

127018, Москва, ул. Сущёвский вал, д. 18
Телефон: +7 (495) 995 4820
Факс: +7 (495) 995 4820
<https://www.CryptoPro.ru>
E-mail: info@CryptoPro.ru



Средство Криптографической Защиты Информации	КриптоПро HSM версия 2.0 R3 Комплектации 1 и 2 Использование интерфейсных модулей (клиента ПАКМ)
---	---

ЖТЯИ.00096-03 90 02

Листов 45

2023 г.

Содержание

1. Аннотация	3
2. Клиентский компонент ПАКМ	4
3. Каналы взаимодействия с ПАКМ	6
3.1 Канал «K2»	6
3.2 Канал «K»	8
4. Настройка клиента ПАКМ на ОС семейства Unix/Linux	9
4.1 Установка дистрибутива ПО	9
4.2 Настройка ПО «СКЗИ «КриптоПро CSP»	9
4.3 Настройка stunnel	11
4.4 Регистрация пользователя ПАКМ	12
4.5 Запуск stunnel	14
4.6 Меры защиты от НСД и дополнительные настройки ОС Unix/Linux с установленным СКЗИ	14
5. Настройка клиента ПАКМ на ОС семейства Windows	15
5.1 Установка дистрибутива ПО «Клиент КриптоПро HSM»	15
5.2 Устанавливаемые криптопровайдеры	15
5.3 Дополнительные настройки параметров криптопровайдера	21
5.4 Настройка Конфигурации с несколькими ПАКМ	24
6. Контроль целостности	33
Приложение 1. Пример конфигурационного файла ПАКМ «КриптоПро HSM» на серверах с ОС Linux	34
Приложение 2. Утилита командной строки HsmGenArm	43
Коды ошибок	43
Параметры журналирования	44
Требования безопасности при использовании утилиты	44

1. АННОТАЦИЯ

Данный документ содержит описание настройки и правила использования клиентского компонента ПАКМ «КриптоПро HSM».

Документ предназначен для администраторов информационной безопасности учреждений, осуществляющих установку, обслуживание, контроль за соблюдением требований к эксплуатации средств СКЗИ, а также для администраторов Серверов, сетевых ресурсов предприятия и других работников службы информационной безопасности, осуществляющих настройку рабочих мест для работы со средствами СКЗИ.

Инструкции администраторам безопасности и пользователям различных автоматизированных систем, использующих ПАКМ «КриптоПро HSM», должны разрабатываться с учетом требований настоящего документа.

2. КЛИЕНТСКИЙ КОМПОНЕНТ ПАКМ

Взаимодействие любого приложения на рабочих станциях пользователей или серверах с ПАКМ «КриптоПро HSM» осуществляется через посредника — клиентский компонент ПАКМ (клиент ПАКМ).

В качестве клиентского компонента ПАКМ должно использоваться сертифицированное СКЗИ «КриптоПро CSP» версии 5.0. Для ОС семейства Windows в состав клиентского компонента входит дополнительное ПО «Клиент КриптоПро HSM» (КриптоПро HSM Client), предоставляющее графический интерфейс настройки клиента ПАКМ.

Также в качестве клиентского компонента ПАКМ может использоваться сертифицированное СКЗИ «КриптоПро CSP» соответствующего уровня защиты, в эксплуатационной документации на которое заявлена возможность такого использования.

Клиент ПАКМ обеспечивает:

- трансляцию вызовов функций интерфейсов «КриптоПро CSP» от приложений к удаленному разделяемому ПАКМ «КриптоПро HSM»;
- аутентификацию пользователей СКЗИ перед ПАКМ и ПАКМ перед пользователями;
- защищенный (шифрованный) канал передачи информации «К»/«К2» (см. раздел 3) между рабочими станциями/серверами и ПАКМ.

В состав клиентского компонента ПАКМ входит утилита командной строки HsmGenArm, предназначенная для формирования и экспорта ключей в формате PKCS#12. Утилита предназначена для работы в ОС семейства Windows и Linux. Порядок использования утилиты описан в Приложении 2.

Порядок установки и настройки СКЗИ «КриптоПро CSP» для ОС семейства Unix/Linux и дополнительные настройки, выполняемые администратором сервера с установленной ОС семейства Unix/Linux, описаны в разделе 4 данного документа.

Порядок установки и настройки ПО «Клиент КриптоПро HSM» для ОС семейства Windows описан в документе «ЖТЯИ.00096-03 93 01. КриптоПро HSM. Руководство пользователя». Дополнительные настройки, выполняемые администратором сервера с установленной ОС Windows, описаны в разделе 5 данного документа.

Установка СКЗИ «КриптоПро CSP» выполняется в соответствии с эксплуатационной документацией на используемую версию СКЗИ.

«Клиент КриптоПро HSM» использует отличные от «КриптоПро HSM» (см. п. 2.4 документа «ЖТЯИ.00096-03 90 01. КриптоПро HSM. Инструкция по использованию») имена криптопровайдеров. Названия данных криптопровайдеров имеют вид «Crypto-Pro GOST R 34.10-2001 xxx CSP», где xxx обозначает уровень защиты СКЗИ: KC1, KC2 или KC3.

В комплект поставки ПАКМ «КриптоПро HSM» входит компакт-диск с клиентским компонентом ПАКМ, содержащий необходимое ПО для ОС семейства Windows и ОС семейства Unix/Linux, которое должно быть установлено на ПЭВМ, взаимодействующую с ПАКМ «КриптоПро HSM».

По согласованию с пользователем клиентский компонент ПАКМ комплектуется аппаратными сертифицированными средствами защиты от НСД и ФСДЧ (ПАК «Соболь», «Аккорд» и т.п. в соответствии с комплектацией используемого СКЗИ «КриптоПро CSP»). Исполнения СКЗИ уровня защиты КС2 и выше должны включать данные средства.

Клиентский компонент ПАКМ в первую очередь предназначен для встраивания в прикладное программное обеспечение. Встраивание клиентского компонента ПАКМ должно осуществляться с учетом требований раздела 10 документа «ЖТЯИ.00096-03 95 01. КриптоПро HSM. Правила пользования» и в соответствии с положениями «ЖТЯИ.00096-01 92 01. КриптоПро HSM. Руководство программиста».

На ПЭВМ с установленным клиентским компонентом ПАКМ необходимо выполнять требования по защите аппаратного и программного обеспечения от НСД в соответствии с документацией (в частности, Правилами пользования и Руководством администратора безопасности) на входящее в состав клиентского компонента СКЗИ «КриптоПро CSP» соответствующей версии.

3. КАНАЛЫ ВЗАИМОДЕЙСТВИЯ С ПАКМ

3.1 КАНАЛ «K2»

Взаимодействие клиента с ПАКМ осуществляется по логическому защищенному каналу «K2».

Канал «K2» обеспечивает двустороннюю идентификацию и аутентификацию пользователя СКЗИ перед ПАКМ и ПАКМ перед пользователем при помощи ключей и сертификатов аутентификации (ключ клиента, ключ сервера).

Канал «K2» реализуется на основе протокола TLS.

На ключ подписи ПАКМ формируется самоподписанный сертификат. На ключи TLS сервера ПАКМ и ключи аутентификации (доступа) пользователей/администраторов серверов также формируются сертификаты, которые подписываются ключом подписи ПАКМ.

При обновлении ключей соответствующие сертификаты переиздаются.

Каждому пользователю при его регистрации в ПАКМ формируются ключи и сертификат аутентификации, которые записываются на ключевой носитель.

Для каждого пользователя может существовать только один рабочий сертификат аутентификации, который хранится в профиле учетной записи пользователя.

Сертификат аутентификации пользователя (т.е. пользователь) в ПАКМ может быть заблокирован. Сервис ПАКМ не ведет Список заблокированных сертификатов. В процессе аутентификации пользователя производится проверка как на соответствие сертификата пользователя, указанного в профиле пользователя, так и на блокирование пользователя.

Для доступа к ключам аутентификации клиентское ПО запрашивает у пользователя pin-код. Если ключ и сертификат выдан Администратору сервера, т.е. в сертификате присутствует соответствующее расширение, то pin-код не запрашивается. Серверные приложения (сервисы, демоны) обычно не имеют консоли для интерактивного взаимодействия с пользователем, они запускаются в момент загрузки ОС. Карточка с ключом и сертификатом ключа доступа должна быть вставлена до запуска соответствующего сервиса и иметь фиксированный pin-код – восемь единиц.

Активировав ключ доступа, обычный пользователь (не являющийся администратором сервера) может извлечь смарт-карту из считывателя. Работа с данным ключом может продолжаться до выхода пользователя из текущей Windows сессии. В некоторых случаях ПАКМ может разрывать неактивное соединение, если пользователь долго не использовал канал. В этом случае пользователю придется заново установить соединение и пройти процедуру аутентификации, включая ввод pin-кода для контейнера ключа доступа.

На серверах, приложения которых используют криптопровайдер «Crypto-Pro HSM Svc CSP» (и другие с суффиксом "...Svc..." в имени криптопровайдера) должна использоваться

только карточка с ключом и сертификатом ключа доступа, в котором есть расширение «Администратор сервера» (см. п. 6.9 документа «ЖТЯИ.00096-03 91 01. КриптоПро HSM. Руководство администратора безопасности»). Карточка с ключом должна постоянно находиться в считывателе, т.к. периодически, примерно 1 раз в час производится процедура смены сессионного ключа протокола TLS, которая требует присутствия закрытого ключа обмена. Это требует нахождения сервера в контролируемой зоне, доступ в которую строго регламентирован.

Для такой конфигурации можно использовать канал K2s. Для увеличения производительности серверных приложений, базирующихся на ОС семейства Windows, имеется возможность организовать нешифрованный и/или не аутентифицированный канал «K2s» при соблюдении требований по безопасности, включающих организационные меры по размещению ПАКМ и сервера в одной серверной стойке. Аутентификация в соответствии с протоколом TLS происходит в полном объеме, но передача данных между сервером и ПАКМ происходит без шифрования её сессионным ключом. Повышение производительности сервера при этом может достигать 25-30%.

Для обеспечения возможности использования канала «K2s» необходимо:

- установить соответствующую опцию Enable K2s в настройках ПАКМ в значение «YES» («1») (подробнее см. п. «Просмотр и изменение параметров ПАКМ» документа «ЖТЯИ.00096-03 90 01. КриптоПро HSM. Инструкция по использованию»);
- подключить сервер/серверную группу, расположенную в отдельном сегменте локальной сети на отдельный сетевой интерфейс ПАКМ;
- соответствующим образом настроить этот сетевой интерфейс ПАКМ (см. ниже в данном документе);
- соответствующим образом настроить правила межсетевого экрана ПАКМ, разрешив доступ через указанный сетевой интерфейс к порту 1503 для соответствующего сетевого адреса/подсети;
- разместить сервер/группу серверов и ПАКМ в одной контролируемой зоне;
- на серверах сделать соответствующие настройки – прописать параметр WithoutEnc в Реестре Windows (см. п. 5.3) .

Канал «K2» использует порт для входящих соединений 1501.

Канал «K2s» использует порт 1503.

3.2 КАНАЛ «К»

Взаимодействие клиента ПАКМ с ПАКМ для Головного удостоверяющего центра осуществляется по логическому защищенному каналу «К».

Канал «К» обеспечивает двустороннюю идентификацию и аутентификацию пользователя при помощи специально предназначенных для этих целей ключей (ключ канала «К», находящийся на смарт-карте, и мастер-ключ ПАКМ, находящийся внутри ПАКМ).

Администратор ПАКМ может выпустить несколько смарт-карт с ключами канала «К» для использования одновременно на нескольких серверах приложений.

При обращении серверов приложений к ПАКМ смарт-карта должна постоянно находиться в считывателе сервера.

Доступ к карте не требует ввода pin-кода.

Канал «К» использует порт для входящих соединений 1502.

4. НАСТРОЙКА КЛИЕНТА ПАКМ НА ОС СЕМЕЙСТВА UNIX/LINUX

Для настройки клиентского компонента ПАКМ под управлением ОС семейства Unix/Linux необходимо:

1. Установить модули СКЗИ «КриптоПро CSP» (п. 4.1)
2. Выполнить настройку криптопровайдеров (п. 4.2)
3. Выполнить настройку приложения для создания TLS-туннеля stunnel (п. 4.3)
4. Выполнить регистрацию нового пользователя ПАКМ (п. 4.4)
5. Запустить службу stunnel (п. 4.5)



Примечание. Для быстрой и корректной настройки криптопровайдеров и stunnel (п.п. 4.2–4.5) на клиенте рекомендуется воспользоваться скриптом **channel_k2.sh**, включенным в состав дистрибутива ПАКМ.

4.1 УСТАНОВКА ДИСТРИБУТИВА ПО

Для взаимодействия приложений пользователей/серверов приложений на ПЭВМ с ОС семейства Unix/Linux с ПАКМ используется канал «K2» (кроме Головного удостоверяющего центра). Для его реализации на сервер необходимо установить и настроить ПО СКЗИ «КриптоПро CSP».

Установка СКЗИ «КриптоПро CSP» на ОС Unix/Linux выполняется в соответствии с разделом «Установка дистрибутива ПО СКЗИ» Руководства администратора безопасности для используемой ОС, входящего в состав эксплуатационной документации на СКЗИ.

