Перевод действующего аккредитованного УЦ (использующего ПАК "КриптоПро УЦ" версии 1.5) из режима корневого в режим подчинённого.

Действующий аккредитованный УЦ, использующий ПАК "КриптоПро УЦ" версии 1.5 и работающий в режиме корневого ЦС может быть переведён в режим подчинённого ЦС с сохранением информации из баз данных серверов ЦС, ЦР, т.е. всех пользователей, запросов и выданных ранее сертификатов. При этом остаётся возможность отзыва ранее выданных сертификатов пользователей и публикации списков отозванных сертификатов.

Замечания.

- Сроки действия всех сертификатов, которые будут выдаваться на УЦ после перехода в подчинённый режим, не могут превышать срок действия сертификата подчинённого ЦС, выдаваемого в УЦ Минкомсвязи.
- 2. После перехода УЦ в подчинённый режим для работы с сертификатами, выданными на этом УЦ будет требоваться доступ к актуальным спискам отозванных сертификатов (СОС) вышестоящих УЦ Минкомсвязи - ГУЦ и УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ). Это касается как серверов самого УЦ, так и клиентских компьютеров или серверов, на которых будут использоваться выданные на этом УЦ сертификаты (в том числе для операций проверки подписи электронных документов).

На сервере ЦС служба сертификации может быть переведена из режима корневого ЦС в режим подчинённого ЦС путём изменения параметра реестра САТуре в разделе реестра:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\CertSvc\Configuration\<имя ЦС>

Примечание. Название раздела <имя ЦС> совпадает со значением компонента имени Common Name в сертификате ЦС – в случае использования латинских букв непосредственно, для русских - каждая из них кодируется пятью символами – восклицательный знак и 4 шестнадцатеричные цифры.

Значение параметра САТуре для режима "изолированный корневой ЦС" равно 3.

Значение параметра САТуре для режима "изолированный подчинённый ЦС" равно 4.

Для перевода службы сертификации в подчинённый режим нужно задать значение 4.

Для создания запроса на сертификат подчинённого ЦС в соответствии с требованиями Минкомсвязи нужно добавить настройку для включения в запрос критического расширения "Основные ограничения" с заданием ограничения на длину пути со значением 0.

Это делается путём добавления в файл capolicy.inf в корневом каталоге Windows строк:

[BasicConstraintsExtension] PathLength=0 Critical=True

Если в этом файле есть значение расширения 1.2.643.100.112 — то его нужно убрать (и OID, и его значение), поскольку данное расширение требуется только для неподчинённого режима работы УЦ.

Пример файла capolicy.inf для варианта исполнения 1 КриптоПро УЦ (с КриптоПро CSP 3.6 по классу КС2):

[Version]
Signature="\$Windows NT\$"
[CRLDistributionPoint]
URL=""
[BasicConstraintsExtension]
PathLength=0
Critical=True
[PolicyStatementExtension]
Policies=PolicyKC1,PolicyKC2,PolicyAll
[PolicyKC1]
OID=1.2.643.100.113.1
[PolicyKC2]
OID=1.2.643.100.113.2
[PolicyAll]
OID=2.5.29.32.0
[Extensions]
1.2.643.100.111 = DCsiOJrRgNC40L/RgtC+0J/RgNC+IENTUCIgKNCy0LXRgNGB0LjRjyAzLjYp

После проверки файла политик можно делать запрос на сертификат подчинённого УЦ. Для этого в оснастке управления службой сертификации нужно выбрать в контекстном меню "Все задачи" – "Обновить сертификат ЦС":

🧱 certsrv -	[Центр сертификации (Локал	ьный)\Удостоверяющий центр Vas	-2012-05]		
Файл Дей	ствие Вид Справка				
🗢 🔿 🖄	💻 4 🞦 😹 🖸 🗐				
🙀 Центр сертификации (Локальный) Имя					
🕀 🛃 Удос	Все задачи 🔰 🕹	Запуск службы			
	Вид 🕨	Остановить службу			
	Обновить	Выдать новый запрос			
	Экспортировать список	Архивация ЦС			
	Свойства	Восстановление ЦС			
	Справка	Установить сертификат ЦС Обновить сертификат ЦС			
1					
Увеличить вр	емя жизни этого ЦС, запросив но	вый сертификат			

