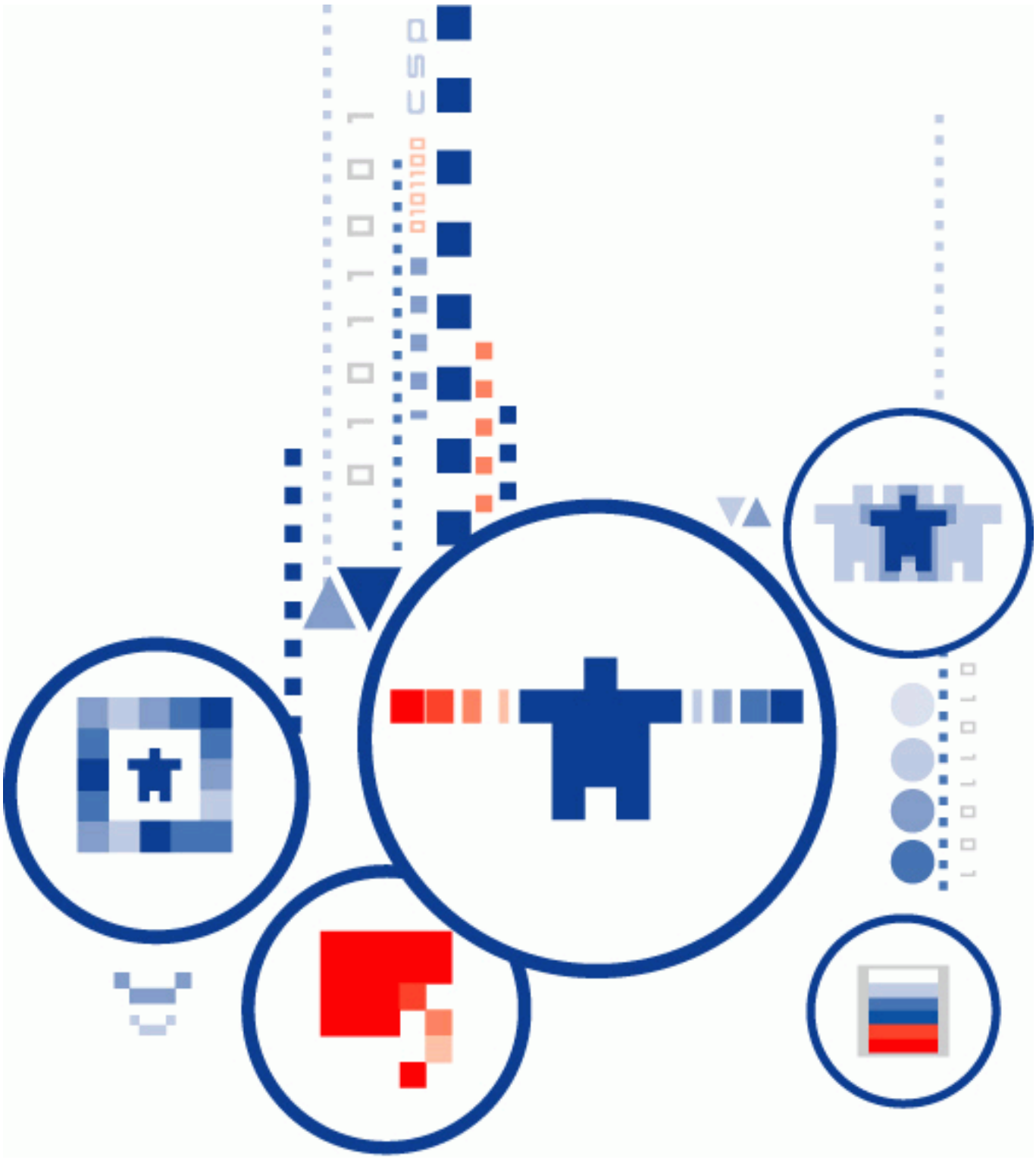


Средство применения электронной подписи «КриптоПро SSF»

Инструкция по использованию

АННОТАЦИЯ

Настоящий документ содержит описание средства применения электронной подписи «КриптоПро SSF», предназначенного для защиты открытой информации в информационных системах общего пользования (вычисление и проверка электронной подписи) и защиты конфиденциальной информации, не содержащей сведений, составляющих государственную тайну, в корпоративных информационных системах.

Документ предназначен для пользователей и администраторов программных продуктов, построенных на платформе SAP Netweaver ABAP (SAP ERP, SAP SRM, SAP CRM, SAP SCM), как ознакомительный материал перед установкой и эксплуатацией модуля «КриптоПро SSF».

Информация о разработчике «КриптоПро SSF»:

ООО «Крипто-Про»
105318 г. Москва, ул. Ибрагимова. Д. 31, офис 30Б
Телефон/Факс: +7 (495) 995-48-20
+7 (495) 984-07-90
http://www.CryptoPro.ru
E-mail: info@CryptoPro.ru

СОДЕРЖАНИЕ

1. Общие положения

Средство применения электронной подписи «КриптоПро SSF» предназначено для оборудования автоматизированных рабочих мест пользователей программных продуктов, построенных на платформе SAP Netweaver ABAP (SAP ERP, SAP SRM, SAP CRM, SAP SCM), и выступает как программная «обертка» прикладных данных, применяющихся в различных сценариях для защиты данных и документов с использованием механизмов на основе сертификатов X.509 и электронной подписи:

- идентификация пользователей и процессов систем документооборота;
- электронная подпись прикладных данных, обрабатываемых в решениях SAP;
- хранение данных в защищенном формате;
- защищенная передача данных через публичные сети;
- гарантирование аутентичности и целостности данных.

Программное средство применения электронной подписи «КриптоПро SSF» представляет собой модуль динамически подгружаемой библиотеки (dll), реализующей интерфейс (API) «Secure Store & Forward (SSF)» и обеспечивающей в соответствие с этим выполнение следующих задач:

- Формирование и проверку усиленной квалифицированной электронной подписи данных;
- Шифрование и расшифрование данных;
- Вычисление значение хеш-функции;
- Поддержку формата криптографических сообщений согласно RFC 3852 "Cryptographic Message Syntax (CMS)" с учетом RFC 4490 "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)";
- Поддержку формата криптографических сообщений усовершенствованной электронной подписи - CAdES X Long ("CMS Advanced Electronic Signatures") с фиксацией времени подписания электронного документа посредством реализации протокола TSP согласно рекомендациям RFC 3161 («Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP)») и сохранением информации о статусе сертификата ключа проверки ЭП подписчика на момент времени подписания электронного документа посредством реализации протокола OCSP согласно рекомендациям RFC 2560 («Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP») и хранением всех доказательств подлинности этой электронной подписи;

При этом обеспечивается использование квалифицированных сертификатов ключей проверки электронной подписи, изготавливаемых и выдаваемых удостоверяющими центрами.

Средство применения электронной подписи использует средство криптографической защиты информации (средство электронной подписи), обеспечивающее выполнение следующих основных функций:

- генерацию и управление ключевой информацией;
- формирование электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001;
- подтверждение подлинности электронной подписи электронного документа в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-94;
- подсчет значения хеш-функции в соответствии с ГОСТ Р 34.11-94;
- шифрование и расшифрования данных в соответствии с ГОСТ 28147-89;

- формирование закрытых и открытых ключей электронной подписи и шифрования;
- идентификацию, аутентификацию, шифрование, имитозащиту TLS соединений.

Средство криптографической защиты информации (средство электронной подписи) должно соответствовать криптографическому интерфейсу компании Microsoft - Cryptographic Service Provider (CSP).

Средство криптографической защиты информации (средство электронной подписи) должно реализовывать ГОСТ Р 34.10-2001, ГОСТ Р 34.10-94, ГОСТ Р 34.11-94 и ГОСТ 28147-89 с учетом RFC 4491 "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms".

Средство криптографической защиты информации (средство электронной подписи) должно поддерживать сертификаты открытых ключей стандарта X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Средство криптографической защиты информации (средство электронной подписи) должно поддерживать формат криптографических сообщений согласно RFC 3852 "Cryptographic Message Syntax (CMS)" с учетом RFC 4490 "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)".

Программное средство применения электронной подписи для оборудования автоматизированных рабочих мест пользователей функционирует в 32–ух и 64-и разрядных средах следующих операционных систем:

- Microsoft Windows 2000 / XP / 2003 / Vista / 2008 / W7 / 2008 R2 /2012;
- ОС семейства Linux, удовлетворяющих LSB 3.1 и выше;
- FreeBSD 7.x и выше;
- AIX 5.3 и 6.x;
- Solaris 10 и выше.

2. Инсталляция ПО «КриптоПро SSF»

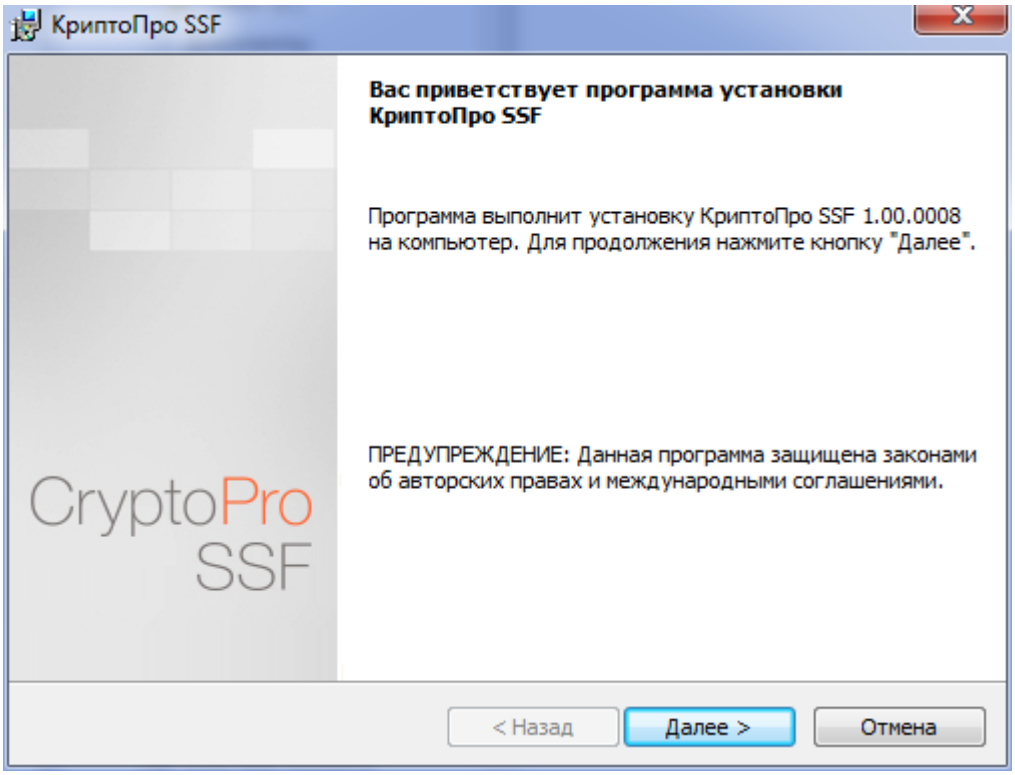
2.1. Установка СКЗИ КриптоПро CSP.

Для функционирования модуля «КриптоПро SSF» необходимо, чтобы на целевом компьютере было предварительно установлено СКЗИ КриптоПро CSP (возможно использование СКЗИ КриптоПро HSM). Сведения и инструкции по установке, указанных СКЗИ приведены в соответствующей документации на данные продукты.

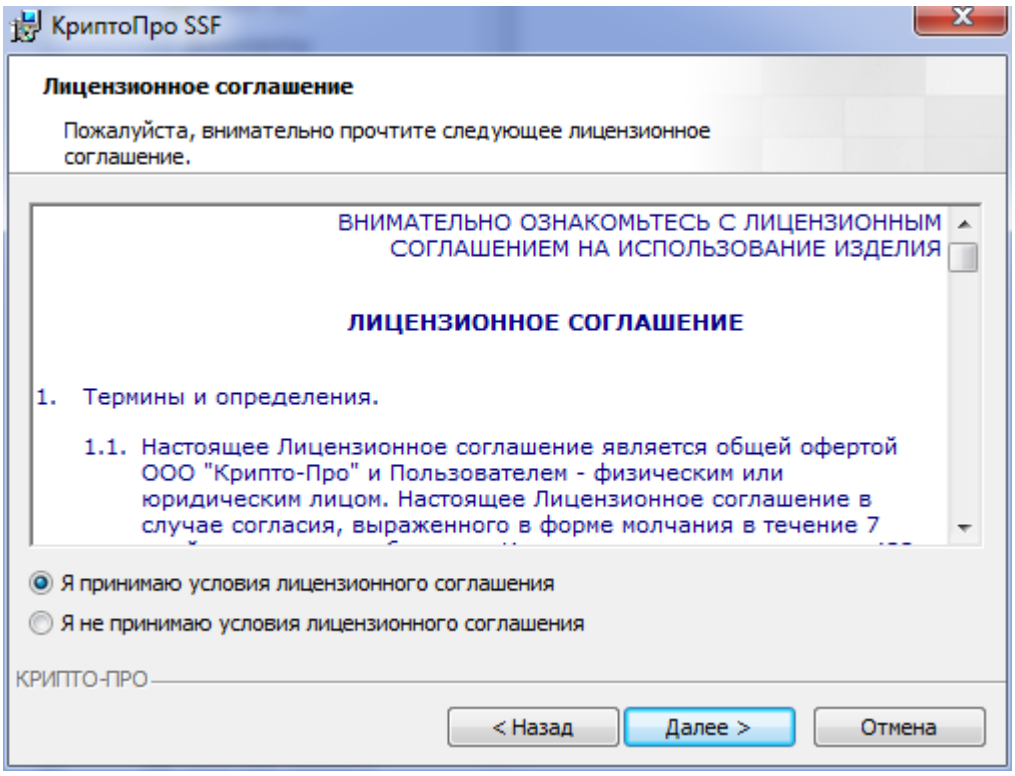
2.2. Установка дистрибутива КриптоПро SSF

Установка дистрибутива КриптоПро SSF должна производиться пользователем, имеющим права администратора.

