



JaCarta для Microsoft Windows

Руководство по внедрению

Версия 2.0

Оглавление

О документе.....	4
Назначение документа.....	4
На кого ориентирован данный документ	4
Контакты	4
Авторские права, товарные знаки, ограничения.....	5
Лицензионное соглашение	6
1. Введение	8
2. Системные требования.....	10
Требования к серверам.....	10
Требования к программному обеспечению	10
Требования к аппаратному обеспечению	10
Требования к рабочим станциям.....	10
Требования к программному обеспечению	10
Требования к аппаратному обеспечению	11
3. Технологии безопасности.....	12
Использование цифровых сертификатов и полный отказ от паролей	12
Общие сведения	12
Процедуры выдачи сертификатов.....	12
Шаблоны сертификатов	12
Настройка центра сертификации.....	13
Объект групповой политики для автоматической выдачи сертификатов.....	26
Сертификат агента регистрации для централизованной выдачи сертификатов	28
Получение сертификата пользователя и запись его в память электронного ключа JaCarta.....	31
Вход в домен с электронным ключом JaCarta.....	41
Блокирование компьютера и принудительный выход пользователя при отсоединении электронного ключа JaCarta.....	44
Запуск приложений от имени другого пользователя	45
Организация VPN-соединения для доступа к информационным ресурсам....	46
Настройка сервера маршрутизации и удалённого доступа	46
Установка сертификата сервера	47
Установка роли Службы политики сети и доступа	49
Настройка служб политики сети и доступа	50
Настройка учётной записи пользователя	56
Настройка рабочей станции.....	57
Подключение к удалённому рабочему столу.....	61
Настройка рабочих станций и серверов	61

Действия пользователя	62
Доступ к информационным ресурсам по HTTPS.....	65
Общие сведения.....	65
Настройка сервера	66
Настройка доступа к Outlook Web Access / Outlook Web App	70
Действия пользователя	71
Защита электронной почты.....	71
Возможности электронных ключей JaCarta по защите электронной корреспонденции.....	71
Microsoft Outlook 2010 (из пакета Microsoft Office 2010).....	71
Цифровая подпись и шифрования при использовании OWA	73
Шифрование данных на жёстком диске (EFS).....	76
Общие сведения.....	76
Запись сертификата EFS в память электронного ключа JaCarta.....	76
Зашифрование данных на жёстком диске	78
Шифрование диска BitLocker с использованием JaCarta.....	81
Общие сведения.....	81
Системные требования.....	81
Дополнительная настройка шаблона сертификата	82
Настройка компьютера пользователя.....	87
Шифрование дисков.....	91
Проверка предоставления доступа к зашифрованному диску	98
Известные проблемы при шифровании дисков средствами BitLocker с использованием JaCarta и их решение.....	101
4. Установка служб сертификации (Windows Server 2008)	105
Основные отличия между автономным ЦС и ЦС предприятия	111
Шаблоны сертификатов	112
5. Настройка Mozilla Firefox	114
Установка сертификата центра сертификации в Mozilla Firefox	114
Настройка Mozilla Firefox.....	116
Настройка конфигурации Mozilla Firefox	118
Действия пользователя.....	118

О документе

Назначение документа

Настоящий документ представляет собой руководство по внедрению и использованию электронных ключей JaCarta в среде Windows для обеспечения безопасности в сетях, включающих серверы и клиентские рабочие станции. Электронные ключи JaCarta можно использовать с операционными системами Windows XP/Server 2003/Vista/Server 2008/7.

Действия по внедрению электронных ключей JaCarta представлены на примерах операционных систем Windows Server 2008 R2 Enterprise и Windows 7. Для осуществления аналогичных действий на операционных системах Windows XP, Windows Server 2003 и Windows Vista следует обратиться к документации Microsoft.

Следование приведённым в настоящем документе инструкциям является верным, но не всегда единственно возможным способом установки и работы с данным решением. В этом смысле они носят рекомендательный характер. Рассмотрение всех возможных способов настройки и использования данного решения не входит в задачи настоящего документа.

На кого ориентирован данный документ

Для эффективного внедрения и управления электронными ключами JaCarta в сетевой среде Windows требуется квалифицированный системный администратор, обладающий навыками администрирования вычислительных сетей, включающих серверы Windows Server 2008 R2 Enterprise и рабочие станции Windows 7.

Контакты

Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р. Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: <https://www.aladdin-rd.ru>

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:
www.aladdin-rd.ru/support/index.php.

Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р. Д."

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р. Д." обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р. Д."

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

Ограничение ответственности.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены ЗАО "Аладдин Р. Д." без предварительного уведомления.

ЗАО "Аладдин Р. Д." не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

ЗАО "Аладдин Р. Д." не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе ЗАО "Аладдин Р. Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

ЗАО "Аладдин Р. Д." НЕ НЕСЁТ ОТВЕТСТВЕННОСТИ (КАК В СИЛУ ДОГОВОРА, ГРАЖДАНСКОГО ПРАВОНАРУШЕНИЯ, ВКЛЮЧАЯ ХАЛАТНОСТЬ, ТАК И В ЛЮБОЙ ИНОЙ ФОРМЕ ПЕРЕД ВАМИ ИЛИ ЛЮБОЙ ТРЕТЬЕЙ СТОРОНОЙ ЗА ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ (ВКЛЮЧАЯ КОСВЕННЫЕ, ФАКТИЧЕСКИЕ ИЛИ ПОБОЧНЫЕ УБЫТКИ), ВКЛЮЧАЯ БЕЗ ОГРАНИЧЕНИЙ ЛЮБЫЕ ПОТЕРИ ИЛИ УБЫТКИ ПРИБЫЛЬНОСТИ БИЗНЕСА, ПОТЕРЮ ДОХОДНОСТИ ИЛИ РЕПУТАЦИИ, УТРАЧЕННУЮ ИЛИ ИСКАЖЁННУЮ ИНФОРМАЦИЮ ИЛИ ДОКУМЕНТАЦИЮ ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ ЗАО "Аладдин Р. Д." БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

Государственное регулирование и экспортный контроль.

Описываемый в данном документе продукт (или продукты) может являться или содержать в себе средство криптографической защиты информации (СКЗИ), являющееся предметом экспортного контроля.

Вы соглашаетесь с тем, что продукт не будет поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону образом.

Вы гарантируете, что будете соблюдать накладываемые на экспорт и реэкспорт продукта ограничения.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

© ЗАО "Аладдин Р. Д.", 1995—2018. Все права защищены.

Лицензионное соглашение

Пожалуйста, внимательно прочитайте данное лицензионное соглашение прежде, чем использовать содержимое данного комплекта и/или прежде, чем загружать или устанавливать программное обеспечение.

Все указания по использованию программного обеспечения, предоставляемые Закрытым акционерным обществом "Аладдин Р. Д." (или любым его дочерним предприятием – каждое из них упоминаемое как "компания"), подчиняются и будут подчиняться условиям, оговоренным в данном соглашении. Загружая данное программное обеспечение (как определено далее по тексту) и/или устанавливая данное программное обеспечение на Ваш компьютер и/или используя данное программное обеспечение иным способом, Вы принимаете данное соглашение и соглашаетесь с его условиями.

Если Вы не согласны с данным соглашением, не загружайте и/или не устанавливайте данное программное обеспечение и незамедлительно (не позднее 7 (семи) дней с даты ознакомления с настоящим текстом) верните этот продукт в ЗАО "Аладдин Р. Д.", удалите данное программное обеспечение и все его части со своего компьютера и не используйте его никоим образом.

Настоящее лицензионное соглашение (далее "Соглашение") является договором, заключённым между Вами (физическим или юридическим лицом) — конечным пользователем (далее "Пользователь") — и ЗАО "Аладдин Р. Д." (далее "Компания") относительно передачи неисключительного права на использование настоящего программного обеспечения, являющегося интеллектуальной собственностью Компании.

Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ. Программное обеспечение, включая все переработки, исправления, модификации, дополнения, обновления и/или усовершенствования к нему (далее по всему тексту и любой его части определяемое как Программное обеспечение или ПО), и связанная с ним документация предназначена НЕ ДЛЯ ПРОДАЖИ и является и остаётся исключительной собственностью Компании.

Все права на интеллектуальную собственность (включая, без ограничений, авторские права, коммерческую тайну, товарные знаки, и т.д.), подтверждённые или включённые в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

Данное соглашение не передаёт Вам права на Программное обеспечение, а лишь предоставляет ограниченное право на использование, которое подлежит отмене согласно условиям данного Соглашения. Ничто в данном Соглашении не подтверждает отказ Компании от прав на интеллектуальную собственность по какому бы то ни было законодательству.

Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного Соглашения.

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;
- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;
- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;
- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

Программное обеспечение должно использоваться и обслуживаться строго в соответствии с описаниями и инструкциями Компании, приведёнными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (<http://developer.aladdin-rd.ru/>).

Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;
- встраивать ПО любым способом в продукты и решения Пользователя;
- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и импортом таких средств в другие страны. В частности, ограничения и дополнительные требования могут возникать при распространении ПО через магазины приложений, содержащие различные приложения для мобильных устройств.

Условия использования, изложенные в настоящем соглашении, действуют в отношении всего содержимого ПО, в частности в отношении:

- дизайна (графики, расположения элементов оформления и т.п.);
- всех иных элементов, в том числе изображений, фонограмм, текстов.

Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

Компания сохраняет за собой все исключительные права на ПО и входящие в него компоненты, включая права на предоставление неисключительных и исключительных прав третьим лицам.

Пользователь вправе осуществлять использование ПО в пределах, предусмотренных настоящим Соглашением, исключительно на территории Российской Федерации.

Обслуживание и поддержка

Компания не несёт обязательств по предоставлению поддержки, обслуживания, модификации или выходу новых релизов ПО.

Ограниченная гарантия

Компания гарантирует, что программное обеспечение с момента приобретения его Вами в течение 12 (двенадцати) месяцев будет функционировать в полном соответствии с его

технической/эксплуатационной документацией, при условии, что ПО будет использоваться на компьютерном аппаратном обеспечении и с операционной системой, для которой оно было разработано.

Отказ от гарантий

Компания не гарантирует, что программное обеспечение будет соответствовать Вашим желаниям и требованиям, или что его работа будет бесперебойной или безошибочной. В объёме, предусмотренном законодательством РФ, компания открыто отказывается от всех гарантий, не оговоренных здесь, от всех иных подразумеваемых гарантий. Ни один из дилеров, дистрибьюторов, продавцов, агентов или сотрудников компании не уполномочен производить модификации, расширения или дополнения к данной гарантии.

Если Вы произвели какие-либо модификации ПО или любой из его частей во время гарантийного периода, ПО подверглось повреждению, неосторожному или неправильному обращению, если Вы нарушили любое из условий настоящего Соглашения, то гарантия, упомянутая выше в разделе 5, будет немедленно прекращена.

Гарантия недействительна, если ПО используется в сочетании с иным аппаратным и/или программным обеспечением, отличным от описанных в технической/эксплуатационной документации, или используется на компьютере с любым установленным нелегальным программным обеспечением.

Ограничение возмещения

В случае нарушения гарантии, оговоренной выше, Компания может по собственному усмотрению:

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;
- возместить стоимость, выплаченную Вами за ПО.

Гарантийные требования должны быть выставлены в письменном виде в течение гарантийного периода, но не позднее 7 (семи) дней с момента обнаружения дефекта, и содержать в себе подтверждения, удовлетворяющие Компанию. Всё ПО (все экземпляры, имеющиеся у Вас) должно быть возвращено Компании и отправлено возвращающей стороной с оплаченной стоимостью перевозки и, при необходимости, страховки. Экземпляры ПО должны быть отправлены с копией платёжных документов и накладных.

Исключение косвенных убытков

Стороны признают, что Программное обеспечение не может быть полностью лишено ошибок. Компания не несёт ответственности (как в силу договора, гражданского правонарушения, включая халатность, так и в любой иной форме) перед Вами или любой третьей стороной за любые потери или убытки (включая косвенные, фактические, побочные или потенциальные убытки), включая, без ограничений, любые потери или убытки прибыльности бизнеса, потерю доходности или репутации, утраченную или искажённую информацию или документацию вследствие какого-либо использования данного программного обеспечения и/или любой компоненты данного ПО, даже если компания письменно уведомлена о возможности подобных убытков.

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов

или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного обеспечения не будет превышать суммы, выплаченной вами ЗАО "Аладдин Р. Д." за это ПО.

Прекращение действия соглашения

В случае невыполнения Вами условий данного Соглашения действие Вашей лицензии и настоящего Соглашения будет прекращено.

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;
- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

Данное Соглашение должно быть истолковано и определено в соответствии с законодательством Российской Федерации (за исключением конфликта применения правовых норм), и только российский суд уполномочен осуществлять правосудие в любых конфликтах и спорах, вытекающих из данного Соглашения. Невозможность для любой из сторон воспользоваться любым из прав, предоставленных ей по данному Соглашению, или принять меры против другой стороны в случае любого нарушения своих обязательств по Соглашению не должно рассматриваться как отказ этой стороны от последующего принуждения к признанию своих прав или совершению последующих действий в случае дальнейших нарушений.

Государственное регулирование и экспортный контроль

Вы соглашаетесь с тем, что ПО не будет Вами поставляться, передаваться или экспортироваться в какую-либо страну, а также использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

Разное

Настоящее Соглашение представляет собой полное соглашение, относящееся к данной лицензии, и может быть изменено только посредством письменного соглашения, подписанного обеими сторонами. Если выполнение какого-либо условия настоящего Соглашения представляется невозможным, такое условие будет скорректировано только в пределах, обеспечивающих возможность выполнения данного условия.

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

1. Введение

Применение смарт-карт и USB-токенов JaCarta для аутентификации пользователей, доступа к внутрикорпоративным и интернет-ресурсам, защиты документов и почтовой переписки позволяет полностью раскрыть потенциал Windows Server 2008 R2 Enterprise как надёжной платформы для ведения современного бизнеса.

Использование аутентификации на основе сертификатов X.509 в сетях на базе серверов Windows Server 2008 R2 Enterprise позволяет полностью отказаться от парольной аутентификации. Внедрение решения — это кардинальное снижение влияния человеческого фактора на безопасность системы.

Примечание

*Подробная информация по настройке Windows Server 2008 и рабочих станций, а также информация, касающаяся использования цифровых сертификатов, представлена в книгах **Ошибка! Источник ссылки не найден.** и **Ошибка! Источник ссылки не найден.** (см. "Список литературы" в конце данного документа).*

Использование электронных ключей JaCarta позволяет извлекать наибольшую пользу из новых возможностей Windows Server 2008 R2 Enterprise.

- Пользовательские шаблоны сертификатов: единожды настроенный шаблон сертификата пользователя делает процедуру запроса сертификата наглядной и удобной.
- Аутентификация с использованием смарт-карт при подключении к удалённому рабочему столу: администратор может управлять сервером удалённо, аутентифицируясь с помощью своего электронного ключа JaCarta. При использовании Windows Server 2008 R2 Enterprise в качестве сервера приложений аутентификация пользователей на сервере также осуществляется с помощью электронного ключа JaCarta.

Помимо регистрации пользователя в домене Windows и использования подключения к удалённому рабочему столу (RDP), возможности электронных ключей JaCarta могут использоваться для дополнительной защиты:

- VPN-соединений;
- доступа к информационным ресурсам посредством HTTPS (SSL);
- электронной почты;
- шифрования данных на жёстком диске (EFS).

Один и тот же электронный ключ JaCarta можно использовать для аутентификации в домене Windows и для работы с множеством приложений, использующих электронные ключи JaCarta. Это позволяет уменьшить суммарную стоимость владения. При использовании российских сертифицированных СКЗИ электронные ключи JaCarta могут использоваться как средство защищённого хранения ключевой информации. Решение может быть внедрено как на небольших предприятиях, так и в крупных корпорациях с инфраструктурой сети любой сложности.

