSP сервера проверки статуса сертификатов (основного и атрибутного), добавленных при проверке ЭЦП, параметр контроля атрибута – УНП=123456789:

```
AvCmUt4.exe -v out.p7s -o result -A
1.2.112.1.2.1.1.1.1.2=123456789 -VERIFYTIME "2017-03-06
16:15:00"
```

Результат выполнения в командной строке (ответ OCSP сервера - личный сертификат **действителен,** атрибутный сертификат **действителен):**

```
Проверка ЭЦП
```

```
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 06.03.2017 15:49:23
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 06.03.2017 16:00:26
Сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
Субъект:
<…>
Серийный номер сертификата: 40E4D9553E59321A0000419B
Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
ЭЦП сообщения верна
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 06.03.2017 16:00:26
Сертификат действителен
ЭЦП действительна
```

Результат выполнения в командной строке (ответ OCSP сервера - личный сертификат **недействителен**, атрибутный сертификат **действителен**):

```
Найден атрибутный сертификат серийный номер:
40E4E8172851059C00000006
Получение статуса атрибутного сертификата от OCSP сервера
Ответ OCSP сервера от 27.03.2017 10:27:00
Атрибутный сертификат не действителен: Сертификат
отозван.
Параметры отбора сертификата не подходят для проверки ЭЦП
№1
Ошибка: В сообщении нет подходящих подписей
Проверка ЭЦП
Обработка файла: out.p7s
Запись файла result
Проверка ЭЦП
Дата/время подписи: 09.03.2017 9:53:17
Найден атрибутный сертификат серийный номер:
40E4E59463C7A6B300000001
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 09.03.2017 9:53:52
Сертификат действителен
Атрибутный сертификат подходит для удостоверения ЭЦП
Субъект:
<…>
Серийный номер сертификата: 40E4D9553E59321A0000419B
Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
ЭЦП сообщения верна
```

```
Проверка ответов OCSP сервера добавленных в сообщение
Ответ OCSP сервера от 09.03.2017 9:53:52
Сертификат не действителен: Сертификат отозван.
Ошибка: Сертификат отозван.
```

6. ВЫРАБОТКА КОНТРПОДПИСИ

Контрподпись (countersignature) - электронно-цифровая подпись, удостоверяющая другую подпись.

Контрподпись используется при необходимости заверить другую подпись, т.е. является подписью не данных, а другой подписи.

Подробнее см. **СТБ 34.101.23-2012 Информационные технологии и безопасность. Синтаксис криптографических сообщений**.

6.1. Удостоверить ЭЦП сообщения (добавить контрподпись) (-ADDCS)

AvCmUt4.exe –V <входной файл> -ADDCS

Контрподпись добавляется при проверке ЭЦП сообщения с использованием параметра -V (см. **п. Функции выработки ЭЦП).** При этом допускается задание выходного файла параметром –o, если параметр «выходной файл» не был задан, выходной файл с удостоверяющей подписью будет записан в файл с расширением «.p7s».

Пример:

Проверка файла с ЭЦП test.p7s с добавлением удостоверяющей ЭЦП:

```
AvCmUt4.exe -V test.txt.p7s -R –ADDCS
```

Результат выполнения в командной строке (в случае, если ЭЦП верна):

```
ЭЦП сообщения верна
Сертификат действителен
ЭЦП верна
ЭЦП удостоверена личным ключом
Запись файла test.txt.p7s.p7s
```

Выходной файл test.txt.p7s.p7s будет включать первоначальную ЭЦП и контрподпись.

6.2. Удостоверить контрподпись (-ADDRECS)

AvCmUt4.exe –V <входной файл> -ADDRECS

Добавляется в сообщение с контрподписью при проверке ЭЦП сообщения с использованием параметра –V (см. **п. 3.2.4. Проверка ЭЦП без записи исходного файла (-V)).** При этом допускается задание выходного файла параметром –o (см. **п. 4.2.1. Указание выходного файла (-o))**, если параметр «выходной файл» не был задан, выходной файл с удостоверяющей подписью будет записан в файл с расширением «.p7s».