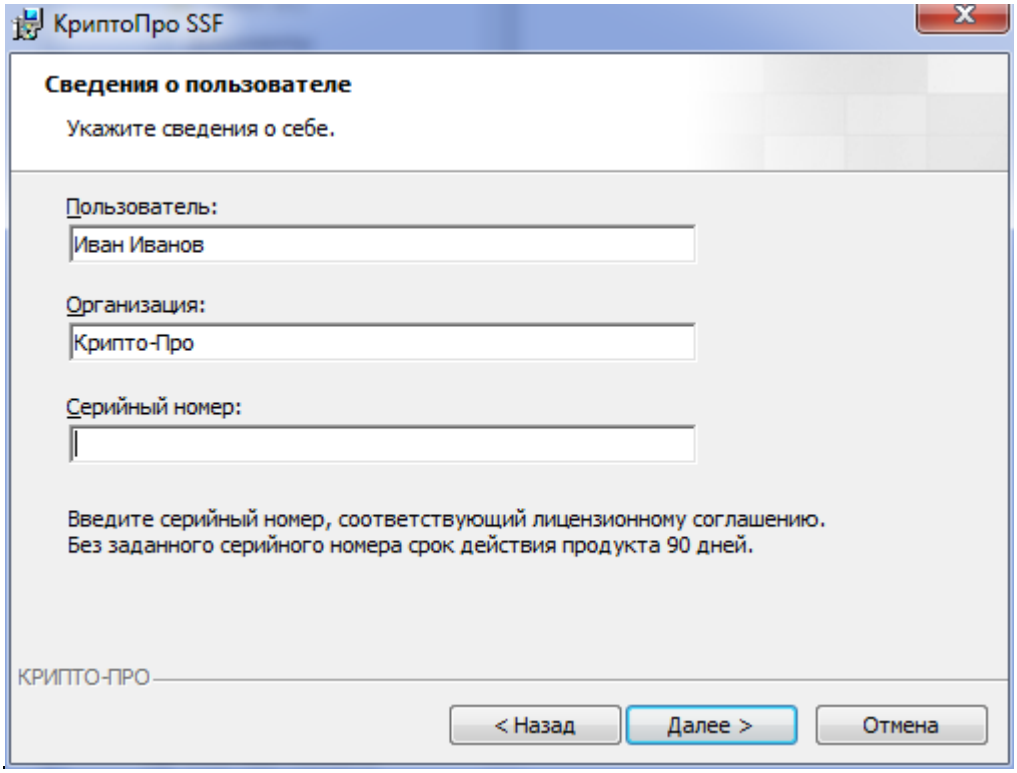
Для установки программного обеспечения запустите установочный msi модуль, соответствующий разрядности целевой ОС, или модуль SSFSetup.exe с дистрибутивного диска. При этом будет запущен мастер установки модуля «КриптоПро SSF».



В следующем окне мастера установки ознакомьтесь с лицензионным соглашением на использование ПО КриптоПро SSF. Если Вы согласны со всеми пунктами соглашения, выделите пункт «Я принимаю условия лицензионного соглашения», и нажмите **Далее**.

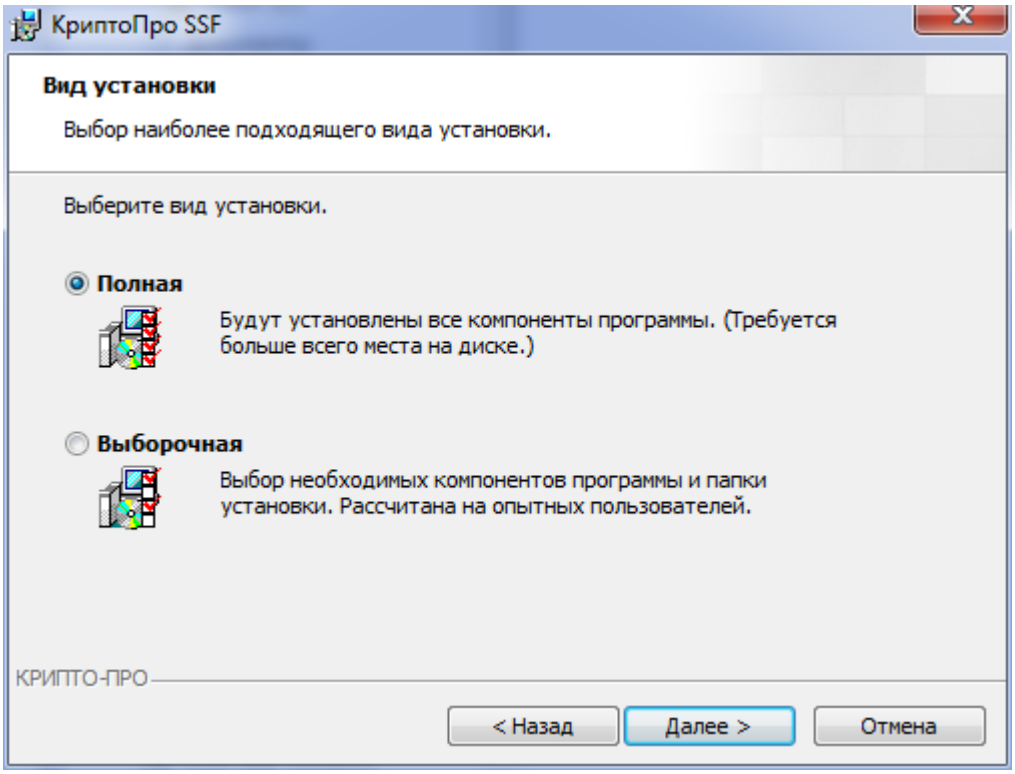


Для дальнейшей установки КриптоПро SSF нажмите **Далее**. Следующим шагом необходимо ввести информацию о пользователе, производящем установку, организации и предоставленной лицензии на использование модуля.



Если не вводить Серийный номер лицензии, то будет установлена временная (на 3 месяца) ознакомительная лицензия. Серийный номер лицензии можно будет ввести позже, с использованием консоли управления лицензиями Крипто-Про (см. п. 3.1 Ввод серийных номеров лицензий для модулей «КриптоПро SSF»).

После нажатия кнопки **Далее** программа установки отобразит диалоговое окно, в котором необходимо выбрать вид установки.



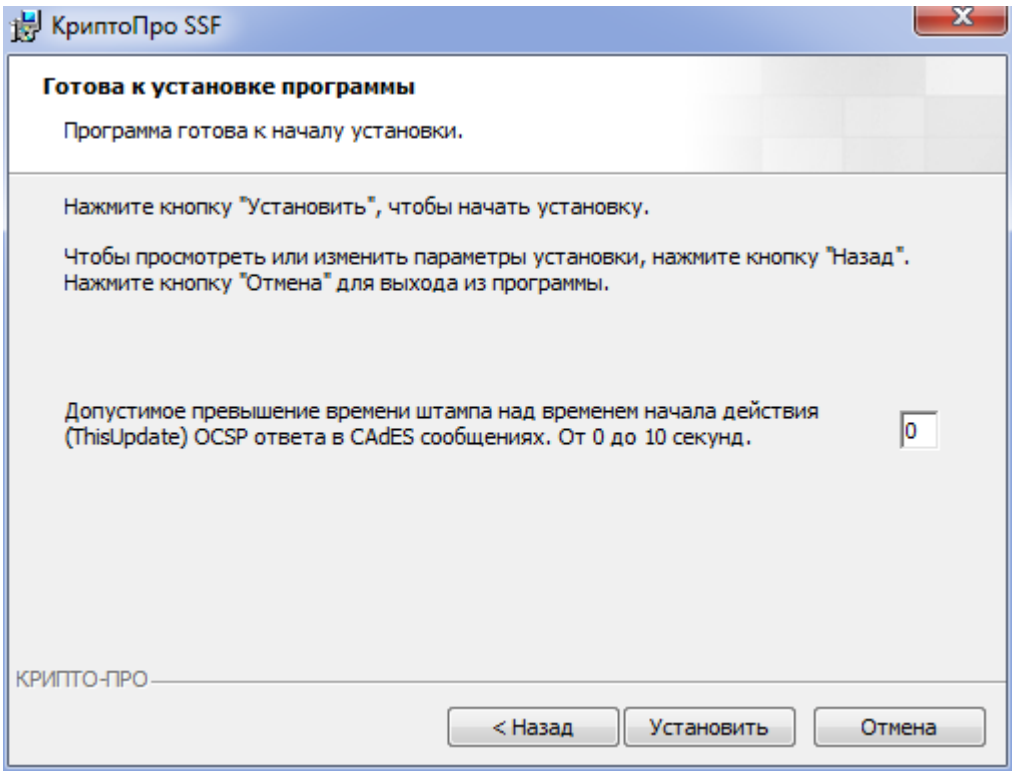
Выборочная установка позволяет выбрать место в каталоге, куда необходимо установить модуль КриптоПро SSF.

Следующее окно мастера служит для подтверждения установки. При необходимости можно вернуться назад и переопределить параметры установки.

В данной реализации формата CADES не допускается использование OCSP ответов, у которых поле ThisUpdate (время начала действия OCSP ответа) меньше времени, указанном в штампе времени. Т.е. информация об отзыве сертификата должна быть «свежей», дабы исключить использование недостоверной информации о статусе сертификата на момент подписи. Кроме этого при отсутствии в OCSP ответе поля NextUpdate (срок окончания действия информации о статусе сертификата в данном конкретном OCSP ответе), Значение поля ThisUpdate не должно превышать время, указанное в штампе времени более чем на 5 минут. Поэтому необходимо следить за синхронизацией времен указанных служб (TSP, OCSP), особенно, если они располагаются на разных серверах.

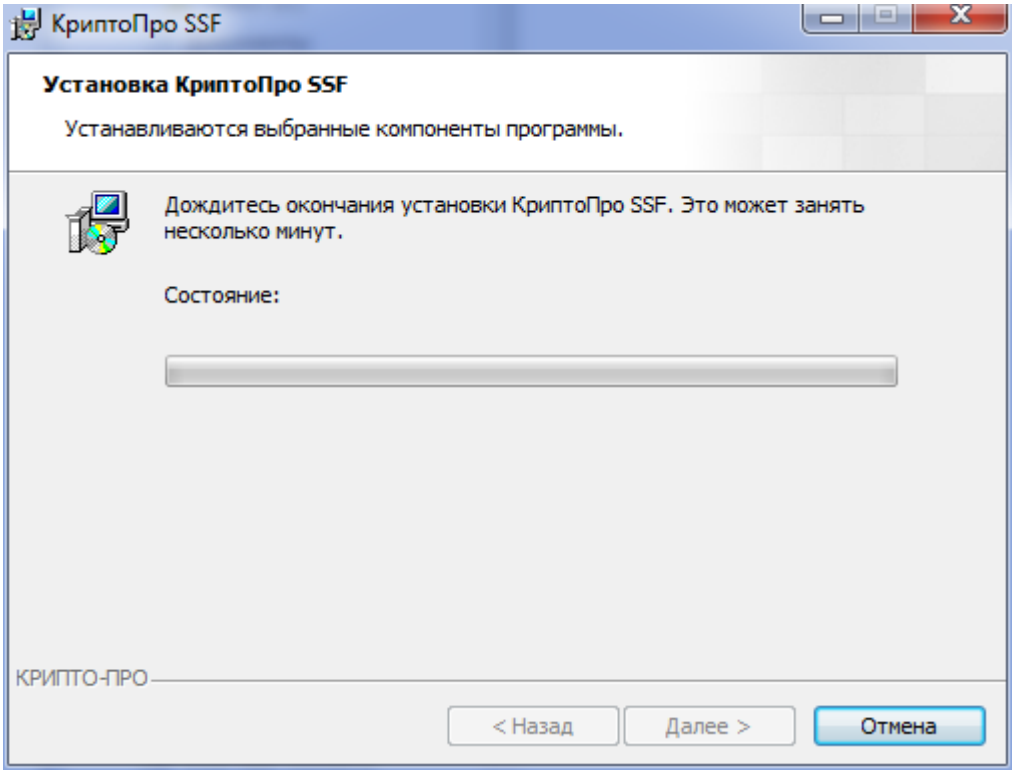
При формировании сообщений ЭП по формату CADES в том случае, если модуль «КриптоПро SSF» получает OCSP ответ от службы OCSP со значением временем в поле ThisUpdate меньшим, чем в полученном штампе времени, он будет продолжать посылать OCSP запросы с некоторым интервалом до тех пор, пока эти времена не станут, хотя бы равными.