Далее после остановки службы сертификации выбрать вариант создания нового ключа ЦС:

бновление сертификата ЦС	x
При получении нового сертификата для вашего центра сертификации (ЦС) можно также создать новый ключ подписи.	
Нужен новый личный сертификат для вашего ЦС, если:	
Срок действия используемых в данный момент сертификатов истекает.	
Нужен новый ключ подписи, если:	
Омеющийся ключ скомпрометирован.	
Используется программа, требующая, чтобы для нового сертификата ЦС использовался новый ключ подписи.	
Текущий список отзыва сертификатов (CRL) слишком велик, и вы хотите перенести часть информации в новый CRL.	
Хотите создать новую пару из открытого и закрытого ключей? Поставщик служб шифрования и хэш-алгоритм будут сохранены. Если текущая длина ключа меньше 1024 бит, она может быть увеличена.	
€∐а	
О <u>Н</u> ет	
ОК Отмена	

Затем после создания ключевого контейнера и записи его на выбранный носитель появится окно:

Запрос сертификата ЦС				
Отправлять запрос напрямую в работающий ЦС				
Имя компьютера:				
<u>Р</u> одительский ЦС:				
Чтобы отправить запрос к ЦС вне сети, нажмите кнопку "Отмена" и отправьте файл запроса в C:\vas-ca15r2_!0423!0434!043e!0441!0442!043e!0432!0435!0440!044f!044e!0449!0 !0446!0435!043d!0442!0440 Vas-2012-05(11).req на родительский ЦС.				
ОК Отмена				

В нём написано имя файла (и полный путь на диске), куда будет сохранён файл запроса. Для завершения процесса формирования запроса нужно нажать кнопку Отмена, поскольку обработка файла запроса в УЦ Минкомсвязи не будет выполнена в онлайне.

Далее файл запроса с анкетой УЦ передаётся в Минкомсвязи для получения сертификата подчинённого УЦ. После получения сертификата установка его делается в оснастке управления службой сертификации:

🊋 certsrv - [Центр сертификации	(Локальный)]		
Файл Действие Вид Справка			
🙀 Центр сертификации (Локальный)	Имя	Описание	
Удостоверяющий нонто Иза Эб Все задачи •	Запуск службы	Центр сертификации	
Обновить	Остановить службу		
Сеойства	Выдать новый запрос		
Справка	Архивация ЦС		
	Восстановление ЦС		
	Установить сертификат ЦС Обновить сертификат ЦС		
-		1	
•			
Завершение установки иерархии ЦС			

Если в присланном файле имеется только сертификат подчинённого УЦ, то необходимо отдельно установить сертификат Головного удостоверяющего центра – в хранилище "Доверенные корневые ЦС" локального компьютера, сертификат выдающего УЦ (УЦ1 ИС ГУЦ или УЦ2 ИС ГУЦ) - в хранилище "Промежуточные ЦС" локального компьютера.

Кроме этого, требуется установить списки отозванных сертификатов (СОС) ГУЦ и УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ) - в хранилище "Промежуточные ЦС" локального компьютера.

В дальнейшем нужно следить за сроками действия этих СОС, поскольку работа подчинённого УЦ будет невозможна без актуальных СОС вышестоящих УЦ.

Вместо помещения СОС в хранилище можно настроить доступ к ним по точкам публикации из сертификатов УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ) и полученного сертификата подчинённого УЦ.

Сервер ЦС не рекомендуется подключать к сетям общего пользования (интернет), поэтому доступ к СОС вышестоящих УЦ в онлайне невозможен. Но можно организовать на любом доступном с сервера ЦС веб-сервере (в качестве него можно использовать сервер ЦР) виртуальную папку с именем cdp в корневом каталоге IIS и настроить по расписанию задание для помещения в эту папку актуальных файлов СОС вышестоящих УЦ. Тогда на сервере ЦС достаточно будет в файле hosts (%windir%\system32\drivers\etc\hosts) поместить строку:

<ip-адрес веб-сервера> <DNS-имя (имена) сервера cdp из сертификатов УЦ>

Пример, когда в качестве веб-сервера с СОС выступает сервер ЦР:

