

Настройка шаблонов сертификатов

Для работы с Indeed Certificate Manager 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 Indeed CM.

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 **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 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.

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).

The screenshot shows the 'Indeed Smart Card Logon' properties dialog box with the 'Требования выдачи' (Issuance Requirements) tab selected. The dialog has a tabbed interface with 'Общие' (General), 'Совместимость' (Compatibility), and 'Обработка запроса' (Request Processing). The 'Требования выдачи' sub-tab is active, showing options for registration and reenrollment requirements.

Требования для регистрации:

- ☒ Одобрения диспетчера сертификатов ЦС
- ☒ Указанного числа авторизованных подписей:

Автоматическая регистрация не разрешена (если требуется более одной подписи).

В подписи требуется указать тип политики:

Политика применения:

Политика применения:

Агент запроса сертификата:

Политики выдачи:

Требовать для повторной регистрации:

- ☒ Тех же условий, что и для регистрации
- ☐ Подтвердить существующий сертификат

☐ Разрешить обновление на основе ключей (*)

Требует предоставлять данные о субъекте в запросе сертификата.

* Элемент управления отключен из-за [параметров совместимости](#).

Buttons at the bottom: OK, **Отмена** (highlighted), Применить, Справка.

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.

The screenshot shows the 'Свойства: Indeed Smart Card Logon' dialog box with the 'Имя субъекта' (Subject Name) tab selected. The 'Предоставляется в запросе' (Presented in request) section has two options: 'Использовать данные о субъекте из существующих сертификатов для запросов обновления автоматической подачи заявок (*)' (Use subject data from existing certificates for request updates) and 'Строится на основе данных Active Directory' (Build from this Active Directory information), which is selected. Below this, a text box explains: 'Выберите этот параметр для повышения согласованности имен субъектов и упрощения администрирования сертификатов.' (Select this parameter to improve subject name consistency and simplify certificate administration). The 'Формат имени субъекта:' (Subject name format) dropdown is set to 'Полное различающееся имя' (Fully distinguished name). Below this, there are three checkboxes: 'Включить имя электронной почты в имя субъекта' (Include e-mail name in subject name), 'Включить эту информацию в альтернативное имя субъекта:' (Include this information in alternative subject name:), and 'Имя субъекта-пользователя (UPN)' (User principal name (UPN)), which is checked. At the bottom, a note states: '* Элемент управления отключен из-за параметров совместимости.' (Control element disabled due to compatibility parameters). The dialog has buttons for 'ОК', 'Отмена', 'Применить', and 'Справка'.

Свойства: Indeed Smart Card Logon

Устаревшие шаблоны Расширения Безопасность Сервер

Общие Совместимость Обработка запроса

Шифрование Аттестация ключей **Имя субъекта** Требования выдачи

☐ Предоставляется в запросе

☐ Использовать данные о субъекте из существующих сертификатов для запросов обновления автоматической подачи заявок (*)

☒ **Строится на основе данных Active Directory**

Выберите этот параметр для повышения согласованности имен субъектов и упрощения администрирования сертификатов.

Формат имени субъекта:

Полное различающееся имя

☐ Включить имя электронной почты в имя субъекта

Включить эту информацию в альтернативное имя субъекта:

☐ Имя электронной почты

☐ DNS-имя

☒ **Имя субъекта-пользователя (UPN)**


☐ Имя субъекта-службы (SPN)

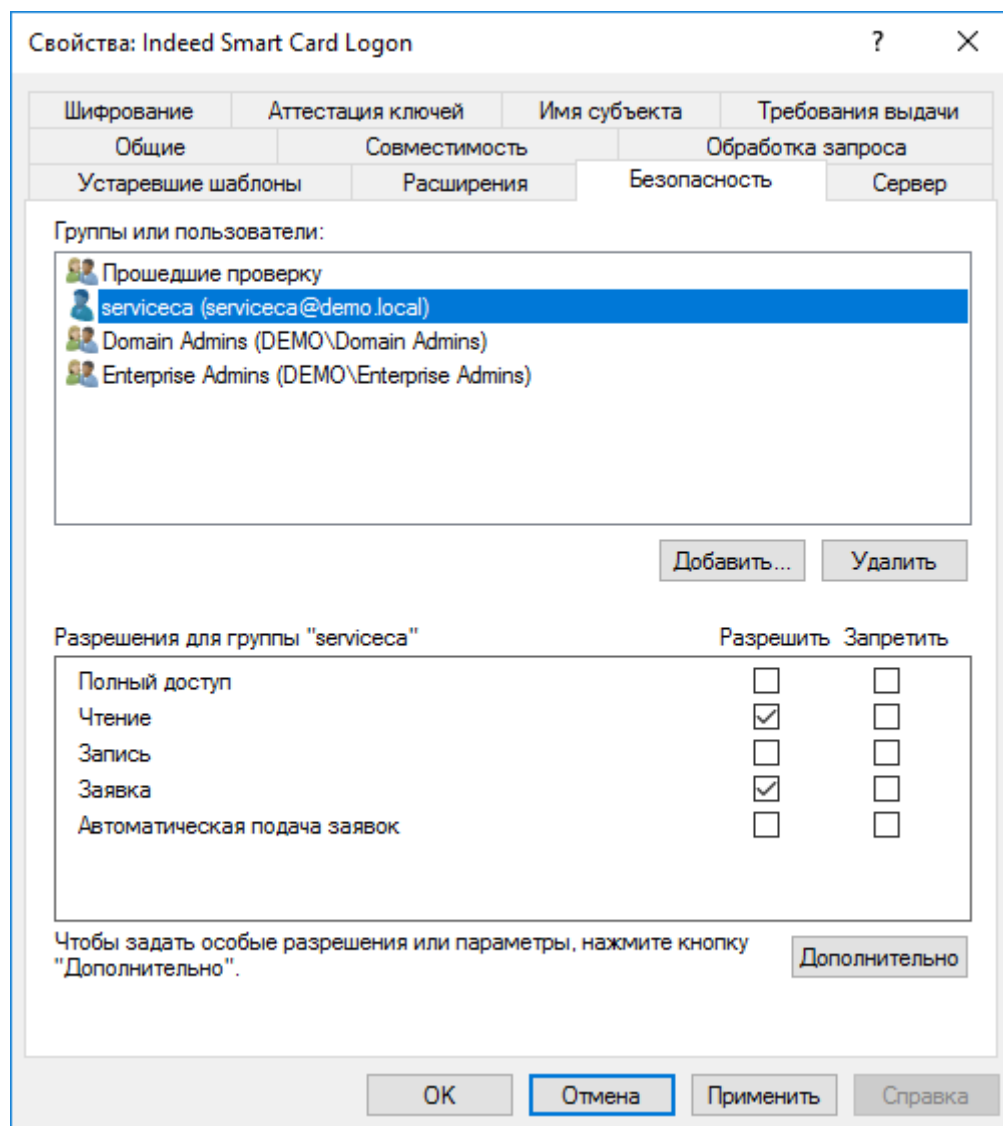
* Элемент управления отключен из-за [параметров совместимости](#).

ОК **Отмена** Применить Справка

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 шаблона **Агент регистрации** (Enrollement Agent) и для всех шаблонов сертификатов, которые будут использоваться Indeed CM.



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