В случае, когда для формирования ЭП по формату CAdES используются программные средства других производителей, которые в этот момент не проверяют расхождение времени штампа времени и OCSP ответа, может возникнуть ситуация, когда округленное до секунд время OCSP ответа окажется меньше неокругленного времени штампа (до 0.5 сек). Модуль КриптоПро SSF при проверке ЭП таких сообщений может выдать ошибку. Для предотвращения таких ситуаций может использоваться параметр AllowedExceedingTSPoverOCSPTime в настройках политики модуля CAdES («Допустимое превышение времени штампа над временем начала действия (ThisUpdate) OCSP ответа в CAdES сообщениях. От 0 до 10 секунд»). Значение данного параметра может быть задано при установке модуля КриптоПро SSF на представленном ниже экране. В результате указанное значение будет занесено в Реестр Windows в ключ HKLM\Software\Policies\Crypto-Pro\CAdES\.

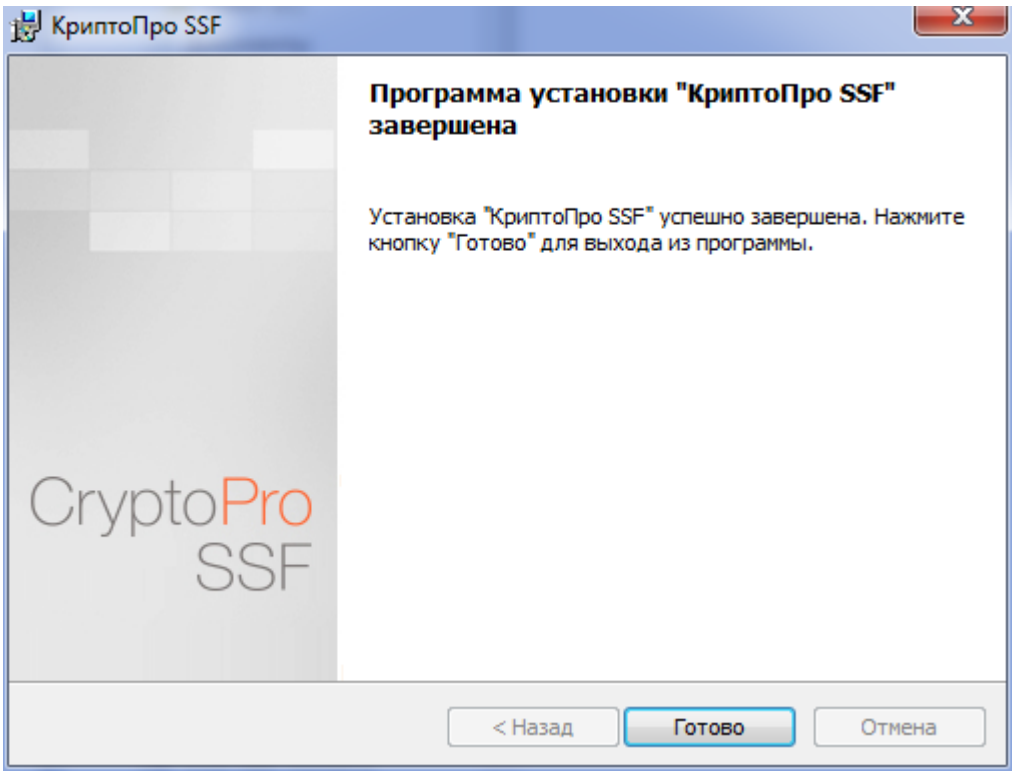


Для подтверждения нажмите кнопку **Установить**.

После выполнения всех описанных шагов мастер устанавливает ПО КриптоПро SSF, сопровождая действия комментариями.



По окончании установки мастер показывает окно с подтверждением успешной установки, где необходимо нажать кнопку **Готово**.



При переустановке/удалении дистрибутива КриптоПро SSF следует переустановить и ПО КриптоПро CSP.

2.3. Установка дистрибутива КриптоПро SSF в ОС UNIX/Linux

В ОС семейства UNIX/Linux дистрибутивы продуктов Крипто-Про представляют собой установочные пакеты, общепринятые для каждой конкретной ОС.

Например, для ОС Linux – это rpm пакеты, для ОС Solaris - .tar.gz пакеты и т.д.

Для установки используются стандартные установщики ОС.

Для функционирования модуля «КриптоПро SSF» необходимо, чтобы на целевом компьютере было предварительно установлено СКЗИ КриптоПро CSP (возможно использование СКЗИ КриптоПро HSM) версии 4.0 и старше. Сведения и инструкции по установке, указанных СКЗИ приведены в соответствующей документации на данные продукты.

Далее необходимо установить либо 3 отдельных пакета в указанном порядке:

- Клиент службы штампов времени
- Клиент службы OCSP
- CADES SDK

либо установить набор «КриптоПро ЭЦП» версии 2.0 или новее согласно документации на данный продукт.

После указанных шагов необходимо установить пакет «КриптоПро SSF»

Например, в ОС Linux по первому варианту необходимо выполнить команды:

rpm –ivh lsb-cprocsp-tsp-util-64-4.0.0-4.x86_64.rpm

rpm –ivh lsb-cprocsp-ocsp-util-64-4.0.0-4.x86_64.rpm

rpm –ivh lsb-cprocsp-cades-64-4.0.0-4.x86_64.rpm

rpm –ivh lsb-cprocsp-sapssf-64-4.0.0-4.x86_64.rpm

В ОС Solaris пакеты сначала разархивируются:

gzip –d <имя пакета>.tar.gz

tar –xf <имя пакета>.tar

Потом устанавливаются командой pkgadd:

pkgadd –na ./admin –d . CPROTSPutlx

pkgadd –na ./admin –d . CPROOCSPutx

pkgadd –na ./admin –d . CPROCadesx

pkgadd –na ./admin –d . CPROssfx

При установке пакетов автоматически прописываются временные ознакомительные лицензии (для клиента TSP, OCSP и для модуля КриптоПро SSF), действующие в течение 3-х месяцев с момента первой установки.

По истечении трех месяцев использование данных модулей будет возвращать ошибку. В журнале она может быть идентифицирована по коду ошибки – 0x8007064A.

Для установки постоянных лицензий необходимо воспользоваться командами:

- для клиента TSP:

/opt/cprocsp/bin/<процессорная архитектура>/tsputil license –s <номер лицензии>

- для клиента OCSP:

/opt/cprocsp/bin/<процессорная архитектура>/ocsputil license –s <номер лицензии>

- для модуля КриптоПро SSF:

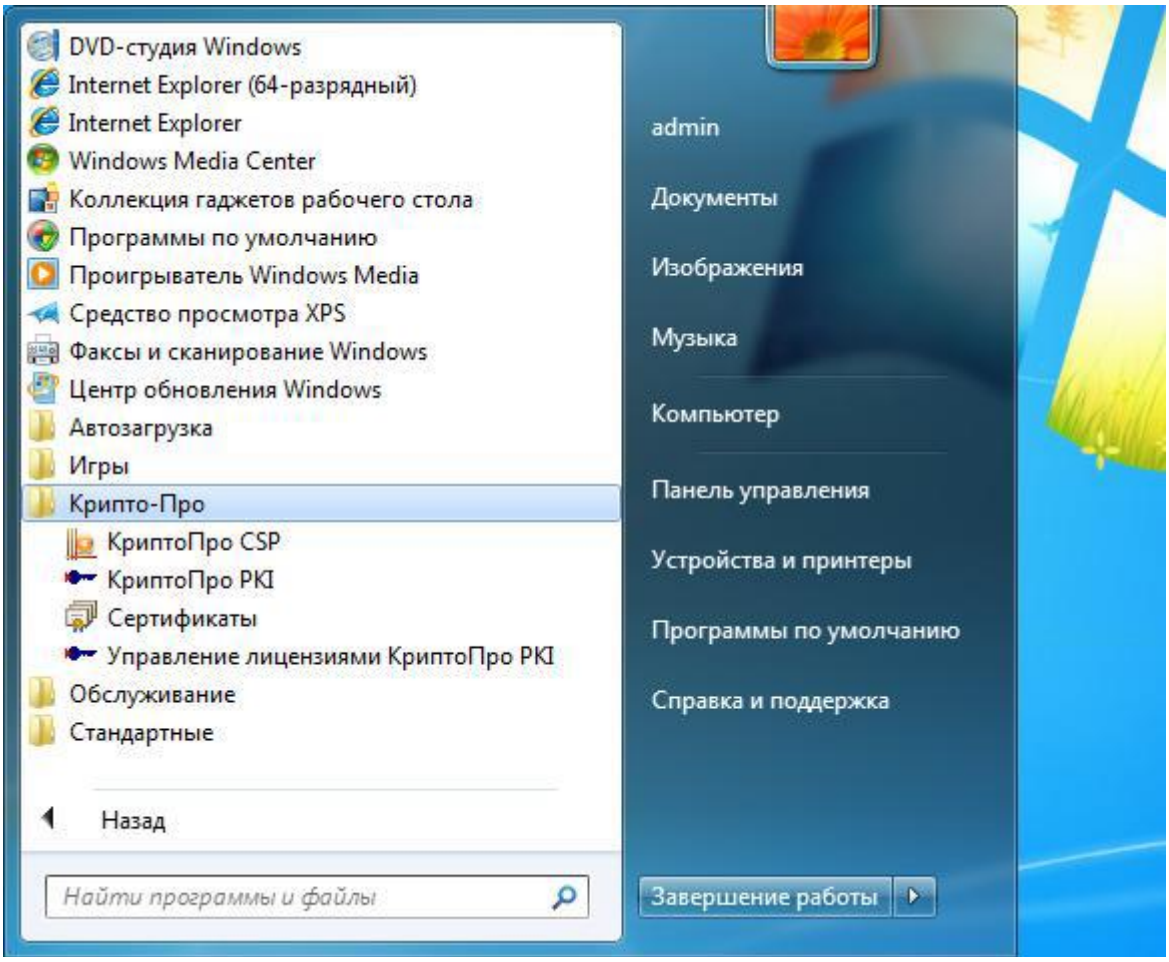
/opt/cprocsp/bin/<процессорная архитектура>/ssflicense <номер лицензии>

3. Настройка ПО «КриптоПро SSF»

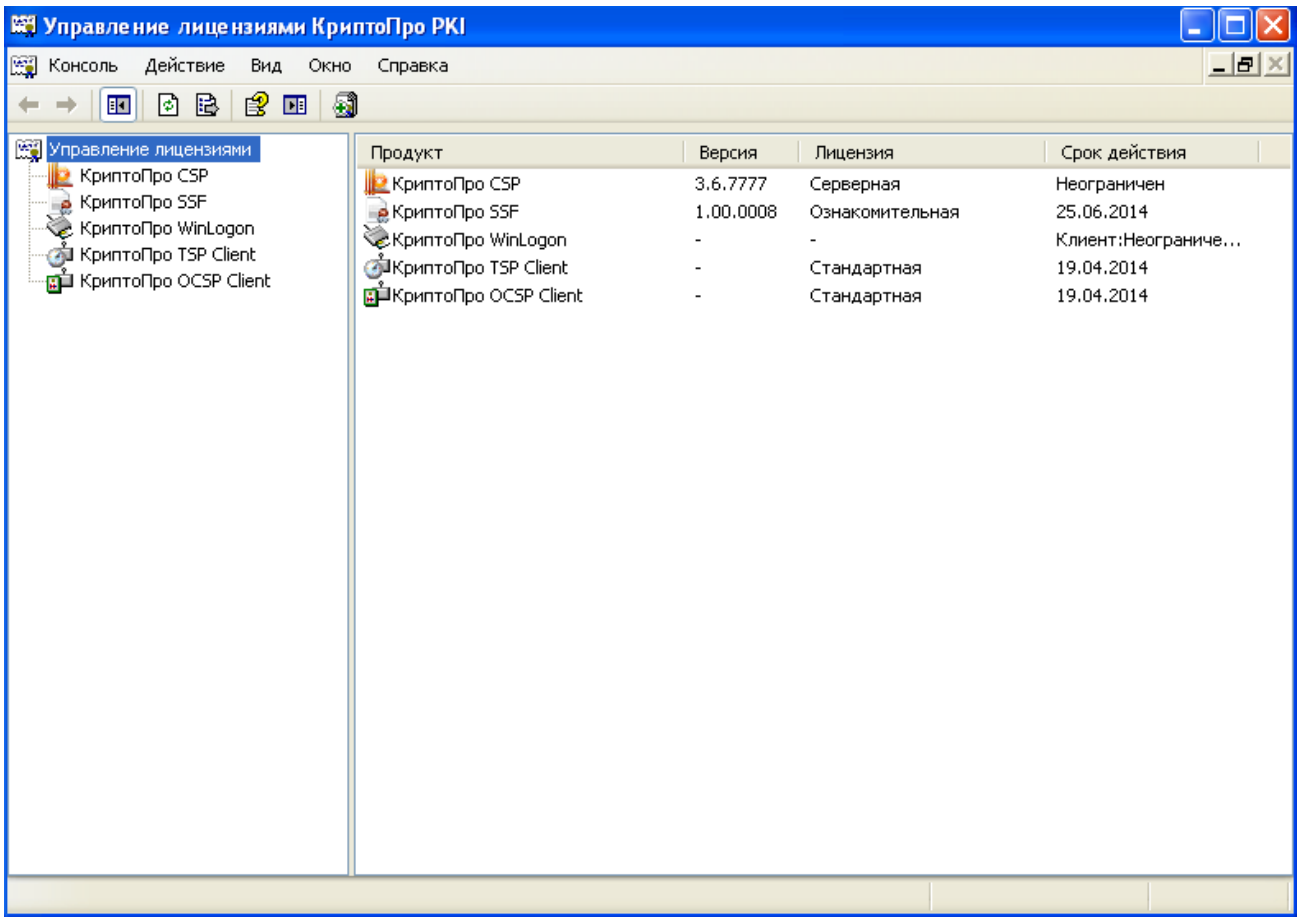
3.1. Ввод серийных номеров лицензий для модулей «КриптоПро SSF»

При установке программного обеспечения «КриптоПро SSF» без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования «КриптоПро SSF» после окончания этого срока пользователь должен ввести серийный номер с бланка Лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта.

