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 Комплектация 3 Использование интерфейсных модулей

ЖТЯИ.00096-02 90 02

Листов 64

2020 г.

Содержание

1. АННОТАЦИЯ

Данный документ содержит правила пользования интерфейсных модулей ПАКМ «КриптоПро HSM», их состав и описание ключевой системы.

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 настоящих Правил.

2. ПО «КРИПТОПРО HSM CLIENT»

Взаимодействие любого приложения на рабочих станциях пользователей или серверах с ПАКМ «КриптоПро HSM» осуществляется через посредника – «КриптоПро HSM Client».

«КриптоПро HSM Client» является неотъемлемой частью ПАКМ и представляет собой набор программных модулей, устанавливаемых на рабочих станциях пользователей/серверах.

Данное ПО зависит от используемой платформы, и от назначения целевого компьютера. ПО «КриптоПро HSM Client» предназначено для:

- трансляции вызовов функций интерфейса MS CryptoAPI от приложений к удаленному разделяемому ПАКМ «КриптоПро HSM»;
- обеспечения процедур аутентификации пользователей СКЗИ перед ПАКМ и ПАКМ перед пользователями;
- обеспечения защищенного (шифрованного) канала передачи информации между рабочими станциями/серверами и ПАКМ.

Для взаимодействия специальных серверных приложений на ПЭВМ с ОС семейства Unix/Linux (Головного удостоверяющего центра) с ПАКМ используется канал «К». Для его реализации на сервер необходимо установить соответствующие интерфейсные модули, входящие в состав дистрибутивного диска поставки ПАКМ «КриптоПро HSM».

Для взаимодействия приложений пользователей/серверов приложений на ПЭВМ с ОС семейства Windows или Unix/Linux с ПАКМ используется канал «К2». Для его реализации на сервер необходимо установить ПО «КриптоПро HSM Client», также входящее в состав дистрибутивного диска поставки ПАКМ «КриптоПро HSM».

Порядок установки и настройки данного программного обеспечения описаны в документе «ЖТЯИ.00096-02 94 01. КриптоПро HSM. Руководство пользователя».

Дополнительные настройки, выполняемые администратором сервера с установленной ОС Unix/Linux, описаны в разделе 6 данного документа. Дополнительные настройки, выполняемые администратором сервера с установленной ОС Windows, описаны в разделе 7 данного документа.

3. КАНАЛ «К2»

Взаимодействие ПО «КриптоПро HSM Client» с ПАКМ осуществляется по логическому защищенному каналу «К2».

Канал «К2» обеспечивает двустороннюю идентификацию и аутентификацию пользователя СКЗИ перед ПАКМ и ПАКМ перед пользователем при помощи ключей и сертификатов аутентификации (ключ клиента, ключ сервера).

Канал «К2» 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 ПО «КриптоПро HSM Client» 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» должна использоваться только карточка с ключом и сертификатом ключа доступа, в котором есть расширение «Администратор сервера» (см. п. 4.3.9 документа «ЖТЯИ.00096-02 90 01. КриптоПро HSM. Инструкция по использованию»). 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») (см. ниже в данном документе);
- 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. 6.3) .

Канал «K2» использует порт для входящих соединений – 1501.

Канал «K2s» использует порт 1503.

4. КАНАЛ «К»

Взаимодействие ПО «КриптоПро HSM Client» для Головного удостоверяющего центра с ПАКМ 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.

5. ОПИСАНИЕ РЕАЛИЗАЦИИ «КРИПТОПРО HSM CLIENT»

Клиентская компонента ПАКМ «КриптоПро HSM» — «КриптоПро HSM Client» — представляет собой набор программных, а также аппаратных модулей, устанавливаемых на рабочие станции пользователей или сервера, обеспечивающих поддержку вызовов из приложений криптографических функций по поддерживаемым программным интерфейсам (Crypto API, PKCS#11).

«КриптоПро HSM Client» является ответной частью, устанавливаемой на рабочие станции и сервера, необходимой для трансляции криптографических вызовов к ПАКМ «КриптоПро HSM» по безопасным каналам «К», «К2».

ПАКМ «КриптоПро HSM» предполагает различные варианты комплектации, включающие автономные СКЗИ по различным уровням защиты:

- Комплектация 1 Исполнение 1 ПАКМ «КриптоПро HSM», уровень защиты КВ/КВ2
- Комплектация 1 Исполнение 2 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 1 Исполнение 3 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 1 Исполнение 4 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 1 Исполнение 5 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 2 Исполнение 1 ПАКМ «КриптоПро HSM», уровень защиты КС1
- Комплектация 2 Исполнение 2 ПАКМ «КриптоПро HSM», уровень защиты КС2
- Комплектация 2 Исполнение 3 ПАКМ «КриптоПро HSM», уровень защиты КС3
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 1-Base», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 2-Base», уровень защиты КС2
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 3-Base», уровень защиты КС3
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 1-Lic», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + CSP версия 4.0 Исполнение 2-Lic», уровень защиты КС2
- Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС1 Исполнение 1-Base», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС2 Исполнение 2-Base», уровень защиты КС2
- Комплектация 3 Исполнение «DSS + CSP версия 5.0 КС3 Исполнение 3-Base», уровень защиты КС3

- Комплектация 3 Исполнение «DSS + JCP версия 2.0 Исполнение 2», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + SIM (QES)», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + SIM (M2M)», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + myDSS», уровень защиты КС1
- Комплектация 3 Исполнение «DSS + AirKey Lite», уровень защиты КС1
- Комплектация 3 Исполнение «myDSS SDK», уровень защиты КС1
- Комплектация 3 Исполнение «Сбербанк myDSS SDK», уровень защиты КС1
- Комплектация 3 Исполнение «DSS Client SDK», уровень защиты КС1

Примечание: Комплектации 2 и 3 могут использоваться с любой аппаратной компонентой Комплектации 1.

Компонент «КриптоПро HSM Client» обеспечивает:

- интерфейс к прикладным криптографическим функциям в соответствии со спецификацией Microsoft Cryptographic Service Provider, PKCS#11;
- проверку целостности критичного к безопасному функционированию ПО;
- генерацию случайных чисел в т.ч. и с использованием аппаратного ДСЧ;
- генерацию закрытого ключа/ключа ЭП с использованием исходного материала, предоставленного уполномоченной организацией;
- ввод закрытого ключа/ключа ЭП с отчуждаемых ключевых носителей в т.ч. и на интеллектуальной карте;
- выполнение функций создания и проверки электронной подписи (ЭП) согласно ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), вычисление хэш-функции согласно ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018);
- шифрование и имитозащита согласно ГОСТ 28147-89;
- поддержку алгоритмов RSA в части генерации ключей, формирования и проверки ЭП, шифрования и расшифрования;
- возможность встречной работы с ПАКМ «КриптоПро HSM» и «КриптоПро CSP».

«КриптоПро HSM Client» использует отличные от «КриптоПро HSM» (см.п. п. 3.4 «Сведения об используемых криптопровайдерах» документа «ЖТЯИ.00096-02 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:

- КС1
- КС2
- КС3

Средствами «КриптоПро HSM Client» НЕ ДОПУСКАЕТСЯ защищать информацию, составляющую государственную тайну.

По согласованию с пользователем компонент комплектуется аппаратными сертифицированными средствами защиты от НСД и ФСДЧ (электронный замок «Соболь», «Аккорд» и т.п. в соответствии с комплектацией используемого СКЗИ «КриптоПро CSP»). Исполнение СКЗИ по уровню защиты КС2 и выше ДОЛЖНО включать данные средства.

5.1 РЕАЛИЗУЕМЫЕ АЛГОРИТМЫ

Алгоритм зашифрования/расшифрования данных и вычисления имитовставки реализован в соответствии с ГОСТ 28147-89 «СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ. ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ»;

Алгоритм формирования и проверки ЭП реализован в соответствии с ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018) «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ПРОЦЕССЫ ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ»;

Алгоритм выработки значения хэш-функции реализован в соответствии с ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018) «ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ. КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ. ФУНКЦИЯ ХЭШИРОВАНИЯ».

Ключевая система «КриптоПро HSM Client» обеспечивает возможность парно-выборочной связи абонентов сети с использованием для каждой пары абонентов уникальных ключей, создаваемых на основе принципа открытого распределения ключей.

5.2 АРХИТЕКТУРА ПО И ОБЩИЕ ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ

Основной архитектурной особенностью ПО «КриптоПро HSM Client» является то, что среда функционирования (СФ) не имеет непосредственного доступа к ключевой и криптографически значимой информации. Все операции с закрытыми и сессионными (симметричными) ключами, незавершенными значениями хэш-функций и т. п. осуществляются через дескрипторы соответствующих объектов; дескриптор объекта непосредственно не содержит его адреса. В качестве дополнительной меры защиты реализован **Криптографический сервис** для хранения объектов в отдельном от СФ адресном пространстве (уровни защиты КС2, КС3, КВ/КВ2).

В состав программного обеспечения для всех платформ входят ПО «КриптоПро HSM Client», модуль сетевой аутентификации КриптоПро TLS.

Общая структура «КриптоПро HSM Client» представлена на следующем рисунке:

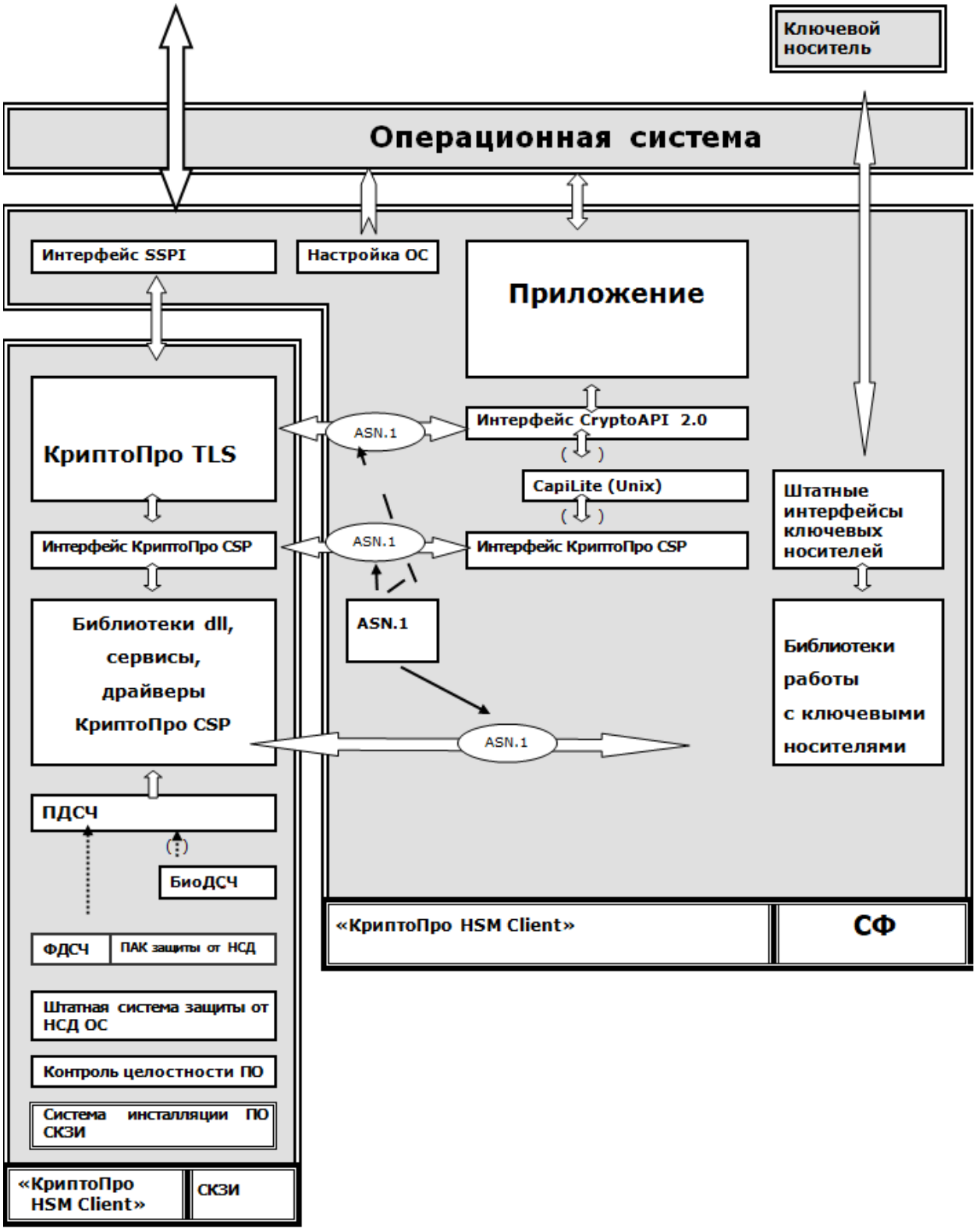


Рисунок 1. Общая структура «КриптоПро HSM Client»

5.3 МОДУЛЬ ПОДДЕРЖКИ СЕТЕВОЙ АУТЕНТИФИКАЦИИ КРИПТОПРО TLS

Модуль поддержки сетевой аутентификации КриптоПро TLS реализован на базе протокола TLS v.1.0 и российских стандартов криптографической защиты информации (алгоритмы шифрования в соответствии с ГОСТ 28147-89, алгоритмы выработки и проверки электронной подписи в соответствии ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), хэширования в соответствии с ГОСТ Р 34.11-2012 (ГОСТ 34.11-2018)). Используется также алгоритм Диффи-Хеллмана открытого распределения ключей на базе ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018).

