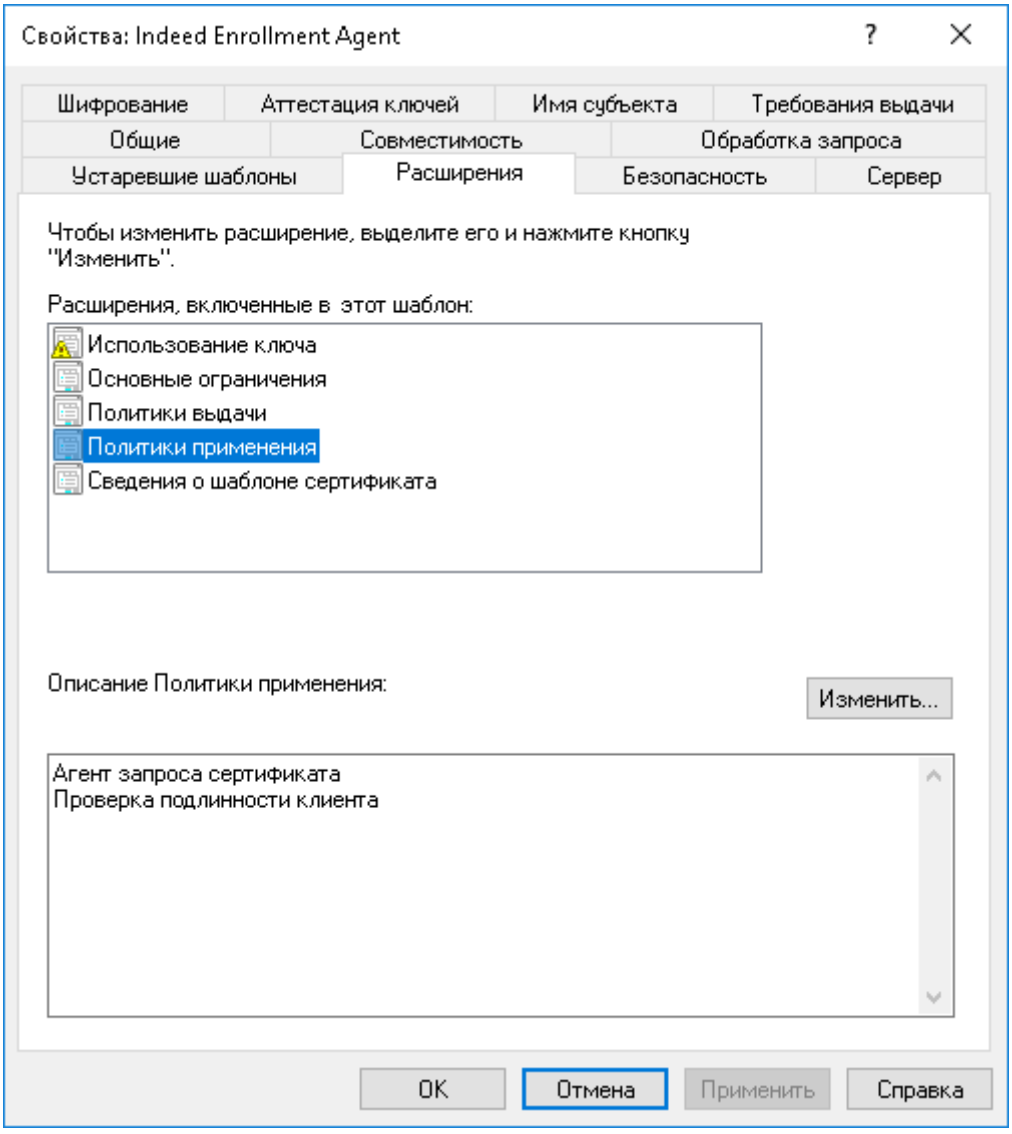
Настройка шаблонов сертификатов

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

Настройка шаблона сертификата Агент Регистрации

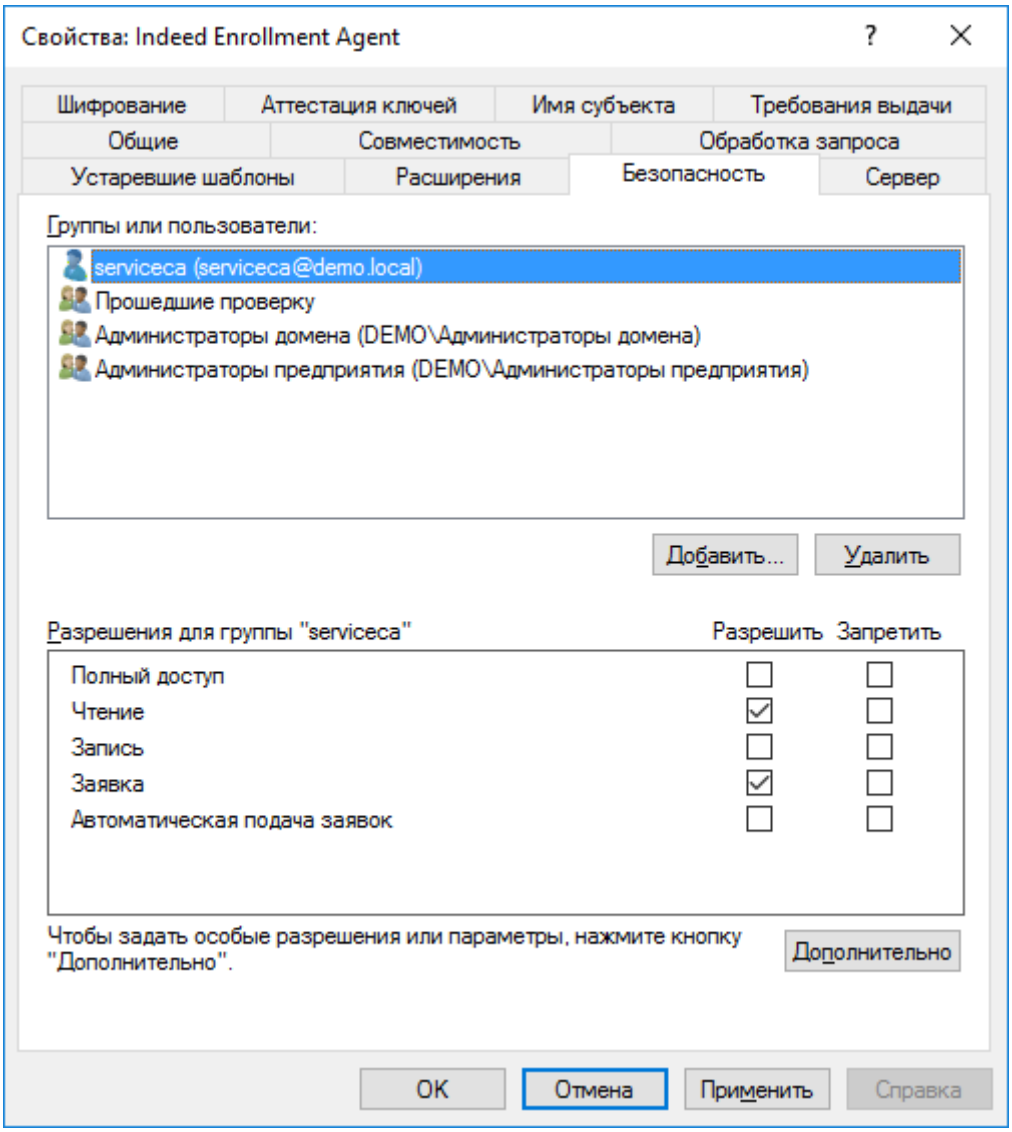
Ниже описан процесс создания и настройки шаблона сертификата для сервисной учетной записи на примере стандартного шаблона **Агент регистрации** (Enrollment Agent).

1. Откройте консоль управления **Центр сертификации** (Certification Authority).
2. Перейдите в раздел **Шаблоны сертификатов** (Certificate Templates), щелкните правой кнопкой мыши и выберите **Управление** (Manage).
3. Щелкните правой кнопкой мыши по шаблону **Агент регистрации** (Enrollment Agent) и выберите **Скопировать шаблон** (Duplicate Template).
4. Перейдите на вкладку **Общие** (General) и в поле **Отображаемое имя шаблона** (Template display name) введите **Indeed Enrollment Agent**. Измените **Период действия** (Validity period) в соответствии с потребностями вашей организации.
5. На вкладке **Шифрование** (Cryptography) в поле **Минимальный размер ключа** (Minimum key size) укажите необходимую длину ключа (рекомендуемая длина ключа 2048 бит).
6. На вкладке **Расширения** (Extensions) выберите расширение **Политики применения** (A pplication Policies) и нажмите кнопку **Изменить...** (Edit...), в появившемся окне нажмите кнопку **Добавить...** (Add...) и выберите из предложенного списка политику применения **Проверка подлинности клиента** (Client Authentication) и нажмите **ОК**.