Для ввода лицензии выполните Пуск -> Программы -> Крипто-Про -> Управление лицензиями КриптоПро PKI. В оснастке Управление лицензиями КриптоПро PKI выберите продукт, лицензию на который Вы хотите ввести. В контекстном меню выберите Все задачи - Ввести серийный номер.



Кроме использования лицензии на использование модуля «КриптоПро SSF», в случае необходимости в формировании усовершенствованной электронной подписи (формат CADES), необходимо также ввести серийные номера лицензий на использование клиентов служб OCSP и TSP.



3.2. Ввод серийных номеров лицензий для модулей «КриптоПро SSF» для ОС UNIX/Linux

При установке дистрибутивных пакетов в ОС семейства UNIX/Linux автоматически прописываются временные ознакомительные лицензии (для клиента TSP, OCSP и для модуля КриптоПро SSF), действующие в течение 3-х месяцев с момента первой установки.

По истечении трех месяцев использование данных модулей будет возвращать ошибку. В журнале она может быть идентифицирована по коду ошибки – 0x8007064A.Для установки постоянных лицензий необходимо воспользоваться командами:

- для клиента TSP:

/opt/cprocsp/bin/<процессорная архитектура>/tsputil license –s <номер лицензии>

- для клиента OCSP:

/opt/cprocsp/bin/<процессорная архитектура>/ocsputil license –s <номер лицензии>

- для модуля КриптоПро SSF:

/opt/cprocsp/bin/<процессорная архитектура>/ssflicense <номер лицензии>

Соответственно, просмотреть информацию об установленных лицензиях можно при помощи команд:

/opt/cprocsp/bin/<процессорная архитектура>/tsputil license

/opt/cprocsp/bin/<процессорная архитектура>/ocsputil license

/opt/cprocsp/bin/<процессорная архитектура>/ssflicense

3.3. Настройка параметров усовершенствованной электронной подписи

Сообщения на основе формата «CADES» представляют собой сообщения усовершенствованной электронной подписи (ЭП) - CAdES X Long Type 1("CMS Advanced Electronic Signatures"). Фиксация времени подписания электронного документа в данном формате реализуется посредством включения в сообщения штампов времени согласно рекомендациям RFC 3161 («Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP)»). Сохранение информации о статусе сертификата ключа проверки ЭП подписчика на момент времени подписания электронного документа обеспечивается посредством включения в сообщение подписанного ответа службы OCSP, формируемого согласно рекомендациям RFC 2560 («Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP»). Кроме этого в сообщение включаются все прочие доказательства подлинности конкретной электронной подписи.

Для формирования сообщений усовершенствованной ЭП необходим доступ к службе штампов времени и службе актуальных статусов сертификатов. Данные службы обычно разворачиваются в инфраструктуре удостоверяющих центров и предоставляют открытый доступ к своим сервисам. Доступ, в большинстве случаев, осуществляется по протоколу HTTP(s). Время на серверах служб должно быть синхронизировано. Например, Формат ЭП cades при формировании ЭП не допускает расхождения времени штампа и времени ocsp-ответа более чем на 60 сек.

Если адрес службы актуальных статусов сертификатов (OCSP) извлекается из сертификата, то адрес службы штампов времени необходимо указывать приложениям явно через возможные файлы конфигурации или через программный интерфейс.

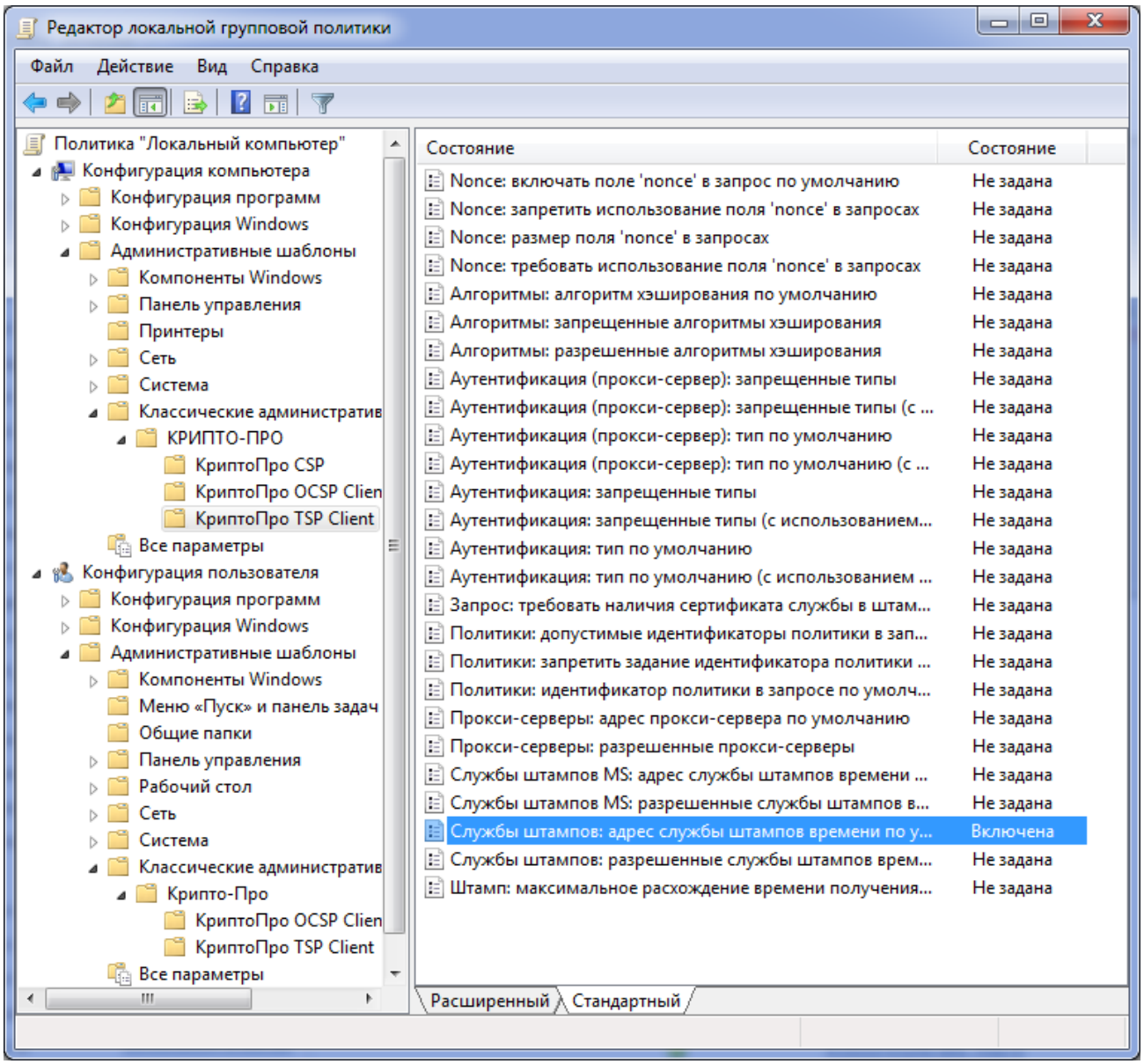
Модуль «КриптоПро SSF» использует для этого настройки групповых политик в ОС Windows. Дистрибутив «КриптоПро SSF» устанавливает шаблоны групповых политик клиентов служб OCSP и TSP. Для доступа к ним запустите консоль управления групповыми политиками ОС Windows при помощи команды:

gpedit.msc

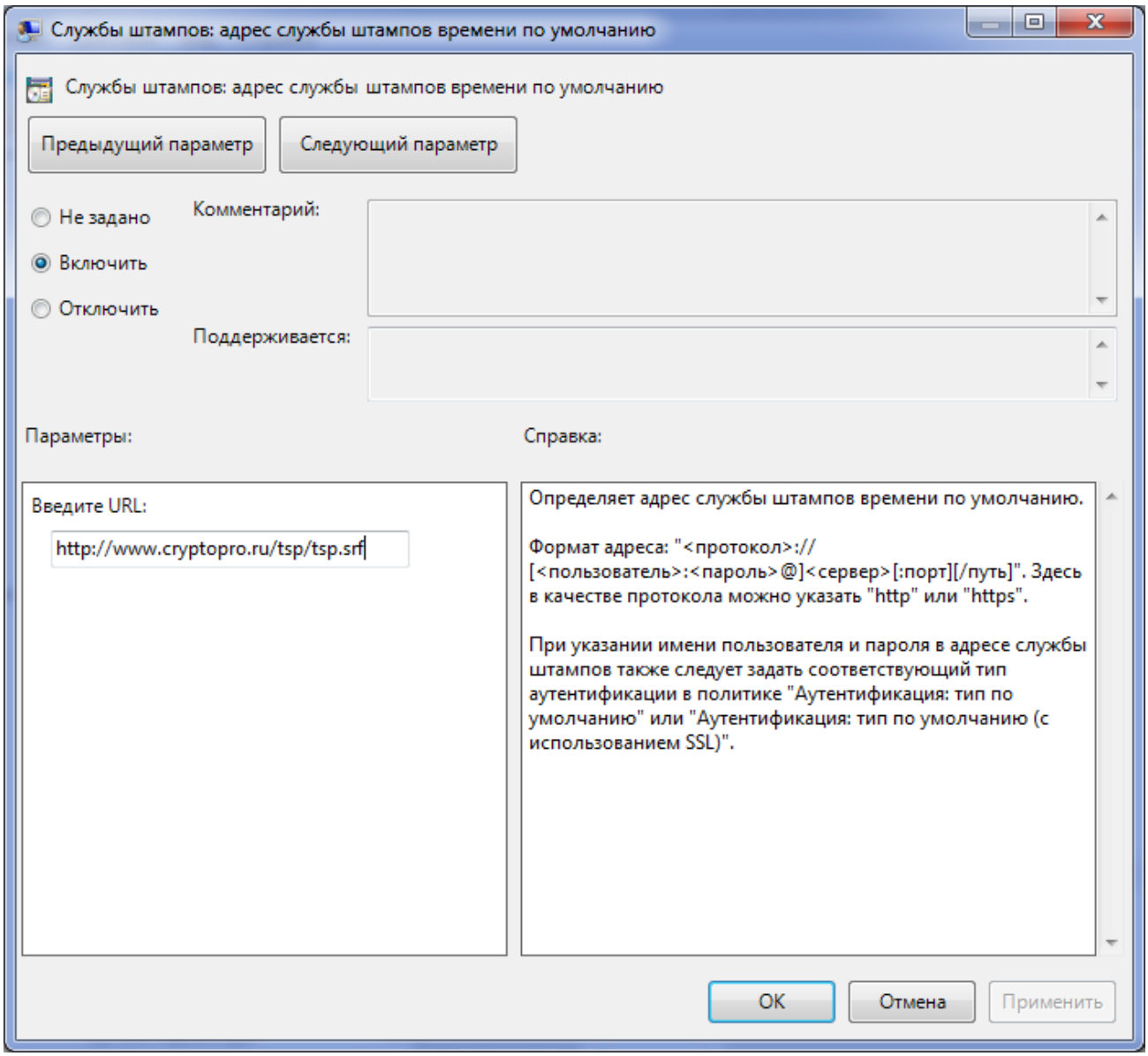
на 64-разрядных машинах с установленной 32 разрядной версией модуля необходимо запускать команду:

mmc -32 gpedit.msc

В открывшейся консоли:



выберите ветвь «Административные шаблоны» -> «Классические административные шаблоны» -> «КРИПТО-ПРО» -> «КриптоПро TSP Client» и задайте значение параметра «Службы штампов: адрес службы штампов времени по умолчанию»:



Введите URL, используемый для доступа к целевой службе.

Для изменения групповых политик в пространстве политик «Локальный компьютер» требуются права Администраторов локальной машины. При этом данные настройки будут действовать для всех пользователей данного компьютера.

Службы УЦ КриптоПро поддерживают балансировку нагрузки. Т.е. можно развернуть несколько серверов служб, при этом обращаясь к ним по одному адресу.

В случае, если требуется обеспечить надежность функционирования системы, путем развертывания нескольких служб TSP, к которым обращение осуществляется с использованием разных адресов, дополнительные адреса таких служб можно указать в переменной окружения или в значении параметра файла настроек ssf.ini - **CP_SSF_ADD_TSP**. Адреса служб при этом разделяются символом ";". Например,

CP_SSF_ADD_TSP=http://testca.cryptopro.ru/tsp/tsp.srf;http://testca.cryptopro.ru/tsp1/tsp.srf

При этом процедура подписи будет пытаться сначала обращаться по основному адресу службы, указанному в оснастке групповой политики, а в случае неудачи, повторять процедуру с использованием адресов служб указанных в переменной окружения или в значении параметра файла настроек ssf.ini.

