


Параметры шаблонов сертификатов



Параметры шаблонов поддерживаемых сертификатов приведены в Таблице 2.

Таблица 2 – Настройки шаблонов сертификатов в Indeed Certificate Manager.

Параметр	Описание	MSCA	КПЗ. 0	DSS
Имя	Имя шаблона сертификата.	+	+	+
Сервер	Имя сервера DSS.	-	-	+
УЦ	Имя удостоверяющего центра.	+	+	+
Шаблон сертификата УЦ	Загружается из выбранного удостоверяющего центра.	+	+	+
Префикс имени ключа	<p>Если префикс не задан, то имя контейнера, содержащего ключевую пару, будет сформировано случайным образом.</p> <p>Если указан префикс, то он добавится перед именем контейнера.</p> <p>Значение префикса отображается в Indeed CM (имя контейнера в разделе СКЗИ) и в стороннем ПО для работы с контейнерами закрытого ключа (КриптоПро CSP, клиенты устройств и пр.). Имя контейнера с префиксом может не поддерживаться устройством.</p>	+	+	-
Выпускать сертификат на указанного пользователя	Если опция включена, то в свойствах шаблона отобразится поле поиска пользователя в каталоге ЦР КриптоПро УЦ, на которого будут выпускаться сертификаты. Отображение опции включается в Мастере настройки Indeed CM в разделе Функции системы > КриптоПро УЦ 2.0 . Изменить значение опции при редактировании шаблона нельзя.	-	+	-
Использовать аппаратную криптографию, если поддерживается	<p>Если опция включена, то при выпуске сертификата ключевая пара будет создаваться с использованием криптографических алгоритмов, поддерживаемых устройством.</p> <p>Если устройство не поддерживает аппаратную криптографию, то будет использоваться КриптоПро CSP, установленный на рабочей станции, к которой подключено устройство. Изменить значение опции при редактировании шаблона нельзя.</p>	-	+	-
Создать резервную копию ключа	<p>Если опция включена, то в этом случае при генерации ключевой пары на смарт-карте будет применена опция её архивации. Это значит, что ключевая пара будет сгенерирована на смарт-карте и ее копия (открытый и закрытый ключи) будут отправлены на сервер Indeed CM и затем в хранилище системы. Архивация ключевой пары возможна только один раз.</p> <p>Если опция выключена, то ключ шифрования сразу генерируется на устройстве.</p>	+	+	-

Записывать копию ключа при временной замене устройства	<p>Если опция включена, то копии сертификатов и закрытых ключей будут записаны на временное устройство при замене, как и в случае с постоянной заменой.</p> <p>Если опция отключена, то копии сертификатов и закрытых ключей не будут записаны на временное устройство при замене.</p>	-	+	-
Использовать ключи повторно	Если опция включена, то при обновлении сертификатов, записанных на устройство, существующий ключ шифрования будет использован повторно.	+	-	-
Импортировать ключ, если существует	Если опция включена, то система будет искать существующие ключи на устройстве (для указанного пользователя, УЦ и шаблона) и использовать их, не создавая новых ключей. Импорт ключа невозможен, если устройство будет инициализировано перед выпуском.	+	+	-
Не удалять ключ при обновлении /очистке устройства	<p>Если опция включена, то при обновлении устройства истекающий (истекший) сертификат не будет удален с устройства и отозван на УЦ. Будет запрошен новый сертификат с новым закрытым ключом и записан на устройство.</p> <div>  Для шаблона сертификата MSCA: <p>Если включена опция Использовать ключи повторно, то при обновлении устройства истекающий (истекший) сертификат будет удален с устройства. На устройство будет запрошен и записан новый сертификат со старым закрытым ключом.</p> </div> <p>Истекающий (истекший) сертификат будет удален, если устройство изъято с инициализацией.</p>	+	+	-
Импортировать сертификат, если существует	Если опция включена, то система будет искать существующие сертификаты (для указанного пользователя, УЦ и шаблона) и использовать их, не создавая новых.	-	-	+
Отзывать сертификат при отзыве или выключении устройства	<p>Если опция включена, то сертификаты пользователя будут отозваны при выключении или отзыве устройства.</p> <p>Если опция выключена, то при выключении или отзыве устройства сертификаты не будут отозваны.</p>	+	+	+
Устанавливать сертификат в локальное хранилище	Если опция включена, то при выпуске (обновлении) устройства через Self Service записанные на него сертификаты добавятся в локальное хранилище пользователя на рабочей станции.	+	+	-

