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:

Устаревшие ша	аблоны	Расширени	я Безопа	сность	Сервер
Общие		Совместимост	ь	Обработка з	апроса
Шифрование	Аттеста	ация ключей	Имя субъекта	Требов	ания выдачи
Требовать для ре Одобрения дис Указанного чи Автоматическ	гистрации спетчера с ісла авторі кая регист	: ертификатов ЦС изованных подпис рация не разреше	сей: эна (если требуето	1	й подписи).
В подписи тре	буется ука	зать тип политик	и:		
Политика при	именения				\sim
Политика при	менения:				
Агент запрос	а сертифи	ката			~
				Дot	бавить далить
Требовать для по	вторной ре	егистрации:			
Тех же услови	й, что и для	я регистрации			
Подтвердить с	уществую	щий сертификат			
	обновлен	ие на основе клю	ней (*)		
Разрешить		данные о субъект	е в запросе серт	ификата.	
Разрешить Требует предо	оставлять,	, ,			

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** (Cr yptography) 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 (КВ 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).

Свойства: Копия "В	ход со см	арт-картой"				?	×
Устаревшие ша	блоны	Расширен	Расширения		асность	Серве	ep
Общие		Совместимос	Совместимость		Обработка за	апроса	
Шифрование	Аттеста	ация ключей	Имя с	убъекта	Требова	эния выда	ачи
 Предоставляет Использова обновления Строится на ос Выберите этот п упрощения адми Формат имени Полное различ Включить им 	ся в запри ать данны автомати нове данн параметр инистриро субъекта: ающееся я электро	осе е о субъекте из ической подачи ых Active Directo для повышения вания сертифик имя имя	существу заявок (*) оту согласова катов. ия субъек	ющих сер анности и та	отификатов дл	ви	OB
ылючиль эту ин ☐ Имя электро ☐ DNS-имя ☑ Имя субъект ☐ Имя субъект	формация нной почт а-пользов а-службы	ы ы ателя (UPN) (SPN)	ное ими (
* Элемент управле	ния откли	очен из-за <u>пара</u>	метров со	вместим	ости.		
		ОК	Отг∧	ена	Применить	Спра	вка

Рисунок 8 – Настройка шаблона сертификата Microsoft СА: 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:

Officient Belice Construction Construction

Шифрование	Аттеста	ция ключей	Имя с	субъекта	Требо	вания вы	дачи
Общие	-	Совместимо	сть	F	Обработка	запроса	
Устаревшие шаб	блоны	Расширен	ния	Безопас	ность	Сер	вер
руппы или пользо	ователи:						
🎎 Прошедшие пр	роверку						
🧸 serviceca (serv	viceca@den	no.local)					
Администрато 	оры домена	а (DEMO\Адми	нистратој	ры домена)			
🎎 Администрато	оры предпр	иятия (DEMO\	Админист	граторы пре	едприятия)		
				Дod	бавить	9дали	πь
				Дot	бавить	Удали	πь
^р азрешения для гр	руппы "serv	viceca''		Дod	бавить Разрешит	Удали ъ Запрет	пь ить
^а азрешения для гр Полный доступ	руппы "serv	viceca''		Дot	бавить Разрешит	Удали ъ Запрет	пь ить
^р азрешения для гр Полный доступ Чтение	руппы "serv	viceca''		Дot	бавить Разрешит П	Удали ъ Запрет	пь :ить
^р азрешения для гр Полный доступ Чтение Запись	руппы "serv	viceca''		Дot	бавить Разрешит П	Удали ть Запрет	пь :ить
^а азрешения для гр Полный доступ Чтение Запись Заявка	руппы "serv	viceca''		Дot	бавить Разрешит П П П	Удали ть Запрет П П	пь ить
² азрешения для гр Полный доступ Чтение Запись Заявка Автоматическая	руппы ''serv я подача за	и́сеса''		Дot	бавить Разрешит П П П П	Удали гь Запрет П П П	ть
^у азрешения для гр Полный доступ Чтение Запись Заявка Автоматическая	руппы ''serv я подача за	чісеса'' явок		Дot	бавить Разрешит П П П П	Удали ть Запрет П П П П	пь ить
² азрешения для гр Полный доступ Чтение Запись Заявка Автоматическая	руппы "serv я подача за	исеса'' явок		Дot	бавить Разрешит П П П П	Удали ть Запрет — — — — — —	ть
Разрешения для гр Полный доступ Чтение Запись Заявка Автоматическая Чтобы задать особ	руппы ''serv я подача за бые разрец	исеса" явок	аметры. н	Доб	бавить Разрешит П П П	<u>Удали</u> ть Запрет П П П	ть
Разрешения для гр Полный доступ Чтение Запись Заявка Автоматическая Чтобы задать особ	руппы "serv я подача за бые разрец	иісеса'' явок шения или пара	аметры, н	Доб	бавить Разрешит П П Опку Д	Удали ть Запрет П П П П П П П	пь
Разрешения для гр Полный доступ Чтение Запись Заявка Автоматическая Чтобы задать особ	руппы ''serv я подача за бые разрец	иісеса'' явок цения или пара	аметры, н	Доб	бавить Разрешит П П Опку Д	Удали ть Запрет П П П П П П П П П П П П П	ить

Рисунок 9 – Настройка шаблона сертификата Microsoft CA: Безопасность.

10. Сохраните настройки, нажав ОК.