Пример:

Проверка файла test.p7s.p7s, включающего в себя ЭЦП и контрподпись, с добавлением подписи, удостоверяющей контрподпись:

```
AvCmUt4.exe -V test.p7s.p7s -o result -ADDRECS
```

Результат выполнения в командной строке:

```
Проверка ЭЦП
Обработка файла: test.txt.p7s.p7s
Проверка ЭЦП
Дата/время подписи: 07.03.2017 12:59:04
Субъект:
<>
Серийный номер сертификата: 40E4D9553E59321A0000419B
Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
ЭЦП сообщения верна
Сертификат действителен
ЭЦП удостоверена. Проверка контрподписей 1
Подпись удостоверил:
   Субъект:
<…>
   Серийный номер сертификата: 40E4E574555FFD2F000041A4
   Идентификатор открытого ключа:
BA71B86C6F902C89769D2AAC98CE9B614FDC74CE
   Дата/время подписи: 07.03.2017 14:00:36
ЭЦП удостоверяющей подписи верна
Сертификат действителен
Удостоверяющая подпись удостоверена личным ключом
ЭЦП действительна
Запись файла result
```

Выходной файл result будет включать ЭЦП, контрподпись и подпись, удостоверяющую контрподпись.

6.3. Использовать контрподпись заданного сертификата при проверке ЭЦП (-USECS)

AvCmUt4.exe <операция> <входной файл> -USECS <certificate filter>

Используется при проверке ЭЦП (см. **пп. 3.2.3. Проверка ЭЦП (-v)** и **3.2.4. Проверка ЭЦП без записи исходного файла (-V)**).

При указании данного параметра будут проверены ВСЕ ЭЦП, содержащиеся в документе, и валидность только того сертификата, которым была выполнена контрподпись при соответствии его заданным параметрам отбора.

Параметры отбора сертификатов <certificate filter> включают:

1. **обязательные** (предопределенные) поля сертификата (KeyID, SerialNumber и т.д.);
2. **необязательные поля**: атрибуты имени субъекта или специального дополнения, которые задаются либо в виде RDN_OID данного атрибута, либо присвоенного

названия – указаны в секци [AliasOID] файла AvCmMsg.ini (например, CN или 2.5.4.3 – общее имя; O или 2.5.4.10 – сокращенное название организации и т.д.).

Надо указывать параметры отбора сертификата, которым была выполнена последняя контрподпись. В случае, если параметры отбора были указаны для другого сертификата или заданы неправильно, то будут проверены все ЭЦП и действительность всех сертификатов в сообщении и будет выведена ошибка::

```
Сертификат не подходит для удостоверения подписи
Ошибка: Сертификат/СОС не удовлетворяет условиям отбора.
```

Для ввода значения атрибута его нужно экранировать одиночными кавычками, если значение атрибута содержит пробелы, то все значение надо экранировать двойными кавычками:

```
-USECS "CN='ALEXEY IVANOV'"
```

Если в атрибутах параметров есть кавычки, то их нужно удваивать, например:

```
-USECS "O=='ЗАО ""Организация""'"
```

Параметров может быть задано несколько.

Для отбора сертификатов, соответствующих **всем** заданным параметрам, используется операнд <**and**>:

```
-USECS "CN='ALEXEY IVANOV' and C='BY'"
```

Для отбора сертификатов, соответствующих **хотя бы одному** параметру используется точка с запятой **<;>**

```
-USECS "CN='ALEXEY IVANOV'; O='ОАО ""Организация""'"
```

Более подробно параметры отбора сертификатов описаны в AvCryptSQL.pdf (документ включен в состав ПК AvPCM).

