Создание сертификата подписи

Сертификат подписи используется для выдачи сертификатов рабочим станциям пользователей, к которым подключаются устройства AirKey. Клиентский сертификат выдается автоматически при первом подключении устройства AirKey к компьютеру. Обращаясь к серверу клиентский компьютер предоставляет свой сертификат, сервер Indeed AirKey Enterprise проверяет подлинность клиентского сертификата и разрешает подключение виртуальной карты.

Для создания сертификата подписи воспользуйтесь утилитой **Indeed.AKES.CertificateGenerator.exe** и выполните следующие действия:

1. Запустите в командной строке, запущенной от имени администратора, на сервере Indeed AirKey Enterprise утилиту **Indeed.AKES.CertificateGenerator.exe**. После завершения работы утилиты в оснастке **Сертификаты** (Certificates) локального компьютера появится сертификат **AirKey Enterprise Server CA**.

2. Выдайте серверу AirKey **права на чтение закрытого ключа сертификата** сервера. Для этого:

   - В оснастке **Сертификаты** (Certificates) локального компьютера.
   - Кликните правой кнопкой мыши на сертификате **AirKey Enterprise Server CA**.
   - 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\IndeedAKES** (если используется IIS 7.5 и более поздние версии).
   - Выставьте право на **Чтение** (Read).
   - Нажмите **Применить** (Apply).

3. Добавьте сертификат **AirKey Enterprise Server CA** в список **Доверенных Корневых Центров Сертификации** (Trusted Root Certification Authorities) на сервере AirKey и рабочих станциях пользователей, к которым будут подключаться устройства AirKey.