На ПЭВМ клиента и на сервере устанавливается ПО «КриптоПро HSM Client» с модулем поддержки сетевой аутентификации КриптоПро TLS.

Аутентификация клиент-сервер может быть односторонней и двусторонней.

Односторонняя аутентификация обеспечивает минимально необходимый уровень защиты, и включает в себя:

- обязательную аутентификацию сервера без аутентификации клиентов;
- шифрование трафика между клиентом и сервером.

При работе в данном режиме сервер на этапе "рукопожатия" не запрашивает сертификат клиента и устанавливается "анонимное" защищенное соединение. В этом случае клиент может не иметь закрытого ключа и сертификата, однако при этом он лишается возможности формировать электронную подпись под документами. Режим с односторонней аутентификацией сервера может использоваться для предоставления некоторой группе пользователей конфиденциальной информации на основании парольной защиты, однако пароль в этом случае будет предъявляться пользователем только после установления защищенного TLS-соединения с TLS-сервером, что повышает уровень защиты от несанкционированного доступа по сравнению с передачей пароля по открытым соединениям. При односторонней аутентификации сервер запрашивает сертификат клиента, но его отсутствие не считается ошибкой.

В «КриптоПро HSM Client» используется двусторонняя аутентификация.

Двусторонняя аутентификация включает в себя:

- взаимную аутентификацию клиента и сервера с помощью их сертификатов;
- шифрование трафика между клиентом и сервером;
- формирование и проверку электронной подписи под электронными данными, формируемыми пользователями.

Двусторонний метод аутентификации позволяет обеспечить доступ к «КриптоПро HSM» только зарегистрированным владельцам сертификатов. При этом нужно иметь в

виду, что разграничение доступа к информационным ресурсам сервера, основанное на проверке сертификатов клиентов, гораздо надежнее, чем просто парольная защита.

В данном режиме работы клиенту необходимо сгенерировать закрытый и открытый ключи и получить сертификат открытого ключа в Удостоверяющем центре.

Требования к техническим и программным средствам компьютера, на который устанавливается Web(TLS) сервер, определяются в документации, поставляемой вместе с данным сервером. Дополнительно, на компьютер должен быть установлен «КриптоПро HSM Client», включающий модуль поддержки сетевой аутентификации КриптоПро TLS.

Для возможности установления защищенного соединения между клиентом и сервером необходимо вначале выпустить сертификат открытого ключа, который будет использоваться для серверной аутентификации по протоколу TLS.

Требования к сертификату:

- имя сертификата (Common name) должно совпадать с именем публикуемого TLS-сервера прикладной системы. Например: pif.nikoil.ru (либо IP адрес сервера);
- область использования ключа должна содержать: "Аутентификация Сервера".

Данный сертификат должен быть установлен на сервер в привязке с ключом ЭП (закрытым ключом).

Выпуск и установка сертификата осуществляется через Удостоверяющий центр. Порядок действий определяется в инструкции пользователю.

5.4 КЛЮЧИ И КЛЮЧЕВЫЕ НОСИТЕЛИ

«КриптоПро HSM Client» является системой с открытым распределением ключей. Открытые ключи/ключи проверки ЭП обычно представляются в виде сертификатов открытых ключей/ключей проверки ЭП.

В «КриптоПро HSM Client» ключ ЭП подписи может быть использован только для формирования ЭП. Закрытый ключ шифрования может быть использован как для формирования ключа связи с другим пользователем, так и для создания ЭП.

При работе с СКЗИ каждый пользователь, обладающий правом подписи и/или шифрования, вырабатывает на своем рабочем месте или получает у администратора безопасности (в зависимости от принятой политики безопасности) личные закрытый ключ (ключ ЭП) и открытый ключ (ключ проверки ЭП). На основе каждого открытого ключа (ключа ЭП) третьей стороной (Центром Сертификации) формируется сертификат открытого ключа (ключа ЭП).

Должны быть приняты меры, обеспечивающие сохранение в тайне ключей ЭП и закрытых ключей и соответствующий порядок работы с ключевой документацией и сертификатами ключей проверки ЭП и сертификатами открытых ключей.

При формировании закрытый ключ шифрования и ключ ЭП «КриптоПро HSM Client» записываются на ключевой носитель (ключевой контейнер).

Ключевой контейнер может содержать:

- только ключ подписи (ключ ЭП);
- только ключ шифрования;
- ключ ЭП и ключ шифрования одновременно.

Единственный ключ ключевого контейнера либо ключ подписи в дальнейшем называется главным ключом, а ключ шифрования, в случае хранения в контейнере двух ключей, — вторичным ключом.

Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т. п.

Каждый ключевой контейнер (независимо от типа носителя), является самодостаточным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми (и соответствующими им открытыми) ключами.

Ключевой контейнер содержит следующую информацию: главный ключ, маски главного ключа, контрольную информацию главного ключа, вторичный ключ (опциональный), резервную копию ключевого контейнера.

Каждый закрытый ключ и ключ ЭП хранится в формате, дополнительно содержащем все константы, необходимые для формирования и экспорта открытого ключа.

Структура ключевого контейнера обеспечивает чтение ключей и соответствующих масок отдельными операциями в раздельные области памяти, для чего он разбит на шесть зон (реализация зон зависит от типа ключевого носителя).

Ключевой контейнер содержит также дополнительную информацию, необходимую для обеспечения восстановления контейнера, при возникновении различных программно-аппаратных сбоев (дополнительная информация включается в тех случаях, когда размер ключевого контейнера не ограничен размерами памяти физического носителя).

Формирование ключей пользователя производится с использованием функции **CPGenKey** и спецификацией типа формируемого ключа: AT_KEYEXCHANGE или AT_SIGNATURE.

Формирование ключей возможно если:

- контекст криптопровайдера «КриптоПро HSM Client» открыт функцией **CPAcquireContext** с флагом CRYPT_NEWKEYSET и несуществующим именем ключевого контейнера, специфицированным параметром **pszContainer**;
- Контекст криптопровайдера «КриптоПро HSM Client» открыт функцией **CPAcquireContext** с указанием ранее созданного ключевого контейнера, специфицированного параметром **pszContainer**.

Примечания.

1. Ключи ЭП и закрытые ключи шифрования формируются с использованием программного и физического ДСЧ входящего в комплект СЗИ от НСД/АПМДЗ и с применением доверенной случайной информации, поставляемой уполномоченной организацией.

2. При использовании считывателей смарт-карт или устройств чтения таблеток Touch-Memory DALLAS необходимо проверить настройки COM, USB портов ПЭВМ в BIOS и ОС. При отключенных портах (disabled) работа со считывателями будет невозможна.

3. Перед использованием процессорные карты должны быть "выпущены" с использованием транспортного пин-кода и ПО выпуска карт (поставляются дистрибутором карт).

Формирование закрытых ключей для уровня защиты КВ может производиться на следующие отчуждаемые ключевые носители:

- USB-флеш-накопитель;
- российские интеллектуальные карты (Оскар, Магистра на базе микроконтроллера ST23L80A) с использованием считывателей смарт-карт, поддерживающий протокол PC/SC (GemPC TWIN USB);
- USB token.

Примечание. Перечень ключевых носителей может расширяться.

Личные ключевые носители пользователей рекомендуется хранить в сейфе. Пользователь несет персональную ответственность за хранение личных ключевых носителей.

При централизованном хранении ключевых носителей администратор безопасности организации несет персональную ответственность за хранение личных ключевых носителей пользователей. Личные ключевые носители администратора безопасности должны храниться в его личном сейфе.

Ключи на ключевых носителях (включая Touch Memory и смарт-карты), срок действия которых истек, уничтожаются путем переформатирования ключевых носителей средствами ПО СКЗИ, после чего ключевые носители могут использоваться для записи на них новой ключевой информации.

5.4.1 РАЗМЕРЫ КЛЮЧЕЙ

Размеры ключей электронной подписи:

ключ ЭП — 256 бит или 512 бит

ключ проверки ЭП — 512 бит или 1024 бита

Размеры ключей, используемых при шифровании:

закрытый ключ — 256 бит или 512 бит

открытый ключ — 512 бит или 1024 бита

симметричный ключ — 256 бит

5.5 РЕКОМЕНДАЦИИ ПО ВСТРАИВАНИЮ И ИСПОЛЬЗОВАНИЮ

Для обеспечения защиты электронных документов и создания защищенной автоматизированной системы, в первую очередь, используют криптографические методы защиты, которые позволяют обеспечить защиту целостности, авторства и конфиденциальности электронной информации и реализовать их в виде программных или аппаратных средств, встраиваемых в автоматизированную систему.

Использование криптографических средств требует, как правило, применения также организационно-технических мер защиты.

При создании защищенной автоматизированной системы необходимо определить модель угроз и политику ее безопасности. В зависимости от политики безопасности определяется уровень защиты требуемого СКЗИ и необходимый набор криптографических функций и организационно-технических мер, реализуемых в создаваемой системе.

«КриптоПро HSM Client» в первую очередь предназначено для встраивания в прикладное программное обеспечение. Функции данного ПО могут быть использованы:

- через интерфейс библиотеки capilite.dll, являющейся подмножеством интерфейса **CryptoAPI 2.0.** Для этих целей **в комплект поставки включается документ «**ЖТЯИ.00096-02 92 01. КриптоПро HSM. Руководство программиста СКЗИ КриптоПро HSM».
- непосредственным вызовом функций СКЗИ после загрузки модуля с использованием функции **LoadLibrary**. Для этих целей в комплект поставки

включается документ «ЖТЯИ.00096-02 92 01. КриптоПро HSM. Руководство программиста», описывающий состав функций и тестовое ПО.

Примечание. При использовании на «КриптоПро HSM Client» в ОС Unix/Linux для получения бинарных модулей прикладного ПО необходимо установить пакет разработчика для соответствующей платформы lsb-cprocsp-devel-N1.N2.N3-N4.noarch.rpm (для LSB совместимых ОС) (в стандартную поставку не входит).

Ниже приведен основной перечень требований, реализуемых при помощи криптографических методов.

Конфиденциальность информации

При передаче данных в сети обеспечивается использованием функций шифрования.

Для обеспечения НСД к информации при хранении (на дисках, в базе данных) допускается использование шифрования на производном (например, от пароля) ключе.

Идентификация и авторство

При сетевом взаимодействии (установлении сеанса связи) обеспечивается функциями ЭП при использовании их в процессе аутентификации (например, в соответствии с рекомендациями X.509). Одновременно при аутентификации должна использоваться защита от переповторов. Для этих целей может использоваться функция имитозащиты с вычислением имитовставки на сессионном ключе (симметричный ключ шифрования).

При электронном документообороте обеспечивается использованием функций ЭП электронного документа. Дополнительно должна быть предусмотрена защита от навязывания, переповтора электронного документа и целостность справочников ключей проверки ЭП.

Целостность

Обеспечивается использованием функций ЭП электронного документа. При использовании функций шифрования (без использования ЭП) обеспечивается имитозащитой. Для обеспечения целостности хранимых данных может быть использована функция хэширования или имитозащиты, но при этом не обеспечивается авторство информации.

Неотказуемость от передачи электронного документа

Обеспечивается использованием функций ЭП (подпись документа отправителем) и хранением документа с ЭП в течение установленного срока приемной стороной.

Неотказуемость от приема электронного документа

Обеспечивается использованием функций ЭП и квитированием приема документа (подпись квитанции получателем), хранением документа и квитанции с ЭП в течение установленного срока отправляющей стороной.

Защита от переповторов

Обеспечивается использованием криптографических функций ЭП, шифрования или имитозащиты с добавлением уникального идентификатора сетевой сессии (электронного документа) с последующей их проверкой приемной стороной или разработкой специализированного протокола аутентификации (обмена электронными документами).