Примеры:

1. Проверка ЭЦП и удостоверяющей подписи в файле -v test.txt.p7s.p7s с отбором и проверкой действительности сертификата, которым была выполнена контрподпись, по параметру Идентификатор ключа субъекта KeyID=22CA80968321BD8E9C5C9F40F775A4B518394D0B:

   ```
   AvCmUt4.exe -v test.txt.p7s.p7s -USECS
   "KeyID='22CA80968321BD8E9C5C9F40F775A4B518394D0B'"
   ```

   Результат выполнения в командной строке (найден **действительный** сертификат, которым была выполнена удостоверяющая подпись, сертификат **удовлетворяет** заданному параметру):

   ```
   Проверка ЭЦП
   ```

```
Обработка файла: test.txt.p7s.p7s
Запись файла test.txt.p7s
Проверка ЭЦП
Дата/время подписи: 06.03.2017 10:45:50
Субъект:
<…>
Серийный номер сертификата: 40E4E531850CDAFA000041A3
Идентификатор открытого ключа:
BB67CED6067AAA248237C064BF2AB163DEE5441C
ЭЦП сообщения верна
ЭЦП удостоверена. Проверка контрподписей
Подпись удостоверил:
   Субъект:
<…>
   Серийный номер сертификата: 40E4D9553E59321A0000419B
   Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
   Дата/время подписи: 06.03.2017 10:46:34
ЭЦП удостоверяющей подписи верна
Сертификат действителен
Сертификат подходит для удостоверения подписи
ЭЦП действительна
```

2. Проверка ЭЦП и контрподписи в файле -v test.txt.p7s.p7s с отбором и проверкой действительности сертификата, которым была выполнена контрподпись, по параметрам Общие данные CN и Адрес электронной почты E (заданы в виде присвоенных названий):

```
AvCmUt4.exe –v test.txt.p7s.p7s -USECS "CN='Иванов Михаил
Юрьевич' and E='mail@mail.by'"
```

Результат выполнения в командной строке (найден **действительный** сертификат, которым была выполнена удостоверяющая подпись, сертификат **удовлетворяет** заданному параметру):

```
Проверка ЭЦП
Обработка файла: test.txt.p7s.p7s
Запись файла test.txt.p7s
Проверка ЭЦП
Дата/время подписи: 06.03.2017 10:45:50
Субъект:
<…>
Серийный номер сертификата: 40E4E531850CDAFA000041A3
Идентификатор открытого ключа:
BB67CED6067AAA248237C064BF2AB163DEE5441C
ЭЦП сообщения верна
ЭЦП удостоверена. Проверка контрподписей
Подпись удостоверил:
   Субъект:
<…>
   Серийный номер сертификата: 40E4D9553E59321A0000419B
```

```
   Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
   Дата/время подписи: 06.03.2017 10:46:34
ЭЦП удостоверяющей подписи верна
Сертификат действителен
Сертификат подходит для удостоверения подписи
ЭЦП действительна
```

3. Проверка ЭЦП и удостоверяющей подписи в файле -v test.txt.p7s.p7s с отбором и проверкой действительности сертификата, которым была выполнена контрподпись. Параметры отбора: общие данные CN или населенный пункт 2.5.4.7 (название задано в виде OID атрибута) и должность 2.5.4.12 (название задано в виде OID атрибута):

```
AvCmUt4.exe -v test.txt.p7s.p7s -USECS "CN='ALEXEY
IVANOV'; 2.5.4.7 ='д. Каменюки' and 2.5.4.12='директор'"
```

Результат выполнения в командной строке (найден **действительный** сертификат, которым была выполнена контрподпись, сертификат **удовлетворяет** заданному параметру):

```
Проверка ЭЦП
Обработка файла: test.txt.p7s.p7s
Запись файла test.txt.p7s
Проверка ЭЦП
Дата/время подписи: 06.03.2017 10:45:50
Субъект:
<…>
Серийный номер сертификата: 40E4E531850CDAFA000041A3
Идентификатор открытого ключа:
BB67CED6067AAA248237C064BF2AB163DEE5441C
ЭЦП сообщения верна
ЭЦП удостоверена. Проверка контрподписей
Подпись удостоверил:
   Субъект:
<…>
   Серийный номер сертификата: 40E4D9553E59321A0000419B
   Идентификатор открытого ключа:
22CA80968321BD8E9C5C9F40F775A4B518394D0B
   Дата/время подписи: 06.03.2017 10:46:34
ЭЦП удостоверяющей подписи верна
Сертификат действителен
Сертификат подходит для удостоверения подписи
ЭЦП действительна
```

7. ОБРАБОТКА ФАЙЛОВ ПО МАСКЕ

Утилита AvCmUt может выполнять групповые операции с файлами, при этом используется маска имени файла, содержащая символы подстановки «*» и «?».