если ЦС имеет ip-адрес 192.168.1.1 и подключен только к серверу ЦР с ip-адресом 192.168.1.2, то в файл hosts нужно поместить:

192.168.1.2 rostelecom.ru reestr-pki.ru

Тогда ЦС сможет в автоматическом режиме получать доступ к СОС по адресам из сертификатов, например:

http://rostelecom.ru/cdp/guc.crl http://reestr-pki.ru/cdp/guc.crl http://reestr-pki.ru/cdp/vguc1_4.crl http://rostelecom.ru/cdp/vguc1_4.crl

На сервере ЦР нужно установить сертификаты вышестоящих УЦ и полученный сертификат подчинённого УЦ и следить за сроками их действия. Если сервер ЦР имеет подключение к интернету — то СОС вышестоящих УЦ могут быть автоматически получены по адресам точек распространения СОС из сертификатов УЦ1 ИС ГУЦ (или УЦ2 ИС ГУЦ) и полученного сертификата подчинённого УЦ. Для организации доступа к файлам СОС вышестоящих УЦ с сервера ЦС на сервере ЦР нужно создать виртуальную папку:

- 1. Создать на локальном диске папку, например, с:\cdp
- 2. В IIS создать в корневом каталоге веб-узла виртуальную папку с именем cdp

Орайл Реким Справка Подключения Действия
Файл Режим Справка Подключения Действия Действия
Подключения Действия Действия
Пачелльная страница Deriault web Site Мивтры: Аринтра: Презиние Приводник Правать разрешения Аринт Правать разрешения Правать разрешения Пр

Название сайта:	Default Web Site	
Путь:	1	
Псевдоним:		
cdp		
Пример: изображен	ния	
Физический путь:		
c:\cdp		
Проверка подлинн	ости	
Подкл. как	Тест настроек	

Рекомендуется настроить для этой папки срок действия веб-содержимого в функции "Заголовки ответов HTTP" — "Настроить стандартные заголовки" (для исключения ненужного кеширования файлов со стороны IIS):

Установка стандартных заголовков ответов НТТР	<u>?</u> ×
Разрешить поддержку открытых соединений НТТР	
Срок <u>де</u> йствия веб-содержимого истекает:	
О <u>Н</u> емедленно	
• Через:	
1 минут 💌	
О <u>В</u> указанное время (UTC):	
27 марта 2016г. 💌 0:00:00	*
ОК Отмен	a

Далее осталось настроить задания, которые будут брать файлы СОС вышестоящих УЦ из интернета и помещать их в эту папку cdp на диске.

Для этого можно использовать специально модифицированный файл задания переноса СОС JOBTCRLLib.dll. Этот файл размещён в <u>ftp://ftp.cryptopro.ru/pub/CRLfromGUC</u>

Его нужно поместить в папку на сервере ЦР вместо существующего там:

c:\Program Files (x86)\Common Files\Crypto Pro\Shared\JOBTCRLLib.dll

После этого для каждого адреса, с которого будет доставляться СОС, в оснастке управления ЦР (Пуск – Программы – КриптоПро – Параметры Центра регистрации, Свойства на "ЦР на ... вебузле") на вкладке Задания нужно создать новое задание:

Свойства пакета	×
Описание CRL from GUC	
Задания	ProolD исполнителя
•	
Добавить Свойства.	
	ОК Отмена

Имя можно задать любое, затем нажать Добавить:

Выбор компонента	×
ProgID	Комментарий
CPCCJOB TransferCRL	Задание для переноса СОС
CPCCJOB_TransferDskCRL	Задание для переноса СОС с исп
CPCCJOB_RevHoldCert	Задание для отзыва сертификат
CPCCJob_DistributeMsg	Задание для рассылки сообщени
CPCCJOB_KeySExpInformer	Задание для оповещения о скор
CPCCJOB_CertExpInformer	Задание для оповещения об исте
CPCCJOB_PendRegs	Задание для оповещения админи
CPCCJOB_KeyExpInformer	Задание для оповещения об око
CPCCJOB_ClearUsers	Задание для удаления неактивн
CPCCJOB_ActiveUserInformer	Задание для оповещения всех ак
CPCCJOB_CertCExInformer	Задание для оповещения о прев
CPCCJob_UnholdRemind	Задание для оповещения о скор
	ОК Отмена