В данном документе в качестве примера используется следующая конфигурация JC-Client и дополнительного ПО:

Серверная операционная система	Windows Server 2008 R2 Enterprise
Клиентская операционная система	Windows 7 (64-бит)
Режим работы центра сертификации	ЦС Предприятия
Версия используемых шаблонов сертификатов	Шаблоны версии 2 (доступны начиная с версии ОС Windows Server 2003 и выше)
Версия MS Outlook	2010
Используемый браузер	Internet Explorer 8
Режим установки JC-Client	CSP (поставщик служб шифрования: Athena ASECard Crypto CSP)

2. Системные требования

Требования к серверам

Требования к программному обеспечению

Операционная система

Решение предполагает использование серверов с установленной операционной системой Windows Server 2008 R2 Enterprise. По меньшей мере, один из серверов должен являться контроллером домена, а другие серверы должны входить в лес доменов Windows в качестве контроллеров домена (доменов) или рядовых серверов.

Internet Information Services

На сервере, на котором будет развёрнут центр сертификации, должна быть установлена роль **Веб-сервер (IIS)**. Это необходимо для корректной работы Web-узла центра сертификации. (Если данная роль не установлена, необходимые компоненты будут установлены во время установки служб сертификации Active Directory.) Информацию по установке IIS см. в документации Windows Server 2008 R2 Enterprise.

Центр сертификации

Для работы с сертификатами необходимо иметь предустановленный корневой или подчинённый центр сертификации предприятия. Об установке центра сертификации см. документацию Windows Server 2008 R2 Enterprise.

Драйвер устройства чтения смарт-карт

В случае использования устройства чтения смарт-карт на компьютере должен быть установлен драйвер этого устройства.

JC-Client

На каждом компьютере, на котором используются электронные ключи JaCarta, должен быть установлено ПО JC-Client версии 6.0 или выше. (Информация, касающаяся установки и настройки JC-Client, представлена в документе "*JC-Client. Руководство администратора*".)

Требования к аппаратному обеспечению

Сервер должен удовлетворять требованиям к аппаратному обеспечению, изложенным в документации соответствующей редакции Windows Server 2008 R2 Enterprise.

Каждый компьютер, на котором используются смарт-карты JaCarta, должен быть оборудован устройством чтения смарт-карт.

На каждом компьютере, на котором используются USB-токены JaCarta, должен быть доступен хотя бы один свободный порт USB.

Требования к рабочим станциям

Требования к программному обеспечению

Операционная система

На каждой рабочей станции должна быть установлена операционная система Windows 7. Каждая рабочая станция должна входить в домен (функциональный уровень домена Windows Server 2003 или Windows Server 2008).

Драйвер устройства чтения смарт-карт

В случае использования устройства чтения смарт-карт на компьютере должен быть установлен драйвер этого устройства.

JC-Client

На каждом компьютере, на котором используются электронные ключи JaCarta, должен быть установлено ПО JC-Client версии 6.0 или выше. (Информация, касающаяся установки и настройки JC-Client, представлена в документе "*JC-Client. Руководство администратора*".)

Требования к аппаратному обеспечению

Рабочие станции должны удовлетворять требованиям к аппаратному обеспечению, изложенным в документации к Windows 7.

Каждый компьютер, на котором используются смарт-карты JaCarta, должен быть оборудован устройством чтения смарт-карт.

На каждом компьютере, на котором используются USB-токены JaCarta, должен быть доступен хотя бы один свободный порт USB.

3. Технологии безопасности

Использование цифровых сертификатов и полный отказ от паролей

Общие сведения

Применение электронных ключей JaCarta снимает необходимость в использовании паролей для регистрации в сети, а также обеспечивает пользователям удобство работы и мобильность. При этом аутентификация пользователя производится при помощи сертификата открытого ключа (расширение PKINIT спецификации протокола Kerberos), который хранится в памяти электронного ключа JaCarta и привязывается к учётной записи пользователя в Active Directory.

Примечание:

Разные версии ОС Windows Server 2008 различаются в том, что касается управления службами сертификации. Информация о доступности компонентов и возможностей представлена в приложении "Поддержка функций центра сертификации в различных версиях Windows Server 2008" в конце данного документа.

Процедуры выдачи сертификатов

В зависимости от правил, принятых в вашей организации, вы можете выбрать одну из трёх процедур выдачи сертификатов:

- автоматическая выдача сертификатов (пользователю автоматически предлагается получить сертификат при входе в систему);
- децентрализованная выдача сертификатов (каждый пользователь составляет запрос и записывает сертификат в память своего электронного ключа JaCarta самостоятельно);
- централизованная выдача сертификатов (для получения сертификата необходимо участие агента подачи заявок).

Для разных групп и пользователей вы можете использовать разные процедуры выдачи сертификатов. Процедуры выдачи сертификатов, доступные для данного пользователя, определяются настройками центра сертификации.

Шаблоны сертификатов

Для удобства работы с электронными ключами JaCarta и для максимально эффективного применения новых возможностей Windows Server 2008 R2 Enterprise при настройке центра сертификации будут созданы два шаблона сертификата пользователя, которые будут использоваться при издании сертификатов для пользователей электронных ключей JaCarta:

- *Пользователь JaCarta* — шаблон для автоматической и децентрализованной выдачи сертификатов;
- *Пользователь JaCarta (централизованная процедура)* — шаблон для централизованной выдачи сертификатов.

Если вы не планируете использовать централизованную процедуру выдачи сертификатов, то можете не создавать шаблон *Пользователь JaCarta (централизованная процедура)* или не включать его. Если вы планируете использовать только централизованную процедуру, то можете не создавать шаблон *Пользователь JaCarta* или не включать его.

По желанию вы можете выбрать для шаблонов другие имена. Указанные имена используются в настоящем документе для наглядности.

Настройка центра сертификации

Компьютер, с которого осуществляется настройка

Настроить центр сертификации для работы с электронными ключами JaCarta вы можете как на самом сервере, так и с любого компьютера, входящего в домен. Компьютер, с которого осуществляется настройка центра сертификации, должен работать под управлением операционной системы Windows Server 2008 R2 Enterprise или Windows 7.

В последнем случае на клиентском компьютере необходимо установить средства удалённого администрирования сервера (обновление KB958830, доступно для загрузки на сайте Microsoft).

План настройки

Настройка центра сертификации предприятия состоит из трёх этапов:

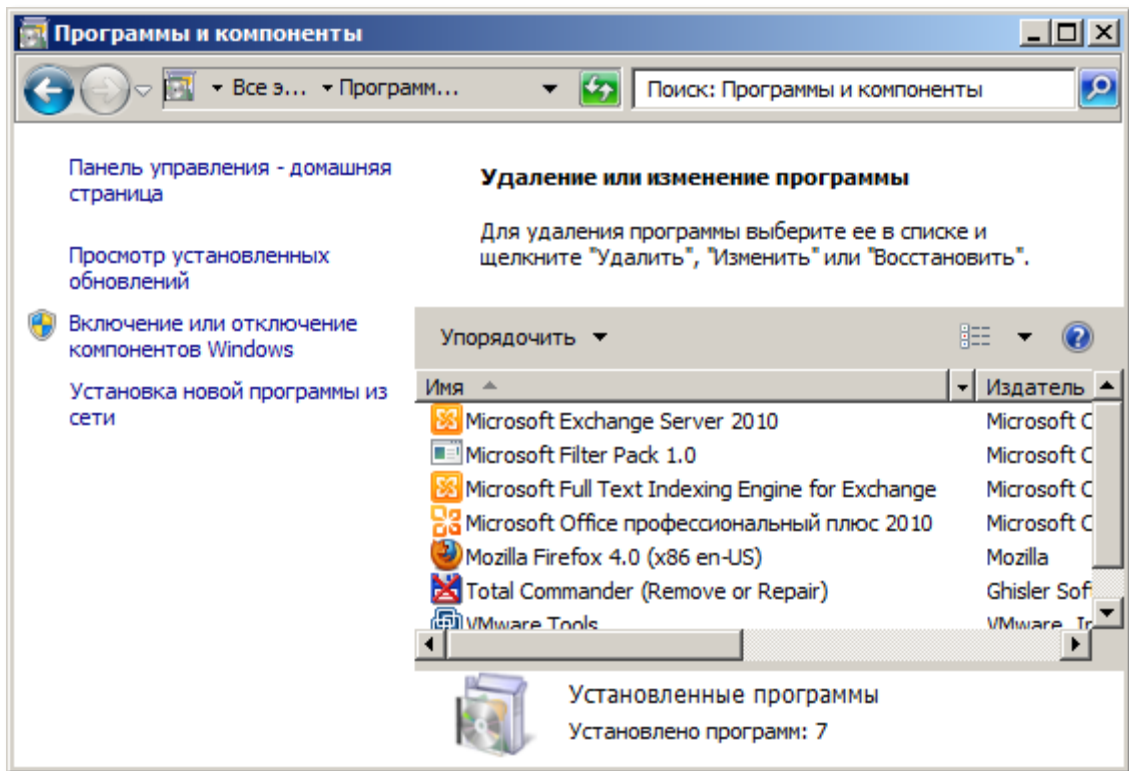
- 1 **Подготовка консоли.** Этот этап необходим, если на вашем компьютере нет готовой консоли для управления центром сертификации.
- 2 **Создание шаблонов сертификатов.** В зависимости от процедур получения сертификатов, которые вы собираетесь использовать, создайте шаблоны сертификатов, соответствующие этим процедурам. Внимательно относитесь к выбору параметров создаваемых шаблонов. Все сертификаты, созданные по шаблону, будут иметь срок действия, указанный в соответствующем шаблоне.
- 3 **Включение шаблонов сертификатов.** Для того чтобы начать использование созданных вами шаблонов сертификатов, необходимо включить их. Для централизованной процедуры выдачи сертификатов необходимо также, чтобы был включен стандартный шаблон **Агент регистрации**.

Подготовка консоли

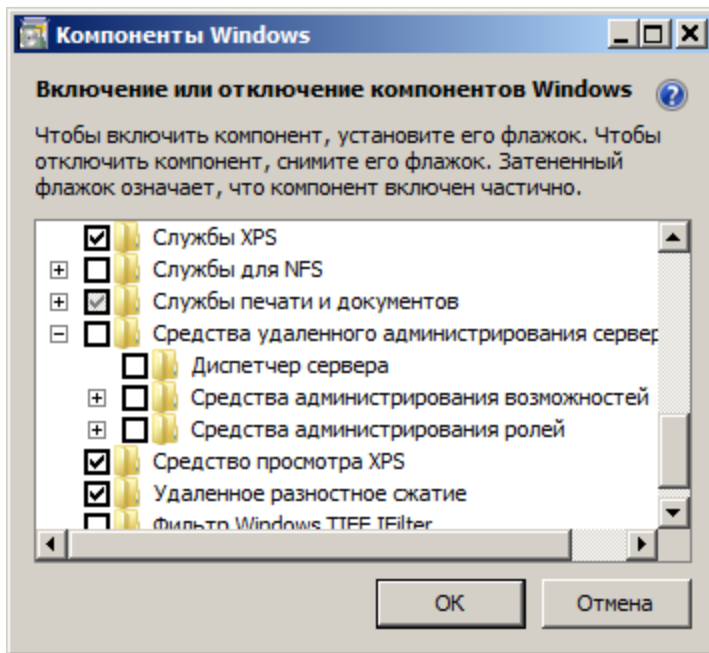
Если на вашем компьютере нет готовой консоли для управления центром сертификации, подготовьте ее, выполнив следующие шаги.

- 1 Загрузите с сайта Microsoft и установите средства удалённого администрирования сервера (обновление KB958830).
- 2 После установки средств удалённого администрирования сервера на клиентском компьютере необходимо включить соответствующий компонент управления центром сертификации. Для этого Выберите **Пуск > Все программы > Панель управления > Программы и компоненты**.

Отобразится следующее окно.

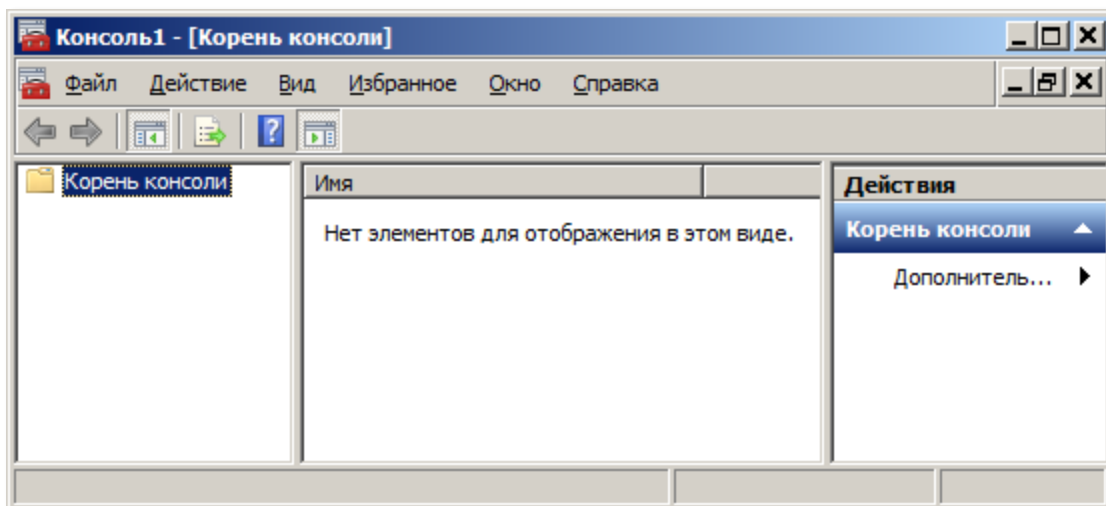


3 В левой части окна щёлкните на ссылке Включение или отключение компонентов Windows. Отобразится следующее окно.



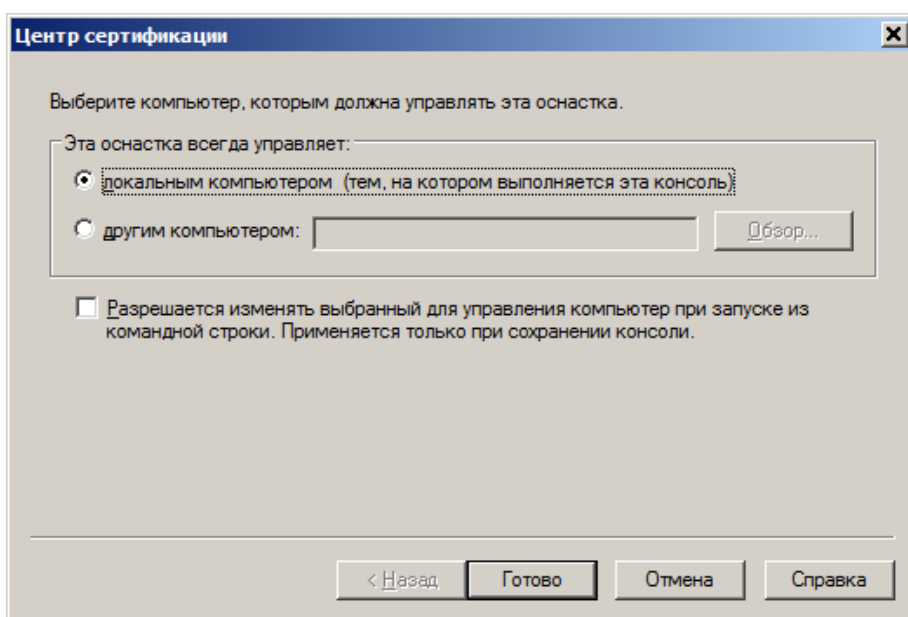
- 4 Разверните ветвь **Средства удалённого администрирования сервера > Средства администрирования ролей > Средства служб сертификации Active Directory** и отметьте **Средства центра сертификации**.
- 5 После включения компонента нажмите ОК и закройте окно компонентов Windows.
- 6 Добавьте оснастку управления центром сертификации в консоль управления. Для этого выберите **Пуск > Все программы > Стандартные** щёлкните правой кнопкой на пункте **Командная строка** и выберите **Запуск от имени администратора**.
- 7 В окне командной строки введите **mmc** и нажмите клавишу **ВВОД**.