Символ «?» в маске означает ровно один произвольный символ.

Символ «*» в маске означает любую последовательность символов произвольной длины.

Указание маски файла допустимо при всех основных операциях, выполняемых утилитой (выработка/проверка ЭЦП, зашифрование/расшифрование, вычисление значения функции хэширования и т.д).

При использовании маски файла задание имени выходного файла **недопустимо**, выходным файлам будет присвоено значение по умолчанию (например, *.p7s – при подписи, *.p7e – при зашифровании).

Если предназначенный для обработки файлу не находится в одной папке с утилитой AvCmUt, нужно прописать его полную директорию, имена каталогов при задании пути к файлу надо прописывать полностью.

Примеры**:**

1) Выработка ЭЦП для всех файлов в формате txt:
```
AvCmUt4.exe -s *.txt
```
Подпишутся все файлы формата txt, формат выходных файлов - txt.p7s.

2) Проверка ЭЦП для всех файлов в формате txt.p7s:
```
AvCmUt4.exe -v *.txt.p7s
```
Формат выходных файлов – txt.

3) Зашифрование файлов с любым расширением, в именах которых содержат до пяти символов:
```
AvCmUt4.exe -e ?????.*
```
Формат выходных файлов – p7e.

4) Вычисление значения функции хэширования по алгоритму СТБ 34.101.31-2020 (Belt) для файлов с именем, начинающимся на «Av» и расширением dll:
```
AvCmUt4.exe -H Av*.dll
```

5) Вычисление значения функции хэширования по алгоритму СТБ 1176.1-99 (BHF) для всех файлов в указанной папке:
```
AvCmUt4.exe -h "c:\test AvCmUt\*"
```

8. ПРИМЕРЫ ПРИМЕНЕНИЯ

1. Выработка ЭЦП с указанием параметров аутентификации пользователя (идентификатора открытого ключа и значения пароля):

```
AvCmUt4.exe s input.txt -o output.p7s -l
8F22ECC42DFC14D21D6BBEC6CF49A66C7AD37933 -p 12345678
```

2. Проверка ЭЦП, выработанной ALEXEY IVANOV, без создания выходного файла:

```
AvCmUt4.exe -V input.p7s -c "ALEXEY IVANOV"
```

3. Выработка раздельной ЭЦП без сохранения исходного документа в выходном файле:

```
AvCmUt4.exe -s input.txt -o output.p7s -T
```

4. Проверка раздельной ЭЦП с записью файла лога в указанную папку:

```
AvCmUt4.exe -v input.p7s -o output.txt -F input.txt -LOG
"c:\LOG FOLDER\AvCmUt4.log"
```

5. Проверка ЭЦП без аутентификации с отбором сертификатов, выпущенных на организацию Общество с ограниченной ответственностью "Тестовая организация":

```
AvCmUt4.exe -v input.p7s -o output.txt -X 2.5.4.41="Общество с
ограниченной ответственностью ""Тестовая организация""" -NA
```

6. Зашифрование на получателя с указанием идентификатора открытого ключа получателя, выполненное без аутентификации:

```
AvCmUt4.exe -e input.txt -o output.p7e -k
4B5CAFE0235786E28FB55744A756C9B91E822E66 -NA
```

7. Расшифрование подписи с указанием файла для записи идентификатора открытого ключа:

```
AvCmUt4.exe -d input.p7e -o output.txt -O sub_key_id
```

8. Выработка ЭЦП и зашифрование с указанием папки для помещения выходных файлов:

```
AvCmUt4.exe -E input.txt -o output.p7e -P "c:\Program
Files\output"
```

