Конвертация ключевых контейнеров формата «КриптоПро CSP» в формат криптобиблиотеки C-Терра ST - PKCS#15. Версия 4.2

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.
Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Введение

Криптобиблиотека C-Терра ST использует формат ключевого контейнера PKCS#15 в соответствии с рекомендациями ТК26.

В соответствии с Правилами Пользования «C-Терра VPN»:
Сертификаты ключей проверки ЭП и списки аннулированных сертификатов должны быть выпущены в формате, совместимом с сертифицированным УЦ «КриптоПро», и подписаны с использованием сертифицированного СКЗИ.

Продукты C-Терра со встроенной криптобиблиотекой C-Терра ST допускают два подхода к формированию ключевой информации:

1) Ключевая информация и сертификат открытого ключа выпускаются Удостоверяющим Центром (или Центром Сертификации) в формате, совместимом с «КриптоПро CSP» (например, «КриптоПро УЦ» или сервис MS CA с криптопровайдером «КриптоПро CSP»);
2) Ключевая информация в формате PKCS#15 и запрос на сертификат открытого ключа в формате PKCS#10 создаются локально на VPN-устройстве или на АРМ Администратора (с помощью утилит компании C-Терра), подписывает запрос и выпускает сертификат открытого ключа Удостоверяющий Центр (или Центр Сертификации, например, «КриптоПро УЦ» или сервис MS CA с криптопровайдером «КриптоПро CSP»).

Первый подход требует конвертации ключевого контейнера в формат криптобиблиотеки C-Терра ST. Варианты конвертации рассмотрены в данном документе.

Утилиты конвертации контейнеров

Конвертацию ключевых контейнеров из формата «КриптоПро CSP» в формат PKCS#15 реализуют утилиты: cpkey_conv и cpkey_conv_exp.

Утилита cpkey_conv работает с ключевыми контейнерами напрямую, а cpkey_conv_exp использует оснастки «КриптоПро CSP», которые в свою очередь обращаются к ключевым контейнерам. В связи с этим, для корректной работы cpkey_conv_exp требуется установленный криптопровайдер «КриптоПро CSP» (все компоненты). Это и другие отличия указаны в таблице:

Критерий	cpkey_conv	cpkey_conv_exp
Поддержка ГОСТ Р 34.10-2012 (256)	+	+
Поддержка ГОСТ Р 34.10-2012 (512)	-	+
Поддержка конвертации на токенах	-	+
Поддержка конвертации неэкспортируемых ключей	+	-
Наличие в составе С-Терра Шлюз	+	-
Наличие в составе С-Терра Клиент AdminTool	+	+
Необходимость установки криптопровайдера «КриптоПро CSP» (все компоненты)	-	+

Примеры использования утилит

В примерах используются: S-Terra Client AdminTool st версии 4.2.18579, КриптоПро CSP 4.0.9944, токен Рутокен (драйвер версии 4.1.0.0).

1. **Конвертация контейнера, находящегося в файловой системе АРМ Администратора**

   Пусть ключевой контейнер хранится в файловой системе АРМ Администратора. Тогда процесс конвертации состоит из нескольких шагов:

   1.1 Определите имя контейнера

   Определите имя ключевого контейнера в оснастке «КриптоПро CSP», для этого:

   ```
   c:\Program Files (x86)\Crypto Pro\CSP>csptest.exe -keyset -machinekeyset -verifycontext -enum_containers -unique -fqcn
   ```

   Вывод команды будет содержать короткое (дружественное) имя контейнера и полное имя контейнера. Аргумент **–machinekeyset** показывает принадлежность контейнера к «машинным», не пользовательским, например:

   ```
   CSP (Type:80) v4.0.9017 KC1 Release Ver:4.0.9944 OS:Windows CPU:IA32
   FastCode:READY:AVX.
   AcquireContext: OK. HCRYPTPROV: 49491496
   \\.\REGISTRY\LORD                                |\\.\REGISTRY\REGISTRY\\LORD
   ```

   1.2 Варианты конвертации

   1.2.1 Конвертация утилитой cpkey_conv. Рекомендуем указывать полное имя контейнера:

   ```
   C:\Program Files (x86)\S-Terra Client AdminTool st>cpkey_conv -cpCont
   \\.\REGISTRY\REGISTRY\LORD -stCont -key exch-to-sign file_p15://sterraucnt9 -stPIN
   1234 -cpPIN 1234
   ```

Аргумент **–key exch-to-sign** преобразует тип ключа из exchange в sign. Если тип ключа sign, то преобразования не требуется, утилита автоматически опустит аргумент.

