


# КриптоПро DSS 2.0

ПАК "КриптоПро DSS" версии 2.0 предназначен для защищенного хранения закрытых ключей пользователей, а также для удаленного выполнения операций по созданию электронной подписи. Интеграция с Indeed Certificate Manager 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 Indeed Certificate Manager с КриптоПро DSS в окружении компании должны быть развернуты:

- Сервер Indeed CM версии 5.1 и выше.
- ПАК "КриптоПро УЦ" 2.0
- ПАК "КриптоПро DSS" 2.0
- 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

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

1. Добавьте сертификат **Оператора DSS** в **локальное хранилище компьютера** (Local Computer) на сервере Indeed CM.
2. Добавьте корневой сертификат КриптоПро УЦ 2.0 и корневой сертификат DSS в **Доверенные корневые центры сертификации** (Trusted Root Certification Authorities) на сервере Indeed CM.
3. Выдайте системе **права на чтение закрытого ключа сертификата Оператора DSS**.
  - Перейдите в оснастку **Сертификаты** (Certificates) компьютера, на котором установлен сервер Indeed CM.
  - Кликните правой кнопкой мыши на сертификате, выберите **Все задачи** (All tasks) > **Управление закрытыми ключами...** (Manage Private Keys...).
  - Нажмите **Добавить** (Add), укажите сервер в меню **Размещение** (Location), укажите локальную группу **IIS\_IUSRS** в поле **Введите имена выбранных объектов** (Enter the object names to select), нажмите **Проверить имена** (Check Names) и **ОК**.
  - Выставьте 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 добавьте в неё учётную запись **Оператор DSS**.
2. Откройте свойства папки, где будут располагаться пользователи DSS, перейдите на вкладку **Безопасность** и добавьте созданную группу **DSS Operators**.
3. Выдайте группе разрешения согласно таблице.

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

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