

Общие сертификаты

Общие сертификаты используются в сценарии, когда уже выпущенный вне системы Рутокен KeyBox сертификат и закрытый ключ необходимо записать на устройства множества пользователей средствами Рутокен KeyBox.

Особенности работы системы с общими сертификатами:

- Поддерживаются сертификаты с ключами RSA и ГОСТ.
- Для записи ГОСТ-сертификатов требуется наличие КриптоПро CSP на сервере Rutoken KeyBox и рабочей станции, к которой подключено устройство.
- Общие сертификаты не могут быть приостановлены и отозваны, обновление возможно через удаление старого PFX и добавление нового.
- Общие сертификаты не публикуются в Active Directory, файловое хранилище и базу приложений ЦФТ, не помещаются средствами Рутокен KeyBox в хранилище сертификатов пользователя.
- Отправка почтовых уведомлений для события **Общие сертификаты истекают** задается в пункте **Уведомления администратора**. Рассылка происходит при достижении 10% до окончания срока действия сертификата. Для истекших сертификатов уведомления перестают отправляться.

Уведомление доступно только для администраторов, так как оно привязано к политике выпуска устройств, а не к самому устройству.

Для добавления общего сертификата в политику использования устройств выберите файл PFX, укажите пароль для доступа к содержимому файла и нажмите **Добавить**.

Общие сертификаты

+

Добавить общий сертификат

Добавить общий сертификат

PFX файл

Пароль

☐ Необязательный сертификат

Добавить

Отмена

При включении опции **Необязательный сертификат** общий сертификат будет предлагаться к выбору для записи на устройство при его выпуске или обновлении. При отключенной опции сертификат будет записан на устройство без предоставления возможности выбора.