Защита от навязывания информации

Защита от нарушителя с целью навязывания им приемной стороне собственной информации, переданной якобы от лица санкционированного пользователя (нарушение авторства информации). Обеспечивается использованием функций ЭП с проверкой атрибутов электронного документа и ключа проверки ЭП отправителя. В случае навязывания информации про компрометации ключа обеспечивается организационно-техническими мероприятиями. Например, созданием системы централизованного управления ключевой информацией (оповещением абонентов) или специализированных протоколов электронного документооборота.

Защита от закладок, вирусов, модификации системного и прикладного ПО

Обеспечивается совместным использованием криптографических средств и организационных мероприятий.

При встраивании «КриптоПро HSM Client» в прикладное программное обеспечение или использовании его в составе стандартного прикладного ПО должны выполняться следующие требования:

1. Должны использоваться сертификаты открытых ключей (обмена/подписи).
2. При использовании сертификатов открытых ключей, заверенных подписью доверенной стороны, должна быть обеспечена безопасная доставка и хранение сертификата открытого ключа доверенной стороны, с использованием которого проверяются остальные сертификаты открытых ключей пользователей.
3. При вызове функций «КриптоПро HSM Client» в прикладном программном обеспечении необходимо проверять код завершения функции.

5.6 РЕКОМЕНДАЦИИ ПО УСТАНОВКЕ ПО СКЗИ НА ЭВМ

К эксплуатации программного обеспечения, имеющего в своем составе СКЗИ, допускаются лица, прошедшие соответствующую подготовку и изучившие эксплуатационную документацию на соответствующие программные средства.

При установке программного обеспечения СКЗИ, следует:

1. На технических средствах, оснащенных СКЗИ, использовать только лицензионное программное обеспечение фирм-изготовителей. Установленное программное обеспечение не должно содержать средств разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам.
2. Перед установкой СКЗИ проверить программное обеспечение ЭВМ на отсутствие вирусов и программных закладок. Также рекомендуется исключить из программного обеспечения средства разработки и отладки программ. На ЭВМ должна быть обеспечена антивирусная защита программных компонентов ПАКМ и СФ.
3. При использовании СКЗИ ПЭВМ и устройства ввода/вывода должны быть опечатаны.
4. Предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части рабочей станции с установленным СКЗИ (путем опечатывания системного блока и разъемов ПЭВМ).
5. После завершения процесса установки провести контроль целостности установленного ПО, а также его окружения.

5.7 СОСТАВ КОМПОНЕНТ ПО ПАКМ

В комплект поставки ПАКМ «КриптоПро HSM» входит CDROM «ЖТЯИ.00096-02 99 02. КриптоПро HSM. Интерфейсные модули».

На данном CDROM содержится необходимое ПО для платформ Windows, Alt Linux и других LSB-совместимых 32/64-разрядных ОС семейства Unix/Linux, которое должно быть установлено на ПЭВМ, использующую ПАКМ «КриптоПро HSM».

Структура диска:

```
|
\---Windows
|   |   hsm-win32-eng.msi
|   |   hsm-win32-rus.msi
|   |   hsm-x64-eng.msi
|   |   hsm-x64rus.msi
+---HsmClient
|   +   KC1
```

```
|     +  x32
|     |  …модули…
|     + x86_64
|  +  KC2
|     +  x32
|     |  …модули…
|     + x86_64
|          …модули…
|  +  KC3
|     +  x32
|     |  …модули…
|     + x86_64
|          …модули…
|  +  KB
|     +  x32
|     |  …модули…
|     + x86_64
|          …модули…
|          …модули…
+---HsmClient_A
|  +  KC1
|     +  x32
|     |  …модули…
|     + x86_64
|  +  KC2
|     +  x32
|     |  …модули…
|     + x86_64
|          …модули…
|  +  KC3
|     +  x32
|     |  …модули…
|     + x86_64
|          …модули…
|  +  KB
      +  x32
      |  …модули…
      + x86_64
           …модули…
```

5.8 ОБЩИЕ МЕРЫ ЗАЩИТЫ ОТ НСД ПО С УСТАНОВЛЕННЫМИ СКЗИ

При использовании ПЭВМ для решения задач, связанных с защитой информации, необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы. При этом должна решаться задача не только как обеспечения дополнительной защиты сервера и ОС от НСД, так и обеспечения бесперебойного режима работы и исключения «отказа в обслуживании», вызванного внутренними причинами (например, переполнением файловых систем).

К организационно-техническим мерам относятся:

- обеспечение физической безопасности сервера;
- установка программных обновлений;
- организация процедуры резервного копирования и хранения резервных копий.

Дополнительные настройки ОС касаются следующего:

- ограничение доступа пользователей и настройки пользовательского окружения;
- ограничение сетевых соединений;
- ограничения при монтировании файловых систем;
- ограничения на запуск процессов;
- контроль загрузки ОС и контроль целостности системного и прикладного программного обеспечения должен обеспечиваться при помощи программно-аппаратного комплекса защиты от НСД, что означает:
  - обеспечение контроля доступа при помощи идентификации пользователя с использованием системы Touch Memory;
  - выполнение загрузки с фиксированного носителя после его контроля;
  - обеспечение контроля целостности ОС и прикладного программного обеспечения до загрузки на загрузочном диске и других подключенных дисках.
- дополнительные настройки ядра ОС;
- настройка сетевых сервисов;
- ограничение количества «видимой извне» информации о системе;
- настройка подсистемы протоколирования и аудита.

Должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

1) С целью исключения возможности загрузки ОС, отличной от установленной на HDD/SSD ПЭВМ, ПЭВМ и устройства загрузки должны быть опечатаны. Должен быть обеспечен необходимый контроль целостности печатей.

2) Обеспечение физической безопасности сервера

Следует исключить возможность доступа неавторизованного персонала к консоли, системе питания и дополнительным устройствам, подключенным к

защищаемому серверу путем установки оборудования в специально выделенное и запираемое помещение (аппаратную или серверную комнату).

Доступ персонала в серверную комнату должен быть регламентирован внутренним распорядком эксплуатирующей организации и должностными инструкциями.

Для исключения сбоев компьютера, вызванных отключением электропитания, необходимо обеспечить электропитание сервера от источника бесперебойного питания достаточной мощности. Как минимум, мощности батарей источника бесперебойного питания должно хватать на время, достаточное для корректного автоматического завершения работы сервера.

3) Организация процедуры резервного копирования и хранения резервных копий.

При определении регламента резервного копирования и хранения резервных копий следует обеспечить ответственное хранение резервных копий в запираемых сейфах (шкафах) и определить процедуру выдачи резервных копий ответственному персоналу и уничтожения вышедших из употребления носителей (однократно записываемых дисков и пр.).

Стандартными мерами по организации ответственного хранения носителей являются:

- маркировка носителей;
- составление описи хранимых носителей с указанием серийных (инвентарных) номеров, дат записи носителей, фамилией сотрудника, создавшего копию для каждого шкафа (сейфа);
- периодическая сверка описи и содержимого сейфов (шкафов);
- организация ответственного хранения и выдачи ключей от сейфов (шкафов);
- возможное опечатывание (опломбирование) сейфов (шкафов).

Уничтожение вышедших из употребления носителей должно производиться комиссией с составлением акта об уничтожении.

4) При использовании ПАКМ «КриптоПро HSM» на ПЭВМ, подключенных к общедоступным сетям связи, должны быть предприняты дополнительные меры, исключающие возможность несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционируют СКЗИ, и к компонентам СКЗИ со стороны указанных сетей.

5) Право доступа к рабочим местам с установленным ПО ПАКМ «КриптоПро HSM» предоставляется только лицам, ознакомленным с правилами пользования и изучившим эксплуатационную документацию на программное обеспечение, имеющее в своем составе «КриптоПро HSM».

6) На технических средствах, оснащенных ПАКМ КриптоПро HSM должно использоваться только лицензионное программное обеспечение фирм-производителей.

7) В BIOS определяются установки, исключающие возможность загрузки операционной системы, отличной от установленной на HDD/SSD: отключается возможность загрузки с гибкого диска, привода CD-ROM и прочие нестандартные виды загрузки ОС, включая сетевую загрузку. Не применяются ПЭВМ с BIOS, исключающим возможность отключения сетевой загрузки ОС.

8) До загрузки ОС (для Комплектации 2 Исполнения 2, 3) или до начала работы СКЗИ (для Комплектации 2 Исполнение 1) должен быть реализован контроль целостности файлов, критичных для загрузки ОС, и программы CPVERIFY.

9) При загрузке ОС должен быть реализован контроль целостности программного обеспечения, входящего в состав ПАКМ «КриптоПро HSM», самой ОС и всех исполняемых файлов, функционирующих совместно с СКЗИ с использованием программы CPVERIFY.

10) Средствами BIOS должна быть исключена возможность работы на ЭВМ, если во время его начальной загрузки не проходят встроенные тесты ЭВМ (POST).

11) На ПЭВМ устанавливается только одна ОС. На ПЭВМ не устанавливаются средств разработки и отладки ПО. Если средства отладки приложений нужны для технологических потребностей организации, то их использование должно быть санкционировано администратором безопасности. В любом случае запрещается использовать эти средства для просмотра и редактирования кода и памяти приложений, использующих СКЗИ.

12) Должно быть реализовано физическое затирание содержимого удаляемых файлов с использованием программы Wipefile из состава СКЗИ.

13) Должны быть отключены все неиспользуемые сетевые протоколы.

14) В случае подключения ПЭВМ с установленным СКЗИ к общедоступным сетям передачи данных должно быть отключено использование JavaScript, VBScript, ActiveX и других программных объектов, загружаемых из сети, в прикладных программах.

15) Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения, в которых установлены технические средства ПАКМ «КриптоПро HSM», по роду своей деятельности не являющихся персоналом, допущенным к работе в указанных помещениях.

16) Должно быть запрещено оставлять без контроля вычислительные средства, на которых эксплуатируется ПАКМ «КриптоПро HSM» после ввода ключевой информации. При уходе пользователя с рабочего места должно использоваться автоматическое включение парольной заставки.

17) Из состава системы должно быть исключено оборудование, которое может создавать угрозу безопасности ОС. Также необходимо избегать использования нестандартных аппаратных средств, имеющих возможность влиять на функционирование ПЭВМ или ОС.

18) ПЭВМ, на которые устанавливается ПО СКЗИ, должны быть допущены установленным порядком для обработки информации ограниченного доступа и иметь соответствующие Предписания на эксплуатацию.

19) На все директории, содержащие системные файлы ОС и каталоги СКЗИ, необходимо установить права доступа, запрещающие всем пользователям, кроме Владельца (Owner), запись.

20) Для ограничения возможности влияния аппаратных компонентов СВТ на функционирование СКЗИ необходимо проведение исследований ПО BIOS СВТ, на которых установлено СКЗИ, на соответствие действующим требованиям ФСБ России по исследованию ПО BIOS СВТ.

6. ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСНЫХ МОДУЛЕЙ НА СЕРВЕРАХ С ОС UNIX/LINUX

6.1 УСТАНОВКА ДИСТРИБУТИВА ПО

ПО «КриптоПро HSM Client» поставляется на CD-ROM совместно с ПАКМ «КриптоПро HSM». Предусмотрена поставка этих компонент отдельно от ПАКМ «КриптоПро HSM» в соответствующей комплектации согласно Формуляру ЖТЯИ.00096-02 30 01.

В ОС семейства Unix/Linux для установки, удаления и обновления ПО применяются *пакеты* (packages). Пакет – архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды. Пакеты, представленные в виде файла с расширением .rpm, содержат в себе непосредственно файлы ПО и информацию для конфигурирования среды. Инсталляция дистрибутива выполняется путем запуска утилиты rpm. Для установки/обновления/удаления приложений с помощью RPM необходимо обладать привилегиями root.

Для идентификации дистрибутива как пакета в нём содержится 4 файла, описывающие архив (contents, comment, desc и mtree_dirs). Инсталляция дистрибутива выполняется путём запуска утилиты rpm, обращающейся к дистрибутивному архиву для его распаковки и осуществляющей все необходимые настройки в системе.