4.2 НАСТРОЙКА ПО «СКЗИ «КРИПТОПРО CSP»

Настройка ПО СКЗИ «КриптоПро CSP» осуществляется с помощью конфигурационного файла. Конфигурационный файл СКЗИ в среде операционных систем семейства Unix/Linux является аналогом ветви реестра в операционной системе Windows. В зависимости от ОС месторасположение и имя конфигурационного файла может варьироваться. Для 64-разрядных версий ОС файл имеет имя **config64.ini**, для 32-разрядных — **config.ini**.

В LSB совместимых ОС конфигурационный файл расположен в:

/etc/opt/cprocp/

Структура конфигурационного файла приводится в Приложении 1.

В конфигурационном файле СКЗИ после пункта [Defaults\Provider] необходимо добавить секции (или убедиться в их наличии):

```
[Defaults\Provider\Crypto-Pro GOST R 34.10-2012 HSM CSP]
```

```
"Image Path" = "/opt/cproscsp/lib/amd64/libcspr.so"
```

```
Type = 80
```

```
Channel = ".clientk2"
```

```
Media = "HSMDB"
```

```
"Function Table Name" = CPSRV_GetFunctionTable
```

```
[Defaults\Provider\Crypto-Pro HSM RSA CSP]
```

```
"Image Path" = "/opt/cproscsp/lib/amd64/libcspr.so"
```

```
Type = 1
```

```
Channel = ".clientk2"
```

```
Media = "HSMDB"
```

```
"Function Table Name" = CPSRV_GetFunctionTable
```



Примечание. Параметр **Channel** должен содержать имя сокета, аналогичное имени сокета, указанного в параметре **accept** в конфигурационном файле stunnel, без пути к файлу (см. п. 4.3).

Если требуется подключение второго HSM, нужно зарегистрировать еще один провайдер (с другим именем) с тем же именем сокета (параметр Channel), указанного в конфигурационном файле stunnel (параметр **accept**) для второго HSM:

```
[Defaults\Provider\Crypto-Pro GOST R 34.10-2012 HSM CSP 01]
```

```
"Image Path" = "/opt/cproscsp/lib/amd64/libcspr.so"
```

```
Type = 80
```

```
Channel = ".clientk2a"
```

```
Media = "HSMDB"
```

```
"Function Table Name" = CPSRV_GetFunctionTable
```

Таким образом, для обращения к разным HSM с одного клиента нужно использовать разные криптопровайдеры (в примере выше — Crypto-Pro GOST R 34.10-2012 HSM CSP и Crypto-Pro GOST R 34.10-2012 HSM CSP 01).

Для конфигурации PKCS#11 в конфигурационный файл СКЗИ после секции [PKCS11] необходимо добавить секцию (или убедиться в её наличии):

```
[PKCS11\slot0]
```

```
ProvRSA = "Crypto-Pro HSM RSA CSP"
```

```
ProvGOST = "Crypto-Pro GOST R 34.10-2012 HSM CSP"
```

```
reader = "HSMDB"
```

```
#reader = "HDIMAGE"
```

После настройки проверьте работоспособность провайдера с помощью команды:

```
/opt/cprocsp/bin/amd64/csptest -enum -provider "Crypto-Pro GOST R 34.10-2012 HSM CSP" -info
```

И перезапустите службу cprocsp (пример для ОС, использующих Init скрипты):

```
/etc/init.d/cprocsp stop  
/etc/init.d/cprocsp start
```

4.3 НАСТРОЙКА STUNNEL

Настройка stunnel осуществляется с помощью конфигурационного файла **stunnel.conf**. Если конфигурационный файл stunnel располагается по пути /etc/opt/cprocsp/stunnel/stunnel.conf, запуск stunnel возможен без дополнительных параметров. Иначе при запуске утилиты необходимо указывать путь к файлу конфигурации:

```
/opt/cprocsp/sbin/amd64/stunnel/"путь к файлу конфигурации"
```

Пример конфигурационного файла:

```
setuid = root  
setgid = root  
pid = /var/opt/cprocsp/tmp/stunnel-K2.pid  
output=/var/log/stunnel-K2.log  
#socket = l:TCP_NODELAY=1  
socket = r:TCP_NODELAY=1  
debug = 0  
max_clients = 25  
for_hsm = yes
```

```
[clientk2]  
client=yes  
connect=192.168.70.74:1501  
accept = /var/opt/cprocsp/tmp/.clientk2  
cert=/root/cert.cer
```

Описание опций stunnel:

client=yes	Режим клиента (удаленный сервис использует TLS/SSL).
connect=[host:]port	IP-адрес HSM и его порт для канала K2 (1501)

accept = [host:]port	Unix-сокеты, который будет слушать stunnel (куда будут обращаться приложения по вызовам CryptoAPI)
cert = cert_file	Путь к файлу сертификата ключа доступа к HSM (сертификат также должен быть установлен в хранилище сертификатов «My» пользователя, под которым запускается stunnel, и иметь там «связку» с закрытым ключом)

Подробное описание всех возможных опций stunnel также приведено в документе «Приложения для создания TLS-туннеля», входящем в состав эксплуатационной документации на СКЗИ «КриптоПро CSP».

Если требуется подключение второго HSM, необходимо дополнительно выполнить следующее действие:

1. Добавить еще одного слушателя на другой сокет:

```
[clientk2]
client=yes
connect=192.168.70.75:1501
accept=/var/opt/cproscsp/tmp/.clientk2a
cert=/root/client/client2.cer
```

4.4 РЕГИСТРАЦИЯ ПОЛЬЗОВАТЕЛЯ ПАКМ

Далее в ПАКМ регистрируется новый пользователь, для него формируются ключ и сертификат ключа доступа к ПАКМ.



Примечание. Сформированный ключ доступа должен иметь тот же уровень защиты, что и используемое СКЗИ «КриптоПро CSP».

Возможны несколько вариантов формирования ключа и сертификата пользователя:

1. Ключ и сертификат могут быть сформированы на смарт-карте с использованием как LCD панели ПАКМ, так и Web-интерфейса ПАКМ (ключи на Web-интерфейсе формируются с классом защиты установленного СКЗИ «КриптоПро CSP» под Windows). В этом случае на машине с ОС Unix/Linux надо настроить считыватель смарт-карт и установить сертификат в хранилище «My» со ссылкой на контейнер на смарт-карте.

2. Также возможно сформировать ключи локально на машине с ОС Unix/Linux (на носителе HDIMAGE), сформировать PKCS10-запрос утилитами из состава «КриптоПро CSP» и через Web-интерфейс ПАКМ по запросу получить сертификат этого ключа. Далее этот сертификат также устанавливается в хранилище «My» с указанием ссылки на ключевой контейнер.

3. Возможна генерация ключа на машине с ОС Windows, генерация контейнера осуществляется на обычный USB-флеш-накопитель. После генерации контейнера необходимо корректно перенести его на машину с ОС Unix/Linux одним из следующих способов:

- Скопировать контейнер с помощью утилиты `csptest` в режиме `-keyset`. В конфигурационном файле СКЗИ «КриптоПро CSP» должны быть зарегистрированы исходный и целевой считыватели (FLASH и HDIMAGE), проверка осуществляется командой:

```
/opt/cproscsp/sbin/amd64/cpconfig -hardware reader -view
```

Полное имя контейнера можно узнать с помощью команды:

```
csptest -keyset -enum_cont -fqcn -verifycontext
```

- Вручную скопировать каталог контейнера в структуру каталога HDIMAGE и установить соответствующие права на каталог контейнера и файлы. Контейнер копируется в каталог `/var/opt/cproscsp/keys/<имя пользователя>/.` Необходимо установить права на чтение и запись на контейнер и все файлы внутри.



Примечание. Класс защиты СКЗИ «КриптоПро CSP» на целевой машине с ОС Unix/Linux должен быть не выше класса защиты СКЗИ на машине с ОС Windows, на которой выполнялась генерация ключа.

После генерации ключа и сертификата необходимо:

1. установить сертификат в хранилище «My» со ссылкой на ключевой контейнер:

```
/opt/cproscsp/bin/amd64/certmgr -inst -cont '\\.\HDIMAGE\contname'
```

2. разместить файл сертификата пользователя (в кодировке DER) в каталоге, указанном в конфигурационном файле `stunnel` (параметр **cert**). Экспорт сертификата в файл осуществляется командой:

```
/opt/cproscsp/bin/amd64/certmgr -exp -dest /root/cert.cer
```

3. установить корневой сертификат ПАКМ в хранилище «root»:

```
/opt/cproscsp/bin/amd64/certmgr -inst -store root -file <путь к корневому сертификату>
```



Примечание. Подробная инструкция по командам СКЗИ «КриптоПро CSP» под управлением ОС Unix/Linux приведена в соответствующем руководстве администратора, входящего в состав эксплуатационной документации на СКЗИ.

4.5 ЗАПУСК STUNNEL

После настроек выполняется запуск `stunnel_fork`:

```
/opt/cprocsp/sbin/amd64/stunnel_fork
```

Проверка работоспособности осуществляется с помощью команды:

```
/opt/cprocsp/bin/amd64/csptest -enum -info -provider "Crypto-Pro GOST R 34.10-2012  
HSM CSP" -info
```

4.6 МЕРЫ ЗАЩИТЫ ОТ НСД И ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ОС UNIX/LINUX С УСТАНОВЛЕННЫМ СКЗИ

При использовании ПЭВМ с установленным клиентским компонентом ПАКМ — СКЗИ «КриптоПро CSP» под управлением ОС Unix/Linux — необходимо предпринять дополнительные меры защиты организационного и технического характера и выполнить дополнительные настройки операционной системы в соответствии с Правилами пользования и Руководством администратора безопасности на используемую версию СКЗИ «КриптоПро CSP».

5. НАСТРОЙКА КЛИЕНТА ПАКМ НА ОС СЕМЕЙСТВА WINDOWS

5.1 УСТАНОВКА ДИСТРИБУТИВА ПО «КЛИЕНТ КРИПТОПРО HSM»

Порядок установки и настройки ПО «Клиент КриптоПро HSM» описан в документе «ЖТЯИ.00096-03 93 01. КриптоПро HSM. Руководство пользователя».

5.2 УСТАНАВЛИВАЕМЫЕ КРИПТОПРОВАЙДЕРЫ

В процессе установки дистрибутива в Реестре ОС Windows регистрируются следующие криптопровайдеры:

- **Crypto-Pro HSM CSP (тип 75)**
- **Crypto-Pro HSM Svc CSP (тип 75)**
- **Crypto-Pro HSM RSA CSP (тип 1)**
- **Crypto-Pro HSM RSA Svc CSP (тип 1)**
- **Crypto-Pro GOST R 34.10-2001 HSM CSP (тип 75)**
- **Crypto-Pro GOST R 34.10-2012 HSM CSP (тип 80)**
- **Crypto-Pro GOST R 34.10-2012 Strong HSM CSP (тип 81)**
- **Crypto-Pro GOST R 34.10-2001 HSM Svc CSP (тип 75)**
- **Crypto-Pro GOST R 34.10-2012 HSM Svc CSP (тип 80)**
- **Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP (тип 81)**

В самом ПАКМ «КриптоПро HSM» зарегистрирован расширенный набор имен криптопровайдеров, которые при необходимости могут быть использованы для доступа к криптографическим функциям ПАКМ. В этом случае в ОС Windows они должны быть зарегистрированы вручную. Полный список возможных имен криптопровайдеров приведен ниже:

- **'Crypto-Pro GOST R 34.10-2012 HSM CSP[01-04]'** (тип 80)
- **'Crypto-Pro GOST R 34.10-2012 HSM Svc CSP'** (тип 80)
- **'Crypto-Pro GOST R 34.10-2012 HSM 1.0 CSP[01-04]'** (тип 80)
- **'Crypto-Pro GOST R 34.10-2012 HSM 1.0 Svc CSP'** (тип 80)
- **'Crypto-Pro GOST R 34.10-2012 Strong HSM CSP[01-04]'** (тип 81)
- **'Crypto-Pro GOST R 34.10-2012 Strong HSM Svc CSP'** (тип 81)
- **'Crypto-Pro GOST R 34.10-2012 Strong HSM 1.0 CSP[01-04]'** (тип 81)
- **'Crypto-Pro GOST R 34.10-2012 Strong HSM 1.0 Svc CSP'** (тип 81)

- **'Crypto-Pro ECDSA and AES HSM CSP[01-04]'** (тип 16)
- **'Crypto-Pro ECDSA and AES HSM Svc CSP'** (тип 16)
- **'Crypto-Pro ECDSA and AES HSM 1.0 Svc CSP'** (тип 16)
- **'Crypto-Pro ECDSA and AES HSM 1.0 CSP[01-04]'** (тип 16)

- **'Crypto-Pro Enhanced RSA and AES HSM CSP[01-04]'** (тип 24)
- **'Crypto-Pro Enhanced RSA and AES HSM Svc CSP'** (тип 24)
- **'Crypto-Pro Enhanced RSA and AES HSM 1.0 CSP[01-04]'** (тип 24)
- **'Crypto-Pro Enhanced RSA and AES HSM 1.0 Svc CSP'** (тип 24)

- **'Crypto-Pro Curve25519 and AES HSM CSP'** (тип 32)
- **'Crypto-Pro Curve25519 and AES HSM Svc CSP'** (тип 32)
- **'Crypto-Pro Curve25519 and AES HSM 1.0 CSP[01-04]'** (тип 32)
- **'Crypto-Pro Curve25519 and AES HSM 1.0 Svc CSP'** (тип 32)

- **'Crypto-Pro HSM RSA CSP[01-08]'** (тип 1)
- **'Crypto-Pro HSM RSA Svc CSP'** (тип 1)
- **'Crypto-Pro RSA HSM CSP'** (тип 1)
- **'Crypto-Pro RSA HSM Svc CSP'** (тип 1)
- **'Crypto-Pro RSA HSM 1.0 CSP[01-04]'** (тип 1)
- **'Crypto-Pro RSA HSM 1.0 Svc CSP'** (тип 1)

- **'Crypto-Pro HSM CSP[01-08]'** (тип 75)
- **'Crypto-Pro HSM Svc CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM Svc CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM 1.0 CSP'** (тип 75)
- **'Crypto-Pro GOST R 34.10-2001 HSM 1.0 Svc CSP'** (тип 75)
- **'Crypto-Pro HSM 1.0 CSP[01-04]'** (тип 75)
- **'Crypto-Pro HSM 1.0 Svc CSP[01-04]'** (тип 75)

Для генерации и хранения ключей используется внутренний считыватель ПАКМ с именем «HSMDB». Его отличительной особенностью является то, что все закрытые ключи/ключи ЭП шифруются на ключах шифрования ПАКМ (подробнее см. раздел 6 «ЖТЯИ.00096-03 91 01. Руководство администратора безопасности»).

