КриптоПро УЦ 2.0 + DSS

ПАК "КриптоПро DSS" предназначен для защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию электронной подписи. Интеграция с Рутокен KeyBox позволяет осуществлять выпуск и централизованный учёт средств облачной аутентификации. Для работы с электронной подписью не требуется устройство (USB-токен или смарт-карта), ключи генерируются и хранятся в хранилище КриптоПро DSS, для доступа и использования электронной подписи применяется облачный криптопровайдер КриптоПро Cloud CSP.

Предварительные условия

Для интеграции Рутокен KeyBox с КриптоПро DSS в окружении компании должны быть развернуты:

- Сервер RutokenKeyBox версии 5.1 и выше;
- ПАК "КриптоПро УЦ" 2.0;
- ПАК "КриптоПро DSS";
- ПАКМ "КриптоПро HSM";
- КриптоПро CSP 5.0;
- Настроенная интеграция КриптоПро УЦ 2.0 с КриптоПро DSS.

Интеграция УЦ и DSS необходима для управления пользователями и их сертификатами в удостоверяющем центре. КриптоПро DSS выступает в роли привилегированного пользователя по отношению к КриптоПро УЦ 2.0. Создание и обновление пользователей, запрос сертификатов и прочие действия на УЦ в этом случае выполняются от имени **Оператора DSS**. Подробная инструкция по интеграции входит комплект поставки ПАК "КриптоПро DSS".

Настройка интеграции в Рутокен KeyBox

Для работы с КриптоПро DSS используется учётная запись **Оператор DSS**, сертификат которой должен хранится на сервере RutokenKeyBox. Для установки сертификата Оператора DSS выполните следующие действия:

1. Добавьте сертификат **Оператора DSS** в **локальное хранилище компьютера** (Local Computer) на сервере RutokenKeyBox.
2. Добавьте корневой сертификат КриптоПро УЦ 2.0 и корневой сертификат DSS в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере RutokenKeyBox.
3. Выдайте системе Рутокен KeyBox **права на чтение закрытого ключа сертификата Оператора DSS**.
    - В оснастке **Сертификаты** (Certificates) компьютера, на котором установлен сервер RutokenKeyBox.
    - Кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) **> Управление закрытыми ключами...**(Manage Private Keys...).
    - Нажмите **Добавить** (Add), укажите локальную группу **IIS_IUSRS** (если используется IIS 7.0) или локальную учетную запись **IIS AppPool\RutokenKeyBox** (если используется IIS 7.5 и более поздние версии).
    - Выставите права **Полный доступ** (FullControl).
    - Нажмите **Применить** (Apply).

Выдайте права на папку с пользователями в КриптоПро УЦ 2.0 для учётной записи **Оператор DSS**:

1. Создайте группу безопасности, например **DSS Operators** и включите в неё учётную запись **Оператор DSS**.
2. Откройте свойства папки, в которой будут располагаться пользователи DSS, перейдите на вкладку безопасность и добавьте созданную группу **DSS Operators**.
3. Выдайте группе разрешения (таблица 2).

Таблица 2 —Набор прав для сервисной группы пользователей DSS Operators.

Наименование разрешения	Тип объекта	Комментарий
Чтение свойств	Папка, Пользователь	Чтение свойств объекта. Если у субъекта нет права чтения свойств объекта, то объект не виден субъекту
Запрос регистрации	Папка	Создание запроса на регистрацию пользователя
Запрос сертификата	Пользователь, шаблон	Создание запроса сертификата для пользователя
Запрос аннулирования	Пользователь	Создание запроса на аннулирование сертификата пользователя
Запрос приостановления	Пользователь	Создание запроса на приостановление сертификата пользователя

Запрос возобновления	Пользователь	Создание запроса на возобновление сертификата пользователя
Одобрение регистрации	Папка	Одобрение запроса на регистрацию пользователя
Одобрение сертификата	Пользователь, шаблон	Одобрение запроса сертификата для пользователю
Одобрение аннулирования	Пользователь	Одобрение запроса на аннулирование сертификата пользователя
Одобрение приостановления	Пользователь	Одобрение запроса на приостановление сертификата пользователя
Одобрение возобновления	Пользователь	Одобрение запроса на возобновление сертификата пользователя
Передача запросов	Пользователь	Передача запросов, подписанных пользователем-получателем услуги, а не подписью пользователя, передающего или одобряющего запрос
Запрос переименования	Пользователь	Создание запроса на изменение данных пользователя
Одобрение переименования	Пользователь	Одобрение запроса на изменение данных пользователя