6.2 УСТАНОВКА ИНТЕРФЕЙСНЫХ МОДУЛЕЙ ПО ПАКМ «КРИПТОПРО HSM»

Перед установкой модулей с дистрибутивного диска «ЖТЯИ.00096-02 99 02. КриптоПро HSM. Интерфейсные модули» на ПЭВМ с установленной ОС семейства Linux необходимо смонтировать диск командой

mount /media/cdrom

войти в каталог, соответствующий устанавливаемому ПО, классу защиты устанавливаемого ПО и используемой разрядности (32 или 64 бита)

cd /media/cdrom/<Client name>/<security level>/<x32|x86_64>

установить модули:

rpm –ivh *.rpm

завершить установку:

cd /

umount /media/cdrom

6.3 СОСТАВ И НАЗНАЧЕНИЕ КОМПОНЕНТ ПО

В состав модулей «КриптоПро HSM Client» входят:

- cprocsp-compat-altlinux-1.0.0-1.noarch.rpm
- cprocsp-curl-[64-]4.0.0-4.{i486|x86_64}.rpm
- cprocsp-rdr-gui-[64-]4.0.0-4.{i486|x86_64}.rpm
- cprocsp-rdr-pcsc-[64-]4.0.0-4.{i486|x86_64}.rpm
- cprocsp-XXX-[64-]4.0.0-4.{i486|x86_64}.rpm
- cprocsp-fenixm-client-[64-]4.0.0-4.{i486|x86_64}.rpm
- cprocsp-stunnel-[64-]4.0.0-4.{i486|x86_64}.rpm
- lsb-cprocsp-base-4.0.0-4.noarch.rpm
- lsb-cprocsp-capilite-[64-]4.0.0-4.{ i486|x86_64}.rpm
- lsb-cprocsp-rdr-[64-]4.0.0-4.{ i486|x86_64}.rpm
- lsb-cprocsp-rdr-sobol-[64-]4.0.0-4.{ i486|x86_64}.rpm
- lsb-cprocsp-pkcs11-[64-]4.0.0-4.{i486|x86_64}.rpm

Пакет **cprocsp-fenixm-client** содержит модули:

- **libcspr** – библиотека интерфейса Crypto-Pro CSP (Microsoft CSP), переадресующая вызовы к сервису взаимодействия с ПАКМ (kchansrv);
- **kchansrv** – сервис (демон), реализующий канал «К», транслирующий вызовы CSP интерфейса к ПАКМ;
- **libcspsrv** – библиотека, обеспечивающая транспорт вызовов между приложениями и сервисом канала «К» (kchansrv).

Пакет **lsb-cprocsp-capilite** содержит модули:

- **cryptcp, csptestf, inittst** - приложения командной строки для работы с сертификатами, шифрования и расшифрования данных, создания и проверки электронной подписи (ЭП), хеширования данных с использованием сертификатов открытых ключей;
- **der2xer** – приложение командной строки конвертации ASN1 структур PKI в XER формат (XML) и обратно;
- **certmgr** - приложение командной строки для работы с хранилищами сертификатов;

- **sv** - приложение командной строки для формирования и проверки электронной подписи файла;
- **libasn1data** – библиотека поддержки ASN1 структур PKI, содержит функции преобразования структур данных в машинно-независимое представление;
- **libcapilite, libcapi20** – библиотеки интерфейса CryptoAPI. Интерфейс модуля capilite является подмножеством интерфейса CryptoAPI v. 2.0;
- **libcpext** – библиотека вспомогательных функций для работы с ключами;
- **libpkixcmp** – библиотека функций высокого уровня для работы с CMP (Certificate Message Protocol) сообщениями, реализации компонент удостоверяющих центров;
- **libssp** – библиотека поддержки Security Support Provider Interface (SSPI);
- **libpkivalidator** – библиотека функций дополнительной проверки цепочки сертификатов, основанной на политиках использования сертификатов;
- **libenroll** – библиотека поддержки генерации запросов на сертификаты открытых ключей;
- **libtsp, libocsp,libtspcli** – библиотеки поддержки форматов запросов к сервисам штампов времени и онлайн проверки статусов сертификатов;
- **Liburlretrieve** – библиотека поддержки доступа к ресурсам по URL адресам.

Пакет **lsb-cprocsp-rdr** содержит модули:

- **cpverify** – утилита командной строки для проверки целостности модулей СКЗИ;
- **cpconfig** – утилита командной строки для конфигурирования СКЗИ (работа с конфигурационным файлом);
- **csptest** – утилита командной строки для проверки работоспособности /тестирования СКЗИ;
- **wipefile** – утилита командной строки для удаления файлов вместе с содержимым при штатных и нештатных (свопирование) ситуациях;
- **libcapi10** – библиотека, реализующая основные функции интерфейса CryptoAPI;
- **librdrdsrf** - библиотека поддержки ДСЧ ДСДР;
- **librdrfat12** – библиотека поддержки считывателей ключевой информации, обеспечивает поддержку доступа к флоппи дисководу, дискете 3,5” и разделу жесткого диска;

- **librdrrdr** – библиотека поддержки считывателей ключевой информации, обеспечивающая унифицированный интерфейс доступа к ключевым носителям вне зависимости от их типа;
- **librdrrndm** – библиотека поддержки ДСЧ;
- **librdrsup** – библиотека дополнительных функций поддержки работы с оборудованием, обеспечивает реализацию общих функций доступа к различным устройствам хранения ключевых носителей.

Пакет **lsb-cprocsp-rdr-sobol** содержит модули:

- **librdrsbl** – библиотека поддержки ДСЧ «Соболь-2».

Пакет **cprocsp-rdr-pcsc** содержит модули:

- **librdrpcsc** – библиотека поддержки считывателей ключевой информации – устройств чтения смарт-карт и eToken, поддерживающих интерфейс PC/SC;
- **librdrric** – библиотека поддержки носителей ключевой информации – смарт карт ОСКАР.

Пакет **lsb-cprocsp-base** содержит модули:

- **cprocsp** – модуль старта/останова сервисов (демонов) обработки криптографических вызовов;
- локализированные версии мануала (man);
- сценарий создания всех каталогов, необходимых для установки и функционирования СКЗИ.

Пакет **cprocsp-compat-altlinux** содержит модули:

- **ld-lsb** – модуль поддержки совместимости ОС ALT Linux с LCB

Пакет **cprocsp-compat-altlinux** содержит модули:

- **ld-lsb** – модуль поддержки совместимости ОС ALT Linux с LCB

Пакет **cprocsp-curl** содержит модули:

- **libcpcurl** – модуль доступа к ресурсам по URL

Пакет **cprocsp-rdr-gui** содержит модули:

- **librdrrndmbio_gui** – модуль поддержки БИО ДСЧ (окно)

- **libxcpui** – модуль поддержки окон ввода pin кодов

Пакет **cprocsp-XXX** содержит модули и сервисы, реализующие основные криптографические функции указанного уровня защиты (XXX).

Пакет **lsb-cprocsp-pkcs11** содержит модули поддержки программного криптографического интерфейса PKCS#11.

Пакет **cprocsp-stunnel** содержит модули, обеспечивающие трансляцию криптографических в ПАКМ «КриптоПро HSM» с использованием протокола TLS (поддержка канала «К2»).

6.4 СТРУКТУРА КАТАЛОГОВ КОМПОНЕНТ СКЗИ

В зависимости от операционной системы компоненты СКЗИ (СФ), устанавливаемые на рабочей станции или сервере, могут располагаться в разных местах.

Наименование компонент	**LSB совместимая ОС**
Разделяемые библиотеки	/opt/cprocsp/lib/…/
Исполняемые Модули	/opt/cprocsp/bin/…/
Исполняемые сервисы(демоны)	/opt/cprocsp/sbin/…/
Конфигурация	/etc/opt/cprocsp/
Прочие каталоги для изменяемой информации	/var/opt/cprocsp///

Примечание: … (три точки) означают наименование подкаталога, соответствующего тому или иному типу процессора.

6.5 СТРУКТУРА КОНФИГУРАЦИОННОГО ФАЙЛА СКЗИ

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 файла имеет имя config64.ini, для 32-разрядных- config.ini.

В LSB совместимых ОС месторасположение файла следующее:

/etc/opt/cprocsp/

Структура конфигурационного файла приводится в Приложении 1.

6.6 МЕРЫ ЗАЩИТЫ ОТ НСД ПО С УСТАНОВЛЕННЫМИ СКЗИ ДЛЯ ОС UNIX/LINUX

В целом защищенные версии ОС Linux по умолчанию обеспечивают достаточный уровень безопасности для выполнения общих задач сервера. При использовании ПЭВМ под управлением ОС Unix/Linux для решения задач, связанных с защитой информации, необходимо предпринять дополнительные меры организационного и технического характера и выполнить дополнительные настройки операционной системы.

Для ОС Linux дополнительно должен быть реализован следующий комплекс организационно-технических мер защиты от НСД:

1) В системе регистрируется один пользователь, обладающий правами администратора, носящий имя root, на которого возлагается обязанность конфигурировать ОС, настраивать безопасность ОС, а также конфигурировать ПЭВМ, на которую установлена ОС.

2) Для пользователя root выбирается надежный пароль входа в систему, удовлетворяющий следующим требованиям: длина пароля не менее 6 символов, среди символов пароля должны встречаться заглавные символы, прописные символы, цифры и специальные символы, срок смены пароля не реже одного раза в месяц, доступ к паролю должен быть обеспечен только администратору.

3) Пользователю root доступны настройки всех пользователей ОС, которые он может просматривать, редактировать, удалять, создавать. Всем пользователям, зарегистрированным в ОС, пользователь root в соответствии с политикой безопасности, принятой в организации, дает минимально возможные для нормальной работы права. Каждый пользователь ОС, не являющийся пользователем root, может просматривать и редактировать только свои установки в рамках прав доступа, назначенных ему пользователем root.

4) Всех пользователей ПЭВМ, которые не пользуются данной системой, и всех стандартных пользователей, которые создаются в ОС во время установки (таких, как «sys», «uucp», «nuucp», и «listen»), кроме пользователя root, следует удалить.

5) В ОС существуют исполняемые файлы, которые запускаются с правами пользователя root. Эти файлы имеют установленный флаг SUID. Пользователь root

должен определить, каким из этих файлов в рамках определенной в организации политики безопасности не требуется запуск с административными полномочиями, и с помощью сброса флага SUID должен свести количество таких файлов к минимуму. Запуск оставшихся файлов с установленным флагом SUID должен контролироваться пользователем root.

6) Следует избегать попадания в систему программ, позволяющих, пользуясь ошибками ОС, получать привилегии root.

7) Должно быть ограничено (с учетом выбранной в организации политики безопасности) использование пользователями команд cron и at – запуска команд в указанное время.

8) Средствами BIOS должна быть исключена возможность отключения пользователями ISA-устройств и PCI-устройств. Для исключения этой возможности вход в BIOS ЭВМ должен быть защищен паролем, к которому предъявляются те же требования, что и к паролю пользователя root. Пароль для входа в BIOS должен быть известен только пользователю root и быть отличным от пароля пользователя root для входа в ОС.

9) В связи с тем, что аварийный дамп оперативной памяти может содержать криптографически опасную информацию, в прикладных программах, использующих СКЗИ, следует отключить возможность его создания с помощью функции setrlimit с параметром RLIMIT_CORE=0.

10) В ОС используется виртуальная память. Область виртуальной памяти должна быть организована на отдельном HDD. По окончании работы СКЗИ содержимое виртуальной памяти должно затираться с использованием средств ОС. В случае аварийного останова ПЭВМ, при следующей загрузке необходимо в режиме «single user» очистить область виртуальной памяти программой wipefile, входящей в состав ПО СКЗИ. В случае выхода из строя HDD, на котором находится область виртуальной памяти, криптографические ключи подлежат выводу из действия, а HDD - не подлежащим ремонту. Этот HDD уничтожается по правилам уничтожения ключевых носителей.

6.6.1 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ОС LINUX

Настройки ОС выполняются путем редактирования (удаления, добавления) различных конфигурационных и командных файлов.

Для сохранения возможности «откатить» внесенные изменения следует сохранять модифицируемые файлы в «безопасном» месте (на внешнем носителе или на не монтируемой автоматически файловой системе).