7. 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 флажок **Разрешить** (Allow) для привилегий **Чтение** (Read) и **Заявка** (Enroll).



8. Сохраните настройки шаблона, нажав **ОК**.

Настройка шаблонов сертификата пользователей

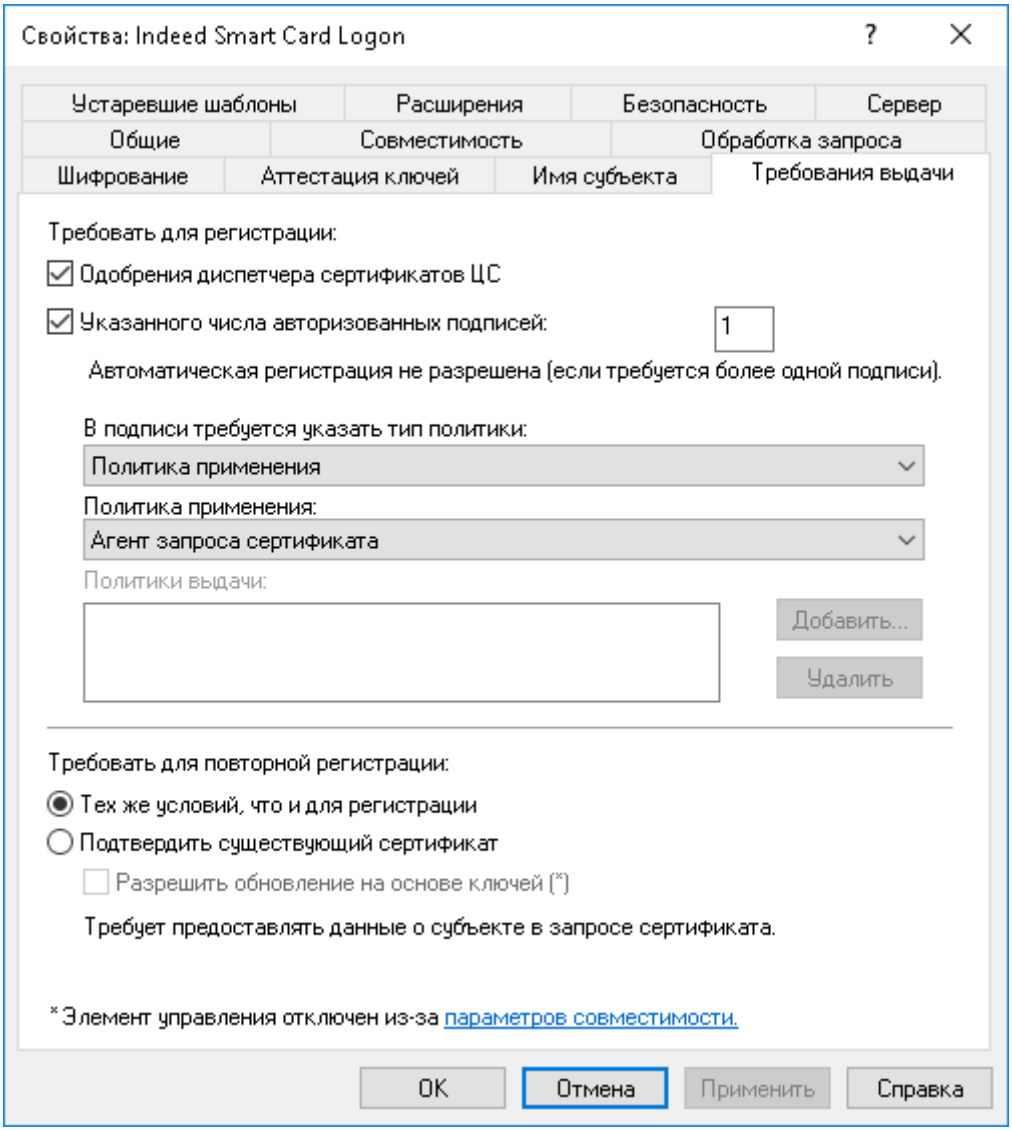
Подготовьте шаблоны сертификатов для различных назначений (политик применения), которые будут использоваться для выпуска сертификатов конечным пользователям системы. Ниже описан процесс создания и настройки шаблона сертификата пользователя на примере шаблона **Вход со смарт-картой** (Smartcard Logon), 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 **Indeed 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.