9. Расшифрование и проверка подписи с отбором сертификатов, выпущенных на организацию Общество с ограниченной ответственностью "Тестовая организация":

```
AvCmUt4.exe -D input.p7s -X 2.5.4.41="Общество с ограниченной
ответственностью ""Тестовая организация""" -o out.txt
```

10. Генерация запроса на сертификат с указанием файла шаблона на сертификат:

```
AvCmUt4.exe -r request.req –t org.tpl
```

11. Импорт СОС:

```
AvCmUt4.exe –C crl.crl
```

12. Обновление СОС и сертификатов УЦ с выводом результата в файл LogCDP.txt:

```
AvCmUt4.exe -CDP CrlDPExt.txt -O "c:\log folder\LogCDP.txt"
```

13. Вычисление значения функции хэширования файла test по алгоритму СТБ 34.101.31-2020 (Belt) с выводом результата в файл result.txt:

```
AvCmUt4.exe –h test –O result
```

9. КОДЫ ВОЗВРАТА

Код возврата	**Краткое описание ошибки**	**Возможные причины возникновения ошибки**
0	Успешное выполнение	
1	Неправильные параметры командной строки	В командной строке введен(ы) неправильный(е) параметр(ы) или отсутствует(ют) обязательный(е) параметр(ы).
2		
3		
4	Ошибка чтения входного файла	– Неправильно указан путь к входному файлу в файле настроек либо в командной строке; – входной файл отсутствует; – входной файл открыт другой программой.
5	Ошибка записи выходного файла	– Неправильно указан путь к выходному файлу в файле настроек либо в командной строке; – выходной файл защищён от записи; – выходной файл открыт другой программой.
6	Не найден требуемый атрибутный сертификат	– Сертификат не удовлетворяет параметрам контроля; – сертификат недействителен.
7	Не найден контейнер с личным ключом, соответствующим личному сертификату	На носителе отсутствуют личные ключи, соответствующие открытым ключам, указанным в действующем сертификате, находящемся в личном справочнике.
8	Введён неверный пароль защиты личного ключа	В параметре **-p** командной строки указан не то значение пароля к контейнеру с личным ключом, которое было задан при формировании личных ключей.
9	Не найдено хранилище сертификатов	– Не найден файл-хранилище сертификатов CertStore.xml; – невозможно подключиться к БД.
10		
11	Неверный формат	Возникает при проверке ЭЦП: – ЭЦП несанкционированно изменена; – файл не подписан ЭЦП.
12	Входной файл имеет нулевой размер	Во входном файле отсутствует информация.
13	Отсутствуют получатели зашифрованного сообщения	Возникает при зашифровании: – сертификата получателя нет в сетевом справочнике сертификатов; – сертификат получателя недействителен (сертификат получателя отозван (приостановлен), срок действия СОС истек, нет доверия сертификату корневого УЦ).

14	Неверный формат	Возникает при расшифровании: – файл несанкционированно изменен после зашифрования; – файл не зашифрован.
15	Невозможно расшифровать сообщение: среди сертификатов получателей сообщения отсутствует личный сертификат аутентифицированного пользователя.	Зашифрованный файл не предназначен абоненту, который пытается его расшифровать
16	Не найден сертификат для проверки ЭЦП	
17	Подпись под сообщением неверна	Возникает при проверке ЭЦП. Подписанный ЭЦП файл был изменен или поврежден.
18	В справочнике списков, отозванных сертификатов имеется более новый (такой же) СОС данного издателя либо объект уже существует (импортируемый СОС уже присутствует в справочнике)	Возникает при импорте СОС
19	В сообщении нет подходящих подписей	Параметры отбора не соответствуют сертификату, которым была выполнена ЭЦП сообщения
20		
21	Срок действия СОС истек или не наступил	Срок действия списка отозванных сертификатов (СОС) УЦ, издавшего сертификат, истек или не наступил.
22	Срок действия сертификата открытых ключей абонента истек	
23	Сертификат отозван	
24	Абонент прервал осуществляемую обработку	Работа программы была прервана пользователем.
25	Нет доверия сертификату	Абонент не установил доверие сертификату УЦ, издавший данный сертификат.
26	Ошибка при обращении к OCSP серверу	
27	Сертификат не действителен	OCSP сервер не подтвердил действительность сертификата.
28		