Отобразится следующее окно.

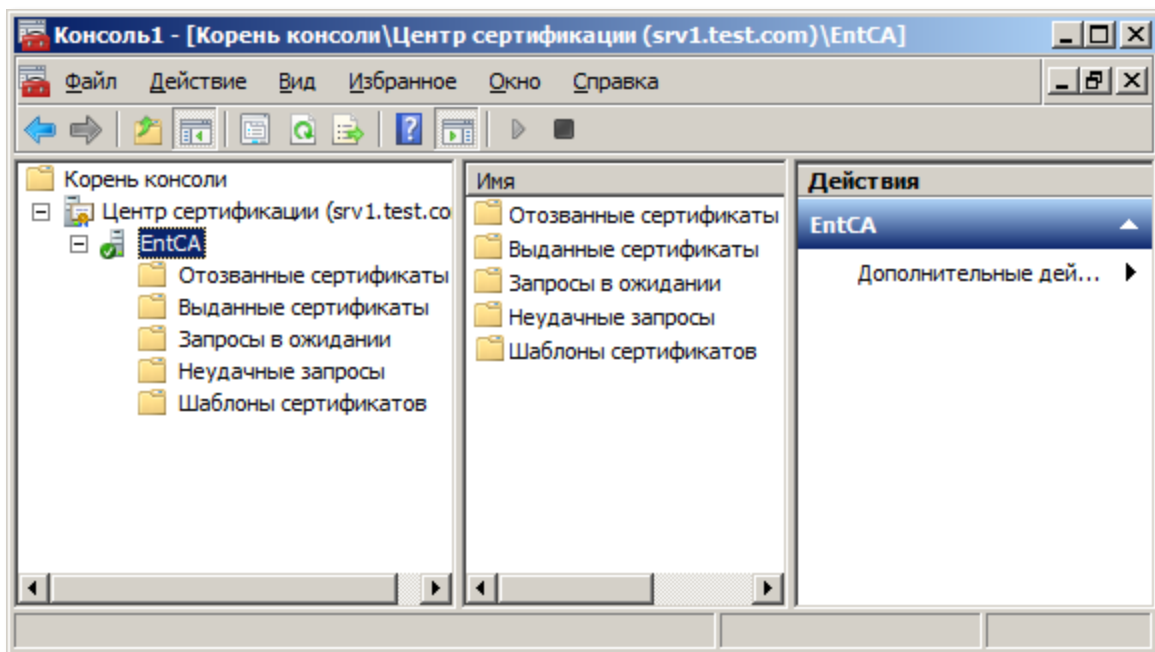


- 8 В панели управления выберите **Файл > Добавить или удалить оснастку**.
- 9 В отобразившемся окне из списка доступных оснасток выберите **Центр сертификации** и нажмите **Добавить**.

Отобразится следующее окно.



- 10 Выберите **другим компьютером** и в соответствующем поле введите имя компьютера, на котором находится центр сертификации. (При необходимости воспользуйтесь кнопкой Обзор.)
- 11 Нажмите **Готово**.
- 12 В окне добавления и удаления оснасток нажмите **ОК**.
- 13 Элементы управления центром сертификации отобразятся в окне консоли управления (см. изображение ниже).



- 14 Сохраните консоль с добавленной оснасткой. Для этого в панели управления выберите **Файл > Сохранить как**.
- 15 В окне сохранения укажите имя (например, "Центр сертификации"), путь сохранения (например, Рабочий стол) и нажмите **Сохранить**.
- 16 Консоль сохранена и впоследствии может быть запущена двойным щелчком мыши.

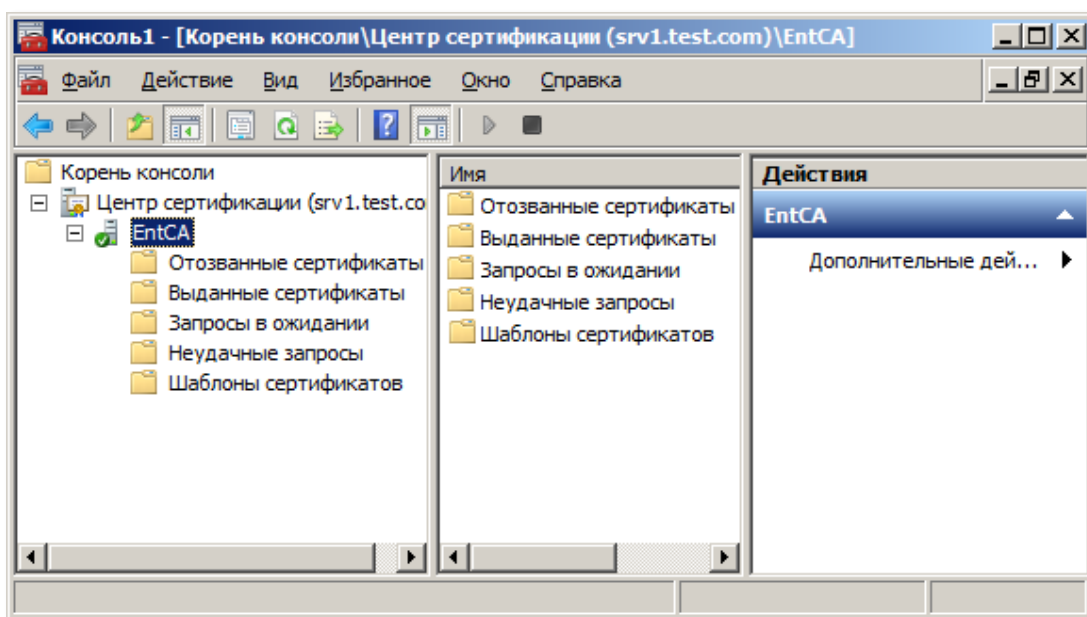
Запуск консоли управления центром сертификации

Чтобы получить доступ к управлению центром сертификации.

- Непосредственно на сервере (Windows Server 2008 R2 Enterprise).
- Выберите **Пуск > Все программы > Администрирование > Центр сертификации (Start > All Programs > Administrative Tools > Certification Authority)**.
- На клиентском компьютере (Windows 7).

Запустите сохранённую ранее консоль управления центром сертификации.

Отобразится окно следующего вида.