3.4. Настройка параметров усовершенствованной электронной подписи в ОС UNIX/Linux

Параметры усовершенствованной электронной подписи, описанные в предыдущем пункте, в ОС семейства UNIX/Linux прописываются в конфигурационном файле СКЗИ КриптоПро CSP:

/etc/opt/cprocsp/config[64].ini

Параметры клиента TSP указываются в секции [cades/tsppolicy], клиента OCSP в секции [cades/ocsppolicy]. Например:

[cades/tsppolicy]

DefaultTSPURL = http://www.cryptopro.ru/tsp/tsp.srf

Полный список политик, которые можно задавать, описан в документации на КриптоПро ЭП SDK (cades).

3.5. Настройка ПО SAP для использования модуля «КриптоПро SSF»

Система SAP должна иметь возможность доступа к функциям модуля «КриптоПро SSF». Для этого необходимо указать расположение модуля на целевой машине и используемые им алгоритмы. На клиентских компьютерах это осуществляется через конфигурационный файл ssfrfc.ini или через переменные окружения. На серверах приложений это задается через параметры профиля или переменные окружения.

На 64 разрядных версиях операционных систем следует правильно указывать имя модуля cpsapssf.dll в ssfrfc.ini (или в переменной окружения). Не используйте 64-разрядную версию библиотеки, если вызывать её будете из 32-х разрядного приложения. Используйте для этого версию библиотеки, установленную в каталог …\Program Files **(x86)**\... SAP приложения на клиентских компьютерах обычно 32-х разрядные!

Информация о пользователях, задействованных в инфраструктуре PKI, также должна быть корректно отражена в системе SAP, в зависимости от используемого ABAP приложения.

Сведения по настройке данных параметров см. в документации на соответствующие продукты SAP.

Некоторые параметры работы модуля КриптоПро SSF можно изменять в переменных окружения или в конфигурационном файле ssf.ini.

Модуль «КриптоПро SSF» ищет файл ssf.ini в каталогах %commonappdata%\Crypto Pro\ (общий каталог для всех пользователей) и в каталоге %localappdata%\Crypto Pro\ (файл в каталоге AppData текущего пользователя, под учетным именем, которого работает приложение).

Дополнительные параметры сначала извлекаются из общего для всех пользователей файла %commonappdata%\Crypto Pro\ssf.ini, если файл отсутствует или в нем отсутствует требуемый параметр, то производится попытка найти значение требуемого параметра в файле %localappdata%\Crypto Pro\ssf.ini. Если и там параметр отсутствует, то производится попытка получить значение параметра из переменной окружения.

Список дополнительных параметров приведен в Приложение. Список переменных окружения и параметров ssf.ini.

Пример содержимого файла настроек:

```
[cpsapssf]
CP_SSF_USERID=CERT_HASH
CP_SSF_ADD_TSP=http://testca.cryptopro.ru/tsp/tsp.srf;http://www.cryptopro.ru/tsp/tsp.srf
CP_SSF_ASK_PIN_WHEN_EMPTY=1
#CP_SSF_VERIFYCERTFLAGS=0x40000000
```

Имя секции [cpsapssf] – обязательно.

Последний параметр в данном примере закомментирован.

3.6. Настройка ПО SAP для использования модуля «КриптоПро SSF» в ОС UNIX/Linux

В ОС семейства UNIX/Linux модуль КриптоПро SSF устанавливается как разделяемая библиотека /opt/cprocsp/lib/<процессорная архитектура>/libcpsapssf.so.1.0.0.

Именно этот путь следует прописывать в настройках SAP для доступа к ней в файле ssfrfc.ini на SAP клиенте или в параметре ssf/ssfapi_lib настроек сервера SAP. Например,

```
ssf/ssfapi_lib = /opt/cprocsp/lib/sparcv9/libcpsapssf.so.1.0.0
ssf/ssf_md_alg = GOST3411
ssf/ssf_symencr_alg = GOST28147
ssf/name = CPSAPSSF
```

В ОС семейства UNIX/Linux параметры модуля КриптоПро SSF задаются только через переменные окружения. Файлов ssf.ini, trace.ini – нет.

4. Реализация программного интерфейса SSF модулем «КриптоПро SSF»

Модуль «КриптоПро SSF» реализует программный интерфейс Secure Store & Forward (SSF) в соответствии с технической документацией «Secure Store & Forward (SSF). API Specifications (Version 1.0)».

Выполнение криптографических функций модулем основано на использовании сертификатов ключей проверки электронной подписи стандарта X.509v3 согласно RFC 5280 "Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile" с учетом RFC 4491 "Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile".

Программный модуль «КриптоПро SSF» представляет собой динамически подгружаемую библиотеку операционной системы Windows, имеет название cpsapssf.dll и находится в каталоге, зависящем от места, выбранного при установке дистрибутива и устанавливаемой конфигурации (win32 или x64) (типовая установка копирует файл в каталог C:\Program Files\Crypto Pro\SSF\ (на 64-х разрядных ОС 32-х битная версия модуля - C:\Program Files (x86)\Crypto Pro\SSF\)).

4.1. Краткий обзор

В соответствии с SSF API модуль «КриптоПро SSF» реализует 17 функций: 10 основных и 7 второстепенных (в основном предназначенных для создания и удаления объектов, используемых в основных функциях).

Основные функции:

SsfEncode
SsfDecode
SsfSign
SsfAddSign
SsfVerify
SsfEnvelope
SsfDevelope
SsfDigest
SsfVersion
SsfQueryProperties

Второстепенные функции:

SsfDELSsfOctetstring
SsfNEWSigRcpSsfInfo
SsfDELSigRcpSsfInfo
SsfINSSigRcpSsfInfo
SsfDELSigRcpSsfInfoList
SsfPRISigRcpSsfInfo
SsfPRISigRcpSsfInfoList

4.2. Символьные обозначения

4.2.1. Форматы криптографических сообщений

Модуль «КриптоПро SSF» реализует два формата криптографических сообщений, имеющих следующие символьные обозначения:

- «PKCS7»
- «CADES»

Наименование PKCS7 говорит само за себя. Сообщения данного формата формируются по правилам международного формата PKCS#7 с некоторыми дополнениями согласно RFC 3852 "Cryptographic Message Syntax (CMS)" с учетом RFC 4490 "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)".

Сообщения на основе формата «CADES» представляют собой сообщения усовершенствованной электронной подписи (ЭП) – «**CAdES X Long Type 1»**("CMS Advanced Electronic Signatures"). Фиксация времени подписания электронного документа в данном формате реализуется посредством включения в сообщения штампов времени согласно рекомендациям RFC 3161 («Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP)»). Сохранение информации о статусе сертификата ключа проверки ЭП подписчика на момент времени подписания электронного документа обеспечивается посредством включения в сообщение подписанного ответа службы OCSP, формируемого согласно рекомендациям RFC 2560 («Internet X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP»). Кроме этого в сообщение включаются все прочие доказательства подлинности конкретной электронной подписи.

Для совместимости с модулями других производителей введены синонимы обозначения формата CADES. Помимо указанного идентификатора «CADES» можно использовать идентификатор «PKCS7_CADES». В некоторых случаях это позволяет использовать один и тот же конфигурационный файл ssfrfc.ini.

В процедуре проверки ЭП можно также использовать идентификатор «PKCS7_ANY». В данном случае модуль будет автоматически определять формат переданного ему криптографического сообщения (PKCS#7 или CADES) и запускать соответствующую обработку. Это позволяет обрабатывать сообщения, не зная заранее по какому типу оно было сформировано контрагентом.

4.2.2. Хэш алгоритмы

Модуль «КриптоПро SSF» поддерживает вычисление хэш значений по следующим алгоритмам:

- MD2
- MD5
- SHA1
- ГОСТ Р 34.11-94

Символьными обозначениями данных алгоритмов, передаваемых в качестве параметров функций, являются соответственно:

- «MD2»
- «MD5»
- «SHA1»
- «GOST3411»

Для совместимости с модулями других производителей введены синонимы обозначения алгоритма ГОСТ Р 34.11-94. Помимо указанного идентификатора «GOST3411» можно использовать идентификатор "GOST-R-34.11-94". В некоторых случаях это позволяет использовать один и тот же конфигурационный файл ssfrfc.ini.

Данные обозначения используются в основном в функции SsfDigest, которая способна вычислить и вернуть хэш значение по любому из указанных алгоритмов. Т.к. модуль «КриптоПро SSF» использует в основном Российские криптографические алгоритмы, в функциях SsfSign, SsfAddSign нельзя указать явное использование хэш алгоритмов “MD2”, “MD5” и “SHA1”. Использование хэш алгоритмов тесно связано с тем, какой алгоритм открытого ключа представлен в соответствующем сертификате ключа электронной подписи. Поэтому данные функции в текущей реализации модуля сами вычисляют, какой из алгоритмов использовать,

исходя из представленного алгоритма открытого ключа в сертификате. Это в принципе позволяет формировать электронные подписи не только по стандартам ГОСТ, но и RSA.

4.2.3. Симметричные алгоритмы шифрования

В качестве симметричного алгоритма шифрования в модуле «КриптоПро SSF» используется только алгоритм ГОСТ 28147-89, имеющий символьное представление «GOST28147». Данное символьное обозначение алгоритма используется в функции SsfEnvelope.

Для совместимости с модулями других производителей введены синонимы обозначения алгоритма ГОСТ 28147-89. Помимо указанного идентификатора «GOST28147» можно использовать идентификатор "GOST-28147-89". В некоторых случаях это позволяет использовать один и тот же конфигурационный файл ssfrfc.ini.

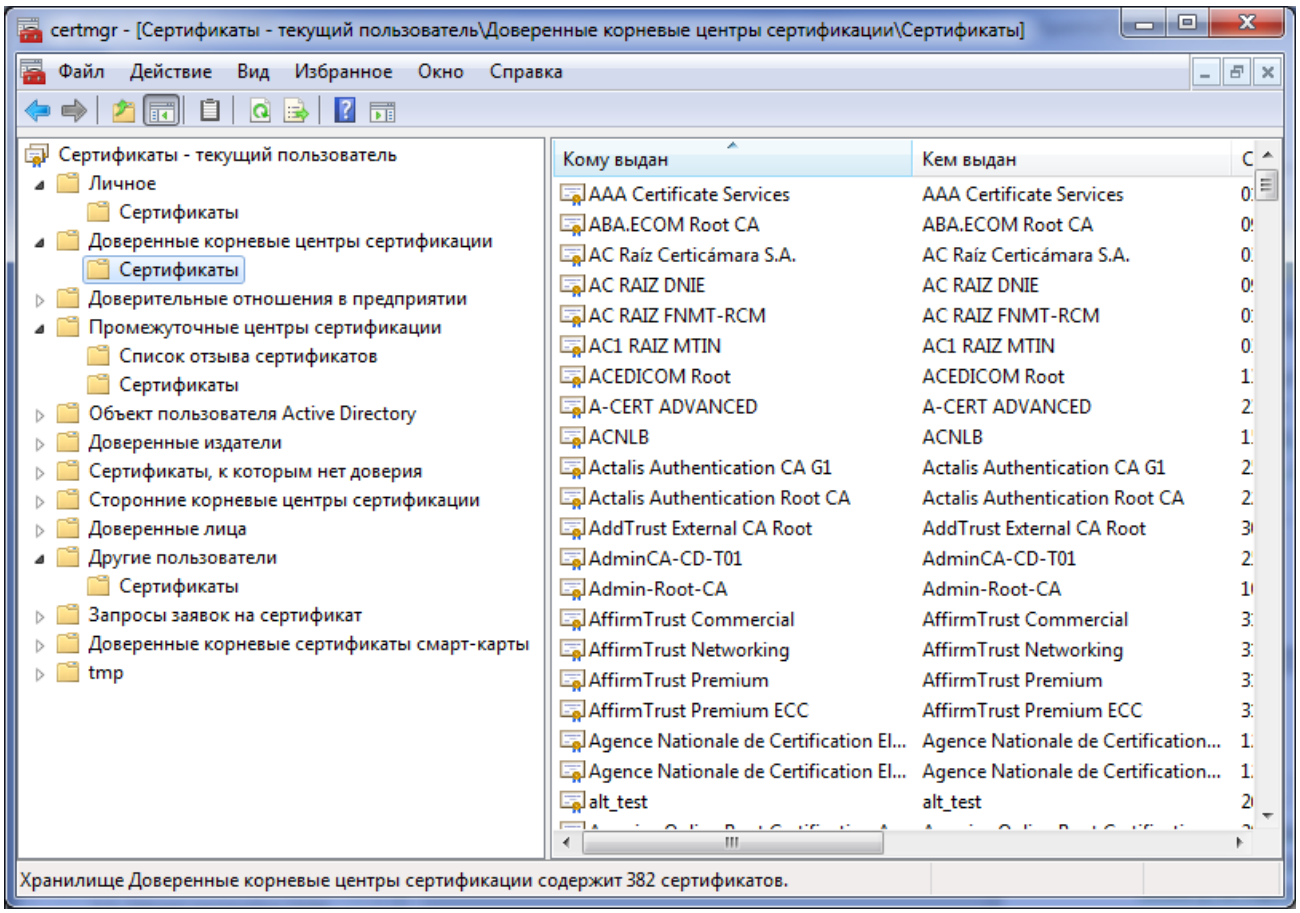
4.3. Идентификаторы, защищенные профили и адресные книги пользователей

Модуль «КриптоПро SSF» использует механизмы безопасности и разграничения доступа, встроенные в операционную систему. Это означает, что каждый пользователь, открывая рабочую сессию операционной системы, проходя при этом встроенные процедуры аутентификации (например, вводя при этом свой логин и пароль или предоставив свою смарт-карту), получает при этом защищенное, изолированное от других пользователей пространство, где может хранить свои личные данные (свои сертификаты ключей проверки электронной подписи, адресную книгу и прочее).