1) Ограничение доступа пользователей и настройки пользовательского окружения

Настройка пользовательского окружения заключается в следующих действиях:

a) В файле /etc/login.defs следует установить следующие директивы:

PASS_MAX_DAYS=30 (параметр задаёт максимальное время использования пароля)

PASS_MIN_DAYS=30 (параметр задаёт минимальное количество дней между сменами пароля)

PASS_MIN_LEN=6 (устанавливает минимальную длину пароля)

b) В файле /etc/profile установить значения umask=022 (параметр задает маску создания файла по умолчанию)

c) Для пользователя root установить маску режима создания файлов 077 или 027:

umask 077 (umask 027);

d) Отредактировать файл /etc/shells и поместить в него имена только для тех исполняемых файлов оболочек, которые установлены в системе. По умолчанию, содержимое файла /etc/shells может быть таким:

/bin/csh

/bin/tcsh

/bin/sh

/bin/bash

e) Удалить файл (если он существует) /.rhosts.

f) Удалить содержимое файла /etc/host.equiv.

g) Отредактировать файл /etc/pam.conf с целью запрета rhosts-аутентификации. Выполняется комментированием всех строк, содержащих подстроку "pam_rhosts_auth.so".

h) Проверить идентификаторы пользователя и группы для всех пользователей, перечисленных в файле /etc/passwd. Следует убедиться, что не существует пользователей, имеющих идентификатор пользователя 0 и идентификатор группы 0 кроме, возможно, пользователя root.

i) Создать перечень программ, которые запускаются с правами администратора, и контролировать его неизменность.

j) Запретить регистрацию в системе пользователей, имеющих следующие «служебные имена»:

Daemon, bin, sys adm, lp, smtp, uucp, nuucp, listen, nobody, noaccess

Действие выполняется путем указания в файле /etc/passwd строки '/bin/false' в поле shell-программы и указания символа 'x' в поле пароля.

2) Ограничения при монтировании файловых систем

Ограничения при монтировании файловых систем реализуются редактированием файла /etc/fstab:

Установить опцию nosuid при монтировании файловой системы /var.

При инсталляции системы следует выделить для файловых систем /, /usr, /usr/local, /var разные разделы диска для предотвращения переполнения критичных файловых систем (/, /var) за счет, например, пользовательских данных и обеспечения возможности монтирования файловой системы /usr в режиме «только для чтения».

3) Ограничения на запуск процессов

Следует ограничить использование в системе планировщика задач cron и средств пакетной обработки заданий. Для нормального функционирования системы минимально необходимым является разрешение использования планировщика задач cron и средств пакетной обработки заданий только пользователю root. Для этого следует выполнить следующие команды (от имени суперпользователя):

```
echo root > /etc/cron.allow
echo root > /etc/at.allow
```

4) Настройка сетевых сервисов

Настройка сетевых сервисов заключается в следующем:

a) Следует ограничить функциональность демона управления сетевыми соединениями xinetd. Действие заключается в редактировании файла /etc/xinetd.conf и файлов в каталоге /etc/xinetd.d. Как минимум, следует запретить следующие сервисы:

Echo discard daytime chargen finger nfsd systat netstat tftp telnet

Если не планируется использовать настраиваемый компьютер в качестве маршрутизатора, необходимо в стартовые файлы поместить команду /sbin/sysctl –w net.ipv4.ip_forward = 0

Следует запретить прием из внешней сети «широковещательных» (broadcast) пакетов, а также передачу ответов на принятые «широковещательные» пакеты.

b) Запретить суперпользователю доступ по ftp, для этого добавить «root» в файл /etc/ftpusers

c) Запустить процедуру регистрации запуска процессов (accounting) выполнением команды /sbin/accton

d) Если планируется использовать на настраиваемом сервере сервис FTP, то следует создать (отредактировать) файл /etc/ftpusers со списком пользователей, для которых запрещен доступ к серверу по протоколу FTP. Файл имеет текстовый формат и

должен содержать по одному имени пользователя в строке. В списке «запрещенных» пользователей, как минимум, должны быть перечислены следующие имена пользователей:

adm
bin
daemon
listen
lp
nobody
noaccess

Для ограничения доступа к системным файлам для непривилегированных пользователей, из командной строки следует выполнить следующие команды:

```
chown root /etc/mail/aliases
chmod 644 /etc/mail/aliases
chmod 444 /etc/default/login
chmod 750 /etc/security
chmod 000 /usr/bin/at
chmod 500 /usr/bin/rdist
chmod 400 /usr/sbin/snoop
chmod 400 /usr/sbin/sync
chmod 400 /usr/bin/uudecode
chmod 400 /usr/bin/uuencode
```

Также следует обнулить флаг SGID для некоторых исполняемых файлов:

```
chmod g-s /bin/mail
chmod g-s /usr/bin/write
chmod g-s /bin/netstat
chmod g-s /usr/sbin/nfsstat
chmod g-s /usr/bin/ipcs
chmod g-s /sbin/arp
chmod g-s /bin/dmesg
chmod g-s /sbin/swapon
chmod g-s /usr/bin/wall
```

5) Ограничение количества «видимой извне» информации о системе

Обычно, начальную информацию о системе потенциальный нарушитель получает из системных приглашений, выдаваемых сетевыми службами сервера (telnet-сервер, ftp-сервер и пр.).

Поэтому, к мерам по ограничению количества «видимой извне» информации о системе относятся:

- Отказ от стандартного «заголовка», выводимого сервером ftp при ответе пользователю. Достигается указанием в файле /etc/default/ftpd следующих директив:

  BANNER=""

- Редактирование файлов /etc/issue, /etc/ftp-banner и /etc/motd с целью разъяснения пользователям правил и политики доступа к серверу ftp.

6) Настройка подсистемы протоколирования и аудита

Следует удостовериться, что только пользователь root имеет доступ на запись для следующих файлов:

/var/log/authlog
/var/log/syslog
/var/log/messages
/var/log/sulog
/var/log/utmp
/var/log/utmpx

Если на настраиваемом сервере используется web-сервер, то следует убедиться, что только «владелец» процесса httpd имеет доступ на запись к протоколам httpd

Ограничить (с учетом выбранной в организации политики безопасности) использование пользователями команд su и sudo – предоставления пользователю административных полномочий

Следует протоколировать попытки использования программ su и sudo. Для этого, в файл /etc/syslog.conf следует добавить запись:

auth.notice /var/log/authlog

или

auth.notice /var/log/authlog, @loghost

Вторая строка аналогична первой, но указывает, что протокол дополнительно передается на сервер сбора протоколов.

Следует обеспечить протоколирование неуспешных попыток регистрации в системе в локальном протоколе. Для этого, следует выполнить следующие команды:

touch /var/adm/loginlog
chown root /var/adm/loginlog
chgrp root /var/adm/loginlog
chmod 644 /var/adm/loginlog

Для протоколирования сетевых соединений, контролируемых демоном xinetd (включая дату/время соединения, IP-адрес клиента, установившего соединение и имя сервиса, обслуживающего соединение), в файл /etc/syslog.conf следует добавить запись: daemon.notice /var/log/syslog

7. ИСПОЛЬЗОВАНИЕ ИНТЕРФЕЙСНЫХ МОДУЛЕЙ НА СЕРВЕРАХ С ОС СЕМЕЙСТВА WINDOWS

7.1 УСТАНОВКА ДИСТРИБУТИВА ПО

Для взаимодействия приложений пользователей/серверов приложений на ПЭВМ с ОС семейства Windows с ПАКМ используется канал «К2». Для его реализации на сервер необходимо установить ПО «КриптоПро HSM Client», входящее в состав дистрибутивного диска поставки ПАКМ «КриптоПро HSM».

Порядок установки и настройки данного программного обеспечения можно прочитать в документе «ЖТЯИ.00096-02 93 01. КриптоПро HSM. Руководство пользователя».

7.2 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)**

Криптопровайдер **Crypto-Pro GOST R 34.10-2001 HSM CSP** (синоним имени Crypto-Pro HSM CSP) основной криптопровайдер 75-го типа, который должен использоваться внешними приложениями. Он реализует:

- 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 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.

Криптопровайдеры **Crypto-Pro GOST R 34.10-2012 HSM CSP и Crypto-Pro GOST R 34.10-2012 Strong HSM CSP** 80 и 81 типа соответственно 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.

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.

Криптопровайдеры, включающие лексему «Svc» в имени, отличаются от криптопровайдеров без её наличия тем, что 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 используется 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.

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»).

В ПАКМ «КриптоПро HSM» устанавливаются криптопровайдеры **Crypto-Pro HSM RSA CSP** (тип 1) и **Crypto-Pro HSM RSA Svc CSP** (тип 1), которые реализуют алгоритмы электронной подписи RSA:

- генерацию ключевых пар с размером открытого ключа до 16К;
- формирование и проверку ЭП (RSA);

- вычисление Hash функции с использованием алгоритмов SHA1, SHA256, SHA384, MD5;
- генерацию симметричных ключей DES, 3DES, 3DES_112;
- шифрование/расшифрование по указанным алгоритмам.

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

Обычному пользователю не следует использовать криптопровайдеры «"… Svc …"». Система всё равно не позволит ему работать 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 (простым языком – «не залогинился»).

Клиентская часть обычных провайдеров (без лексемы Svc в имени) реализована в виде обычного 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 «КриптоПро HSM Client» нет активной Windows сессии (ни одного «залогиненного» пользователя), то никто не сможет обслужить криптографические запросы, обращенные к обычным криптопровайдерам.

Администраторам серверов, наоборот, рекомендуется установить для провайдеров типов 75, 80, 81 по-умолчанию соответствующие имена сервисных провайдеров (включающие лексему «Svc» в имени), т.к. некоторые вызовы сервисы Windows делают, используя провайдеры «по умолчанию».

Кроме этого, обращения к криптопровайдерам, работающим с ПАКМ через сервис, могут быть сделаны только пользователями с учетными именами SYSTEM (LocalSystem), NetworkService, 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 «КриптоПро HSM Client» не изменяет значение провайдера по умолчанию 1 типа. Обычно, в ОС Windows им является криптопровайдер «Microsoft Strong Cryptographic Provider».

В целях обеспечения возможности создания высокопроизводительных систем повышенной надежности, создания пулов из ПАКМ, горячего резервирования средств СКЗИ в ПАКМ «КриптоПро HSM» зарегистрировано дополнительно по 8 имен криптопровайдеров 1-го и 75-го типа:

Crypto-Pro HSM RSA CSP 01

….

Crypto-Pro HSM RSA CSP 08

и

Crypto-Pro HSM CSP 01

….

Crypto-Pro HSM CSP 08,

которые являются дублерами имен, соответственно Crypto-Pro HSM RSA CSP и Crypto-Pro HSM CSP.

По 4 имени криптопровайдеров для 80,81,16 и 24 типов. 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

Приложения могут использовать эти имена для доступа к различным ПАКМ из пула ПАКМ, размещенных в корпоративной сети.

При необходимости эти криптопровайдеры на устройствах доступа должны быть зарегистрированы вручную.

7.3 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 К2 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 КриптоПро HSM Client (hsmtray, сервисом cpcsphclm).

- «Init_pool_size» — Начальное количество одновременных соединений с HSM, устанавливаемое сразу при запуске сервиса cpcsphclm 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.00096-02 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 «КриптоПро HSM Client» 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 «КриптоПро HSM Client» установит новое соединение, если общее количество не превышает заданного максимального количества (Pool_max_connection). Если же используются все возможные соединения, то ПО «КриптоПро HSM Client» 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.