29	Носитель с личным ключом не установлен в считыватель.	В считывателе отсутствует носитель личных ключей.
30	В личном справочнике отсутствует действующий сертификат	В личном справочнике сертификатов отсутствует действующий сертификат.
31	Не найден действующий личный сертификат, соответствующий параметрам отбора.	В личном справочнике сертификатов не найден сертификат, соответствующий параметрам отбора.
32	В личном справочнике сертификатов больше одного сертификата.	В личном справочнике сертификатов имеется больше одного действующего сертификата. Нужно указать параметры отбора для выбора одного сертификата.
33	Носитель личных ключей не зарегистрирован.	
34	Ошибка записи на носитель личных ключей.	Возможно носитель личных ключей повреждён.
35	Внутренняя ошибка библиотеки.	

10. ПОДДЕРЖКА МАКРОСОВ

Для удобства использования утилиты, поддерживаются макросы, которые записываются в файл AvCmUt4.ini в секцию [Alias].

В файл AvCmUt4.ini внесен следующий пример:

```
[Alias]
;Sign=Login -s
;EncAvest=Login Stan Max -e
;Stan=-k=72F3D8E0DCECE3A23578581CA1DFDE3D3F73239D
;Max=-k=72F3D8E0DCECE3A23578581CA1DFDE3D3F732391
;Login=-l "72F3D8E0DCECE3A23578581CA1DFDE3D3F73239D" -
p=12345678
```

Если удалить комментарии «;», то при использовании утилиты вызов:

```
AvCmUt4.exe Sign test.txt
```

будет аналогичен вызову:

```
AvCmUt4.exe -l "72F3D8E0DCECE3A23578581CA1DFDE3D3F73239D"
p=12345678 -s test.txt
```

а вызов:

```
AvCmUt4.exe EncAvest test.txt
```

аналогичен вызову:

```
AvCmUt4.exe -l "72F3D8E0DCECE3A23578581CA1DFDE3D3F73239D"
p=12345678 -k 72F3D8E0DCECE3A23578581CA1DFDE3D3F73239D -k
72F3D8E0DCECE3A23578581CA1DFDE3D3F732391 -e test.txt
```

По аналогии в данном файле можно создавать свои макросы.

ПРИЛОЖЕНИЕ 1

Поддержка криптографических алгоритмов AvCmUt в зависимости от типа установленного криптопровайдера

Операции хэширования

Стандарт / Тип криптопровайдера	СТБ 1176.1-99	СТБ 34.101.31-2020
Avest CSP Base (тип 421)	+	+
Avest CSP Bel (тип 423)	+	+
Avest CSP Bign (тип 424)	+	+

Операции ЭЦП

Стандарт / Тип криптопровайдера	СТБ 1176.2-99 / СТБ 34.101.31-2020	СТБ 34.101.45-2013 / СТБ 34.101.31-2020
Avest CSP Base (тип 421)	+	-
Avest CSP Bel (тип 423)	+	+
Avest CSP Bign (тип 424)	+	+

Операции шифрования

Стандарт / Тип криптопровайдера	ГОСТ 28147-89	СТБ 34.101.31-2020
Avest CSP Base (тип 421)	+	-
Avest CSP Bel (тип 423)	+	+
Avest CSP Bign (тип 424)	+	+

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

АС – атрибутный сертификат;
БД – база данных;
ИОК – инфраструктура открытых ключей;
КУЦ – корневой удостоверяющий центр;
НКИ – носитель ключевой информации;
ПО – программное обеспечение;
ПУЦ – подчиненный удостоверяющий центр;
САС – служба атрибутных сертификатов;
СОК – сертификат открытого ключа;
СОС – список отозванных сертификатов;
ЦС – центр сертификации;
УЦ – удостоверяющий центр;
ЭЦП – электронная цифровая подпись;
OCSP (Online Certificate Status Protocol) – онлайновый протокол проверки статуса сертификата, определенный в СТБ 34.101.26.