Создание шаблона сертификата для автоматической и децентрализованной процедуры выдачи сертификатов

Если вы планируете использовать автоматическую или (и) децентрализованную процедуру выдачи сертификатов, создайте шаблон сертификата *Пользователь JaCarta*. Создание и последующее использование этого шаблона совершенно необходимо для автоматической процедуры выдачи сертификатов. Использование того же шаблона в децентрализованной процедуре даёт два основных преимущества:

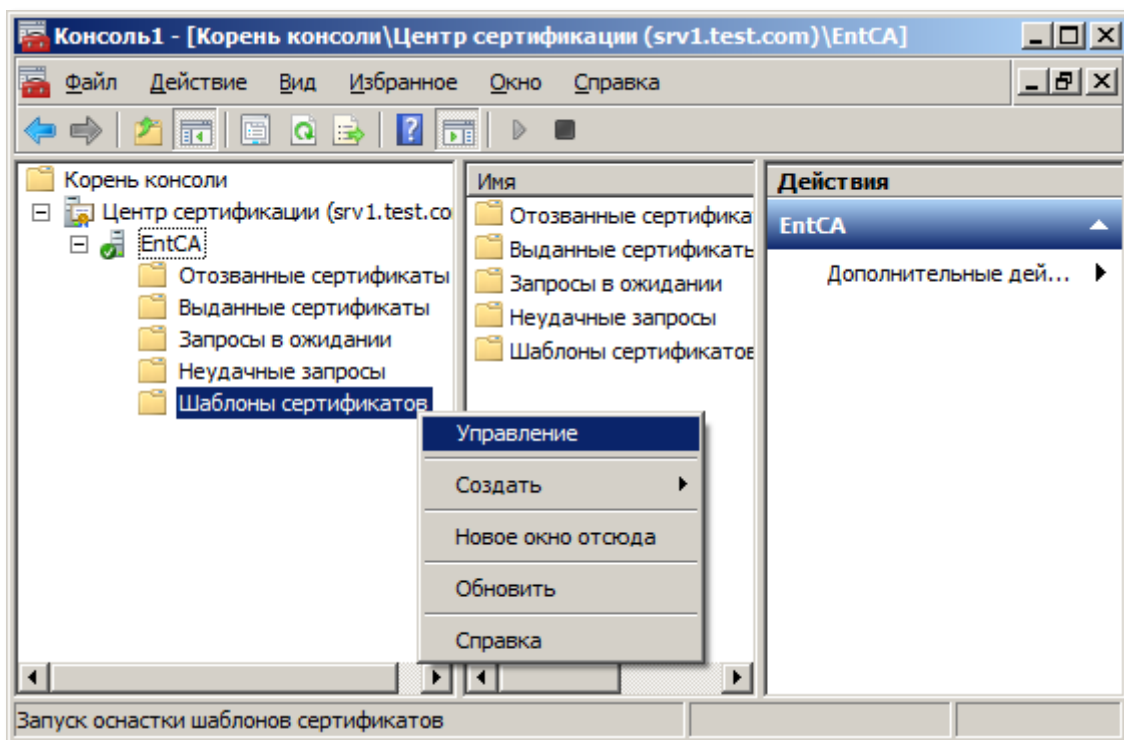
- удобство;
- минимизация возможных ошибок пользователя при составлении запроса на получение сертификата.

Если планируется использовать электронные ключи JaCarta в режиме CSP, на компьютере, с которого осуществляется создание данного шаблона, должен быть установлено ПО JC-Client. Это необходимо для того, чтобы был доступен поставщик служб шифрования (CSP) *Athena ASECard Crypto CSP*.

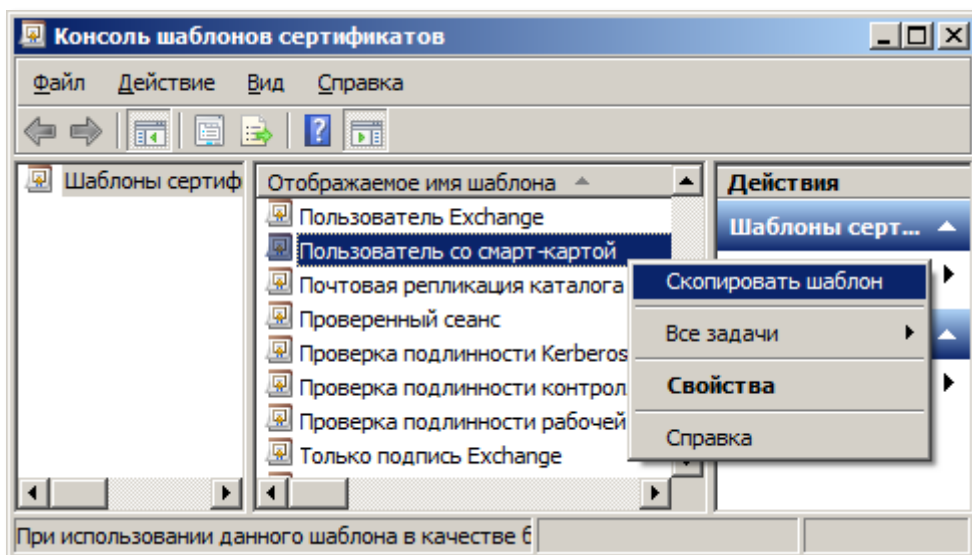
Для того чтобы создать шаблон сертификата *Пользователь JaCarta*, выполните следующее.

- 1 В дереве консоли центра сертификации разверните Центр сертификации (Certification Authority).
- 2 Выберите центр сертификации, который вы хотите настроить.

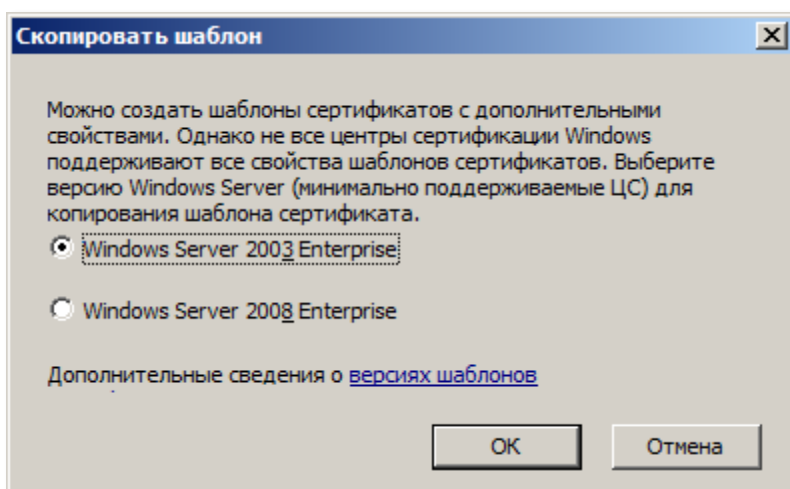
- Щёлкните правой кнопкой мыши на пункте Шаблоны сертификатов (Certificate Templates) и выберите Управление (Manage).



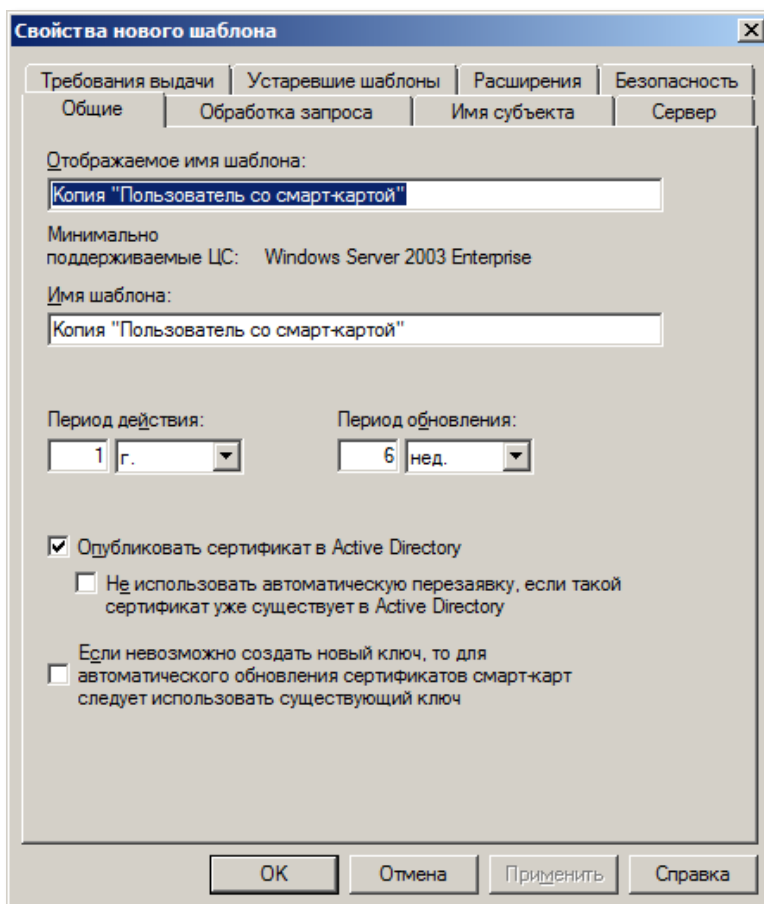
- В открывшемся окне щёлкните правой кнопкой на пункте **Пользователь со смарт-картой (Smartcard User)** и выберите **Скопировать шаблон (Duplicate Template)**.