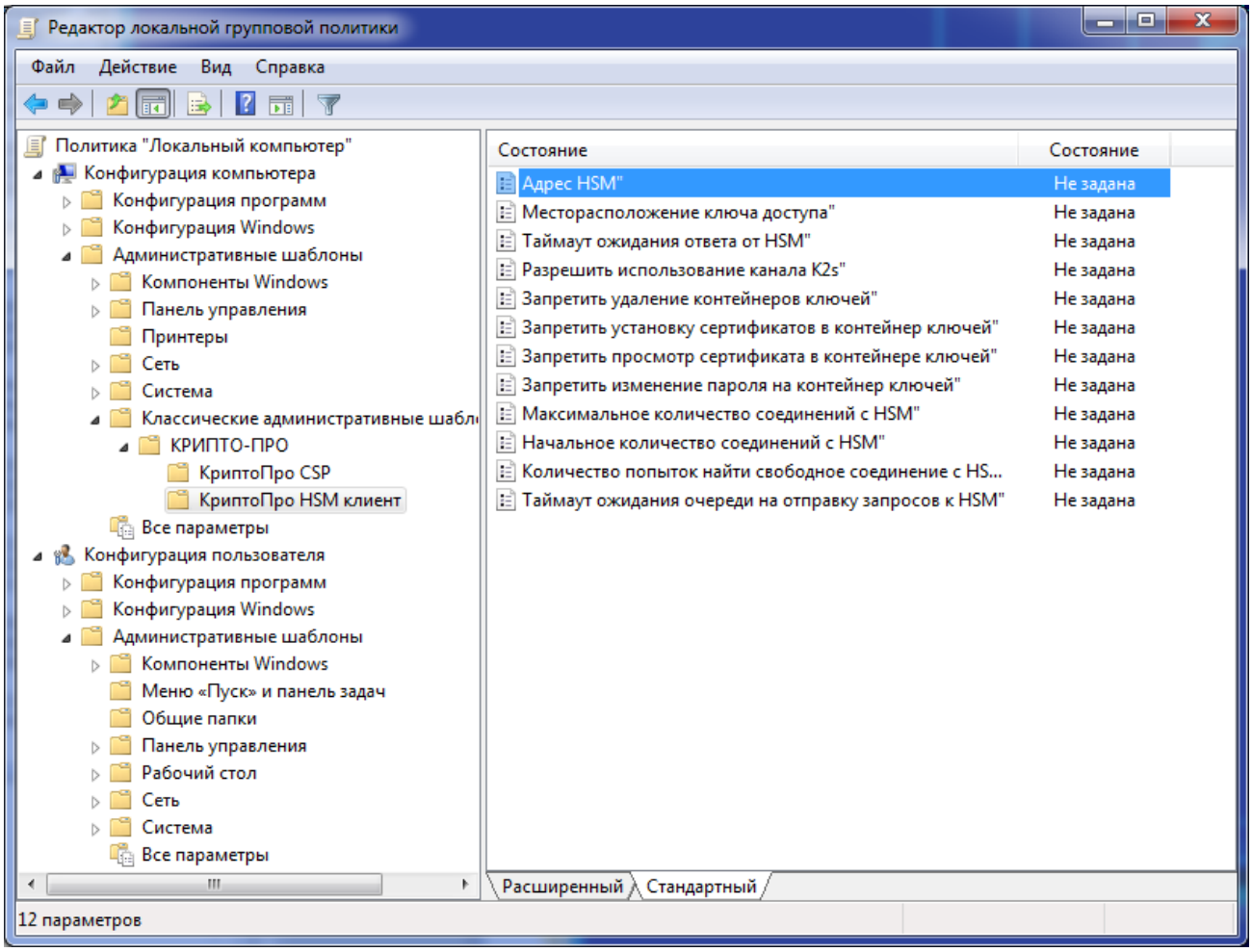
Параметры "DisableDeleteContainer", "DisableInstallCertificate", «DisableViewCertificate», «DisableChangePassword» по умолчанию имеют значения «0» (FALSE), т.е. данные операции разрешены пользователю. Установка их в значение «1» приведет к запрету соответствующей операции.

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.

7.4 КОНФИГУРАЦИЯ С НЕСКОЛЬКИМИ ПАКМ «КРИПТОПРО HSM»

В поставляемой версии ПО «КриптоПро HSM Client» имеется 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

«КриптоПро HSM Client» ничем не отличается от того, что было в предыдущих версиях.

Существующий графический интерфейс пользователя (GUI) по настройке параметров ПО «КриптоПро HSM Client» прописывает значения параметров подключения к ПАКМ в Реестре Windows в ветке:

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

(HKLM\SOFTWARE\Wow6432Node\Crypto Pro\Cryptography\CurrentVersion\HSM – в 64-битных версиях ОС;

HKLM\SOFTWARE\Policy\Crypto Pro\Cryptography\CurrentVersion\HSM – то же, но настраиваемое, как групповая политика;

HKLM\SOFTWARE\Wow6432Node\Policy\Crypto Pro\Cryptography\CurrentVersion\HSM – то же, но настраиваемое, как групповая политика в системах на 64-битной ОС.

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 К2.

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

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 «КриптоПро HSM Client», 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

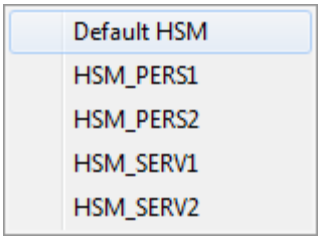
HKLM\SOFTWARE\Crypto Pro\Cryptography\CurrentVersion\HSM\HSMIDs\HSM2

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 «КриптоПро HSM Client», 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 «КриптоПро HSM Client» 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 «-e» 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 «КриптоПро HSM Client» 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 по svchost)

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 уникальное значения опции «-e».

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 трея 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 «КриптоПро HSM Client» 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 «Proxy» 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:

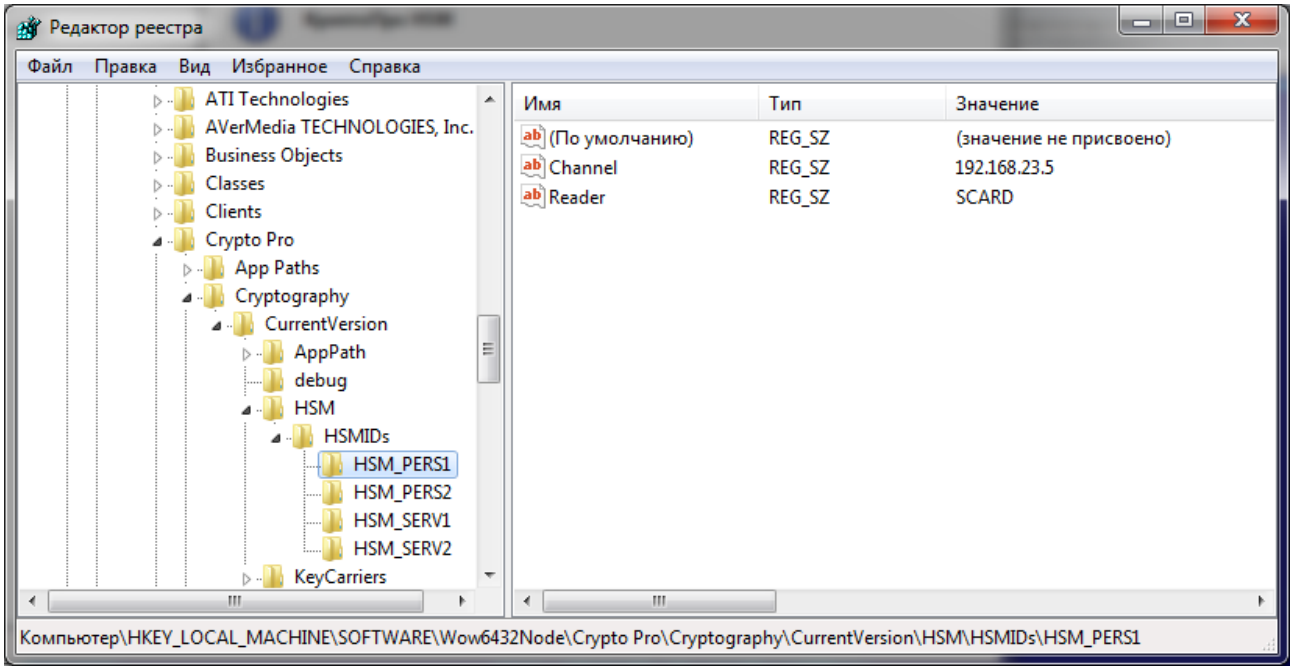
- Crypto-Pro Enhanced RSA and AES HSM CSP 01
- Crypto-Pro Enhanced RSA and AES HSM CSP 02
- Crypto-Pro Enhanced RSA and AES HSM CSP 03
- Crypto-Pro Enhanced RSA and AES HSM CSP 04

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 «Proxy…».

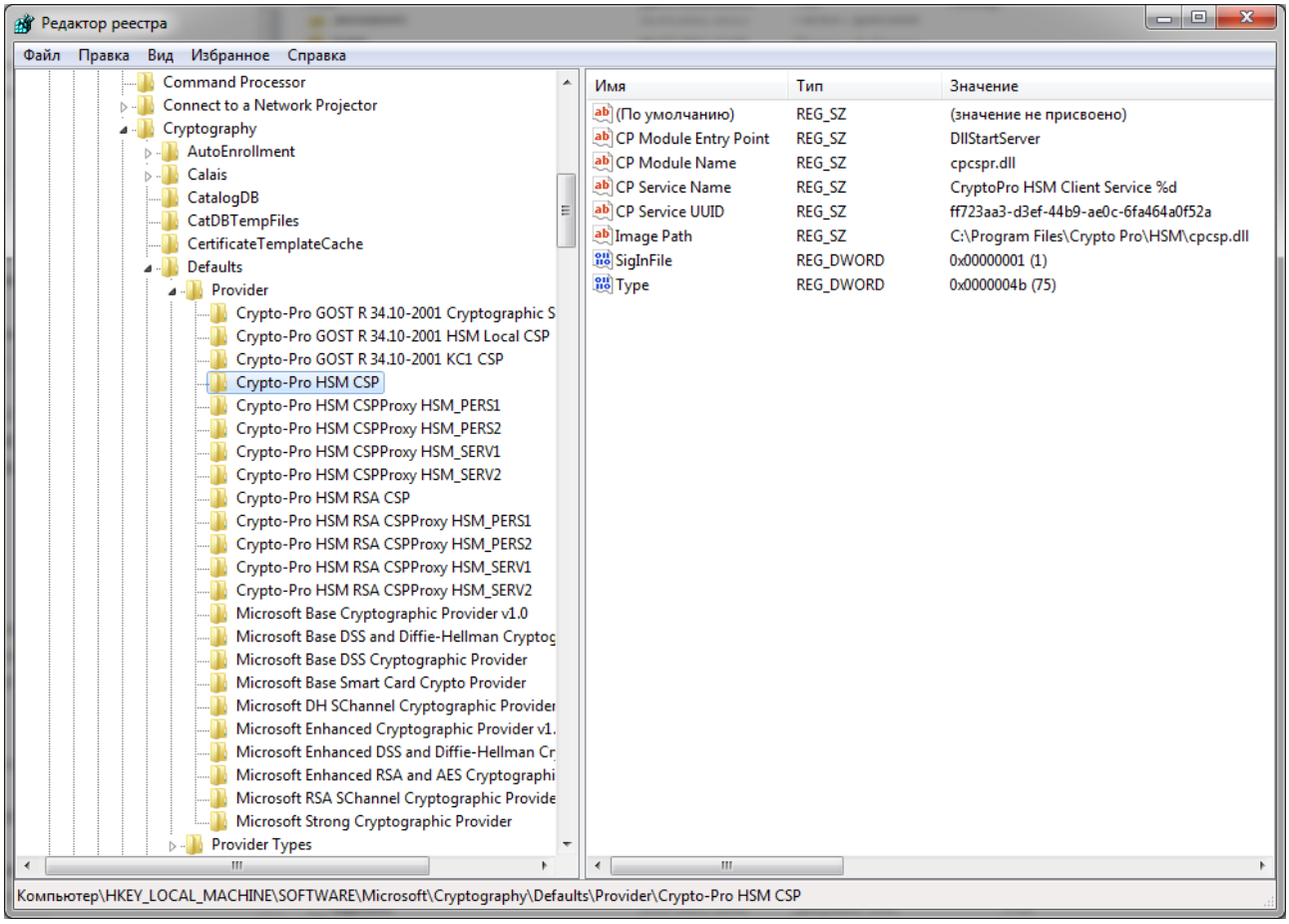
При использовании имен с суффиксом “Proxy …” не рекомендуется использовать в программах вызовы CryptGetProvParam (…, PP_NAME,…), с последующим использованием возвращаемого данным методом имени криптопровайдера в той же программе. Возвращаемое таким образом имя будет отличаться от начального, используемого при открытии контекста, в нем уже будет отсутствовать суффикс «Proxy…». Следующий вызов открытия контекста с новым именем может быть перенаправлен совсем в другой ПАКМ.

Ниже приводится визуальное пояснение всего вышесказанного.

