Настройка шаблонов сертификатов

Для работы с Indeed Certificate Manager обязательно необходим шаблон сертификата **Агент регистрации** (Enrollment Agent), а также все остальные шаблоны сертификатов, которые будут использоваться системой Indeed CM.

Например, создайте копию шаблона **Вход со смарт-картой** (Smartcard Logon), который будет использоваться для выпуска сертификатов, предназначенных для входа в операционную систему по смарт-карте.

1. Откройте оснастку **Центр сертификации** (Certification Authority).
2. Перейдите в раздел **Шаблоны сертификатов** (Certificate Templates) в дереве консоли **Центр сертификации** (Certification Authority), щелкните правой кнопкой мыши выберите **Управление** (Manage).
3. Щелкните правой кнопкой по шаблону **Вход со смарт-картой** (Smartcard Logon) и выберите **Скопировать шаблон** (Duplicate Template).
4. Откройте свойства созданного шаблона сертификата **Копия "Вход со смарт-картой"** (Copy of Smartcard Logon) и перейдите на вкладку **Требования выдачи** (Issuance Requirements).
5. Отметьте опцию **Требовать для регистрации: Указанного числа авторизованных подписей** (This number of authorised signatures) и укажите число подписей, равное **1** (значение по умолчанию).
6. Установите значения политик: **Политика применения** (Application Policy) и **Агент запроса сертификата** (Certificate Request Agent), см. Рисунок 7:

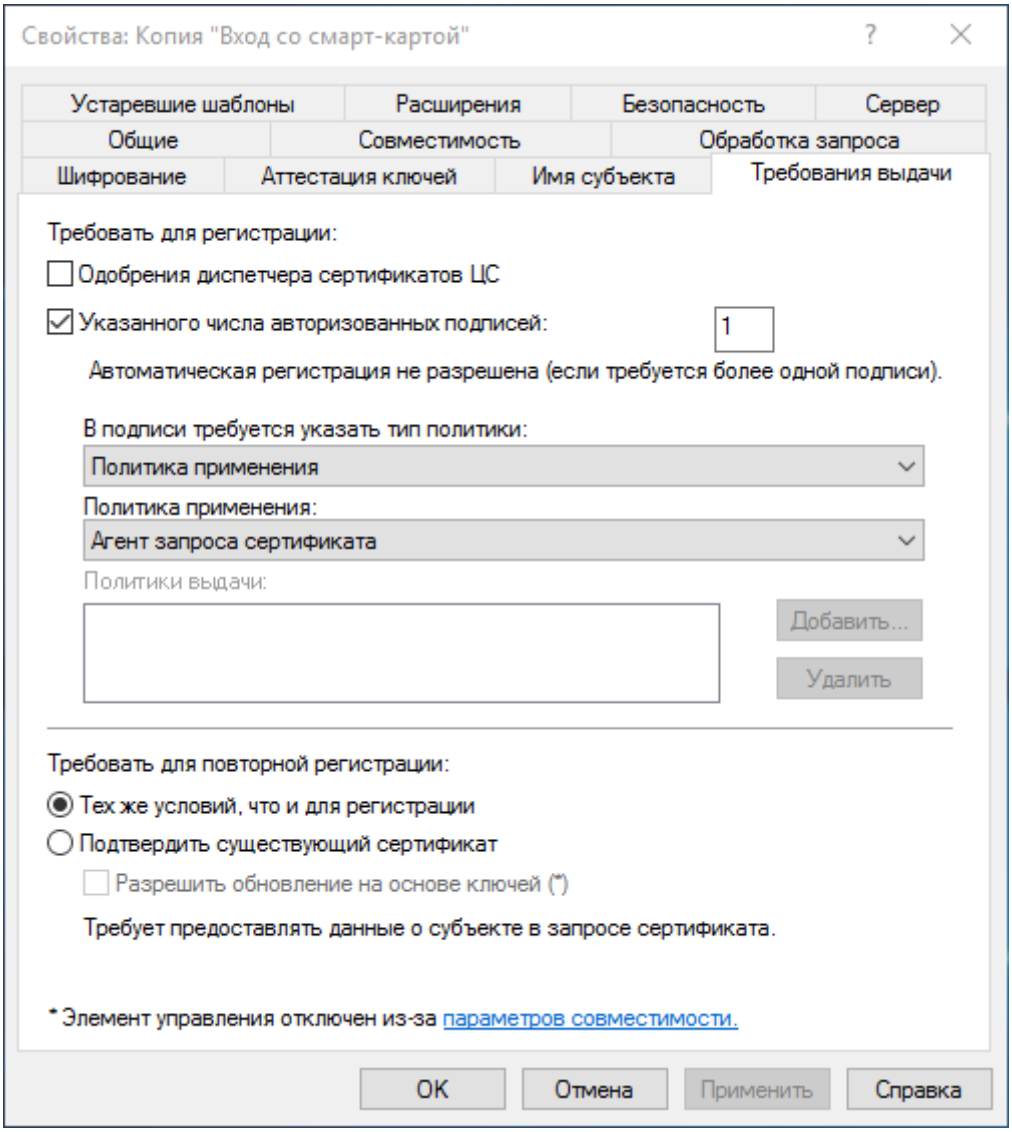

Рисунок 7 – Настройка шаблона сертификата Microsoft CA: Требования выдачи.