В приведенном выше списке криптопровайдеров встречаются имена с суффиксами вида "...[01-04]" или "...[01-08]". Это означает, что кроме основного имени, например, 'Crypto-Pro GOST R 34.10-2012 HSM CSP' зарезервировано ещё несколько синонимов имени

данного криптопровайдера, например, 'Crypto-Pro GOST R 34.10-2012 HSM CSP 01', 'Crypto-Pro GOST R 34.10-2012 HSM CSP 02'..., и т.д. Они служат для создания высокопроизводительных систем повышенной надежности, а именно для создания пулов из ПАКМ. На серверах, использующих СКЗИ «КриптоПро HSM» можно зарегистрировать эти имена таким образом, что при обращении к криптопровайдерам с подобными именами запросы будут направляться в конкретный ПАКМ, связанный с данным именем криптопровайдера. Т.е. манипулируя в приложении именами криптопровайдеров, по сути производится манипуляция IP адресами, по которым будут направляться CryptoAPI запросы, разных клонов «КриптоПро HSM». При необходимости эти имена криптопровайдеров на устройствах доступа должны быть зарегистрированы вручную. Данные имена имеют вид:

Для 80 типа:

- Crypto-Pro GOST R 34.10-2012 HSM CSP 01
- Crypto-Pro GOST R 34.10-2012 HSM CSP 02
- Crypto-Pro GOST R 34.10-2012 HSM CSP 03
- Crypto-Pro GOST R 34.10-2012 HSM CSP 04

Для 81 типа:

- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 01
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 02
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 03
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 04

Для 16 типа:

- Crypto-Pro ECDSA and AES HSM CSP 01
- Crypto-Pro ECDSA and AES HSM CSP 02
- Crypto-Pro ECDSA and AES HSM CSP 03
- Crypto-Pro ECDSA and AES HSM CSP 04

Для 24 типа:

- Crypto-Pro Enhanced RSA and AES HSM CSP 01
- Crypto-Pro Enhanced RSA and AES HSM CSP 02
- Crypto-Pro Enhanced RSA and AES HSM CSP 03
- Crypto-Pro Enhanced RSA and AES HSM CSP 04

Криптопровайдеры с именами, включающими лексему «Svc», отличается от криптопровайдеров без её наличия тем, что их использование позволяет выводить запросы на ввод пин-кодов для ключей пользователей не на «рабочий стол» рабочей станции пользователя, а на LCD панель ПАКМ. Кроме этого они позволяют организовать обмен между сервером и ПАКМ по более производительному нешифрованному каналу, при условии осуществления однозначной двусторонней аутентификации «сервер<->ПАКМ», нахождении

сервера и ПАКМ в одной контролируемой зоне и условии, что используется специальный сертификат ключа доступа, включающий расширение (extended key usage - EKU) «1.2.643.2.2.34.22».

Такие криптопровайдеры используются в основном в серверных конфигурациях серверами приложений, работающими в фоновом режиме и не имеющими консоли для вывода сообщений и/или запроса пин-кодов. Они реализованы в виде отдельного сервиса ОС Windows, запускаемого при загрузке ОС.

Криптопровайдеры с именами, включающими лексему «HSM 1.0», отличается от криптопровайдеров без её наличия тем, что ключевые контейнеры используют считыватель "HSM" вместо "HSMDB".

Считыватель «HSMDB» — это внутренняя память (flash диск) ПАКМ, которая защищается ключами шифрования ПАКМ, т.е. все ключи, сформированные на считывателе «HSMDB», автоматически шифруются. А так как ключи шифрования ПАКМ защищены на разделенном по схеме 3 из 5-ти ключе активации ПАКМ, то все ключи, созданные на считывателе «HSMDB», невозможно открыть без активации ПАКМ (активации разделенного «ключа активации ПАКМ»). При этом ключевые контейнеры хранятся во внутренней Базе данных ПАКМ и могут реплицироваться подсистемой горячего резервирования в другой ПАКМ.

Считыватель «HSM» — это также внутренняя память (flash диск) ПАКМ, которая защищается ключами шифрования ПАКМ также, как и для считывателя «HSMDB». Но ключевые контейнеры хранятся не в БД, а в виде файлов ОС и не могут реплицироваться подсистемой горячего резервирования в другой ПАКМ. Для резервирования таких ключевых контейнеров может быть применено только клонирование ПАКМ (холодное резервирование).

Криптопровайдеры 75-го типа Crypto-Pro GOST R 34.10-2001 HSM CSP (синоним имени "Crypto-Pro HSM CSP") — реализуют:

- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001, возможность вычисления хэш-функции согласно ГОСТ Р 34.11-94;
- возможность шифрования и имитозащиты согласно ГОСТ 28147-89;

Для хранения ключей используется внутренний считыватель ПАКМ с именем «HSMDB».

Алгоритмы подписи данного криптопровайдера выводятся из обращения, используются только для проверки ЭП, и расшифрования ранее созданных криптографических сообщений. Для формирования новых криптографических сообщений используйте более новые алгоритмы и соответствующие криптопровайдеры.

Криптопровайдеры 80 и 81 типа **Crypto-Pro GOST R 34.10-2012 HSM CSP** и **Crypto-Pro GOST R 34.10-2012 Strong HSM CSP** (и их синонимы) реализуют:

- выполнение функций создания и проверки электронной подписи (ЭП) согласно

ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), вычисление хэш-функции согласно ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);

- возможность шифрования и имитозащиты согласно ГОСТ 28147-89, ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018), ГОСТ Р 34.13-2015 (ГОСТ 34.13-2018);

На настоящий момент криптопровайдеры 80-го типа являются основными и используются для всех служебных ключей ПАКМ «КриптоПро HSM».

Помимо криптопровайдеров реализующих алгоритмы ГОСТ в ПАКМ «КриптоПро HSM» устанавливаются криптопровайдеры, реализующие зарубежные алгоритмы.

Криптопровайдеры 1-го типа **Crypto-Pro HSM RSA CSP** и **Crypto-Pro HSM RSA Svc CSP** (тип 1) устаревшей реализации (wine) оставлены для совместимости с предыдущими версиями. Не рекомендуется их использовать в новых приложениях. Следует использовать более новую реализацию - криптопровайдер **Crypto-Pro RSA HSM CSP** (и его синонимы). Они реализуют алгоритмы электронной подписи RSA:

- генерацию ключевых пар с размером открытого ключа до 16K;
- формирование и проверку ЭП (RSA);
- вычисление значения хэш-функции с использованием алгоритмов SHA1, SHA256, SHA384, MD5;
- генерацию симметричных ключей DES, 3DES, 3DES_112;
- шифрование/расшифрование по указанным алгоритмам.

Но, если необходимо использовать зарубежные алгоритмы, рекомендуется использовать более современные их модификации, которые реализуются криптопровайдерами 16-го, 24 и 32 типов: **"... ECDSA and AES ..."**, **"...Enhanced RSA and AES ..."** и **"...Curve25519 and AES ..."**.

Все необходимые криптопровайдеры должны быть зарегистрированы на ПЭВМ, использующих криптографические сервисы.

Обычному пользователю не следует использовать криптопровайдеры **"... Svc ..."**. ПО «Клиент КриптоПро HSM» не позволяет работу с данными провайдерами, если в сертификате ключа доступа к ПАКМ нет соответствующего расширения.

Администраторам серверов при использовании ПАКМ «КриптоПро HSM» с такими сервисами как Microsoft CA, «КриптоПро УЦ», Microsoft IIS и другими, реализованными в виде служб ОС Windows, необходимо использовать криптопровайдеры **"...Svc ..."**. Клиентская часть таких провайдеров (на машине клиента ПАКМ «КриптоПро HSM») реализована в виде службы ОС Windows, которая запускается в момент загрузки ОС и может обслуживать криптографические запросы других служб, даже если никто из пользователей не открыл Windows сессию («не залогинился»).

Клиентская часть обычных провайдеров (без лексемы Svc в имени) реализована в виде пользовательского приложения, которое грузится в момент входа («логона»)

пользователя, и отображается в виде иконки в системном трее. Таким образом, если на ПЭВМ с установленным ПО «Клиент КриптоПро HSM» нет активной Windows сессии (ни одного «залогиненного» пользователя), то никто не сможет обслужить криптографические запросы, обращенные к обычным криптопровайдерам.

Администраторам серверов следует с осторожностью относиться к установке криптопровайдеров «КриптоПро HSM» в качестве «провайдеров по-умолчанию» в ОС Windows. Некоторые системные сервисы ОС Windows перечисляют установленные типы криптопровайдеров и реализуемые ими алгоритмы, путем обращения к этим криптопровайдерам. При этом, если КриптоПро HSM выключен в данный момент, не активирован, или в считывателе отсутствует ключ доступа к ПАКМ, то может наблюдаться эффект зависания ОС. Рекомендуется для «провайдеров по-умолчанию» использовать криптопровайдеры с локальной реализацией криптоалгоритмов. Сервера приложений, которым необходимо использовать криптографию «КриптоПро HSM», должны всегда явно обращаться по именам криптопровайдеров (HSM), а не по типам, и не надеяться на то что прописано в ветках реестра «Провайдеры по умолчанию» (Default Provider Types).

Обращения к криптопровайдерам, работающим с ПАКМ через сервис, могут быть сделаны только пользователями с учетными именами SYSTEM (LocalSystem), пользователями, входящими в группу локальных администраторов компьютера или в группу «Привилегированные пользователи КриптоПро HSM». Группу «Привилегированных пользователей КриптоПро HSM» можно создать вручную и добавить туда, например, учетные имена, под которыми исполняются сервисные приложения (например, пул приложений .NET под управлением Microsoft IIS). Эти же правила действуют при обращении пользователей к любым криптопровайдерам ПАКМ через системный трей, при использовании специального флага в вызовах интерфейса CryptoAPI — CRYPT_MACHINE_KEYSET.

Процесс установки дистрибутива ПО «Клиент КриптоПро HSM» не изменяет значение провайдера по умолчанию для 1 типа. Обычно, в ОС Windows им является криптопровайдер «Microsoft Strong Cryptographic Provider».

5.3 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ПАРАМЕТРОВ КРИПТОПРОВАЙДЕРА

Для более тонкой настройки работы с криптопровайдерами существует ряд параметров, которые нельзя изменить, используя штатные оконные средства панели управления криптопровайдером:

- «RPCTimeout» — таймаут ожидания ответа от ПАКМ на вызов криптографической функции.
- «WithoutEnc» — отключить режим шифрования в канале K2 для увеличения производительности сервера.
- «SENDTimeout» — Таймаут ожидания очереди на отправку запросов к HSM.
- «Pool_max_connection» — Максимальное количество одновременных соединений с HSM, устанавливаемое каждым экземпляром Клиент КриптоПро HSM (hsmtray, сервисом cpcspchlm).
- «Init_pool_size» — Начальное количество одновременных соединений с HSM, устанавливаемое сразу при запуске сервиса cpcspchlm или при установлении подключения к HSM через hsmtray.
- «Connection_pool_max_retry» — Количество попыток найти свободное соединение с HSM в общем пуле соединений для обработки поступившего запроса.
- «DisableDeleteContainer» — Запрет пользователям на удаление ключевых контейнеров в HSM через оснастку <КриптоПро HSM>.
- «DisableInstallCertificate» — Запрет пользователям на установку сертификатов в ключевой контейнер через оснастку <КриптоПро HSM>.
- «DisableViewCertificate» — Запрет пользователям на извлечение и просмотр сертификатов из ключевого контейнера через оснастку <КриптоПро HSM>.
- «DisableChangePassword» — Запрет пользователям на изменение пароля на ключевой контейнер в HSM через оснастку <КриптоПро HSM>.