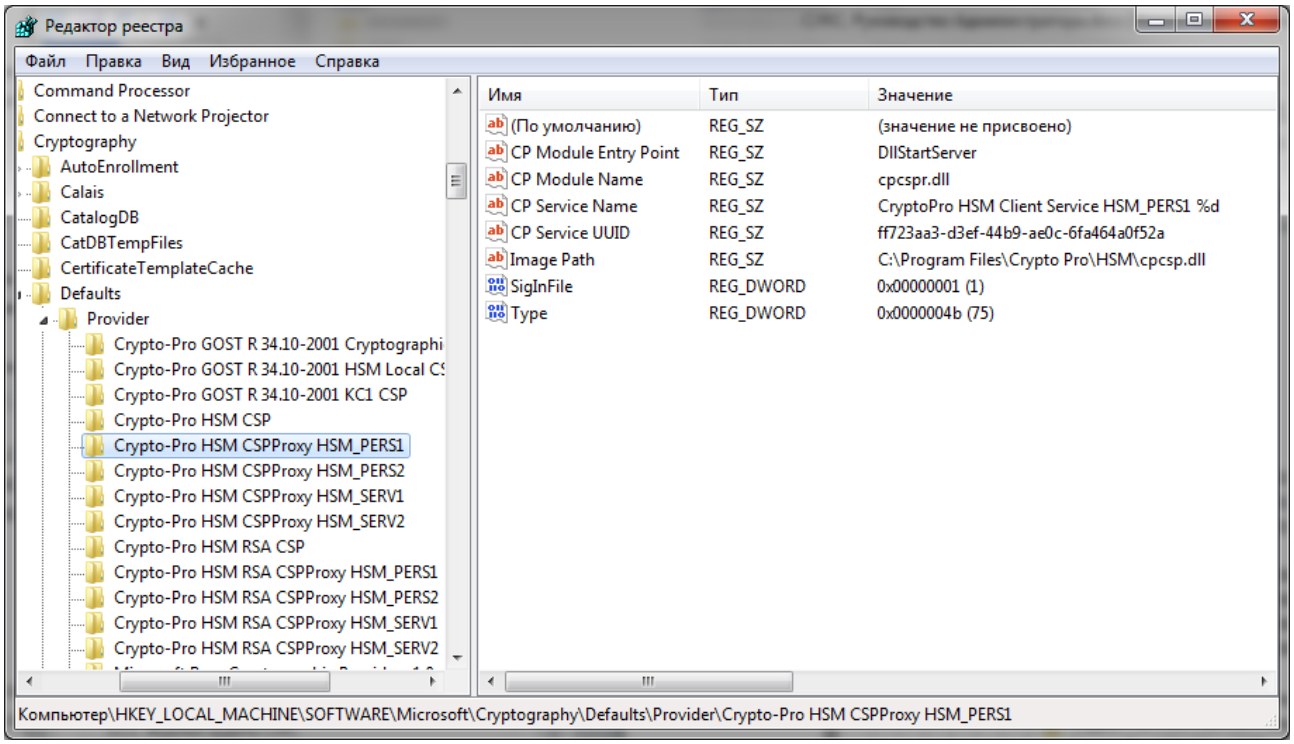
Описание зарегистрированного списка ПАКМ «КриптоПро HSM»:

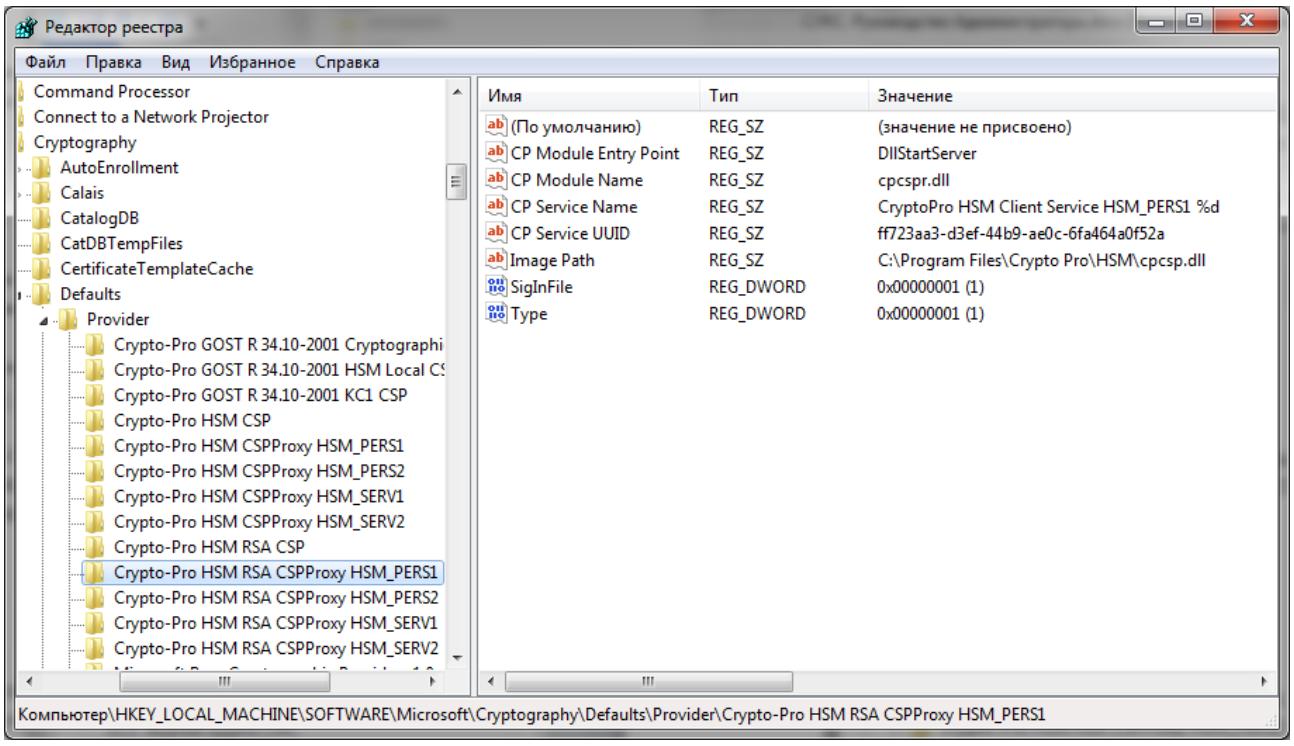


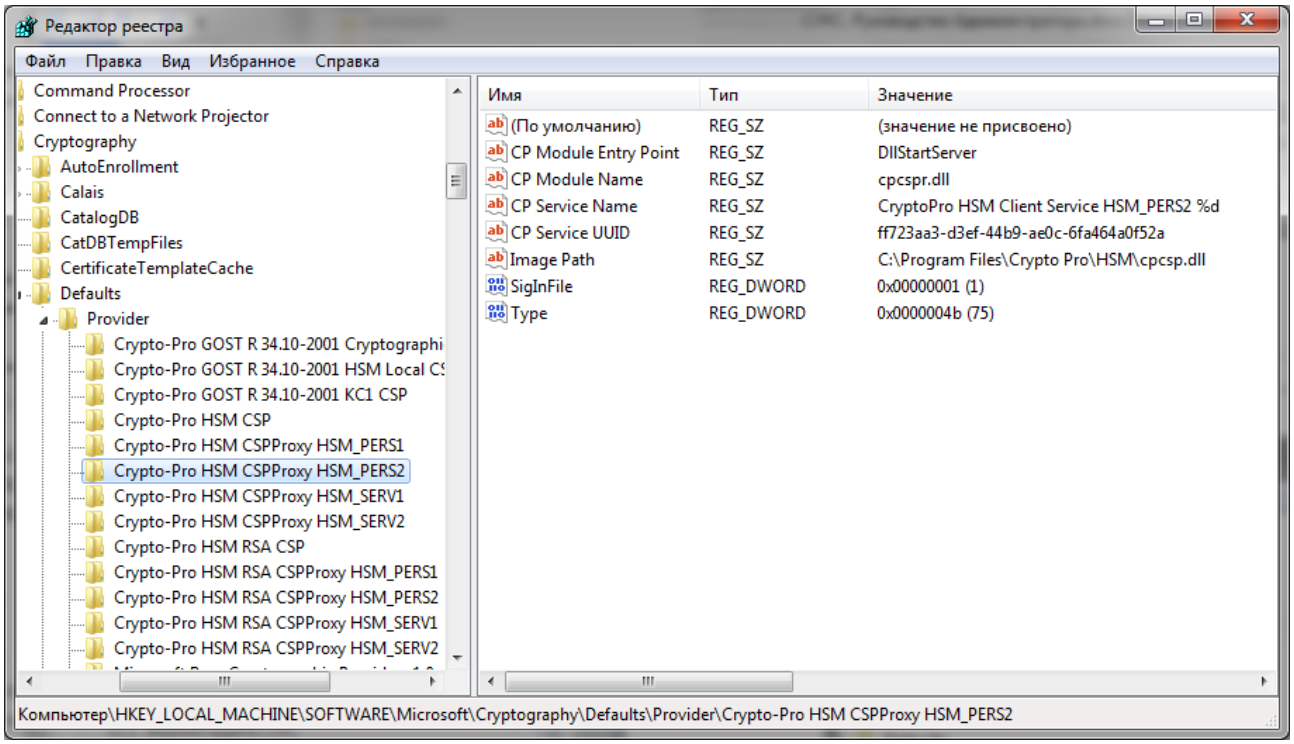
Описание дополнительных имен криптопровайдеров - по одной паре 75-го и 1-го типа для каждого ПАКМ, зарегистрированного в ключе HSMIDs (это удобно делать путем экспорта описаний существующих криптопровайдеров, например, «Crypto-Pro HSM CSP» и «Crypto-Pro HSM RSA CSP» в файлы ".reg", изменением в этих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

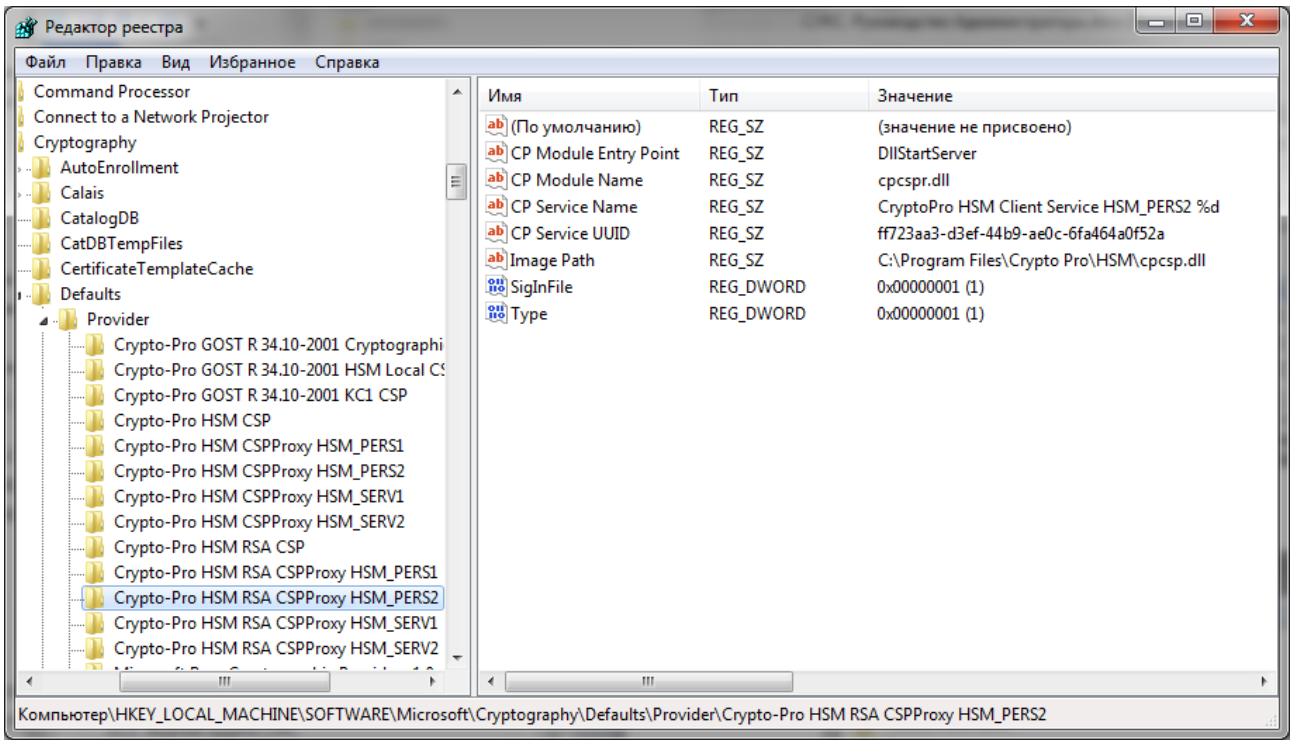


При этом значение параметров «CP Service Name» для каждой пары ГОСТ и RSA криптопровайдеров должны быть одинаковы (т.е. один системный трей будет подключаться к одному ПАКМ, который обрабатывает запросы и для ГОСТ и для RSA криптопровайдера).