И настроить его:

Описание: Перенос СОС ГУЦ Параметры Палка - источник: Расположена на съемном носителе http://rostelecom.ru/cdp/guc.cd Палка - приемник: Расположена на съемном носителе [::\cdp Список e-mail адресов получателей уведомлений об ошибках: [::-mail администратора: Имя очереди: [::-mail администратора: Идентификатор ключа [::-mail администратов. Вы 98 3b 89 18 51 е8	Настройка задания доставки СОС	<
Перенос СОС ГУЦ Параметры Папка - источник: Расположена на съемном носителе http://rostelecom.ru/cdp/guc.crl Папка - приемник: Расположена на съемном носителе C:\cdp Список e-mail адресов получателей уведомлений об ошибках: E-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Асtive Directory: Список ключей проверки ЗП издателей доставляемых СОС Центр сертифик Идентификатор ключа Половной удостов 8b 98 3b 89 18 51 e8 ОК Остакия	Описание:	
Параметры Папка - источник: Расположена на съемном носителе http://rostelecom.ru/cdp/guc.crl Папка - приемник: Расположена на съемном носителе [:\cdp Список e-mail адресов получателей уведомлений об ошибках: 	Перенос СОС ГУЦ	
Папка - источник: Расположена на съемном носителе http://rostelecom.ru/cdp/guc.cl Папка - приемник: Расположена на съемном носителе С:\cdp Список e-mail адресов получателей уведомлений об ошибках: E-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении COC Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых COC Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 е8 ОК От ема	Параметры	
http://rostelecom.ru/cdp/guc.crl Папка - приемник: Расположена на съемном носителе C:\cdp Cписок e-mail адресов получателей уведомлений об ошибках: E-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении COC Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых COC Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 e8 Удалить Настроить	Папка источник: П Расположена на съемном носителе	
Папка - приемник: Расположена на съемном носителе С:\cdp Список e-mail адресов получателей уведомлений об ошибках: E-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 е8 Удалить Настроить	http://rostelecom.ru/cdp/guc.crl	
С:\cdp Список e-mail адресов получателей уведомлений об ошибках: Е-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 e8 Удалить Настроить	Папка - приемник: Г Расположена на съемном носителе	
Список е-mail адресов получателей уведомлений об ошибках: Е-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 е8 Удалить Настроить	C:\cdp	
Е-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 e8 Удалить Настроить	Список e-mail адресов получателей уведомлений об ошибках:	
Е-mail администратора: Имя очереди: Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 е8 Удалить Настроить		
 Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Половной удостов 8b 98 3b 89 18 51 е8 Удалить Настроить 	Е-mail администратора: Имя очереди:	
 Запись в журнал информации об успешном выполнении Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Добавить Головной удостов 8b 98 3b 89 18 51 e8 Удалить Настроить 		
 Выгружать веб-приложения УЦ при обновлении СОС Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Добавить Половной удостов 8b 98 3b 89 18 51 е8 Удалить Настроить 	Запись в журнал информации об успешном выполнении	
Публиковать в Active Directory: Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 e8 Удалить Настроить	🔲 Выгружать веб-приложения УЦ при обновлении СОС	
Список ключей проверки ЭП издателей доставляемых СОС Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 е8 Удалить Настроить	Публиковать в Active Directory:	
Центр сертифик Идентификатор ключа Головной удостов 8b 98 3b 89 18 51 e8 Удалить Настроить	Cписок ключей проверки ЭП издателей доставляемых СОС	
Головной удостов 8b 98 3b 89 18 51 e8 Удалить Настроить	Центр сертифик Идентификатор ключа Добавить	
 Настроить	Головной удостов 8b 98 3b 89 18 51 e8	
Настроить	Эдалить	
	Настроить	
ок отмена	ОК Отмена	1

При необходимости можно настроить оповещение администратора об ошибках переноса СОС.

Затем нужно задать учётную запись, под которой будет выполняться задание (рекомендуется CPRAComPlusAcct&) и расписание его работы.

Для каждого из остальных адресов СОС вышестоящих УЦ нужно сделать отдельное задание и настроить его.