В операционной системе Windows такое пространство называется «пространством текущего пользователя» (Current User space). Кроме этого существует ещё и общее пространство – «пространство локального компьютера» (Local Machine space), где могут храниться общие данные всех пользователей, либо данные, которые должны быть доступны системным сервисам, которые не проходят явным образом процедуру аутентификации. Обычно данные в таком пространстве доступны только привилегированным учетным записям (Администраторам, LocalSystem и подобным). В таком пространстве могут храниться сертификаты ключей проверки ЭП и адресные книги системных сервисов, подписывающих, проверяющих электронную подпись, а также шифрующих и расшифровывающих сообщения в автоматическом режиме.

Закрытые ключи пользователей, с помощью которых они подписывают или расшифровывают сообщения, хранятся обычно под защитой соответствующего средства криптографической защиты информации (СКЗИ). Физически, обычно, они располагаются на отчуждаемых носителях.

Сертификаты ключей проверки ЭП в ОС Windows принято хранить в специальных хранилищах сертификатов на локальном диске. При этом существует несколько хранилищ, различающихся по принадлежности и назначению сертификатов.



Хранилище «My» (внешнее имя – «Личное»), предназначено для хранения личных сертификатов пользователя. Сертификаты в нем, обычно, лежат вместе со ссылкой на закрытый ключ, по которой приложения и обращаются к контейнеру закрытого ключа.

Хранилище «Root» (внешнее имя – «Доверенные корневые центры сертификации») содержит, обычно, сертификаты удостоверяющих центров, которым данный пользователь абсолютно доверяет. Сертификаты хранятся без ссылок на закрытые ключи.

Хранилище «Ca» (внешнее имя – «Промежуточные центры сертификатов») содержит, обычно, сертификаты удостоверяющих центров, которым для завершения цепочки доверия требуется сертификат из хранилища «Root». В этом же хранилище содержатся и списки отозванных сертификатов. Сертификаты хранятся без ссылок на закрытые ключи.

Хранилище «Addressbook» (внешнее имя – «Другие пользователи») содержит, обычно, сертификаты пользователей контрагентов, требующиеся для проверки их электронной подписи, либо для шифрования в их адрес сообщений. Сертификаты этих пользователей также хранятся без ссылок на соответствующие закрытые ключи. Данное хранилище создается почтовым клиентом Windows (например, Microsoft Outlook). Если на вашей машине оно отсутствует, его можно создать вручную, добавив в системный реестр ОС Windows разделы:

[HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\AddressBook]
[HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\AddressBook\Certificates]
[HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\AddressBook\CRLs]
[HKEY_CURRENT_USER\Software\Microsoft\SystemCertificates\AddressBook\CTLs]

Внимание. Правка системного реестра должна осуществляться квалифицированным пользователем ОС Windows.

В адресном пространстве Local Machine (компьютера) – свои хранилища сертификатов с теми же наименованиями. Доступ к этим хранилищам обычно требует специальных прав доступа (прав администратора).

Модуль «КриптоПро SSF» использует названия хранилищ с одно символьным префиксом для указания места, в котором искать требуемые сертификаты. Префикс «u» используется для указания хранилища, расположенного в Current User пространстве, префикс «m» используется для указания хранилища, расположенного в Local Machine пространстве. Например, для указания защищенного профиля пользователя (Security Profile), подписывающего сообщение (в функции SsfSign, SsfAddSign), работающего в интерактивном режиме (с возможностью выдачи окон на ввод пароля) можно указывать «uMy», а для сервиса, подписывающего сообщения автоматически – «mMy». Для указания «адресной книги» пользователя, выполняющего проверку подписи, или шифрование сообщений в адрес других пользователей (в функции SsfVerify, SsfEnvelope), имеющего личную адресную книгу, можно указывать «uAddressbook», а для сервиса – «mAddressbook». Соответственно сертификаты пользователей контрагентов должны быть помещены именно в эти хранилища.

Для совместимости с модулями других производителей можно указывать наименования хранилищ, без префиксов "u" или "m" (например, просто «My»). В этом случае будут открываться хранилища, находящиеся в адресном пространстве пользователя (Current User). В настройках модулей некоторых производителей перед именем хранилища может встретиться 14 символьное обозначение даты (YYYYMMDDHHNNSS), например «20140919120000My» (формируется некоторыми приложениями, которым передается имя «<TIME>My»). Модуль КриптоПро SSF просто отбрасывает эти первые 14 цифр, никак их не обрабатывая, а просто использует следующее за ними наименование хранилища.

В некоторых случаях это позволяет использовать одни и те же настройки SAP приложения при использовании модулей различных производителей.

В ОС семейства UNIX/Linux сертификаты ключей проверки подписи также должны быть установлены в соответствующие хранилища сертификатов пользователей (Current User) или системы/компьютера (Local Machine). Типовые имена хранилищ те же самые, что и для ОС Windows:

my – личные сертификаты;

root - корневые доверенные сертификаты;

ca – сертификаты промежуточных центров сертификации, а также списки отозванных сертификатов;

addressbook – сертификаты контрагентов;

Сертификаты, используемые при формировании ЭП или расшифровании сообщений должны быть установлены в хранилище со ссылкой на закрытый ключ.

Для выполнения операций с сертификатами и хранилищами в ОС семейства UNIX/Linux можно использовать утилиту из состава СКЗИ КриптоПро CSP – certmgr (/opt/cprocsp/bin/<процессорная архитектура>/certmgr).

В качестве идентификатора пользователя/сертификата, требуемого для подписи или расшифровки сообщения, используется «отличительное имя» (Distinguished Name), используемое в сертификате. В данной версии модуля можно указывать не всё имя, а лишь часть этого имени, но она должна уникально идентифицировать пользователя/сертификат пользователя. Например, если в сертификате таким уникальным атрибутом имени выступает e-mail пользователя или ИНН, то можно указывать только строку вида «E=user1@company.com» или «INN=000000000000». По данным атрибутам в указанном хранилище будет найден требуемый сертификат, и именно с ним будет выполняться заданная операция подписи/шифрования/расшифрования/проверки подписи.

К идентификатору пользователя предъявляются следующие требования:

- идентификатор может использовать локализованные имена в национальной кодировке, например в кодировке CP_1251 (кириллица), при этом не допускается формирование данной строки из символов Unicode. Можно использовать имя в виде escape последовательности Unicode представлений символов. Например, в виде:

C=RU, CN=\u0422\u0435\u0441\u0442 \u041A\u0440\u0438\u043F\u0442\u043E-\u041F\u0440\u043E \"SSF\"

- Значение отдельного атрибута имени должно заключаться в двойные кавычки, если выполняется хотя бы одно из следующих условий:
    - Значение содержит лидирующие или хвостовые пробелы

- Значение содержит хотя бы один из следующих символов
  - Запятая (,)
  - Плюс (+)
  - Знак “равно” (=)
  - Обратный слэш с последующим символом n (\n), обозначающие перевод строки
  - Знак “меньше” (<)
  - Знак “больше” (>)
  - Знак “номер” (#)
  - Точка с запятой (;)

- Если Значение атрибута содержит внутри себя символы «двойная кавычка» (”), то они должны экранироваться символом «обратный слэш» (\”), либо второй двойной кавычкой (””).
- Идентификатор пользователя может содержать следующие имена атрибутов:

Имя	**OID**	**Пояснение**
CN	2.5.4.3	COMMON NAME
L	2.5.4.7	LOCALITY NAME
O	2.5.4.10	ORGANIZATION NAME
OU	2.5.4.11	ORGANIZATIONAL UNIT NAME
E,EMAIL	1.2.840.113549.1.9.1	Email адрес
C	2.5.4.6	COUNTRY NAME
S, ST	2.5.4.8	STATE OR PROVINCE NAME
STREET	2.5.4.9	STREET ADDRESS
T, TITLE	2.5.4.12	TITLE
G, GIVENNAME	2.5.4.42	GIVEN NAME
I, INITIALS	2.5.4.43	INITIALS
SN	2.5.4.4	SUR NAME
DC	0.9.2342.19200300.100.1.25	DOMAIN COMPONENT
INN	1.2.643.3.131.1	ИНН
OGRN	1.2.643.100.1	ОГРН
OGRNIP	1.2.643.100.5	ОГРН индивидуального предпринимателя
SNILS	1.2.643.100.3	СНИЛС
PS	2.5.4.65	Псевдоним

Если у атрибута отсутствует короткое имя, то вместо него должен указываться объектный идентификатор. Также, вместо коротких имен можно использовать их объектные идентификаторы.

Порядок следования идентификаторов и их значений не обязательно должен соответствовать порядку в соответствующем сертификате ключа проверки ЭП.

Примеры:

CN=Иванов Иван Иванович, L=город Санкт-Петербург, C=RU

CN=Иванов Иван Иванович, L=город \”Санкт-Петербург\”, C=RU

CN=Иванов Иван Иванович, L=город \”Санкт-Петербург\”, C=RU

CN=” Иванов Иван Иванович”, L=город Санкт-Петербург, C=RU

CN=”Иванов Иван, сын Ивана”, L=город \”Санкт-Петербург\”, C=RU

CN=”Женя + Саша = любовь”, L=город \”Санкт-Петербург\”, C=RU

2.5.4.3=”Женя + Саша = любовь”, L=город \”Санкт-Петербург\”, 2.5.4.6=RU

2.5.4.3=”Женя + Саша = любовь”, L=”город \”Санкт-Петербург\” ”, 2.5.4.6=RU

C=RU, CN=\u0422\u0435\u0441\u0442 \u041A\u0440\u0438\u043F\u0442\u043E-\u041F\u0440\u043E \"SSF\"

C=RU, CN="\u0422\u0435\u0441\u0442 \u041A\u0440\u0438\u043F\u0442\u043E=\u041F\u0440\u043E \"SSF\""

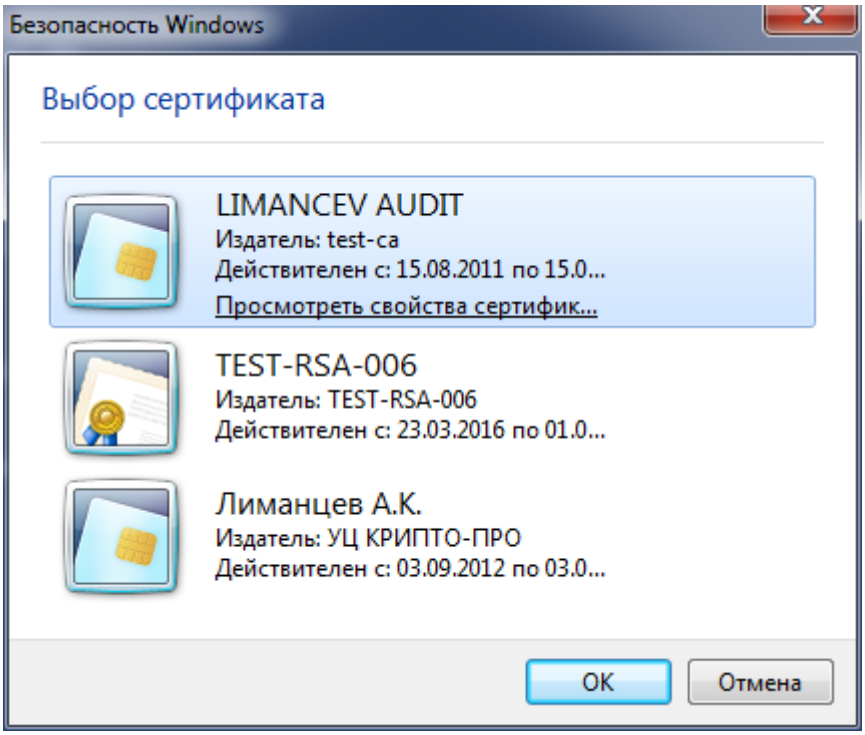
В операции проверки подписи модуль заполняет поле идентификатора пользователя полным отличительным именем, взятым из сертификата ключа проверки ЭП. При этом по возможности используются короткие имена атрибутов. Для конвертации локализованных строк используется кодовая страница «по умолчанию», принятая для сеанса текущего пользователя SAP в операционной системе (CP_ACP).

Необходимо отметить, что очень часто у пользователя появляется несколько сертификатов с одним и тем же отличительным именем. Например, при плановой смене ключа удостоверяющий центр переиздает сертификат с новым значением открытого ключа, но с тем же самым отличительным именем владельца. Модуль «КриптоПро SSF» делает всё возможное, чтобы в подобной ситуации выбрать правильный сертификат. Например, при поиске требуемого сертификата в хранилище, поиск не прекращается до тех пор, пока с помощью указанного пароля не удастся «прогрузить» закрытый ключ, соответствующий связанному с ним сертификату.

Чтобы избежать всех негативных моментов, связанных с кодировкой DN строки сертификатов, в которых используются национальные языки для представления атрибутов имени, в качестве идентификатора пользователя/сертификата можно использовать SHA1 хэш значение сертификата («отпечаток» или «fingerprint») вида «55 20 fe ff bf a3 ad ba 55 6c 67 6f 28 52 da 69 f6 e3 51 4d», который можно просто скопировать с графического отображения сертификата в ОС Windows.

Если при этом указать в переменной окружения или в значении параметра файла настроек ssf.ini **CP_SSF_USERID** значение “CERT_HASH” (CP_SSF_USERID=CERT_HASH), то в операции проверки подписи модуль будет заполнять поле идентификатора пользователя также значением «отпечатка» сертификата, использовавшегося для проверки ЭП. Приложение может сопоставлять этот отпечаток с именем пользователя, хранящимся в его базе данных.