Публиковать сертификат в каталоге пользователей	<p>Если опция включена, то выпущенный сертификат опубликуется в профиле пользователя в Active Directory на вкладке Опубликованные сертификаты (Published Certificates). Сертификат удалится из профиля при включении опции Удалять опубликованный сертификат при отзыве устройства.</p> <div>  Необходимо наличие прав на Запись: userCertificate (Write: userCertificate) для сервисной учетной записи. </div>	-	+	+
Публиковать сертификат в файловое хранилище	Если опция включена, то выпущенный сертификат будет помещен в сетевое хранилище (папку). При отзыве устройства сертификаты из хранилища не удаляются.	-	+	-
Публиковать сертификат в ЦФТ	Если опция включена, то выпущенный сертификат будет помещен в базу приложений ЦФТ. При отзыве устройства сертификаты из базы приложений ЦФТ не удаляются.	-	+	-
Публиковать список отозванных сертификатов	Если опция включена, то при выключении, включении и отзыве устройств будет выполняться внеочередная публикация списка отозванных сертификатов (CRL).	+	+	-
Использовать комментарий устройства в качестве комментария пользователя к запросу на сертификат	Если опция включена, то в поле "Заметки пользователя" запроса сертификата будет добавлен текст комментария устройства.	-	+	-
Автоматически одобрять запрос на сертификат	<p>Если опция включена, то запросы на сертификат будут автоматически одобрены.</p> <p>Если опция выключена, то для завершения выпуска потребуется дождаться одобрения запроса на УЦ или отменить выпуск, если запрос будет отклонен.</p>	+	+	+
Автоматически одобрять подписанный запрос на обновление сертификата	<p>Если опция включена, то запрос на обновление сертификата будет одобрен автоматически.</p> <p>Если опция выключена, то для обновления сертификата потребуется дождаться одобрения запроса на УЦ.</p>	+	+	+

Отслеживаемые атрибуты пользователя	<p>Укажите атрибуты пользователя при изменении которых необходимо обновление сертификата:</p> <ul style="list-style-type: none"> • Общее Имя(CN) • E-mail • UPN-имя пользователя <div data-bbox="399 387 1129 710" style="border: 1px solid red; padding: 10px; margin-top: 10px;"> <p> Изменение E-mail приводит к обновлению сертификата в случае, если этот атрибут включен в свойствах шаблона сертификата в Microsoft CA на вкладке Имя субъекта (Subject Name) опции Включить имя электронной почты в имя субъекта (Include e-mail name in subject name) и Имя электронной почты (E-mail name).</p> </div> <div data-bbox="399 734 1129 866" style="border: 1px solid green; padding: 10px; margin-top: 10px;"> <p> Дополнительный список отслеживаемых атрибутов пользователей задается в Мастере настройки Indeed CM в разделе Обновляемые атрибуты.</p> </div>	+	+	-
Шаблон печати запроса на сертификат	<p>Если параметр: Не задано, то используется стандартный шаблон печати запроса на сертификат.</p> <p>Если в систему добавлены Шаблоны печати запроса сертификата, то выберите шаблон из выпадающего меню.</p>	+	+	-
Шаблон печати сертификата	<p>Если параметр: Не задано, то используется стандартный шаблон печати сертификата.</p> <p>Если в систему добавлены Шаблоны печати сертификата, то выберите шаблон из выпадающего меню.</p>	+	+	-
Использовать по умолчанию	<p>Если опция включена, то сертификат отмечается как используемый по умолчанию для входа в операционную систему Windows XP.</p>	+	-	-
Период обновления (дней)	<p>Период времени, в течение которого сертификат и закрытый ключ можно обновить. Значение по умолчанию – 30 дней.</p>	-	+	+
Необязательный сертификат	<p>Если опция включена, то при выпуске устройства появится возможность выбора сертификатов для записи из числа отмеченных, как необязательные.</p> <p>Если опция выключена, то сертификат считается обязательным для записи на устройство.</p>	+	+	+