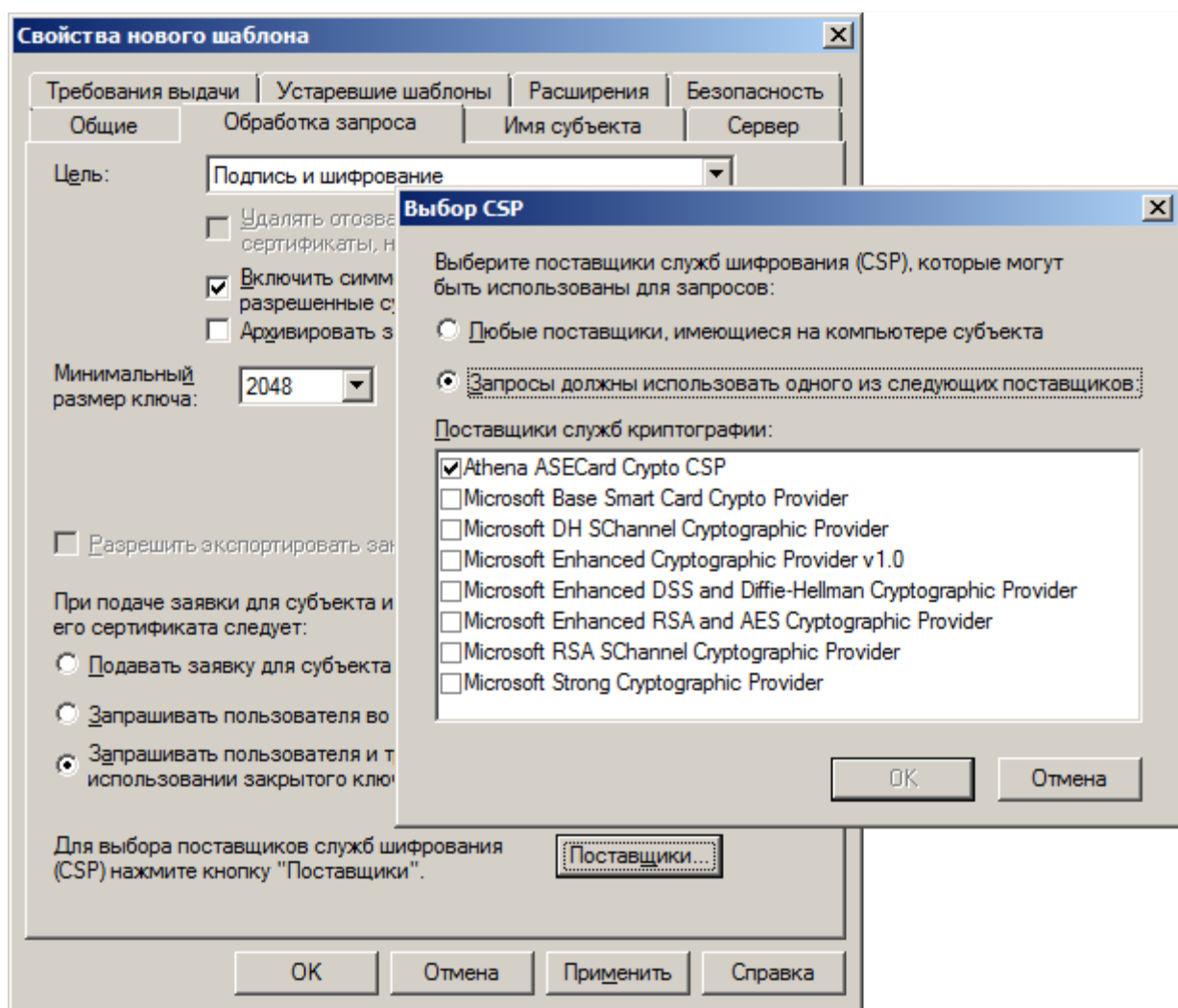
Отобразится следующее окно.



- 5 Выберите версию шаблона сертификата (в данном примере Windows Server 2003, что соответствует шаблону версии 2) и нажмите **ОК**.
- 6 Убедитесь в том, что в окне **Свойства нового шаблона (Properties of New Template)** открыта вкладка **Общие (General)**.



- 7 В поле **Отображаемое имя шаблона (Template Display Name)** введите **Пользователь JaCarta (JaCarta User)**.
- 8 В поле **Период действия (Validity Period)** введите срок действия сертификата. В поле **Период обновления (Renewal Period)** — срок перед окончанием действия сертификата, в течение которого пользователь может обновить сертификат.
- 9 Откройте вкладку **Обработка запроса (Request Handling)**.
- 10 Выберите **Запрашивать пользователя и требовать ответа при использовании закрытого ключа (Prompt the user during enrollment and require user input when the private key is used)**.
- 11 Нажмите **Поставщики (CSPs)**.
- 12 В окне **Выбор CSP** выберите **Запросы должны использовать одного из следующих поставщиков (Requests must use one CSP of the following CSPs)**.



- 13 В списке **Поставщики служб криптографии (CSPs)** выберите **Athena ASECard Crypto CSP**.