Редактор реестра
Файл Правка Вид Избранное Справка
Command Processor
Connect to a Network Projector
Cryptography
AutoEnrollment
Calais
CatalogDB
CatDBTempFiles
CertificateTemplateCache
Defaults
Provider
Crypto-Pro GOST R 34.10-2001 Cryptographi
Crypto-Pro GOST R 34.10-2001 HSM Local C
Crypto-Pro GOST R 34.10-2001 KC1 CSP
Crypto-Pro HSM CSP
Crypto-Pro HSM CSPProxy HSM_PERS1
Crypto-Pro HSM CSPProxy HSM_PERS2
Crypto-Pro HSM CSPProxy HSM_SERV1
Crypto-Pro HSM CSPProxy HSM_SERV2
Crypto-Pro HSM RSA CSP
Crypto-Pro HSM RSA CSPProxy HSM_PERS1
Crypto-Pro HSM RSA CSPProxy HSM_PERS2
Crypto-Pro HSM RSA CSPProxy HSM_SERV1
Crypto-Pro HSM RSA CSPProxy HSM_SERV2
Имя Тип Значение
(По умолчанию) REG_SZ (значение не присвоено)
CP Module Entry Point REG_SZ DllStartServer
CP Module Name REG_SZ cpcspr.dll
CP Service Name REG_SZ CryptoPro HSM Client Service HSM_PERS1 %d
CP Service UUID REG_SZ ff723aa3-d3ef-44b9-ae0c-6fa464a0f52a
Image Path REG_SZ C:\Program Files\Crypto Pro\HSM\cpcsp.dll
SigInFile REG_DWORD 0x00000001 (1)
Type REG_DWORD 0x0000004b (75)
Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Crypto-Pro HSM CSPProxy HSM_PERS1


Редактор реестра
Файл Правка Вид Избранное Справка
Command Processor
Connect to a Network Projector
Cryptography
AutoEnrollment
Calais
CatalogDB
CatDBTempFiles
CertificateTemplateCache
Defaults
Provider
Crypto-Pro GOST R 34.10-2001 Cryptographi
Crypto-Pro GOST R 34.10-2001 HSM Local C
Crypto-Pro GOST R 34.10-2001 KC1 CSP
Crypto-Pro HSM CSP
Crypto-Pro HSM CSPProxy HSM_PERS1
Crypto-Pro HSM CSPProxy HSM_PERS2
Crypto-Pro HSM CSPProxy HSM_SERV1
Crypto-Pro HSM CSPProxy HSM_SERV2
Crypto-Pro HSM RSA CSP
Crypto-Pro HSM RSA CSPProxy HSM_PERS1
Crypto-Pro HSM RSA CSPProxy HSM_PERS2
Crypto-Pro HSM RSA CSPProxy HSM_SERV1
Crypto-Pro HSM RSA CSPProxy HSM_SERV2
Имя Тип Значение
(По умолчанию) REG_SZ (значение не присвоено)
CP Module Entry Point REG_SZ DllStartServer
CP Module Name REG_SZ cpcspr.dll
CP Service Name REG_SZ CryptoPro HSM Client Service HSM_PERS1 %d
CP Service UUID REG_SZ ff723aa3-d3ef-44b9-ae0c-6fa464a0f52a
Image Path REG_SZ C:\Program Files\Crypto Pro\HSM\cpcsp.dll
SigInFile REG_DWORD 0x00000001 (1)
Type REG_DWORD 0x00000001 (1)
Компьютер\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Crypto-Pro HSM RSA CSPProxy HSM_PERS1





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

8. КОНТРОЛЬ ЦЕЛОСТНОСТИ

Установочные модули «КриптоПро HSM Client» и комплект эксплуатационной документации к нему поставляются пользователю Уполномоченной организацией на носителе (CD, DVD - 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 «КриптоПро HSM Client» может быть осуществлена только в случае подтверждения целостности полученных установочных модулей эксплуатационной документации.

	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.

8.1 УТИЛИТА КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ CPVERIFY

Модуль cpverify.exe позволяет осуществлять контроль целостности установленного программного обеспечения. Контроль целостности файлов осуществляется при загрузке файла на исполнение (и периодически во время выполнения) или при ручном запуске программы контроля целостности (см. опцию –rv ниже).

При помощи перечисленных ниже опций модуль cpverify.exe может быть использован для следующих контрольных целей:

1) cpverify -mk filename [-alg algid] [-inverted_halfbytes <inv>] – вычисление значения хэш-функции для файла с именем filename с помощью алгоритма algid. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411). [-inverted_halfbytes <inv>] указывается, если

полубайты в hashvalue перевернуты (по умолчанию для GR3411 inv принимается равным «1», для алгоритмов GR3411_2012_256 и GR3411_2012_512 «0»).

2) cpverify filename [-alg algid] [hashvalue] [-inverted_halfbytes <inv>] – проверка целостности файла с именем filename, используя алгоритм algid и хэш-значение hashvalue. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411). Если hashvalue не указан, то хэш-значение берется из файла filename.hsh. [-inverted_halfbytes <inv>] указывается, если полубайты в hashvalue перевернуты (по умолчанию для GR3411 inv принимается равным «1», для алгоритмов GR3411_2012_256 и GR3411_2012_512 «0»).

3) cpverify -rm [-alg algid] [catname] – вычисление значения хэш-функции для каждого из файлов, содержащихся в каталоге catname в разделе реестра (если catname не указан, то будут пересчитаны все хэш-значения в разделе реестра). Текущее значение хэш-функций при этом заменяется на вновь посчитанное. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411).

4) cpverify –rv [catname] – проверка целостности файлов из каталога catname в разделе реестра (если catname не указан, то будут проверены все файлы в разделе реестра).

5) cpverify -xm in_file out_file [-alg algid] [xmlcatname] – вычисление значения хэш-функции для файлов, перечисленных в xml-файле с именем in_file в каталоге xmlcatname (если xmlcatname не указан, то хэш-значения будут посчитаны для всех фалов, перечисленных в xml-файле с именем in_file), и запись полученных значений в xml-файл с именем out_file. Текущее значение хэш-функций при этом заменяется на вновь посчитанное. Поле algid может принимать значения GR3411, GR3411_2012_256 и GR3411_2012_512 (по умолчанию используется GR3411).

6) cpverify –xv in_file [xmlcatname] – проверка целостности файлов, перечисленных в xml-файле с именем in_file в каталоге xmlcatname (если xmlcatname не указан, то проверка будет выполнена для всех фалов, перечисленных в xml-файле с именем in_file).

7) cpverify –r2x out_file – формирование xml-файла с именем out_file, содержащего список файлов, находящихся в разделе реестра под контролем целостности, и хэш-значения этих файлов.

8) cpverify –x2r in_file – установка под контроль целостности файлов, перечисленных в xml-файле с именем in_file.

Список контролируемых модулей зависит от исполнения и может быть получен при помощи команды cpverify –r2x in_file.

9) cpverify -addreg -file filename – вычисление значения хэш-функции для файла с именем filename и запись полученного значения в реестр.

10) cpverify -delreg -file filename – удаление значения хэш-функции для файла с именем filename из реестра.

11) cpverify -file_sign filename -cont cont_name [-pin password] [-provname имя_провайдера] [-provtype тип_провайдера] – создание подписи файла с именем filename. Параметр cont_name задает имя контейнера ключа, который используется для формирования подписи, password – пароль от контейнера. Параметр тип_провайдера может принимать значения 75, 80, 81 (по умолчанию используется 75).

12) cpverify -file_verify filename [signval] -timestamp date – проверка подписи файла с именем filename. Параметр signval необходимо передавать в виде байтовой строки. Если параметр signval не указан, то значение подписи берется из файла filename.sgn. Параметр date указывает, когда подпись была сформирована, необходимо указывать в формате дд.мм.гггг. Данная команда проверяет подпись с прямой последовательностью полубайт, для проверки подписи с обратной последовательностью байт необходимо использовать команду versign с аналогичным набором параметров. Подпись проверяется на открытом ключе из специального сертификата для подписи кода компании «КРИПТО-ПРО».

Для того, чтобы поставить под контроль целостности установленное программное обеспечение, нужно выполнить следующую последовательность действий:

1. Создать xml-файл, содержащий список устанавливаемых под контроль целостности файлов. Данный xml-файл должен иметь следующую структуру:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<CProIntegrity>
<catalog>
<entry name="calc.exe">
<Path>WINDOWS\system32\calc.exe</Path>
<Algid>00008021</Algid>
</entry>
<entry name="verifier.exe">
<Path>WINDOWS\system32\verifier.exe</Path>
<Algid>00008021</Algid>
</entry>
</catalog>
</CProIntegrity>
```

Значение поля Algid должно равняться 00008021.

2. Запустить модуль cpverify –xm in_file out_file TestControl, указав в качестве параметра in_file имя созданного xml-файла. Результатом работы модуля будет являться xml-файл с именем out_file, содержащий вычисленные значения хэш-функции для перечисленных в in_file файлов и имеющий следующую структуру:

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<CProIntegrity>
<catalog>
<entry name="calc.exe">
<Path>WINDOWS\system32\calc.exe</Path>
<Algid>00008021</Algid>
<Tag>679837307CDC7AA1E4BDBB75194A24D42C782079AF08E2D362D7624A90D6
04C7</Tag>
</entry>
<entry name="verifier.exe">
<Path>WINDOWS\system32\verifier.exe</Path>
<Algid>00008021</Algid>
<Tag>9DF987B89A323BEBC3C29BAC0AED42A4F5BD651892AAE79F1EC1D05288D0
6B9C</Tag>
</entry>
</catalog>
</CProIntegrity>
```

Значение поля Algid должно равняться 00008021.

3. Установить под контроль целостности файлы, для которых было вычислено значение хэш-функции, используя модуль cpverify –x2r in_file TestControl, где параметром in_file является xml-файл, полученный в результате вычисления значения хэш-функции в пункте 2.

ПРИЛОЖЕНИЕ 1. ПРИМЕР КОНФИГУРАЦИОННОГО ФАЙЛА ПАКМ «КРИПТОПРО HSM» НА СЕРВЕРАХ С ОС СЕМЕЙСТВА LINUX

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


[Random\CPSD\Default]
Name = "\xca\xcf\xc8\xcc"
Level = 3
"/db1/kis_1" = "/var/opt/cprocsp/dsrf/db1/kis_1"
"/db2/kis_1" = "/var/opt/cprocsp/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"="librdrfat12.so"
"Group"=1
[KeyDevices\HDimage]
"DLL"="librdrfat12.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"="librdrfat12.so"


[KeyDevices\FLASH]
Dll = "librdrfat12.so"
Script = "mount_flash.sh"

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

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

[KeyDevices\PCSC\"PNP PCSC"\Default]
Name = "All PC/SC readers"
[Capilite\cache_settings]
# Параметры CryptRetriveObjectByURL
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

[Provider]
# Шаблоны провайдеров по типам носителей

# Проверка алгебраических свойств открытого ключа
CheckPublic = true

[apppath]
"librdrfat12.so" = "/opt/cprocsp/lib/amd64/librdrfat12.so"
"librdrrdr.so" = "/opt/cprocsp/lib/amd64/librdrrdr.so"
"librdrrndm.so" = "/opt/cprocsp/lib/amd64/librdrrndm.so"
"librdrdsrf.so" = "/opt/cprocsp/lib/amd64/librdrdsrf.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"
"libpcsclite.so" = "libpcsclite.so.1"
"librdrpcsc.so" = "/opt/cprocsp/lib/amd64/librdrpcsc.so"
"librdrric.so" = "/opt/cprocsp/lib/amd64/librdrric.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 Феникс-М
#   HSMClient - Служба поддержки канала "К" (клиент Феникс-М)
#   CryptSrvKB2 - Служба провайдера КВ
#   CryptSrvKC2 - Служба провайдера КС2


[Services\CryptSrvKC2]
StartService = "cryptsrv"
[Defaults\Provider]
# Провайдеры. Описание провайдера должно содержать поля:
# "Image Path" = путь до разделяемой библиотеки провайдера
# "Type"= тип провайдера (71, 75)

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

```
Channel = ".clientk2"
Media = "HSM"

[Defaults\Provider\"Crypto-Pro GOST R 34.10-2001 KC2 CSP"]
"Image Path" = "/opt/cprocsp/lib/amd64/libcspr.so"
"Function Table Name" = "CPSRV_GetFunctionTable"
Type = 75
Channel = ".cryptsrv"

[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 KC2 CSP"

["dummy section comment for debug"]
# Фильтр отладочных сообщений в формате "Имя модуля"=битовая маска
# Флаги фильтрации (mofname=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
cpext=1
cpext_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
fenixmsrv=1
fenixmsrv_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 B"

[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 = "librdrric.so"


[KeyCarriers\OSCAR\Default]
Name = "\xce\xf1\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 = "librdrric.so"


[KeyCarriers\OSCAR2\CSP]
Name = "\xce\xf1\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 = "librdrric.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 = "librdrric.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
folders = "A\\B\\C\\D"
[KeyCarriers\TRUSTD]
DLL = "librdrric.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}" = "libpkivalidator.so OCSPSigni" \
  "ngImpl"
"{AF74EE92-A059-492F-9B4B-EAD239B22A1B}" = "libpkivalidator.so Timestamp" \
  "SigningImpl"
"{B52FF66F-13A5-402C-B958-A3A6B5300FB6}" = "libpkivalidator.so Signature" \
  "Impl"
4 = "libpkivalidator.so SSLImpl"
```