Для ОС Windows при формировании подписи на стороне клиента в качестве идентификатора пользователя/сертификата можно также указать специальное ключевое слово $SELECT_CERTIFICATE$. В этом случае при формировании ЭП или расшифровании сообщения на экран будет выдан список всех **действующих** сертификатов из указанного хранилища, **имеющих ссылку на закрытый ключ подписи**.



Пользователь сам должен будет выбрать из представленного списка сертификат ключа подписи, при помощи которого будет формироваться ЭП.

Как уже было указано, по умолчанию в данный список попадают сертификаты из указанного хранилища, прошедшие простую проверку по срокам действия сертификата всех сертификатов в цепочке и подписи каждого сертификата в цепочке. Данная процедура не включает проверку сертификатов на отзыв.

Для того, чтобы включить в процедуру проверку сертификатов на отзыв, необходимо указать в переменной окружения или в значении параметра файла настроек ssf.ini CP_SSF_VERIFYCERTFLAGS_ONSELECT соответствующее значение, например, 0x44000000 (см. описание аналогичного параметра CP_SSF_VERIFYCERTFLAGS).

Но надо иметь ввиду, что если у пользователя в данном хранилище находится много сертификатов и при этом при проверке на отзыв задействуются сервисы OCSP или сервис получения актуального списка отзыва, то процедура отбора сертификатов в список может затянуться. В этом случае рекомендуется следить за хранилищем сертификатов и доступностью указанных сервисов. Не следует хранить ненужные сертификаты, например, срок действия которых закончился и т.п.

При использовании данного механизма желательно доверить запрос пароля к ключу подписи также модулю КриптоПро SSF (см. п. 4.4).

Необходимо также помнить, что данный механизм может привести к ошибкам, связанным с человеческим фактором, когда пользователь случайно или намеренно может выбрать не тот сертификат, который должен использоваться для подписания данного вида документов.

4.4. Пароли доступа к защищенным профилям и адресным книгам

Пароль на доступ к адресной книге пользователя не используется. Модуль «КриптоПро SSF» использует механизмы безопасности и разграничения доступа, встроенные в операционную систему. Это означает, что каждый пользователь, открывая рабочую сессию операционной системы, проходя при этом встроенные процедуры аутентификации (например, вводя при этом свой логин и пароль или предоставив свою смарт-карту), получает при этом доступ к личным хранилищам сертификатов.

Для доступа к хранилищам в пространстве Local Machine используйте правила разграничения доступа ОС Windows.

Для доступа к защищенному профилю пользователя (фактически, для доступа к закрытому ключу) требуется пароль. Модуль «КриптоПро SSF» и используемое им средство криптографической защиты информации имеет возможность самостоятельно запрашивать пароль доступа к секретному ключу (выводить на экран окно запроса пароля). При этом действует правило: если длина переданного в функцию пароля меньше либо равна трем символам и первый символ является символом «!» (восклицательный знак), то модуль будет работать в интерактивном режиме, и сам будет запрашивать ввод пароля (это требование спецификации SAP для модулей SSF). В противном случае модуль будет работать в «молчаливом» (silent) режиме и программным путём устанавливать пароль, переданный в аргументах вызываемой функции.

Некоторые уже существующие приложения не поддерживают это требование спецификации SSF API, передавая в качестве пароля пустую строку. Для совместимости с ними в модуль «КриптоПро SSF» была добавлена дополнительная опция/переменная окружения - CP_SSF_ASK_PIN_WHEN_EMPTY.

Данная переменная используется в функциях SSF, где требуется доступ к закрытому ключу пользователя (SsfSign, SsfAddSign, SsfDevelope). Если значение данной переменной равно «1» или «YES» или «TRUE», то в случае, когда приложение передает модулю «КриптоПро SSF» пустую строку в качестве пароля доступа к контейнеру закрытого ключа, модуль будет расценивать это как указание на вывод окна для запроса пароля доступа к закрытому ключу (если на контейнер установлен пароль).

Список дополнительных параметров приведен в «Приложение. Список переменных окружения и параметров ssf.ini».

4.5. Журнал работы модуля КриптоПро SSF

Модуль «КриптоПро SSF» ведет трассировку использования вызовов функций. Данная трассировка помогает разобраться при возникновении ошибочных ситуаций. Она доступна

средствам отладки программ. Для записи трассировки в файл нужно настроить файл Trace.ini, который может располагаться в каталогах:

%commonappdata%\Crypto Pro\

%localappdata%\Crypto Pro\

Модуль «КриптоПро SSF» ищет параметры трассировки сначала в файле %commonappdata%\Crypto Pro\Trace.ini (общий файл для всех пользователей). Если файл отсутствует или там отсутствует нужный параметр, то продолжает искать в файле %localappdata%\Crypto Pro\Trace.ini (файл в каталоге AppData текущего пользователя, под учетным именем, которого работает приложение).

Пример файла настроек трассировки:

```
[Trace]
ProcessFlags=2

cpsapssf.dll=4
cpsapssf.dll.Logfile=cpsapssf.log
cades.dll=4
cades.dll.Logfile=cpsapssf.log
tspcli.dll=4
tspcli.dll.Logfile=cpsapssf.log
ocspcli.dll=2
ocspcli.dll.Logfile=d:\temp\ocspcli.log
```

Данные параметры означают:

- Включить трассировку для модуля cpsapssf.dll с самым детальным уровнем (4)
- Записывать трассировку модуля cpsapssf.dll в файл cpsapssf.log, который будет создан в каталоге %commonappdata%\Crypto Pro\LogFiles\, а при невозможности (отсутствии прав доступа) – в каталоге %localappdata%\Crypto Pro\LogFiles\. Если файл уже существует, то информация в него будет дописываться.
- Включить трассировку для модуля cades.dll с самым детальным уровнем (4)
- Записывать трассировку модуля cades.dll в файл cpsapssf.log, который будет создан в каталоге %commonappdata%\Crypto Pro\LogFiles\, а при невозможности (отсутствии прав доступа) – в каталоге %localappdata%\Crypto Pro\LogFiles\. Если файл уже существует, то информация в него будет дописываться.
- Включить трассировку для модуля tspcli.dll с самым детальным уровнем (4)
- Записывать трассировку модуля tspcli.dll в файл cpsapssf.log, который будет создан в каталоге %commonappdata%\Crypto Pro\LogFiles\, а при невозможности (отсутствии прав доступа) – в каталоге %localappdata%\Crypto Pro\LogFiles\. Если файл уже существует, то информация в него будет дописываться.
- Включить трассировку для модуля ocspcli.dll с уровнем детализации 2.
- Записывать трассировку модуля ocspcli.dll в файл с абсолютным именем d:\temp\ocspcli.log. Если файл уже существует, то информация в него будет дописываться. Права на создание/запись в данный файл должны быть соответствующим образом установлены администратором.

Уровень трассировки может принимать значение от 0 до 4. 0 – трассировка отсутствует, 4 – самый детальный уровень трассировки.

Параметр ProcessFlags отвечает за дополнительную информацию, отображаемой для каждой строки. Если установлен бит 2 значения данного параметра, то кроме содержательного текста в строке будет отображаться информация о месте, в котором возникло событие трассировки (имя функции, имя файла кода, номер строки в файле исходного кода). Это может помочь в выявлении проблемы разработчиком модуля.

Имя файла журнала может быть задано как относительным (только имя и расширение), так и абсолютным, включая полный путь до файла.

Если имя относительное, то сначала производится попытка создать/открыть файл в каталоге общем для всех пользователей %commonappdata%\Crypto Pro\LogFiles\, а при отсутствии прав доступа на данную операцию – в каталоге пользователя %localappdata%\Crypto Pro\LogFiles\.

Имя секции [Trace] – обязательно.

4.6. Журнал работы модуля КриптоПро SSF в ОС UNIX/Linux

В ОС семейства UNIX/Linux Модуль «КриптоПро SSF» может вести трассировку только в системный журнал (syslog). Для этого необходимо в секции [debug] конфигурационного файла СКЗИ КриптоПро CSP /etc/opt/cprocsp/config[64].ini пописать имена модулей, подлежащих трассировке следующим образом:

<Имя модуля>=15

<Имя модуля>_fmt=57

Например:

cpsapssf=15

cpsapssf_fmt=57

ocsp=15

ocsp_fmt=57

tsp=15

tsp_fmt=57

cades=15

cades_fmt=57

4.7. Описание основных функций SSF API

В данном разделе приведены лишь некоторые особенности реализации функций SSF API.

Подробное описание интерфейса приведено в технической документации SAP – «Secure Store & Forward (SSF). API Specifications (Version 1.0)».

4.7.1. SsfVersion

При успешном завершении возвращает строку "Crypto-Pro SSF library for SAP Version 1.01".

4.7.2. SsfQueryProperties

Функция возвращает значения поддерживаемых модулем свойств:

Наименование свойства	Значение
PROPERTIES	"FORMATS;HASHALGS;ENCRALGS;SSF_POPUPS"
FORMATS	"PKCS7;CADES;PKCS7_CADES;PKCS7_ANY"
HASHALGS	"SHA1;GOST3411;GOST-R-34.11-94;MD2;MD5"
ENCRALGS	"GOST28147;GOST-28147-89"
SSF_POPUPS	"1"

4.7.3. SsfEncode

Функция не кодирует каким-либо образом входные данные. Выходные данные являются точной копией входных данных.

Минимально необходимое кодирование выполняется функциями, формирующими PKCS#7, CMS сообщения (SsfSign, SsfAddSign, SsfEnvelope, SsfDigest). Исходные данные при формировании подписанного/зашифрованного сообщения, сообщения, содержащего вычисленное хэш значение, если того требует API вкладываются с автоматической кодировкой в формат PKCS#7 – DATA.

4.7.4. SsfDecode

Функция не декодирует каким-либо образом входные данные. Выходные данные являются точной копией входных данных.

Минимально необходимое декодирование выполняется автоматически функциями, декодирующими исходные PKCS#7, CMS сообщения (SsfVerify, SsfDevelope).

4.7.5. SsfSign

Функция формирует и возвращает сообщение в указанном формате, содержащие электронные подписи одного или более «подписантов».

Как было описано в п. "Форматы криптографических сообщений" возможно формирование простой и усовершенствованной ЭП, включающей все доказательства подлинности конкретной электронной подписи. Для формирования простой подписи используется формат с символьным обозначением «PKCS7». Для формирования усовершенствованной подписи используется формат с символьным обозначением «CADES» или «PKCS7_CADES».

Значение параметра с идентификатором Hash алгоритма не анализируется. Для формирования конкретной подписи используется хэш алгоритм наиболее соответствующий представленному в сертификате ключа проверки ЭП алгоритму открытого ключа и используемому для этого СКЗИ.

Формируемое сообщение может включать или не включать в себя сертификаты ключей проверки ЭП в зависимости от значения соответствующего параметра функции. Сообщения в формате CADES автоматически включают в себя сертификаты и все другие необходимые доказательства подлинности данной ЭП.

Формируемое сообщение может включать (attached) или не включать (detached) в себя исходные (подписываемые) данные в зависимости от значения соответствующего параметра функции.

Результат (подписанное сообщение) формируется лишь в том случае, если сертификаты всех «подписантов» найдены, все закрытые ключи доступны, все пароли к ключам указаны правильно. Т.е. когда подписи всех указанных в списке «подписантов» успешно сформированы.

Для каждого «подписанта» указывается его идентификатор, хранилище сертификатов, как указано в п. «Идентификаторы, защищенные профили и адресные книги пользователей», а также пароль доступа к закрытому ключу, как указано в п. «Пароли доступа к защищенным профилям и адресным книгам».

Более подробно параметры и возвращаемые значения указаны в технической документации «Secure Store & Forward (SSF). API Specifications (Version 1.0)».

4.7.6. SsfVerify

Функция SsfVerify осуществляет проверку всех электронных подписей в переданном подписанном сообщении и формирует список всех «подписантов» данного сообщения, включающий сертификат ключа проверки ЭП, идентификатор «подписанта» (поле Subject x.509 сертификата ключа проверки ЭП), время формирования ЭП (SigningTime). Если в сообщении содержатся исходные (подписываемые) данные, то функция при успешном завершении возвращает также и эти данные. Если сообщение содержит присоединенную ЭП и при этом дополнительно указываются исходные (подписываемые) данные, то дополнительно осуществляется

проверка на идентичность подписанных данных, содержащихся в проверяемом сообщении, с переданными исходными данными. Если эти данные отличаются, то возвращается сообщение об ошибке.

Результат (подписанное сообщение) формируется лишь в том случае, если сертификат «подписанта» найден, закрытый ключ ЭП доступен, пароль на доступ к ключу указан правильно.

Для осуществления проверки подписи необходимо правильно передавать значение формата сообщения, использовавшегося при формировании (подписи) исходного сообщения. Как было описано в п. "Форматы криптографических сообщений" параметр формата может принимать два значения: «PKCS7» - для простой ЭП и «CADES» («PKCS7_CADES») - для усовершенствованной ЭП.

Можно указать значение формата «PKCS7_ANY». В данном случае модуль будет автоматически определять формат переданного ему криптографического сообщения (PKCS#7 или CADES) и запускать соответствующую обработку. Это позволяет обрабатывать сообщения, не зная заранее по какому типу оно было сформировано контрагентом.