Данные параметры по умолчанию не прописываются в Реестре Windows и имеют следующие значения:

«RPCTimeout» для обычных (не сервисных) криптопровайдеров равен 15 секунд. Для сервисных криптопровайдеров ... Svc ...» он равен 60 секунд. Увеличенный таймаут для серверного провайдера объясняется тем, что pin-коды на контейнеры ключей, хранящихся в ПАКМ для данного криптопровайдера запрашиваются с LCD панели ПАКМ. Это может быть довольно длительная процедура, особенно если дополнительно запрашивается подтверждение ввода pin-кода. Pin-коды же для контейнеров ключей, сформированных для

провайдера «Crypto-Pro HSM CSP», запрашиваются на рабочем столе пользователя и данная процедура не входит в интервал ожидания ответа от ПАКМ.

При очень высокой загрузке ПАКМ криптографическими запросами пользователей и серверов приложений время отклика ПАКМ может существенно возрастать, особенно если используется полное журналирование криптографических запросов (событий подписи, шифрования, расшифрования...) в журнале аудита ПАКМ.

Для увеличения значения данного параметра необходимо вручную добавить ключ «RPCTimeout» и его новое значение типа «DWORD» в реестр Windows в ветку:

HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\

Параметр «WithoutEnc» по умолчанию равен 0 (нулю), т.е. используется канал «K2». Данный параметр может быть изменен на значение (DWORD) «1» только при использовании специального сертификата ключа доступа к ПАКМ, включающего расширение «Администратор сервера» и используется обычно криптопровайдером «КриптоПро HSM Svc CSP». Соответствующая настройка должна быть произведена и внутри ПАКМ «КриптоПро HSM» (см. опцию «Enable K2s» в п. «Просмотр и изменение параметров ПАКМ» документа «ЖТЯИ.00096-03 90 01. КриптоПро HSM. Инструкция по использованию»), позволяющая работу (запускающая слушатель на специальный порт 1503) по нешифрованному каналу. При этом TLS аутентификация проходит обычным образом.

Для изменения значения данного параметра – отключения шифрования в канале K2 - необходимо вручную добавить ключ «WithoutEnc» и его новое значение («1») типа «DWORD» в реестр Windows в ветку:

HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\

Для 64 битных версий ОС соответствующая ветка находится:

HKLM\SOFTWARE\WOW6432Node\Crypto Pro\Cryptography\CurrentVersion\HSM\

Для отключения шифрования в канале K2 (K2s), необходимо выполнить следующие инструкции:

- Сервер и ПАКМ должны находиться в одной контролируемой зоне;
- Для работы по нешифрованному каналу должен использоваться отдельный сетевой интерфейс ПАКМ.

ПО «Клиент КриптоПро HSM» является многопоточным приложением. Для обеспечения большей производительности можно создать сразу пул соединений с ПАКМ «КриптоПро HSM». Эти готовые соединения могут быть использованы приложениями пользователя, серверами приложений для доступа к HSM одновременно и без длительного процесса начальной установки соединений.

По умолчанию используется пул из 20-ти возможных соединений с предварительной установкой 1-го соединения. Последующие соединения (19 шт.) будут устанавливаться по мере необходимости. Если какое-либо приложение/поток подаст запрос к ПАКМ, но при этом

все открытые соединения заняты обработкой запросов от других приложений/потоков, то ПО «Клиент КриптоПро HSM» установит новое соединение, если общее количество не превышает заданного максимального количества (`Pool_max_connection`). Если же используются все возможные соединения, то ПО «Клиент КриптоПро HSM» будет пытаться несколько раз (по умолчанию 40) получить освобождающееся соединения из пула. Количество попыток можно изменить, установив соответствующее значение переменной `Connection_pool_max_retry`.

Максимально возможное количество соединений в пуле можно изменить, установив соответствующее значение переменной `Pool_max_connection`.

Начальное количество устанавливаемых соединений с ПАКМ при запуске службы или при подключении `hsmtray` можно изменить, установив соответствующее значение переменной `Init_pool_size`, соответственно оно д.б. меньше либо равно значению `Pool_max_connection`.

Значение параметра «`SENDTimeout`» - (Таймаут ожидания очереди на отправку запросов к HSM) по умолчанию составляет 15 сек.

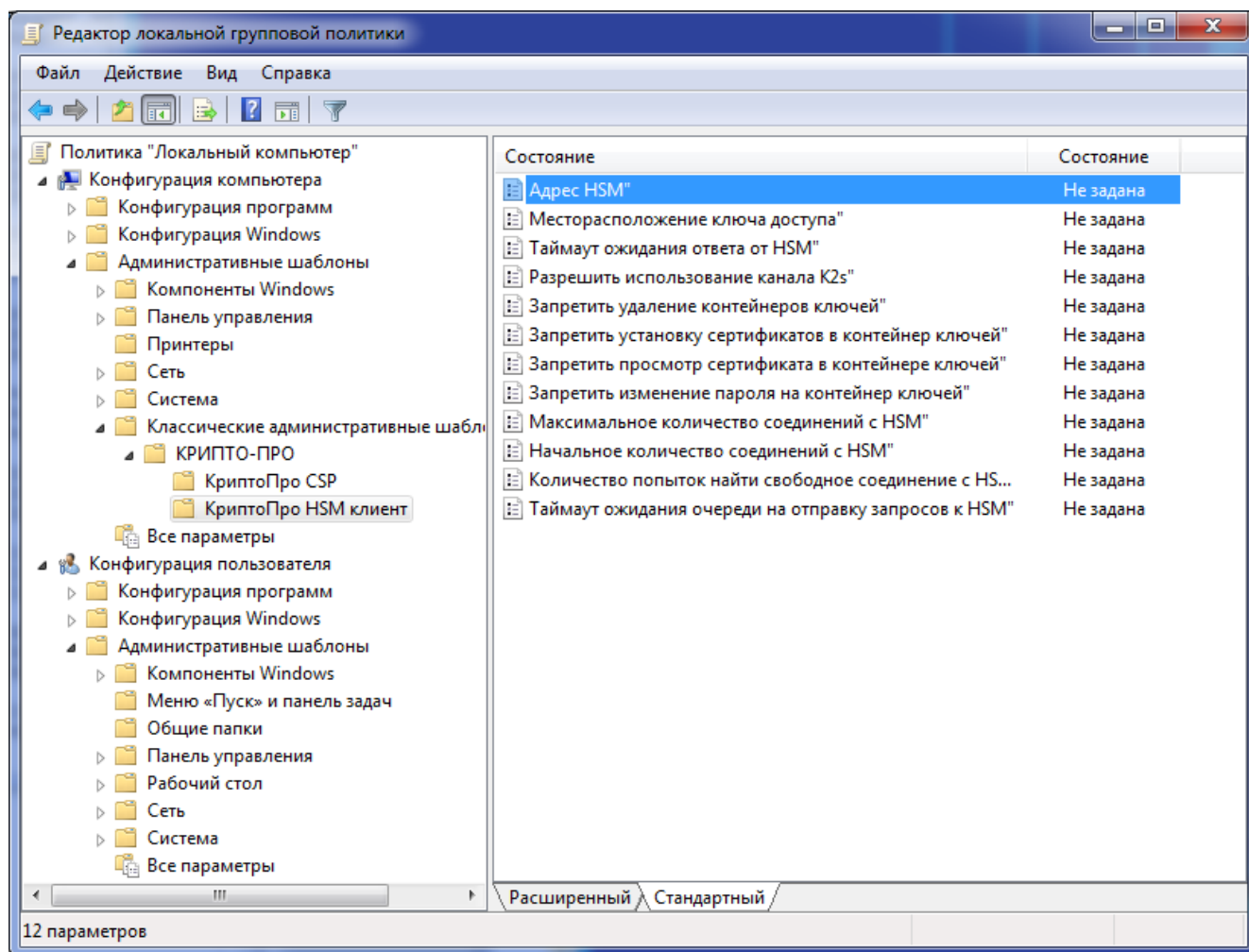
Параметры "`DisableDeleteContainer`", "`DisableInstallCertificate`", «`DisableViewCertificate`», «`DisableChangePassword`» по умолчанию имеют значения «0» (`FALSE`), т.е. данные операции разрешены пользователю. Установка их в значение «1» приведет к запрету соответствующей операции.

Указанные выше параметры могут быть переопределены групповой политикой.

Для редактирования групповой политики используется специальный административный шаблон.

Для доступа к указанной политике используйте команду

`gpedit /32`



Значения переменных групповой политики хранятся в ветке реестра Windows Software\[WOW6432Node\]Policies\Crypto-Pro\HSM и имеют преимущество (если установлены) перед теми, которые хранятся в ветке SOFTWARE\[WOW6432Node\]Crypto Pro\Cryptography\CurrentVersion\HSM.

5.4 НАСТРОЙКА КОНФИГУРАЦИИ С НЕСКОЛЬКИМИ ПАКМ

ПО «Клиент КриптоПро HSM» поддерживает возможность одновременной работы пользователя с одной рабочей станции сразу с несколькими экземплярами ПАКМ «КриптоПро HSM». Данные ПАКМ могут быть как клонами друг друга, например, в целях повышения производительности систем, либо в целях отказоустойчивости, так и различными по наборам ключевой информации и вариантам использования.

В конечном итоге, с точки зрения программного интерфейса MS CryptoAPI, выбор приложения для работы с тем или иным ПАКМ сводится к выбору соответствующего имени криптопровайдера. При наличии только одного ПАКМ «КриптоПро HSM» в системе вся деятельность по настройке и эксплуатации ПАКМ и ПО «Клиент КриптоПро HSM» ничем не отличается от того, что было в предыдущих версиях.

Существующий графический интерфейс пользователя (GUI) по настройке параметров

ПО «Клиент КриптоПро HSM» прописывает значения параметров подключения к ПАКМ в Реестре Windows в ветке:

HKLM\SOFTWARE\[Wow6432Node\]Crypto Pro\Cryptography\CurrentVersion\HSM;

HKLM\SOFTWARE\[Wow6432Node\]Policy\Crypto Pro\Cryptography\CurrentVersion\HSM – то же, но настраиваемое, как групповая политика.

В дальнейшем для упрощения в документе будет указываться только один вариант корня данной ветки.

Прописываются следующие параметры:

"Channel" – строка, содержащая IP адрес или dns имя ПАКМ;

"Reader" – строка с именем используемого считывателя PC/SC для поиска контейнера с ключом доступа к ПАКМ, либо полное имя контейнера данного ключа в Реестре Windows.

Администратор сервера/рабочей станции может прописать там ещё два параметра:

- "RPCTimeout"=dword – значение таймаута до получения ответа от ПАКМ, в секундах;
- "WithoutEnc"=dword – значение 0 или 1, указывающее на возможность отключения шифрования в канале K2.

Если в системе присутствует только один ПАКМ, то этой ветки Реестра достаточно для нормального функционирования сервисов ПО «Клиент КриптоПро HSM».

Если в конфигурации системы присутствует несколько ПАКМ, то параметры, указанные в ветке Реестра HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM, используются как параметры по умолчанию, наследуемые всеми ПАКМ.

Для указания программному обеспечению «Клиент КриптоПро HSM», что в системе используется несколько ПАКМ (более одного), необходимо прописать их идентификаторы в виде ключей ветки Реестра:

HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs

Например,

HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs\HSM1

HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs\HSM2

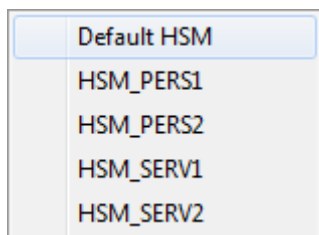
HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs\HSM3

И для каждого можно указать точно такие же параметры, как «параметры по умолчанию», но с отличающимися, а, возможно, и такими же значениями (включая и ip адрес и имя считывателя/контейнера ключа доступа к ПАКМ).

Использование нескольких описаний с одними и теми же параметрами может увеличить производительность сервера (распараллелить обращения нескольких процессов к одному и тому же ПАКМ).

На каждый ПАКМ может быть запущено от одного до нескольких сервисов ПО «Клиент

КриптоПро HSM», а также системных треев. При подключении к ПАКМ через GUI системного трея пользователю будет выдаваться меню из набора идентификаторов ПАКМ (ключей ветки HKLM\SOFTWARE\CryptoPro\Cryptography\CurrentVersion\HSM\HSMIDs) для выбора, к какому ПАКМ осуществить подключение данного экземпляра трея:



Таким образом, если у пользователя нет необходимости в *одновременной* работе с несколькими ПАКМ, то может быть запущен только один экземпляр системного трея. Пользователь может завершить работу с одним ПАКМ, потом подключиться к другому, выбрав из меню идентификаторов соответствующий ПАКМ.

Главным условием запуска нескольких сервисов и системных треев ПО «Клиент КриптоПро HSM» одновременно является то, что они должны использовать разные имена «слушателей» - RPC (Remote Procedure Call) точек подключений (RPC Endpoint).

Для указания имени «RPC точки подключения» используется:

- Флаг «-е» с последующим именем в командной строке запуска трея (например, hsmtray -e "My endpoint 1 %d");
- Параметр «CP Service Name» в ключе реестра windows, описывающем запускаемый сервис.

