Сервер NOMAD 2.10. Инструкция по настройке шифрования документов

В документе описан порядок настройки шифрования документов на сервере NOMAD и в приложении DIRECTUM Solo для iOS.

Основные понятия

NOMAD (Native Offline Mobile Applications for DIRECTUM)

Нативные мобильные приложения для систем DIRECTUM и DirectumRX – DIRECTUM Jazz и DIRECTUM Solo. Предназначены для работы с документами, задачами и заданиями систем посредством мобильных устройств.

Сервер NOMAD

Набор серверных компонент, состоящий из веб-сервиса NOMAD и конфигуратора сервера NOMAD. Предназначен для выполнения функций, запрашиваемых клиентским приложением, предоставления доступа к данным и т.п.

Веб-сервис NOMAD

Серверное приложение, предоставляющее методы авторизации, доступа к данным системы DIRECTUM.

Общие сведения

Приложение DIRECTUM Solo для iOS работает в изолированной области памяти устройства, доступ к которой из других приложений или с компьютера невозможен.

Безопасность данных пользователя обеспечивается на уровне ОС: документы шифруются по AES-алгоритму. Для сохранности данных необходимо использовать блокировку устройства. Рекомендуется использовать PIN-код. Графический ключ или отпечаток пальца не являются достаточными мерами защиты.

В качестве дополнительной защиты данных можно использовать шифрование документов сертифицированными средствами СКЗИ. Перед отправкой в мобильное приложение документы шифруются по ГОСТ-алгоритму на стороне сервиса NOMAD. Это обеспечивает надежную передачу и хранение документов.

В мобильном приложении документы хранятся также в зашифрованном виде. Перед выполнением действий (просмотр, подписание, экспорт) приложение расшифровывает документ во временное хранилище. После завершения действий расшифрованный документ удаляется из временного хранилища. Если во время выполнения действия произошло экстренное завершение работы, например, выключение устройства, при запуске приложение поверяет наличие файлов во временном хранилище и удаляет их, при наличии.

> Примечание
> Во внешнее приложение документ экспортируется в расшифрованном виде. Чтобы обеспечить возможность работы с документом только в приложении DIRECTUM Solo, можно ограничить экспорт документов на сервере NOMAD. Настройка выполняется в секции **permissions** файла IsBuilderAdapter.config. Подробнее см. в документе «Сервер NOMAD. Инструкция по установке и настройке», раздел «Настройка прав доступа к документам и записям справочников».

Шифруются все отправляемые на устройство документы, независимо от режима работы: offline или online, а также документы, вложенные в архивы или контейнеры.

Шифрование производится средствами СКЗИ КриптоПРО на основе сертификата пользователя, указанного в компоненте **Пользователи** системы DIRECTUM. Сертификат должен иметь тип **Шифрование** или **ЭП и Шифрование**.

Шифрование доступно с версии сервера NOMAD 2.5.

Необходимо приобрести лицензии:

- на право использования СКЗИ «КриптоПро CSP» версии 4.0 на одном рабочем месте;
- на право использования СКЗИ «КриптоПро CSP» версии 4.0 на сервере;
- на право использования ПО «КриптоПро .NET» на одном сервере.

Если лицензия СКЗИ «КриптоПро CSP» версии 4.0 для рабочего места была приобретена для подписания документов ЭП, повторно ее приобретать не требуется.

Настройка шифрования выполняется последовательно на сервере NOMAD и в приложении DIRECTUM Solo.

Настройка на сервере NOMAD

Пользователь, от которого работает пул приложений, должен иметь права на контейнер, в котором находится сертификат для шифрования.

Чтобы настроить шифрование документов:

1. На сервере, где установлен сервер NOMAD, установите СКЗИ «КриптоПро CSP» версии 4.0 и КриптоПро.Net.
2. Сгенерируйте сертификат КриптоПро с возможностью шифрования. На странице запроса сертификата укажите необходимые данные. В поле **Тип требуемого сертификата** укажите значение **Сертификат проверки подлинности сервера**.
3. Установите сертификат на сервер.
4. В конфигураторе сервера NOMAD на закладке «Настройки веб-сервиса»:
   - установите флажок **Шифровать документы**;
   - заполните поля **Имя контейнера закрытого ключа** и **Пароль для контейнера закрытого ключа**.
5. Настройте шифрование в мобильном приложении DIRECTUM Solo для iOS.

Настройка в приложении DIRECTUM Solo

Настройка шифрования документов в приложении доступна, если шифрование включено на сервере NOMAD. В этом случае при первом запуске приложения откроется сообщение с предложением настроить шифрование.

Чтобы настроить шифрование документов в приложении:

1. Сгенерируйте сертификат с возможностью шифрования.
2. Загрузите сертификат на устройство с помощью приложения iTunes:
   a) Подключите устройство к компьютеру, на котором установлена программа iTunes.
   b) В программе iTunes перейдите к списку установленных приложений и выберите DIRECTUM Solo.
   c) Сохраните папку cprocsp с подпапками локально на компьютер.
   d) В сохраненную папку cprocsp/keys/mobile скопируйте контейнер с закрытым ключом.
   e) С помощью механизма Drag&Drop добавьте папку cprocsp в папку «Документы» приложения DIRECTUM Solo.
   f) В настройках профиля приложения DIRECTUM Solo **Сертификаты/Открыть настройки КриптоПРО** нажмите на кнопку **Установить сертификат из контейнера**.
   g) В окне подтверждения нажмите на кнопку **Да**.
3. Откройте настройки приложения и включите настройку **Шифрование**.