Значение параметра используемой адресной книги пользователя должно формироваться в соответствии с правилами, описанными в п. «Идентификаторы, защищенные профили и адресные книги пользователей».

Формируемое сообщение может включать или не включать в себя сертификаты ключей проверки ЭП в зависимости от значения соответствующего параметра функции. Сообщения в формате CADES автоматически включают в себя сертификаты и все другие необходимые доказательства подлинности данной ЭП.

Результат работы функции, заполнение полей профиля «подписантов» формируются в соответствии с правилами, описанными в технической документации «Secure Store & Forward (SSF). API Specifications (Version 1.0)».

В данной версии модуля параметр функции bUseCerts (использовать ли при проверке сертификаты вложенные в сообщение) не анализируется. Реализация использует все возможности для поиска сертификата ключа проверки конкретной ЭП. Если сертификат присутствует в сообщении, то он используется, если нет, то сертификат ищется в указанном хранилище сертификата.

После проверки каждой подписи по умолчанию осуществляется и проверка сертификата ключа проверки ЭП. При этом проверяется вся цепочка сертификатов, включая проверку на отзыв каждого сертификата, за исключением корневого.

Если необходимо отключить проверку сертификатов на отзыв в сообщениях PKCS#7 можно указать в переменной окружения или в значении параметра файла настроек ssf.ini **CP_SSF_VERIFYCERTFLAGS** значение 0 (CP_SSF_VERIFYCERTFLAGS=0). В данной переменной можно указывать и другие значения, связанные с проверкой сертификата. Значение представляется 16-ричным значением битовой маски флагов функции CertGetCertificateChain (http://msdn.microsoft.com/en-us/library/windows/desktop/aa376078(v=vs.85).aspx).

Значение данного параметра распространяется только при проверке электронных подписей, сформированных по формату PKCS7. Для формата CADES всегда проверяется подпись и сертификаты по самым строгим правилам, описанным в соответствующем стандарте.

Необходимо отметить, что в данной реализации формата CADES не допускается использование OCSP ответов, у которых поле ThisUpdate (время начала действия OCSP ответа) меньше времени, указанном в штампе времени. Т.е. информация об отзыве сертификата должна быть «свежей», дабы исключить использование недостоверной информации о статусе сертификата на момент подписи. Кроме этого при отсутствии в OCSP ответе поля NextUpdate (срок окончания действия информации о статусе сертификата в данном конкретном OCSP ответе), Значение поля ThisUpdate не должно превышать время, указанное в штампе времени более чем на 5 минут. Поэтому необходимо следить за синхронизацией времен указанных служб (TSP, OCSP), особенно, если они располагаются на разных серверах.

При формировании сообщений ЭП по формату CADES в том случае, если модуль «КриптоПро SSF» получает OCSP ответ от службы OCSP со значением временем в поле ThisUpdate меньшим, чем в полученном штампе времени, он будет продолжать посылать OCSP запросы с некоторым интервалом до тех пор, пока эти времена не станут, хотя бы равными.

В случае, когда для формирования ЭП по формату CAdES используются программные средства других производителей, которые в этот момент не проверяют расхождение времени штампа времени и OCSP ответа, может возникнуть ситуация, когда округленное до секунд время OCSP ответа окажется меньше неокругленного времени штампа (до 0.5 сек). Модуль КриптоПро SSF при проверке ЭП таких сообщений может выдать ошибку. Для предотвращения таких ситуаций может использоваться параметр AllowedExceedingTSPoverOCSPTime в настройках политики модуля CAdES («Допустимое превышение времени штампа над временем начала действия (ThisUpdate) OCSP ответа в CAdES сообщениях. От 0 до 10 секунд»). Значение данного параметра задается при установке модуля КриптоПро SSF (см. п. «Установка дистрибутива КриптоПро SSF»), и заносится в Реестр Windows в ключ HKLM\Software\Policies\Crypto-Pro\CAdES\.

4.7.7. SsfEnvelope

Функция SsfEnvelope формирует зашифрованное сообщение (цифровой конверт-ENVELOPED DATA) для нескольких указанных получателей. Для шифрования используется только симметричный алгоритм шифрования ГОСТ 28147-89. Сертификаты получателей электронного сообщения также должны содержать открытые ключи и подписи сформированные с использованием алгоритмов ГОСТ.

Параметр «формат» в данной функции может принимать как значение «PKCS7», так и «CADES» («PKCS7_CADES»). Какой из них использовать – не имеет никакого значения. На формат итогового сообщения этот выбор никак не влияет.

Значение параметра используемой адресной книги пользователя, а также значения идентификаторов получателей в списке получателей должны формироваться в соответствии с правилами, описанными в п. «Идентификаторы, защищенные профили и адресные книги пользователей».

Итоговое зашифрованное сообщение формируется лишь в том случае, если все получатели известны, их сертификаты найдены в указанной адресной книге и доступны. Коды возврата функции и результата обработки каждого из получателей формируются в соответствии с правилами, описанными в технической документации «Secure Store & Forward (SSF). API Specifications (Version 1.0) ».

4.7.8. SsfDevelope

Функция SsfDevelope расшифровывает сообщение, зашифрованное функцией SsfEnvelope, для одного указанного получателя. Для расшифрования сообщения используется закрытый ключ получателя. Поля защищенного профиля получателя должны быть заполнены в соответствии с правилами описанными в пп. «Идентификаторы, защищенные профили и адресные книги пользователей» и «Пароли доступа к защищенным профилям и адресным книгам».

Параметр «формат» в данной функции может принимать как значение «PKCS7», так и «CADES» («PKCS7_CADES»). Какой из них использовать – не имеет никакого значения. На формат итогового сообщения этот выбор никак не влияет.

Значение параметра используемой адресной книги пользователя должно формироваться в соответствии с правилами, описанными в п. «Идентификаторы, защищенные профили и адресные книги пользователей».

В случае успешного завершения функции возвращается расшифрованное сообщение.

Коды возврата функции и результата обработки каждого из получателей формируются в соответствии с правилами, описанными в технической документации «Secure Store & Forward (SSF). API Specifications (Version 1.0) ».

4.7.9. SsfAddSign

В отличие от функции SsfSign данная функция формирует добавляет ещё одну электронную подпись к уже подписанному сообщению в указанном формате, и возвращает сообщение, включающее все электронные подписи – вновь добавленную и содержавшиеся в исходном (подписываемом сообщении).

Тип нового сообщения (attached либо detached) формируется в зависимости от типа исходного подписываемого сообщения.

Как было описано в п. "Форматы криптографических сообщений" возможно формирование простой и усовершенствованной ЭП, включающей все доказательства подлинности конкретной электронной подписи. Для формирования простой подписи используется формат с символьным обозначением «PKCS7». Для формирования усовершенствованной подписи используется формат с символьным обозначением «CADES» («PKCS7_CADES»).

Значение параметра с идентификатором Hash алгоритма не анализируется. Для формирования конкретной подписи используется хэш алгоритм, наиболее соответствующий представленному в сертификате ключа проверки ЭП алгоритму открытого ключа и используемому для этого СКЗИ.

Формируемое сообщение может включать или не включать в себя сертификаты ключей проверки ЭП в зависимости от значения соответствующего параметра функции. Сообщения в формате CADES автоматически включают в себя сертификаты и все другие необходимые доказательства подлинности данной ЭП.

Результат (подписанное сообщение) формируется лишь в том случае, если сертификат «подписанта» найден, закрытый ключ ЭП доступен, пароль на доступ к ключу указан правильно. Если сообщение содержит присоединенную ЭП и при этом дополнительно указываются исходные (подписываемые) данные, то дополнительно осуществляется проверка идентичность подписываемых данных, содержащихся в подписываемом сообщении с переданными исходными данными. Если эти данные отличаются, то итоговое сообщение не формируется.

Значения полей защищенного профиля «подписанта» указываются в соответствии с правилами, изложенными в пп. «Идентификаторы, защищенные профили и адресные книги пользователей» и «Пароли доступа к защищенным профилям и адресным книгам».

Более подробно параметры и возвращаемые значения указаны в технической документации «Secure Store & Forward (SSF). API Specifications (Version 1.0)».

4.7.10. SsfDigest

Данная функция используется для вычисления Hash значения переданных исходных данных по указанному алгоритму. В результате формируется сообщение формата PKCS#7 DigestData.

Тип нового сообщения: attached либо detached, формируется в зависимости от значения соответствующего параметра функции.

Параметр «формат» в данной функции может принимать как значение «PKCS7», так и «CADES» («PKCS7_CADES»). Какой из них использовать – не имеет никакого значения. На формат итогового сообщения этот выбор никак не влияет.

Значение параметра используемого хэш алгоритма может принимать одно из следующих значений:

- «MD2»
- «MD5»
- «SHA1»
- «GOST3411»

Для совместимости с модулями других производителей введены синонимы обозначения алгоритма ГОСТ Р 34.11-94. Помимо указанного идентификатора «GOST3411» можно использовать идентификатор "GOST-R-34.11-94". В некоторых случаях это позволяет использовать один и тот же конфигурационный файл ssfrfc.ini.

Коды возврата функции формируются в соответствии с правилами, описанными в технической документации «Secure Store & Forward (SSF). API Specifications (Version 1.0) ».

5. Приложение. Список переменных окружения и параметров ssf.ini

Для указания дополнительных настроек модуля КриптоПро SSF можно использовать следующие переменные окружения/параметры файла настроек ssf.ini:

Наименование	Значение
CP_SSF_USERID	Какое представление использовать для обозначения идентификатора сертификата, при помощи которого была проверена ЭП. По умолчанию возвращается «Отличительное имя» владельца сертификата. Если для данной переменной указать значение «CERT_HASH», то будет возвращаться SHA1 хэш значение «отпечатка» сертификата. Пример: CP_SSF_USERID=CERT_HASH
CP_SSF_ADD_TSP	Список дополнительных адресов служб штампов времени, разделенных символом «;» Пример: CP_SSF_ADD_TSP=http://testca.cryptopro.ru/tsp/tsp.srf При этом процедура подписи будет пытаться сначала обращаться по основному адресу службы, указанному в оснастке групповой политики, а в случае неудачи, повторять процедуру с использованием адресов служб указанных в переменной окружения.
CP_SSF_VERIFYCERTFLAGS	Данная переменная используется только при проверке ЭП сформированной по стандарту PKCS#7. При проверке ЭП, сформированных по стандарту CADES, сертификаты на отзыв проверяются всегда, в соответствии со спецификацией CAdES X Long (по включенным в сообщение доказательствам актуальности статуса сертификата – OCSP ответам) Если необходимо отключить проверку сертификатов на отзыв в сообщениях PKCS#7 можно указать в данной переменной значение 0 (CP_SSF_VERIFYCERTFLAGS=0). В данной переменной можно указывать и другие значения, связанные с проверкой сертификата. Значение представляется 16-ричным значением битовой маски флагов функции CertGetCertificateChain (http://msdn.microsoft.com/en-us/library/windows/desktop/aa376078(v=vs.85).aspx). Значение данного параметра распространяется только при проверке электронных подписей, сформированных по формату PKCS7. Для Формат CADES всегда проверяется подпись и сертификаты по самым строгим правилам, описанным в соответствующем стандарте. Пример: CP_SSF_VERIFYCERTFLAGS=10000000 По умолчанию используется значение 0x40000000 (CERT_CHAIN_REVOCATION_CHECK_CHAIN_EXCLUDE_ROOT)
CP_SSF_ASK_PIN_WHEN_EMPTY	Данная переменная используется в функциях SSF, где требует-

	ся доступ к закрытому ключу пользователя (SsfSign, SsfAddSign, SsfDevelope). Если значение данной переменной равно «1» или «YES» или «TRUE», то в случае, когда приложение передает модулю «КриптоПро SSF» пустую строку в качестве пароля доступа к контейнеру закрытого ключа, модуль будет расценивать это как указание на вывод окна для запроса пароля доступа к закрытому ключу (если, конечно, пароль на данный закрытый ключ установлен). Согласно спецификации SAP на SSF API, модуль должен выводить подобное окно, если в качестве первого символа, переданной ему строки пароля, идет «!» (восклицательный знак). Но некоторые уже существующие приложения вместо этого передают пустую строку, поэтому для совместимости с ними в модуль «КриптоПро SSF» была добавлена данная опция.
CP_SSF_VERIFYCERTFLAGS_ONSELECT	Данная переменная используется только при проверке сертификатов в процедуре отбора их в список выбора сертификата подписи. В настройках пользователя в качестве идентификатора сертификата ключа проверки ЭП, при помощи которого будет формироваться ЭП, можно указывать ключевое слово $SELECT_CERTIFICATE$ (значки $$ - обязательны). В этом случае на экран будет выдан список сертификатов. Пользователь сам выбирает из этого списка – какой сертификат использовать. Каждый сертификат, попадаемый в список, должен пройти проверку в соответствии с флагами, указанными в данной переменной. Возможные значения флагов аналогичны переменной CP_SSF_VERIFYCERTFLAGS.

6. Перечень сокращений

CSP	Криптопровайдер (Cryptographic Service Provider)
ОС	Операционная система
СКЗИ	Средство криптографической защиты информации
ЭП	Электронная подпись
Подписант	(Signer) Владелец закрытого ключа и сертификата ключа проверки ЭП, при помощи которых формировалась электронная подпись
Получатель	Владелец закрытого ключа и соответствующего сертификата открытого ключа, в адрес которого шифровалось сообщение. Сертификат открытого ключа используется для выработки сессионного ключа шифрования.