Утилита работает с неэкспортируемыми ключевыми контейнерами;
Не поддерживаются ключи 512 бит;
Не требуется «КриптоПро CSP» на АРМ администратора.

1.2.2 Конвертация утилитой cpkey_conv_exp

```
C:\Program Files (x86)\S-Terra Client AdminTool st>cpkey_conv_exp.exe -cpCont
\\.\REGISTRY\LORD -stCont file_p15://sterraucnt9 -stPIN 1234 -cpPIN 1234 -key exch-
to-sign
```

Аргумент **–key exch-to-sign** преобразует тип ключа из exchange в sign. Если тип ключа sign, то преобразования не требуется, утилита автоматически опустит аргумент.

Неэкспортируемые ключевые контейнеры не поддерживаются;
Поддерживаются ключи 512 бит;
Требуется «КриптоПро CSP» на АРМ администратора;
Утилита не входит в состав С-Терра Шлюз.

2. Конвертация контейнера, находящегося на токене Рутокен, на АРМ Администратора

Пусть ключевой контейнер хранится на отчуждаемом ключевом носителе – токене Рутокен. Конвертация выполняется на АРМ Администратора в несколько шагов:

2.1 Определите имя контейнера

Необходимо узнать имя ключевого контейнера в оснастке КриптоПро, для этого:

```
c:\Program Files (x86)\Crypto Pro\CSP>csptest.exe -keyset -machinekeyset -
verifycontext -enum_containers -unique -fqcn
```

Вывод команды будет содержать короткое (дружественное) имя контейнера и полное имя контейнера. Аргумент **–machinekeyset** показывает принадлежность контейнера к «машинным», не пользовательским, например:

```
CSP (Type:80) v4.0.9017 KC1 Release Ver:4.0.9944 OS:Windows CPU:IA32
FastCode:READY:AVX.

AcquireContext: OK. HCRYPTPROV: 49491496

\\.\Activ Co. ruToken 0\LORD |\\.\ Activ Co. ruToken 0\SDCARD\rutoken_2ab\0A00\4012
```

2.2 Варианты конвертации

2.2.1 Конвертация с токена в файловую систему АРМ администратора:

```
C:\Program Files (x86)\S-Terra Client AdminTool st>cpkey_conv_exp.exe -cpCont "\\.\
Activ Co. ruToken 0\SDCARD\rutoken_2ab\0A00\4012" -stCont file_p15://sterraucnt9 -
stPIN 1234 -cpPIN 1234 -key exch-to-sign
```

2.2.2 Конвертация с токена в токен на АРМ администратора:

```
C:\Program Files (x86)\S-Terra Client AdminTool st>cpkey_conv_exp.exe -cpCont "\\.\
Activ Co. ruToken 0\SDCARD\rutoken_2ab\0A00\4012" -stCont etoken_p15://sterraucnt9 -
stPIN 1234 -cpPIN 1234 -key exch-to-sign
```

Конвертация возможна только утилитой cpkey_conv_exp;
Только для экспортируемых контейнеров;
Требуется наличие КриптоПро CSP на АРМ администратора;
Требуется установка драйверов Рутокен (версия 4.1.0.0);
Необходимо изменить файлы skzi.conf.

3. Конвертация контейнера в файловой системе С-Терра Шлюз

Пусть ключевой контейнер container.000 хранится в файловой системе шлюза в директории /home. Конвертация выполняется локально на шлюзе безопасности:

```
/usr/bin/cpkey_conv -cpCont '/home/container.000' -key exch-to-sign
-stCont file_p15://sterraucnt9 -stPIN 1234 -cpPIN 1234
```

Аргумент **–key exch-to-sign** преобразует тип ключа из exchange в sign. Если тип ключа sign, то преобразования не требуется, утилита автоматически опустит аргумент.

После конвертации контейнер в формате PKCS#15 будет расположен в директории /var/s-terra/containers.

Конвертация возможна только утилитой cpkey_conv;
Токены не поддерживаются;
Только для ключей 256 бит;
Шлюз поддерживает работу с ключами 512 бит в своем формате, однако конвертация утилитой cpkey_conv не поддерживается.