Инсталляция ПО «Клиент КриптоПро HSM» прописывает один сервис cpcsphclm для работы с ПАКМ в фоновых режимах (без обязательного наличия Logon сессии пользователя) - ветки

HKLM\SYSTEM\CurrentControlSet\services\cpcsphclm

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost

(см. документацию на svchost.exe)

и запуск одного системного трея при входе пользователя в систему – ветка:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

При этом параметры, указывающие имена RPC точек подключения, нигде не прописываются. По умолчанию используются следующие имена (прошиты в коде программы)

- "CryptoPro HSM Client Service LM" - для сервиса;
- "CryptoPro HSM Client Service %d" – для трея.

Если в имени точки подключения последние 2 символа %d, то они будут заменены при старте трея/сервиса номером LOGON сессии пользователя (или 0 – для сервиса).

Для запуска ещё одного экземпляра трея необходимо в командной строке его запуска указать уникальные значения опции «-е».

Чтобы запустить ещё один экземпляр сервиса необходимо добавить его описание в систему (см. документацию на svchost.exe), а также в его описании в Реестре добавить строковый параметр «CP Service Name» и указать там уникальное значение имени RPC точки подключения. Для указания, к какому экземпляру ПАКМ данный экземпляр сервиса должен подключаться необходимо там же добавить строковый параметр «HSMID» и указать значение идентификатора ПАКМ, например, «HSM3» (без кавычек), т.е. одно из тех имен, которые прописывались в ветке HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs.

При запуске системного троя в командной строке также можно указать - с каким именно HSMID данный трей должен работать. Для этого используется параметр «-m» с последующим значением идентификатора ПАКМ, например, «-m HSM3». В этом случае данный трей не будет видеть других идентификаторов ПАКМ, прописанных в реестре, и, фактически, будет «закреплен» за конкретным ПАКМ. Это позволяет запускать несколько системных треев при автозагрузке с заранее определенной администратором конфигурацией.

Библиотеки криптопровайдеров КриптоПро для подключения к криптографическим сервисам используют значение параметра «CP Service Name», как имени «RPC точки подключения». Данный параметр прописывается в ключе, описывающем конкретное имя криптопровайдера (см. HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\<имя криптопровайдера>).

Таким образом, если необходимо использовать несколько криптографических сервисов, каждый из которых прослушивает RPC с использованием уникальных имен «RPC точек подключений», необходимо зарегистрировать дополнительные имена криптопровайдеров, у которых прописать значения этих точек подключений.

При этом, если приложению необходимо обратиться к определенному ПАКМ, оно должно обратиться к определенному сервису/трею по согласованной «точке подключения», а фактически использовать для этого правильное имя криптопровайдера.

Т.к. внутри ПАКМ «КриптоПро HSM» набор зарегистрированных имен криптопровайдеров строго определен заранее в момент его изготовления и не может быть расширен в процессе эксплуатации, ПО сервисов/трея «Клиент КриптоПро HSM» в таких случаях пытается сделать замену имени криптопровайдера, транслируя в ПАКМ уже правильное имя. Делает это оно следующим образом:

В имени криптопровайдера, переданном приложением сервису/трею, ищется подстрока «Proху» и если находится, то просто «хвост» имени с этой точки отсекается. Например, в ПАКМ «КриптоПро HSM» и в ОС Windows есть зарегистрированный провайдер с именем «Crypto-Pro HSM CSP». Для того, чтобы использовать еще один сервис с дополнительной точкой подключения можно зарегистрировать дополнительное имя криптопровайдера с именем «Crypto-Pro HSM CSPProxy HSM1», «Crypto-Pro HSM CSPProxy

HSM2» и т.п. В ПАКМ сервис будет передавать строку «Crypto-Pro HSM CSP».

Кроме этого в ПАКМ «КриптоПро HSM» для целей создания кластеров из ПАКМ добавлено по 8 дополнительных имен криптопровайдеров для 1-го и 75-го типов, по 4 дополнительных имени для 80, 81, 16 и 24 типов криптопровайдеров. Данные имена имеют вид:

Для 75 и 1 типа:

- Crypto-Pro HSM CSP NN
- Crypto-Pro HSM RSA CSP NN

Где NN – номера от 1 до 8 с лидирующим нулем (т.е. в виде «01»... «08»).

Для 80 типа:

- Crypto-Pro GOST R 34.10-2012 HSM CSP 01
- Crypto-Pro GOST R 34.10-2012 HSM CSP 02
- Crypto-Pro GOST R 34.10-2012 HSM CSP 03
- Crypto-Pro GOST R 34.10-2012 HSM CSP 04

Для 81 типа:

- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 01
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 02
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 03
- Crypto-Pro GOST R 34.10-2012 Strong HSM CSP 04

Для 16 типа:

- Crypto-Pro ECDSA and AES HSM CSP 01
- Crypto-Pro ECDSA and AES HSM CSP 02
- Crypto-Pro ECDSA and AES HSM CSP 03
- Crypto-Pro ECDSA and AES HSM CSP 04

Для 24 типа:

- Crypto-Pro Enhanced RSA and AES HSM CSP 01
- Crypto-Pro Enhanced RSA and AES HSM CSP 02
- Crypto-Pro Enhanced RSA and AES HSM CSP 03
- Crypto-Pro Enhanced RSA and AES HSM CSP 04

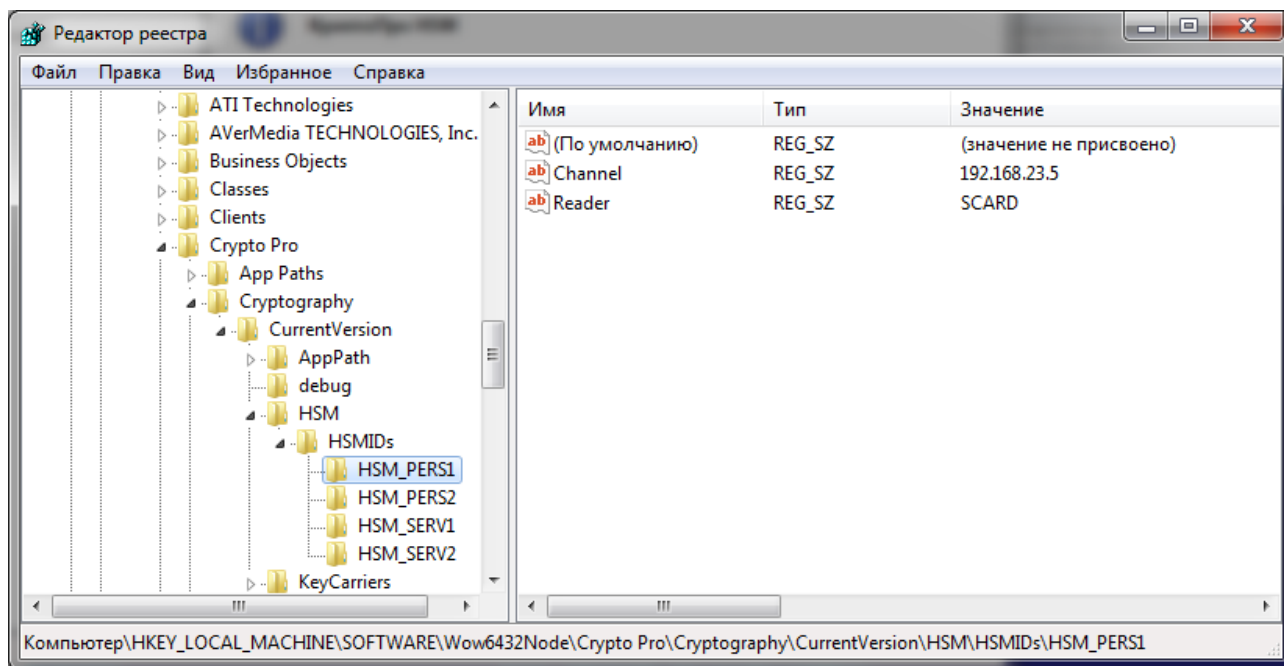
Таким образом, если количество синхронизируемых ПАКМ не превышает указанного числа криптопровайдеров нужного типа, то можно (даже рекомендуется) использовать указанные выше имена, зарегистрированные внутри ПАКМ «КриптоПро HSM». Если количество синхронизируемых ПАКМ более восьми или четырех (в зависимости от типа), в дополнение можно использовать произвольные имена, полученные из зарегистрированных имен с добавлением суффиксов «Proху...».

При использовании имен с суффиксом "Proху ..." не рекомендуется использовать в программах вызовы CryptGetProvParam (... , PP_NAME,...), с последующим использованием

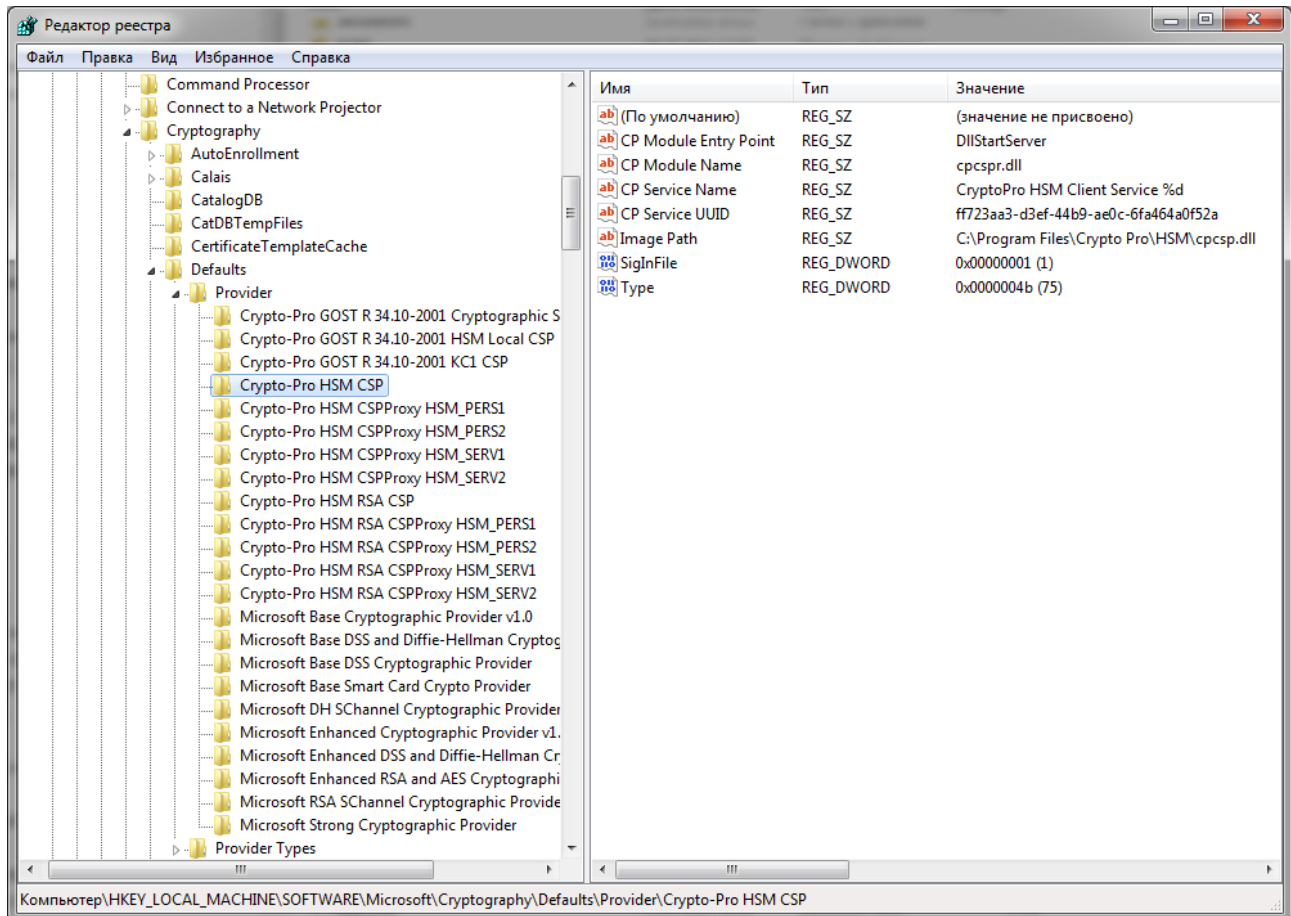
возвращаемого данным методом имени криптопровайдера в той же программе. Возвращаемое таким образом имя будет отличаться от начального, используемого при открытии контекста, в нем уже будет отсутствовать суффикс «Proху...». Следующий вызов открытия контекста с новым именем может быть перенаправлен совсем в другой ПАКМ.

Ниже приводится визуальное пояснение всего вышесказанного.