7. В случае, если необходимо использовать секретный ключ какой-либо определенной длины, укажите необходимую длину ключа на вкладке **Шифрование** (Cryptography) в поле **Минимальный размер ключа** (Minimum key size). Обратите внимание на размер ключей шифрования указанный в свойствах шаблонов сертификатов, которые планируется использовать.

Вкладка **Обработка запроса** (Request Handling) для Microsoft CA 2008/2008R2.

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://support.microsoft.com/kb/2661254.

8. На вкладке **Имя субъекта** (Subject Name) отключите опции **Включить имя электронной почты в имя субъекта** (Include e-mail name in subject name) и **Имя электронной почты** (E-mail name) в свойствах шаблона сертификата, если требуется выпуск сертификата пользователям, у которых не указан E-mail в учетных данных (Рисунок 8).

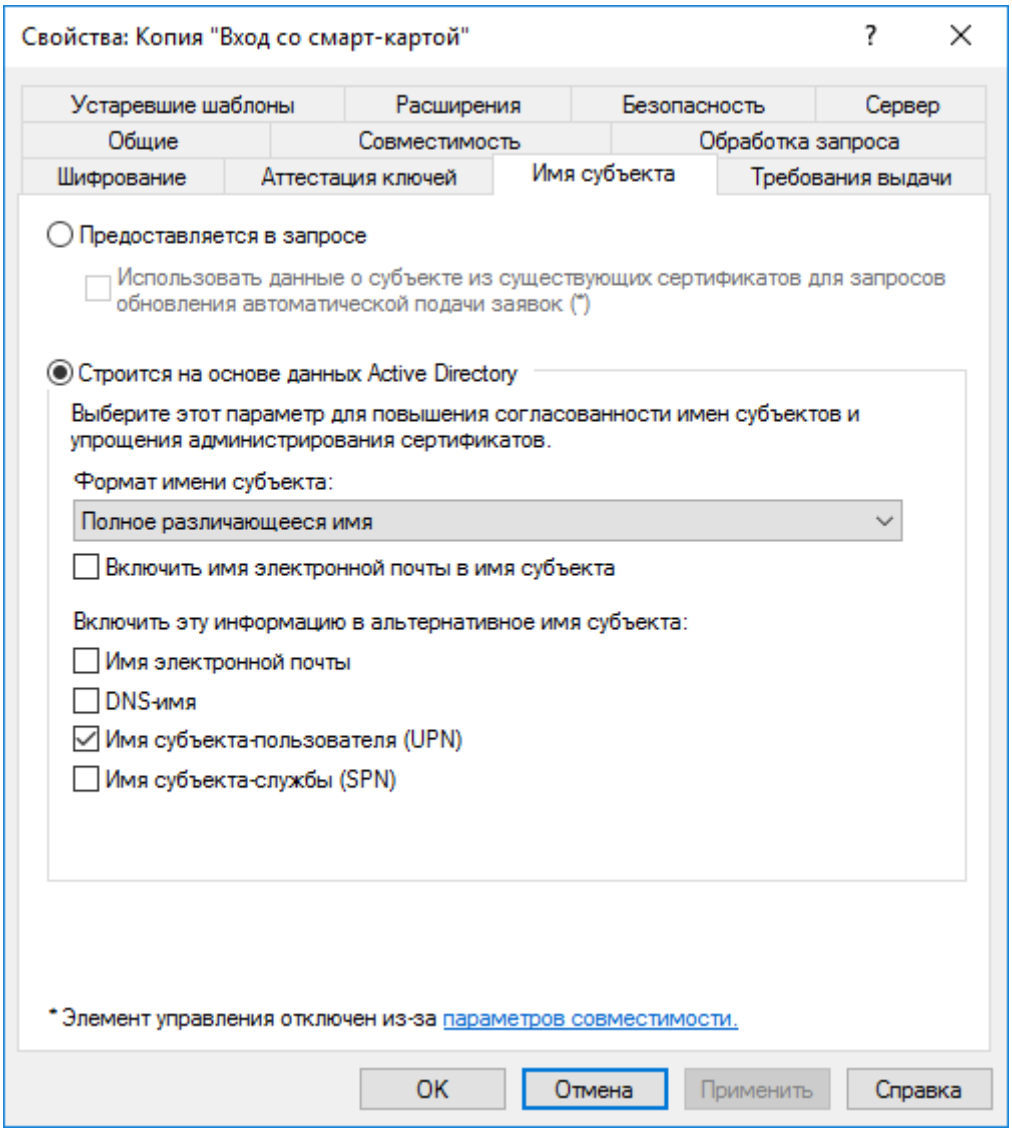

Рисунок 8 – Настройка шаблона сертификата Microsoft CA: Имя субъекта.