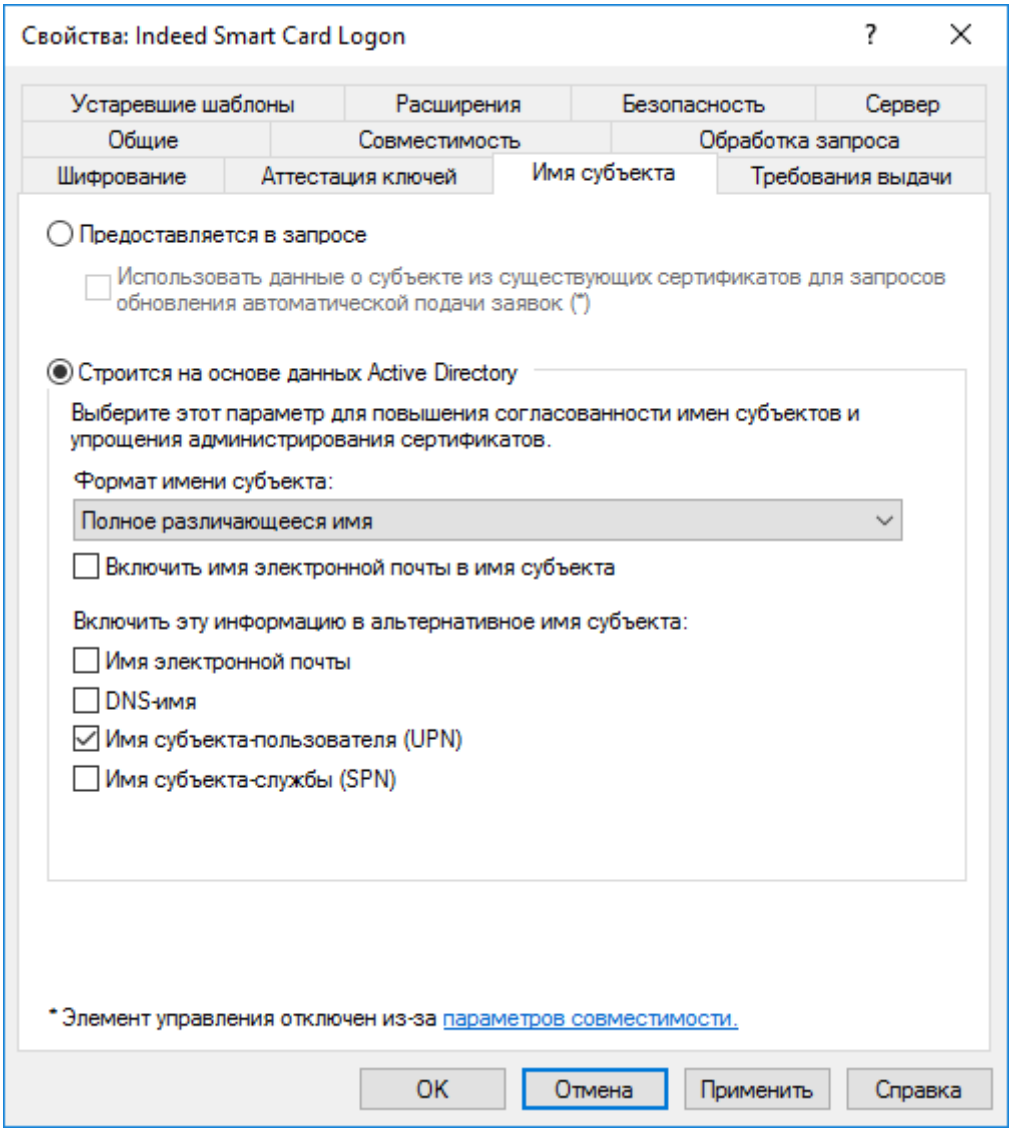
   Опция доступна для Microsoft CA 2008/2008R2 и выше. В предыдущих версиях настройка осуществляется на вкладке **Обработка запроса** (Request Handling).

   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 не связанное 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.

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 authorized 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).