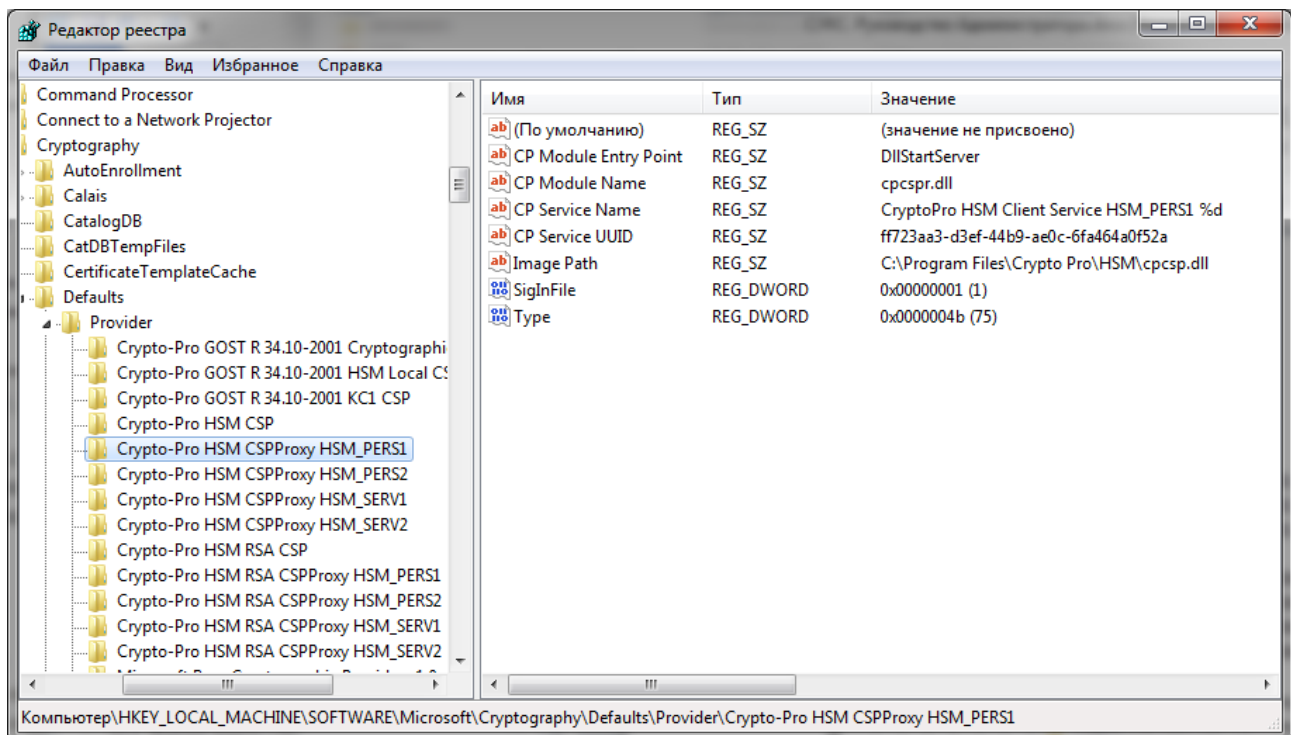
Описание зарегистрированного списка ПАКМ «КриптоПро HSM»:

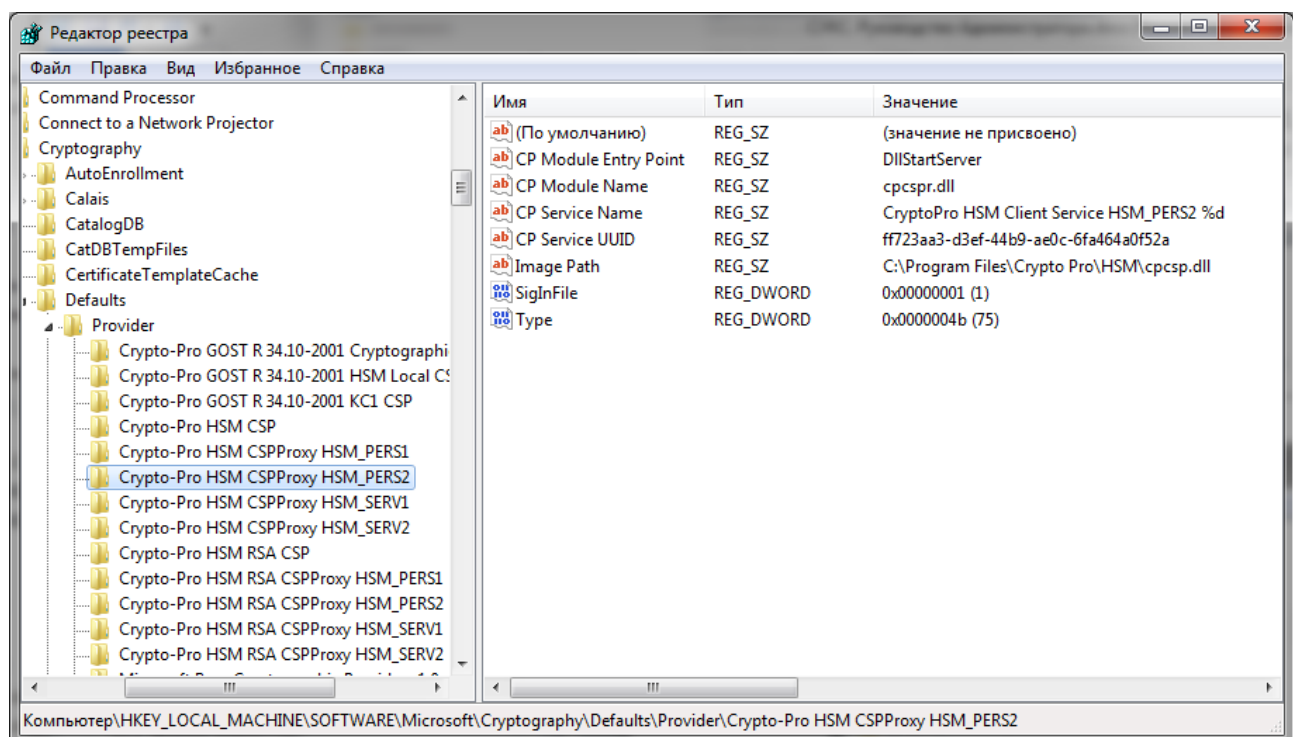
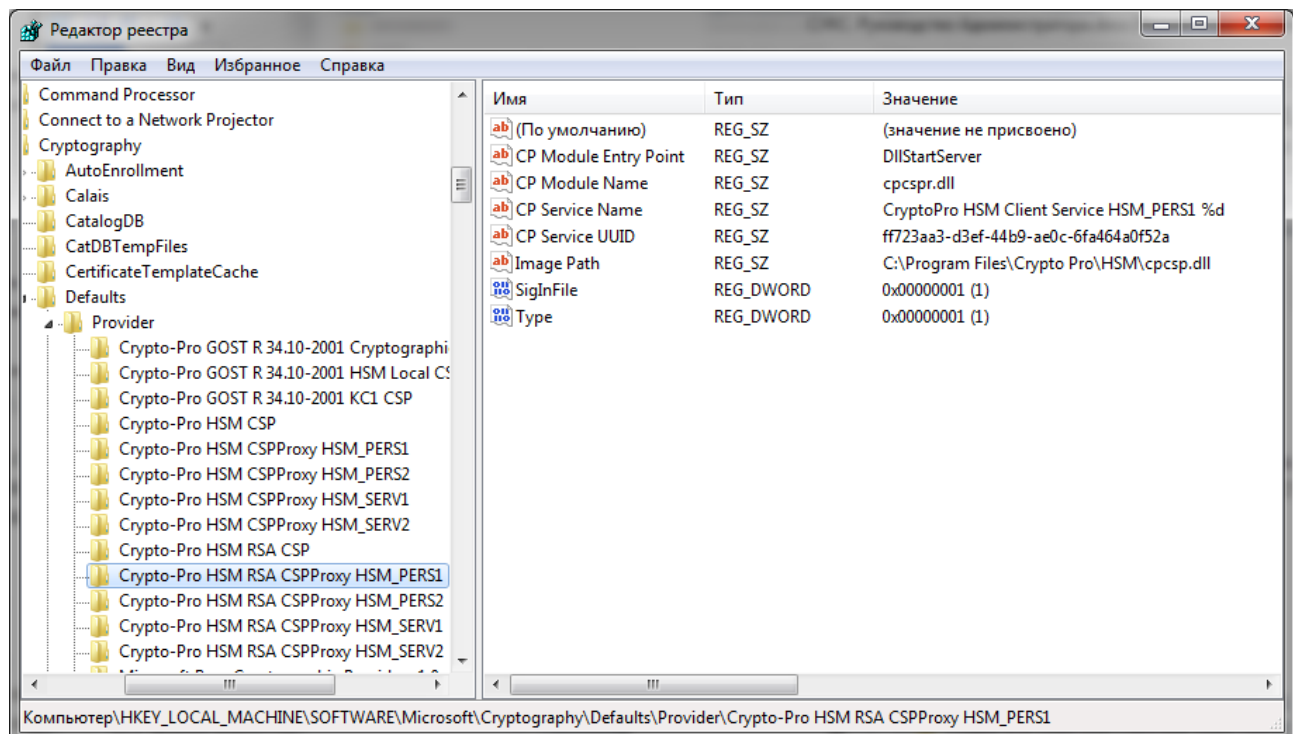


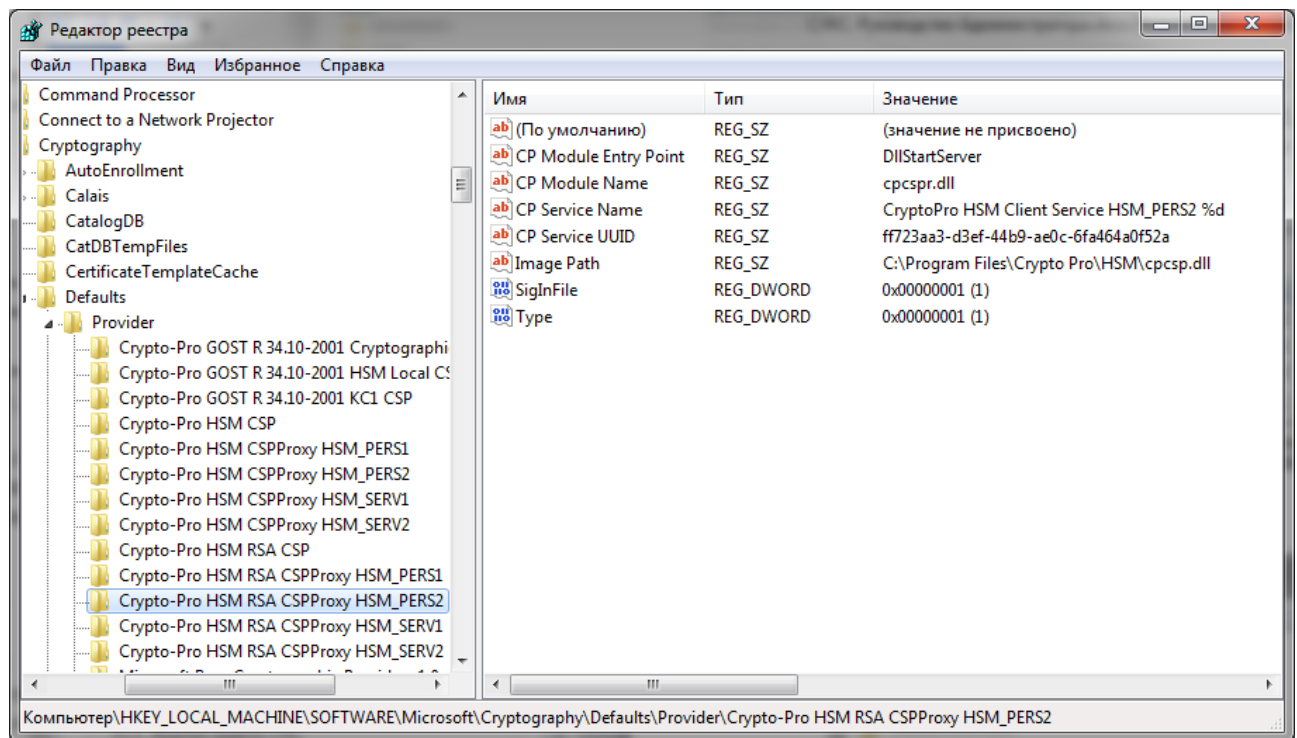
Описание дополнительных имен криптопровайдеров - по одной паре 75-го и 1-го типа для каждого ПАКМ, зарегистрированного в ключе HSMIDs (это удобно делать путем экспорта описаний существующих криптопровайдеров, например, «Crypto-Pro HSM CSP» и «Crypto-Pro HSM RSA CSP» в файлы «.reg», изменением в этих файлах имен Криптопровайдеров и параметров с именем «CP Service Name» (значение RPC точки подключения), и запуском этих обновленных файлов из оболочки Windows Explorer):



При этом значение параметров «CP Service Name» для каждой пары ГОСТ и RSA криптопровайдеров должны быть одинаковы (т.е. один системный трей будет подключаться к одному ПАКМ, который обрабатывает запросы и для ГОСТ и для RSA криптопровайдера).







Если в использовании RSA алгоритмов нет необходимости, то и прописывать соответствующие имена криптопровайдеров не нужно.

6. КОНТРОЛЬ ЦЕЛОСТНОСТИ

Клиентский компонент ПАКМ и комплект эксплуатационной документации к нему поставляются пользователю Уполномоченной организацией на носителе (компакт-диски).