9. На вкладке **Безопасность** (Security) добавьте сервисную учетную запись (**serviceca**) и назначьте для нее права на **Чтение** (Read) и **Заявка** (Enroll), см. Рисунок 9:

> **Обязательно** выдайте аналогичные права для шаблона **Агент регистрации** (Enrollment Agent) и для всех шаблонов сертификатов, которые будут использоваться Indeed CM.

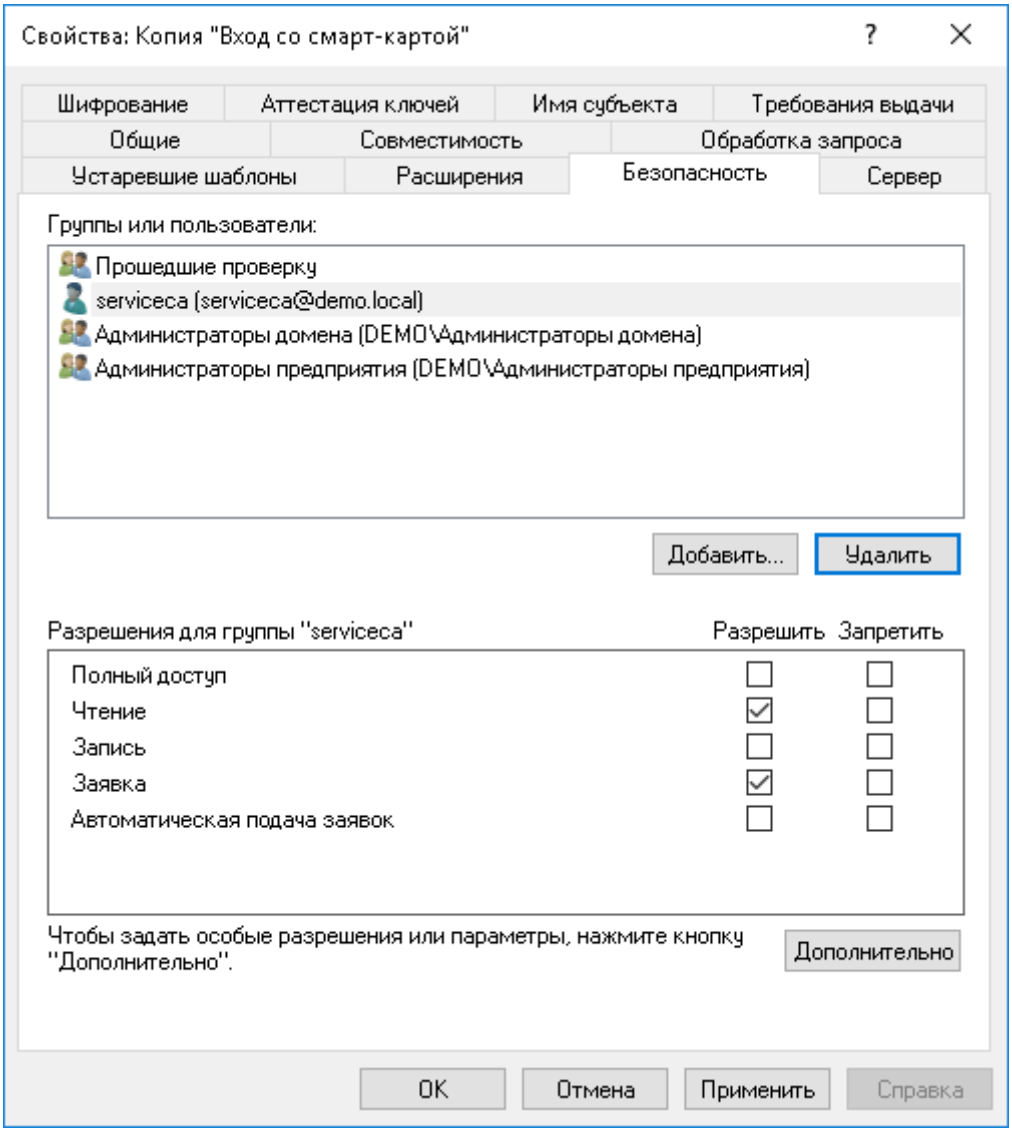

Рисунок 9 – Настройка шаблона сертификата Microsoft CA: Безопасность.

10. Сохраните настройки, нажав **ОК**.