Настройка шаблонов сертификатов

Для работы с Рутокен KeyBox обязательно необходим шаблон сертификата **Агент регистрации** (Enrollment Agent). Сертификат **Агент регистрации** (Enrollment Agent), выданный на имя сервисной учетной записи (**serviceca**) необходим для подписи запроса на сертификат от имени других пользователей по всем остальным шаблонам сертификатов, которые будут использоваться системой Рутокен KeyBox.

Ниже описан процесс настройки шаблона сертификата пользователя на примере шаблона **Вход со смарт-картой** (Smartcard Logon), который будет использоваться для выпуска сертификатов, предназначенных для входа в операционную систему по смарт-карте.

1. Откройте консоль управления **Центр сертификации** (Certification Authority).
2. Перейдите в раздел **Шаблоны сертификатов** (Certificate Templates), щелкните правой кнопкой мыши выберите **Управление** (Manage).
3. Щелкните правой кнопкой мыши по шаблону **Вход со смарт-картой** (Smartcard Logon) и выберите **Скопировать шаблон** (Duplicate Template).
4. Перейдите на вкладку **Общие** (General) и в поле **Отображаемое имя шаблона** (Template display name) введите **Keybox Smart Card Logon**. Измените **Период действия** (Validity period) и **Период обновления** (Renewal period) в соответствии с потребностями вашей организации.
5. На вкладке **Шифрование** (Cryptography) в поле **Минимальный размер ключа** (Minimum key size) укажите необходимую длину ключа.

   Опция доступна для Microsoft CA 2008/2008R2 и выше. В предыдущих версиях настройка осуществляется на вкладке **Обработка запроса** (Request Handling).
   Обратите внимание на размер ключей шифрования указанный в свойствах шаблонов сертификатов, которые планируется использовать. Чтобы снизить риск несанкционированного доступа к конфиденциальной информации компания Майкрософт выпустила несвязанное с безопасностью обновление (KB 2661254) для всех поддерживаемых версий Microsoft Windows. Это обновление блокирует криптографические ключи меньше 1024 бит. Обновление не относится к Windows 8 (и выше) или Windows Server 2012 (и выше), т.к. эти операционные системы уже могут блокировать использование ключей RSA меньше 1024 бит. Подробная информация об этом обновлении содержится на сайте службы поддержки компании Майкрософт: https://learn.microsoft.com/ru-ru/security-updates/SecurityAdvisories/2012/2661254?redirectedfrom=MSDN.
6. На вкладке **Требования выдачи** (Issuance Requirements):

   - Установите опцию **Одобрения диспетчера сертификатов ЦС** (CA certificate manager approval).
   - Установите флажок **Указанного числа авторизованных подписей** (This number of authorised signatures) и укажите число подписей, равное **1** (значение по умолчанию).
   - Выберите **Политики применения** (Application Policy) из списка **В подписи требуется указать тип политики** (Policy type required in signature).
   - Выберите **Агент запроса сертификата** (Certificate Request Agent) из списка **Политика применения** (Application Policy).
   - Выберите параметр **Тех же условий, что и для регистрации** (Same criteria as for enrollment) в разделе **Требовать для повторной регистрации** (Require the following for reenrollment).

7. На вкладке **Имя субъекта** (Subject Name) нажмите **Строится на основе данных Active Directory** (Build from this Active Directory information).
   - Выберите **Полное различающееся имя** (Fully distinguished name) из списка **Формат имени субъекта** (Subject name format).
   - Установите флажок **Имя субъекта-пользователя (UPN)** (User principal name (UPN)).
   - Снимите флажки с опций **Включить имя электронной почты в имя субъекта** (Include e-mail name in subject name) и **Имя электронной почты** (E-mail name), если требуется выпуск сертификатов по данному шаблону пользователям, у которых не указан E-mail в Active Directory.
8. На вкладке **Безопасность** (Security) нажмите кнопку **Добавить...** (Add...).
   - В поле **Введите имена выбираемых объектов** (Enter the object names to select) введите имя сервисной учетной записи (**serviceca**) и нажмите **ОК**.
   - В разделе **Разрешения для группы** (Permissions for) установите галочку **Разрешить** (Allow) для привилегий **Чтение** (Read) и **Заявка** (Enroll).

     Обязательно выдайте аналогичные разрешения сервисной учетной записи для шаблона **Агент регистрации** (Enrollement Agent) и для всех шаблонов сертификатов, которые будут использоваться Рутокен KeyBox.
9. Сохраните настройки шаблона, нажав **ОК**.