Вместе с дистрибутивом и документацией на диске размещается отделенная электронная подпись, для проверки которой необходимо использовать утилиту **cpverify**, полученную доверенным образом и содержащую ключ проверки данной электронной подписи.

Установка клиентского компонента ПАКМ может быть осуществлена только в случае подтверждения целостности полученных установочных модулей эксплуатационной документации.

Порядок использования утилиты **cpverify** описан в Приложении 1 Правил пользования СКЗИ «КриптоПро CSP», входящего в комплектацию клиентского компонента ПАКМ.



1. Средство контроля целостности (cpverify.exe) первоначально должно быть получено пользователем на физическом носителе в офисе компании ООО «КРИПТО-ПРО», либо у официального дилера. Такая утилита считается полученной доверенным образом. Далее полученной доверенным образом признается очередная версия утилиты, полученная любым образом, например, скачанная с сайта www.cryptopro.ru, при условии, что она была проверена другим экземпляром утилиты, полученным ранее доверенным образом, и проверка была успешной.
2. Ключ проверки ЭП, а также информация о нем (дата создания, алгоритм хэш-функции, идентификатор алгоритма подписи) записываются в исходный код утилиты на этапе сборки.

ПРИЛОЖЕНИЕ 1.

ПРИМЕР КОНФИГУРАЦИОННОГО ФАЙЛА ПАКМ «КРИПТОПРО HSM» НА СЕРВЕРАХ С ОС LINUX

```
[Random]
# Датчики случайных чисел
# Bio - Биологический датчик
# Dsrf - Датчик ДСДР
# Sable - Датчик Соболь
[Random\Bio_tui]
"DLL"="libdrdrndmbio_tui.so"

[Random\Dsrf]
"DLL"="libdrdrdsrf.so"

[Random\CPSD]
"DLL"="libdrdrdsrf.so"

[Random\CPSD\Default]
Name = "\xc4\xd1\xd0\xd4"
Level = 3
"/db1/kis_1" = "/var/opt/cproscsp/dsrf/db1/kis_1"
"/db2/kis_1" = "/var/opt/cproscsp/dsrf/db2/kis_1"

[KeyDevices]
# Типы считывателей
# FAT12 - Считыватель "Дисковод"
# HDImage - Считыватель "Структура дискеты на жестком диске"
# PCSC - Считыватель смарт-карт GemPC
[KeyDevices\FAT12]
"DLL"="libdrdrfat12.so"
"Group"=1

[KeyDevices\HDImage]
"DLL"="libdrdrfat12.so"
[KeyDevices\HDIMAGE\Default]
Name = "\xd1\xf2\xf0\xf3\xea\xf2\xf3\xf0\xe0 \xe4\xe8\xf1\xea\xe5\xf2\xfb" \
" \xed\xe0 \xe6\xe5\xf1\xf2\xea\xee\xec \xe4\xe8\xf1\xea\xe5"

[KeyDevices\HSM]
"DLL"="libdrdrfat12.so"

[KeyDevices\FLASH]
Dll = "libdrdrfat12.so"
Script = "mount_flash.sh"

[KeyDevices\FLASH\Default]
Name = "FLASH"

[KeyDevices\PCSC]
DLL = "libdrpcsc.so"
Group = 1

[KeyDevices\PCSC\ "PNP PCSC"\Default]
Name = "All PC/SC readers"

[Capilite\cache_settings]
# Максимальное количество элементов
max_elements=100
fresh_time=3600

[PKCS11]
# настройки для PKCS11
```

```
# [PKCS11\slot0]
# ProvGOST = "Crypto-Pro GOST R 34.10-2001 KC1 CSP"
# ProvRSA = "Microsoft Strong Cryptographic Provider"
# reader = hdimage

[Parameters]
# Параметры провайдера

# Настройки TLS
# tls_client_use_ocsp_extensions=0
# tls_client_disable_revocation_check=0
# tls_client_disable_self_certificate_usage_validation=0
# tls_client_disable_legacy_cipher_suites=0
# tls_server_use_ocsp_extensions=0
# tls_server_disable_revocation_check=0
# tls_server_disable_self_certificate_usage_validation=0
# tls_server_disable_legacy_cipher_suites=0
# tls_server_use_renegotiation_info_extension=0
# tls_server_max_sessions=64
# tls_server_max_certificate_request_cas=100

# Период работы тестера
#TesterPeriod=10
TesterPeriod=600
PKZI_Build=9092
ConfigEncoding="CP1251"
DisableShortcuts=true
max_rpc_session=2048
need_audit = 0
need_stat = 1
DisableSavedPasswords = 1
MaxHandles = 65536

[Provider]
# Шаблоны провайдеров по типам носителей

# Проверка алгебраических свойств открытого ключа
CheckPublic = true

[apppath]
"libdrfat12.so" = "/opt/cprocsp/lib/amd64/libdrfat12.so"
"libdrdrdr.so" = "/opt/cprocsp/lib/amd64/libdrdrdr.so"
"libdrdrndm.so" = "/opt/cprocsp/lib/amd64/libdrdrndm.so"
"libdrdrsrf.so" = "/opt/cprocsp/lib/amd64/libdrdrsrf.so"
"libcpui.so" = "/opt/cprocsp/lib/amd64/libcpui.so"
"libcurl.so" = "/usr/local/lib/64/libcurl.so"
"mount_flash.sh" = "/opt/cprocsp/sbin/amd64/mount_flash.sh"
"libcspr.so" = "/opt/cprocsp/lib/amd64/libcspr.so"
"libpcsc-lite.so" = "libpcsc-lite.so.1"
"libdrpcsc.so" = "/opt/cprocsp/lib/amd64/libdrpcsc.so"
"libdrdric.so" = "/opt/cprocsp/lib/amd64/libdrdric.so"
"libpkivalidator.so" = "/opt/cprocsp/lib/amd64/libpkivalidator.so"
# Пути к библиотекам

[Services]
# Службы и их параметры.
# Параметр "StartService" указывает имя исполняемого файла службы
# (в каталоге @ac_default_prefix@/sbin)
# Остальные параметры зависят от службы
# Секции сервисов:
#   HSMServer - Служба ПАКМ
#   HSMClient - Служба поддержки канала "К" (клиент ПАКМ)
#   CryptSrvKB2 - Служба провайдера KB
#   CryptSrvKC2 - Служба провайдера KC2

[Services\HSMServer]
StartService = "fenixmsrv"

[Services\CryptSrvKC2]
StartService = "cryptsrv"
```

```
[Defaults\Provider]
# Провайдеры. Описание провайдера должно содержать поля:
# "Image Path" = путь до разделяемой библиотеки провайдера
# "Type"= тип провайдера

[Defaults\Provider\Crypto-Pro HSM CSP]
"Image Path" = "/opt/cproscsp/lib/amd64/libcspr.so"
Type = 75
Channel = ".clientk2"
Media = "HSM"
"Function Table Name" = "CPSRV_GetFunctionTable"

[Defaults\Provider\Crypto-Pro GOST R 34.10-2001 HSM CSP]
"Image Path" = "/opt/cproscsp/lib/amd64/libcspr.so"
Type = 75
Channel = ".clientk2"
Media = "HSM"
"Function Table Name" = "CPSRV_GetFunctionTable"

[Defaults\Provider\Crypto-Pro GOST R 34.10-2012 HSM CSP]
"Image Path" = "/opt/cproscsp/lib/amd64/libcspr.so"
Type = 80
Channel = ".clientk2"
Media = "HSM"
"Function Table Name" = "CPSRV_GetFunctionTable"

[Defaults\Provider\Crypto-Pro GOST R 34.10-2012 Strong HSM CSP]
"Image Path" = "/opt/cproscsp/lib/amd64/libcspr.so"
Type = 81
Channel = ".clientk2"
Media = "HSM"
"Function Table Name" = "CPSRV_GetFunctionTable"

[Defaults\Provider Types]
# Типы провайдеров. Описание типа провайдера должно содержать поля:
# "Name"= имя провайдера по умолчанию для данного типа

[Defaults\Provider Types\Type 075]
Name = "Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider"
TypeName = "GOST R 34.10-2001 Signature with Diffie-Hellman Key Exchange"

[Defaults\Provider Types\Type 080]
TypeName = "GOST R 34.10-2012 (256) Signature with Diffie-Hellman Key Ex" \
"change"
Name = "Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider"

[Defaults\Provider Types\Type 081]
TypeName = "GOST R 34.10-2012 (512) Signature with Diffie-Hellman Key Ex" \
"change"
Name = "Crypto-Pro GOST R 34.10-2012 Strong Cryptographic Service Provider"

["dummy section comment for debug"]
# Фильтр отладочных сообщений в формате "Имя модуля"=битовая маска
# Флаги фильтрации (modname=x):
# Потери производительности [нет auth.* в syslog.conf] [есть auth.*]
#   N_DB_ERROR = 1           0%           0%
#   N_DB_TRACE = 2           77%          98%
#   N_DB_CALL = 4            70%          98%
#   N_DB_LOG = 8             1%           30%
# Флаги формата (modname_fmt=x):
#   module 1
#   thread 2
#   file_and_line 4
#   function 8
#   text 16
#   hex 32
#   error 64

[debug]
```

```
cpcsp=1
cpcsp_fmt=57
capi10=1
capi10_fmt=57
cprdr=0
cprdr_fmt=57
cpevt=1
cpevt_fmt=57
capi20=1
capi20_fmt=57
capilite=1
capilite_fmt=57
libcspr=1
libcspr_fmt=57
cryptsrv=1
cryptsrv_fmt=57
kchansrv=1
kchansrv_fmt=57
fenixsrv=1
fenixsrv_fmt=57
libssp=1
libssp_fmt=57
cppkcs11=1
cppkcs11_fmt=57
cpdrv=1
cpdrv_fmt=57
dmntcs=1
dmntcs_fmt=57
ocsp=1
ocsp_fmt=57
tsp=1
tsp_fmt=57
cades=1
cades_fmt=57
pkivalidator=1
pkivalidator_fmt=57
pcsc=0
pcsc_fmt=57
```

```
[OID]
```

```
# Идентификаторы алгоритмов. Описание идентификатора должно содержать поля:
# "Name"= имя идентификатора
# "AlgId"= номер идентификатора (ALG_ID)
# "ExtraInfo"= бинарный блок доп. информации (опционально)
```

```
[OID\1.3.14.3.2.26!1]
```

```
"Name"="sha1"
"AlgId"=32772
```

```
[OID\1.3.14.3.2.18!1]
```

```
"Name"="sha"
"AlgId"=32772
```

```
[OID\1.2.840.113549.1.1.5!4]
```

```
"Name"="sha1/RSA"
"AlgId"=32772
"ExtraInfo"=hex:00,24,00,00,00,00,00,00,01,00,00,00
#"ExtraInfo"=hex:00,00,24,00,00,00,00,00,00,00,00,01
```

```
[OID\1.2.840.113549.1.1.1!3]
```

```
"Name"="RSA"
"AlgId"=9216
"ExtraInfo"=hex:00,00,00,00
```

```
[OID\1.2.643.2.2.19!3]
```

```
"Name"="ГОСТ Р 34.10-2001"
"AlgId"=11811
"ExtraInfo"=hex:00,00,00,00
```

```
[OID\1.2.643.2.2.21!2"]
"Name"="ГОСТ 28147-89"
"Algid"=26142

[OID\1.2.643.2.2.3!4"]
"Name"="ГОСТ Р 34.11/34.10-2001"
"Algid"=32798
"ExtraInfo"=hex:23,2e,00,00,04,00,00,00,4b,00,00,00
#"ExtraInfo"=hex:00,00,2e,23,00,00,00,04,00,00,00,4b

[OID\1.2.643.2.2.30.1!20"]
"Name"="ГОСТ Р 34.11-94, параметры по умолчанию"

[OID\1.2.643.2.2.30.2!20"]
"Name"="ГОСТ Р 34.11-94, параметры хеша 1"

[OID\1.2.643.2.2.30.3!20"]
"Name"="ГОСТ Р 34.11-94, параметры хеша 2"

[OID\1.2.643.2.2.30.4!20"]
"Name"="ГОСТ Р 34.11-94, параметры хеша 3"

[OID\1.2.643.2.2.31.1!20"]
"Name"="ГОСТ 28147-89, параметры по умолчанию"

[OID\1.2.643.2.2.31.2!20"]
"Name"="ГОСТ 28147-89, параметры шифрования 1"

[OID\1.2.643.2.2.31.3!20"]
"Name"="ГОСТ 28147-89, параметры шифрования 2"

[OID\1.2.643.2.2.31.4!20"]
"Name"="ГОСТ 28147-89, параметры шифрования 3"

[OID\1.2.643.2.2.31.5!20"]
"Name"="ГОСТ 28147-89, параметры Оскар 1.1"

[OID\1.2.643.2.2.31.6!20"]
"Name"="ГОСТ 28147-89, параметры Оскар 1.0"

[OID\1.2.643.7.1.2.5.1.1!20"]
"Name"="ГОСТ 28147-89, параметры шифрования ТС26 А"

[OID\1.2.643.2.2.31.12!20"]
"Name"="ГОСТ 28147-89, параметры шифрования ТС26 1"

[OID\1.2.643.2.2.31.13!20"]
"Name"="ГОСТ 28147-89, параметры шифрования ТС26 2"

[OID\1.2.643.2.2.31.14!20"]
"Name"="ГОСТ 28147-89, параметры шифрования ТС26 3"

[OID\1.2.643.2.2.31.15!20"]
"Name"="ГОСТ 28147-89, параметры шифрования ТС26 4"

[OID\1.2.643.2.2.31.16!20"]
"Name"="ГОСТ 28147-89, параметры шифрования ТС26 5"

[OID\1.2.643.2.2.31.17!20"]
"Name"="ГОСТ 28147-89, параметры шифрования ТС26 6"

[OID\1.2.643.2.2.34.1!7"]
"Name"="Аудит TLS трафика"

[OID\1.2.643.2.2.34.2!7"]
"Name"="Идентификация пользователя на Центре Регистрации"

[OID\1.2.643.2.2.34.3!7"]
"Name"="Подпись содержимого сервера Интернет"
```

```
[OID\1.2.643.2.2.34.4!7]
"Name"="Администратор Центра Регистрации"

[OID\1.2.643.2.2.34.5!7]
"Name"="Оператор Центра Регистрации"

[OID\1.2.643.2.2.35.1!20]
"Name"="ГОСТ Р 34.10-2001, параметры по умолчанию"

[OID\1.2.643.2.2.35.2!20]
"Name"="ГОСТ Р 34.10-2001, параметры Оскар 2.x"

[OID\1.2.643.2.2.35.3!20]
"Name"="ГОСТ Р 34.10-2001, параметры подписи 1"

[OID\1.2.643.2.2.36.0!20]
"Name"="ГОСТ Р 34.10-2001, параметры обмена по умолчанию"

[OID\1.2.643.2.2.36.1!20]
"Name"="ГОСТ Р 34.10-2001, параметры обмена 1"

[OID\1.2.643.2.2.9!1]
"Name"="ГОСТ Р 34.11-94"
"Algid"=32798

[OID\1.2.643.2.2.98!3]
"Name"="ГОСТ Р 34.10-2001 DH"
"Algid"=43556

[OID\1.2.643.7.1.1.1.1!3]
"Name"="ГОСТ Р 34.10-2012"
"Algid"=11849

[OID\1.2.643.7.1.1.1.2!3]
"Name"="ГОСТ Р 34.10-2012"
"Algid"=11837

[OID\1.2.643.7.1.1.2.2!1]
"Name"="ГОСТ Р 34.11-2012 256 bit"
"Algid"=32801

[OID\1.2.643.7.1.1.2.3!1]
"Name"="ГОСТ Р 34.11-2012 512 bit"
"Algid"=32802

[OID\1.2.643.7.1.1.3.2!4]
"Name"="ГОСТ Р 34.11-2012/34.10-2012 256 bit"
"Algid"=32801
"ExtraInfo"=hex:49,2e,00,00,04,00,00,00,50,00,00,00
#"ExtraInfo"=hex:00,00,2e,49,00,00,00,04,00,00,00,50

[OID\1.2.643.7.1.1.3.3!4]
"Name"="ГОСТ Р 34.11-2012/34.10-2012 512 bit"
"Algid"=32802
"ExtraInfo"=hex:3d,2e,00,00,04,00,00,00,51,00,00,00
#"ExtraInfo"=hex:00,00,2e,3d,00,00,00,04,00,00,00,51

[OID\1.2.643.7.1.1.6.1!3]
"Name"="ГОСТ Р 34.10-2012 DH 256 бит"
"Algid"=43590

[OID\1.2.643.7.1.1.6.2!3]
"Name"="ГОСТ Р 34.10-2012 DH 512 бит"
"Algid"=43586

[OID\1.2.643.7.1.2.1.2.1!20]
"Name"="ГОСТ Р 34.10-2012 512 bit, параметры по умолчанию"

[OID\1.2.643.7.1.2.1.2.2!20]
"Name"="ГОСТ Р 34.10-2012 512 bit, параметры ТС26 В"
```

```
[OID\ "2.5.4.3!5"]
"Name"="CN"

[OID\ "2.5.4.7!5"]
"Name"="L"

[OID\ "2.5.4.10!5"]
"Name"="O"

[OID\ "2.5.4.11!5"]
"Name"="OU"

[OID\ "1.2.840.113549.1.9.1!5"]
"Name"="E"
"ExtraInfo"=hex:07,00,00,00
#"ExtraInfo"=hex:00,00,00,07

[OID\ "1.2.840.113549.1.9.1!5!a"]
"Name"="Email"
"ExtraInfo"=hex:07,00,00,00
#"ExtraInfo"=hex:00,00,00,07

[OID\ "2.5.4.6!5"]
"Name"="C"
"ExtraInfo"=hex:04,00,00,00
#"ExtraInfo"=hex:00,00,00,04

[OID\ "2.5.4.8!5"]
"Name"="S"

[OID\ "2.5.4.8!5!a"]
"Name"="ST"

[OID\ "2.5.4.9!5"]
"Name"="STREET"

[OID\ "2.5.4.12!5"]
"Name"="T"

[OID\ "2.5.4.12!5!a"]
"Name"="Title"

[OID\ "2.5.4.42!5"]
"Name"="G"

[OID\ "2.5.4.42!5!a"]
"Name"="GN"

[OID\ "2.5.4.42!5!b"]
"Name"="GivenName"

[OID\ "2.5.4.43!5"]
"Name"="I"

[OID\ "2.5.4.43!5!a"]
"Name"="Initials"

[OID\ "2.5.4.4!5"]
"Name"="SN"

[OID\ "0.9.2342.19200300.100.1.25!5"]
"Name"="DC"
"ExtraInfo"=hex:07,00,00,00
#"ExtraInfo"=hex:00,00,00,07

[OID\ "2.5.4.13!5"]
"Name"="Description"

[OID\ "2.5.4.17!5"]
```

```

"Name"="PostalCode"

[OID\2.5.4.18!5]
"Name"="POBox"

[OID\2.5.4.20!5]
"Name"="Phone"
"ExtraInfo"=hex:04,00,00,00
#"ExtraInfo"=hex:00,00,00,04

[OID\2.5.4.24!5]
"Name"="X21Address"
"ExtraInfo"=hex:03,00,00,00
#"ExtraInfo"=hex:00,00,00,03

[OID\1.3.6.1.5.5.7.3.2!7]
"Name"="Client authentication"

[KeyCarriers\OSCAR]
DLL = "libdrdic.so"

[KeyCarriers\OSCAR\Default]
Name = "\xce\xfl\xea\xe0\xf0"
atr = hex: 00,00,00,00,00,00,00,43,52,59,50,54,4f,50,52
mask = hex: 00,00,00,00,00,00,00,ff,ff,ff,ff,ff,ff,ff,ff
folders = "0B00"

[KeyCarriers\OSCAR2]
DLL = "libdrdic.so"

[KeyCarriers\OSCAR2\CSP]
Name = "\xce\xfl\xea\xe0\xf0 CSP 2.0"
atr = hex: 00,00,00,00,00,00,00,43,50,43,53,50,01,01,02
mask = hex: 00,00,00,00,00,00,00,ff,ff,ff,ff,ff,ff,ff,ff
folders = "0B00"
size_1 = 60
size_2 = 70
size_4 = 60
size_5 = 70
size_6 = 62

[KeyCarriers\OSCAR2\KChannel]
Name = "\xca\xe0\xed\xe0\xeb \xca"
atr = hex: 00,00,00,00,00,00,00,43,50,43,53,50,01,01,01
mask = hex: 00,00,00,00,00,00,00,ff,ff,ff,ff,ff,ff,ff,ff
folders = "0B00"
size_1 = 56
size_2 = 36
size_4 = 56
size_5 = 36
size_6 = 62

[KeyCarriers\TRUST]
DLL = "libdrdic.so"

[KeyCarriers\TRUST\Default]
atr = hex: 3b,9e,00,00,80,31,c0,65,4d,47,00,00,00,72,f7,41,81,07
mask = hex: ff,ff,00,00,ff,ff,ff,ff,ff,ff,30,00,00,ff,ff,ff,ff,ff
folders = "A\\B\\C\\D\\E\\F\\G\\H"

[KeyCarriers\TRUSTS]
DLL = "libdrdic.so"

[KeyCarriers\TRUSTS\Default]
Name = "Magistra SocCard"
atr = hex: 3b,9a,00,00,80,31,c0,61,00,72,f7,41,81,07
mask = hex: ff,ff,00,00,ff,ff,ff,ff,30,ff,ff,ff,ff,ff,ff,ff
folders = "A\\B\\C\\D"

[KeyCarriers\TRUSTD]