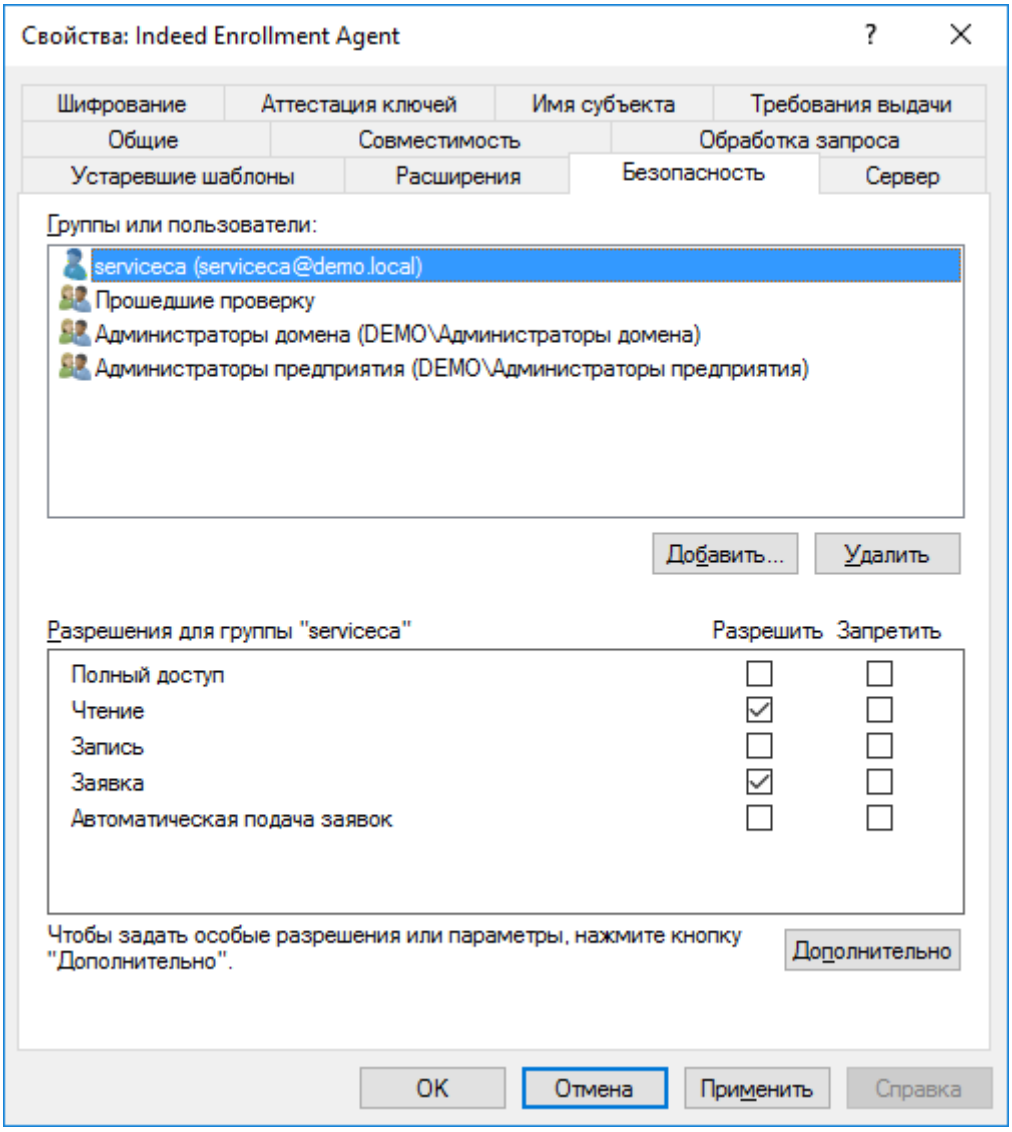


7. На вкладке **Имя субъекта** (Subject Name) нажмите **Строится на основе данных Active Directory** (Build from this Active Directory information).
    - Выберите **Полное различающееся имя** (Fully distinguished name) из списка **Формат имени субъекта** (Subject name format).
    - Установите флажок **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 флажок **Разрешить** (Allow) для привилегий **Чтение** (Read) и **Заявка** (Enroll).

   > **Обязательно** выдайте аналогичные разрешения сервисной учетной записи для всех шаблонов сертификатов, которые будут использоваться в Indeed CM.



9. Сохраните настройки шаблона, нажав **ОК**.