```

```
DLL = "libdrdic.so"

[KeyCarriers\TRUSTD\Default]
atr = hex: 3b,98,00,00,80,31,c0,72,f7,41,81,07
mask = hex: ff,ff,00,00,ff,ff,ff,ff,ff,ff,ff,ff
folders = "A\\B\\C\\D\\E\\F\\G\\H"

[policy\OIDs]
"{A4CC781E-04E9-425C-AAFD-1D74DA8DFAF6}" = "libpkiv validator.so OCSPSigni" \
    "ngImpl"
"{AF74EE92-A059-492F-9B4B-EAD239B22A1B}" = "libpkiv validator.so Timestamp" \
    "SigningImpl"
"{B52FF66F-13A5-402C-B958-A3A6B5300FB6}" = "libpkiv validator.so Signature" \
    "Impl"
5 = "libpkiv validator.so BasicConstraintsImpl"
```

ПРИЛОЖЕНИЕ 2.

УТИЛИТА КОМАНДНОЙ СТРОКИ HSMGENARM

Утилита принимает следующие параметры:

HsmGenArm --pwd=<password> --pfx=<filename> [--curve=<oid>]

Допустимые значения параметров приведены в таблице ниже. Порядок параметров в командной строке не важен.

Параметр	Описание	Значение по умолчанию
--pwd=<password>	Пароль к pfx-файлу	—
--pfx=<filename>	Путь к pfx-файлу	—
[--curve=<oid>] (опциональный параметр)	Параметры генерируемого ключа — идентификатор эллиптической кривой Допустимые значения: 1.2.643.7.1.2.1.1.1 1.2.643.7.1.2.1.1.2 1.2.643.7.1.2.1.1.3 1.2.643.7.1.2.1.1.4	1.2.643.7.1.2.1.1.1

Коды ошибок

В таблице ниже перечислены возможные коды ошибок. Детальная информация выводится в текстовом виде в стандартный поток вывода ошибок утилиты.

Код ошибки	Описание
0	Операция выполнена успешно
1	Произошла внутренняя ошибка
2	Недостаточно памяти
3	Ошибка устройства
4	Криптографическая ошибка
5	Командная строка утилиты задана некорректно
6	Ошибка обращения к HSM
7	Ошибка генерации ключа
8	Ошибка формирования транспортного контейнера (pfx)
10	Невозможно создать файл по указанному пути (pfx)

Параметры журналирования

В процессе работы утилиты при создании ключей ведется аудит экспорта ключей. Параметры журналирования указаны в таблице ниже.

Параметр	Значение	Значение по умолчанию
Дата	Дата в формате dd.mm.yyyy	—
Значение ключа проверки ЭП	Байтовая строка	—
Алгоритм ЭП	Алгоритм подписи ГОСТ Р 34.10-2012 с ключом 256 (OID = 1.2.643.7.1.1.1.1)	Алгоритм подписи ГОСТ Р 34.10-2012 с ключом 256
Параметры алгоритма ЭП	Рабочие параметры А алгоритма подписи ГОСТ Р 34.10-2012 с ключом 256 (OID = 1.2.643.7.1.2.1.1.1) Рабочие параметры В алгоритма подписи ГОСТ Р 34.10-2012 с ключом 256 (OID = 1.2.643.7.1.2.1.1.2) Рабочие параметры С алгоритма подписи ГОСТ Р 34.10-2012 с ключом 256 (OID = 1.2.643.7.1.2.1.1.3) Рабочие параметры D алгоритма подписи ГОСТ Р 34.10-2012 с ключом 256 (OID = 1.2.643.7.1.2.1.1.4)	Рабочие параметры А алгоритма подписи ГОСТ Р 34.10-2012 с ключом 256
Результат выполнения (код ошибки)	Возможные значения приведены в таблице выше.	—

Требования безопасности при использовании утилиты

При разработке информационных систем (ИС) с использованием функций утилиты HsmGenArm должны выполняться следующие требования:

1. Порядок работы с экспортированным с использованием утилиты HsmGenArm ключом определяется с учетом требований ИС, в которой эксплуатируется СКЗИ, должен быть зафиксирован в документации на эту систему и проверен в рамках работ по оценке влияния (см. п. 10.2 документа «ЖТЯИ.00096-03 95 01. Правила пользования»).

2. Должен быть обеспечен контроль срока действия ключа, экспортированного с использованием утилиты HSMGenArm, с учётом требований, предъявляемых к ИС, в которой эксплуатируется СКЗИ.

3. Для ключа, экспортированного с использованием утилиты HSMGenArm, установленным порядком должен быть выпущен сертификат.

4. В случае переноса экспортированных с использованием утилиты HsmGenArm ключей на отделяемые ключевые носители необходимо обеспечить гарантированное удаление rfx-файла с экспортированными ключам (например, с использованием утилиты wipefile).