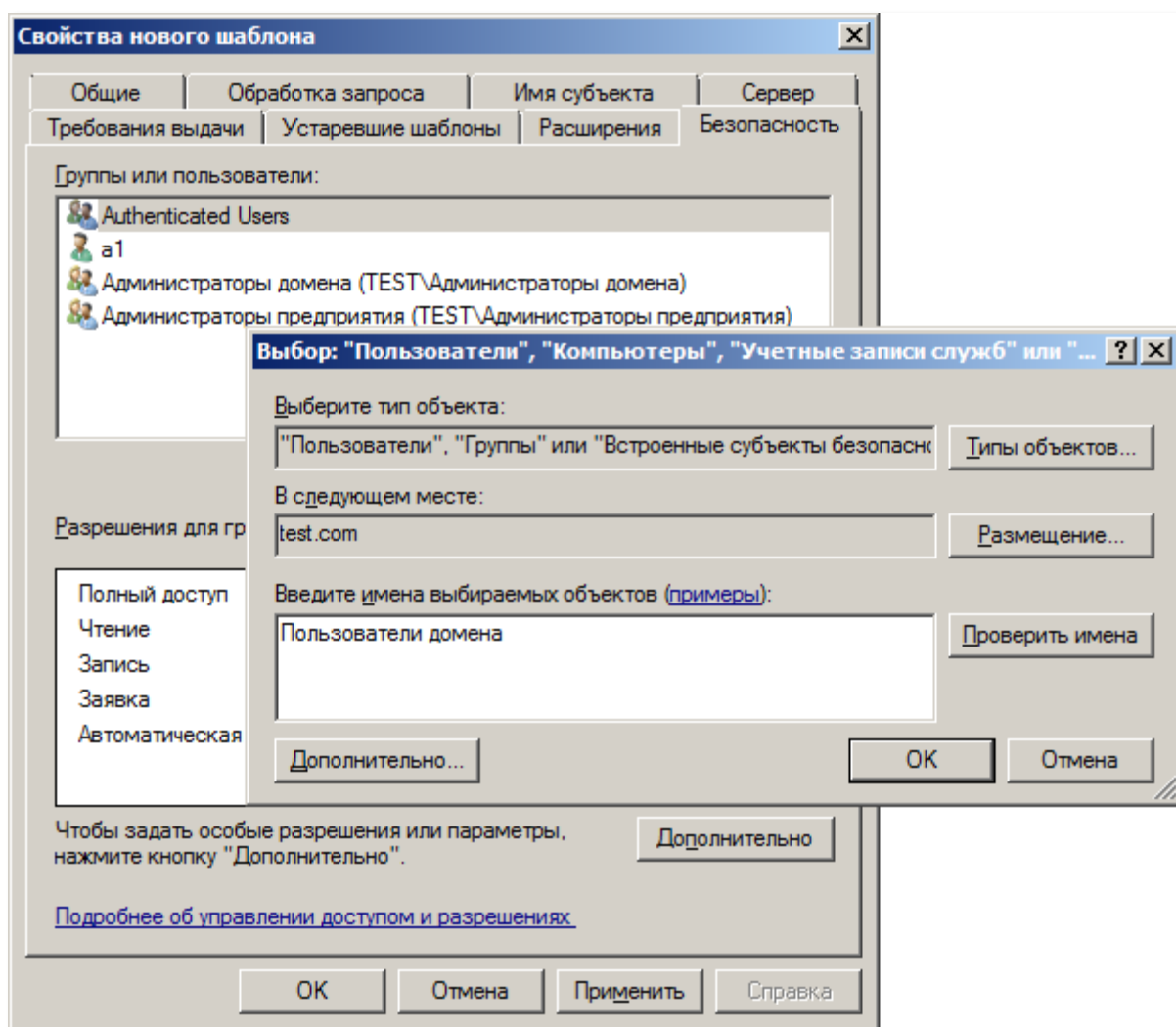
Примечание

Этот поставщик присутствует в списке только если на компьютере, с которого осуществляется настройка создаваемого шаблона, установлен *JC-Client* в режиме *CSP*. Если *JC-Client* установлен в режиме *Minidriver*, следует отметить *Microsoft Base Smart Card Crypto Provider*.

- 14 В окне **Выбор CSP** нажмите **ОК**.
- 15 В окне **Свойства нового шаблона (Properties of New Template)** откройте вкладку **Безопасность (Security)**.

Назначьте группам и пользователям разрешения в зависимости от желаемых процедур выдачи сертификатов:

- для автоматической выдачи сертификатов назначьте разрешение **Заявка (Enroll)** и **Автоматическая подача заявок (Autoenroll)**.
 - для децентрализованной выдачи сертификатов назначьте разрешение **Заявка (Enroll)**.
- 16 При необходимости нажмите кнопку **Добавить (Add)** и воспользуйтесь стандартным диалогом для выбора объектов.



- 17 В окне **Свойства нового шаблона (Properties of New Template)** нажмите **ОК**.
- 18 Убедитесь в том, что шаблон **Пользователь JaCarta (JaCarta User)** появился в списке **Шаблоны сертификатов (Certificate Templates)**.

Создание шаблона сертификата для централизованной процедуры выдачи сертификатов

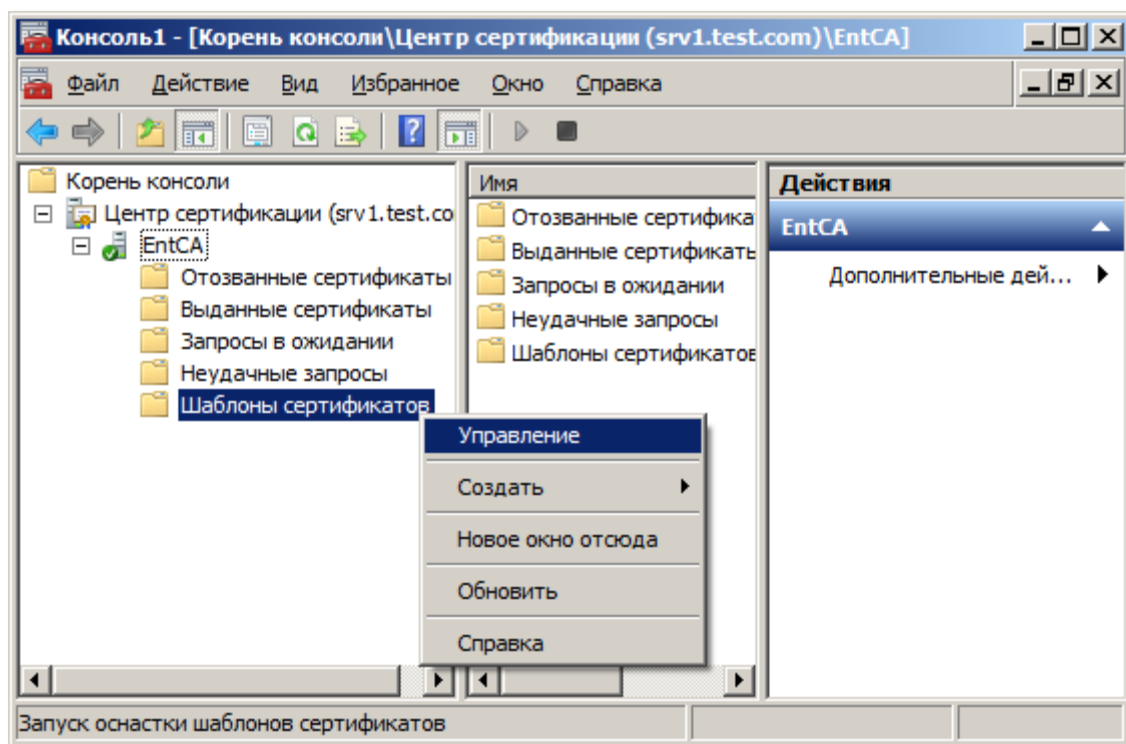
Для централизованной процедуры выдачи сертификатов, создайте шаблон сертификата *Пользователь JaCarta (централизованная процедура)*. Создание и последующее использование этого шаблона дает два основных преимущества:

- удобство;
- минимизация возможных ошибок агентов подачи заявок.

Если планируется использовать электронные ключи JaCarta в режиме CSP, на компьютере, с которого осуществляется создание данного шаблона, должен быть установлено ПО JC-Client. Это необходимо для того, чтобы был доступен поставщик служб шифрования (CSP) *Athena ASECard Crypto CSP*.

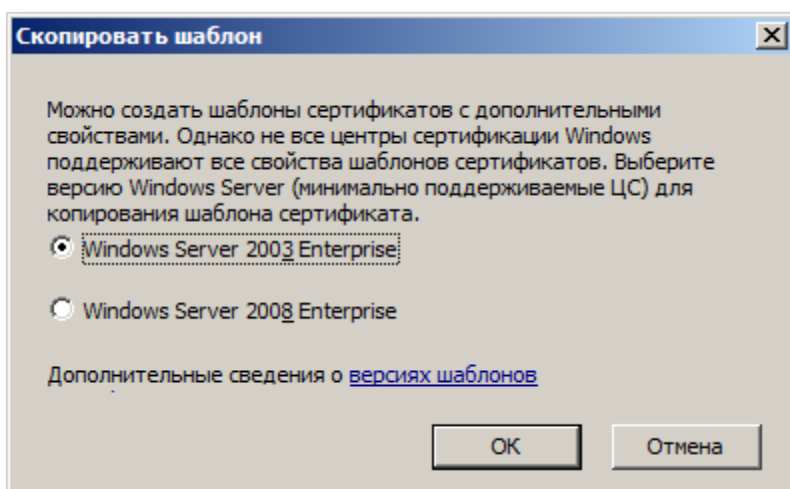
Для того чтобы создать шаблон сертификата *Пользователь JaCarta (централизованная процедура)*, выполните следующее.

- 1 В дереве консоли центра сертификации разверните **Центр сертификации**.
- 2 Выберите центр сертификации, который вы хотите настроить.
- 3 Щёлкните правой кнопкой мыши **Шаблоны сертификатов** и выберите **Управление**.



- 4 В открывшемся окне щёлкните правой кнопкой на **Пользователь со смарт-картой** и выберите **Скопировать шаблон**.

Отобразится следующее окно.



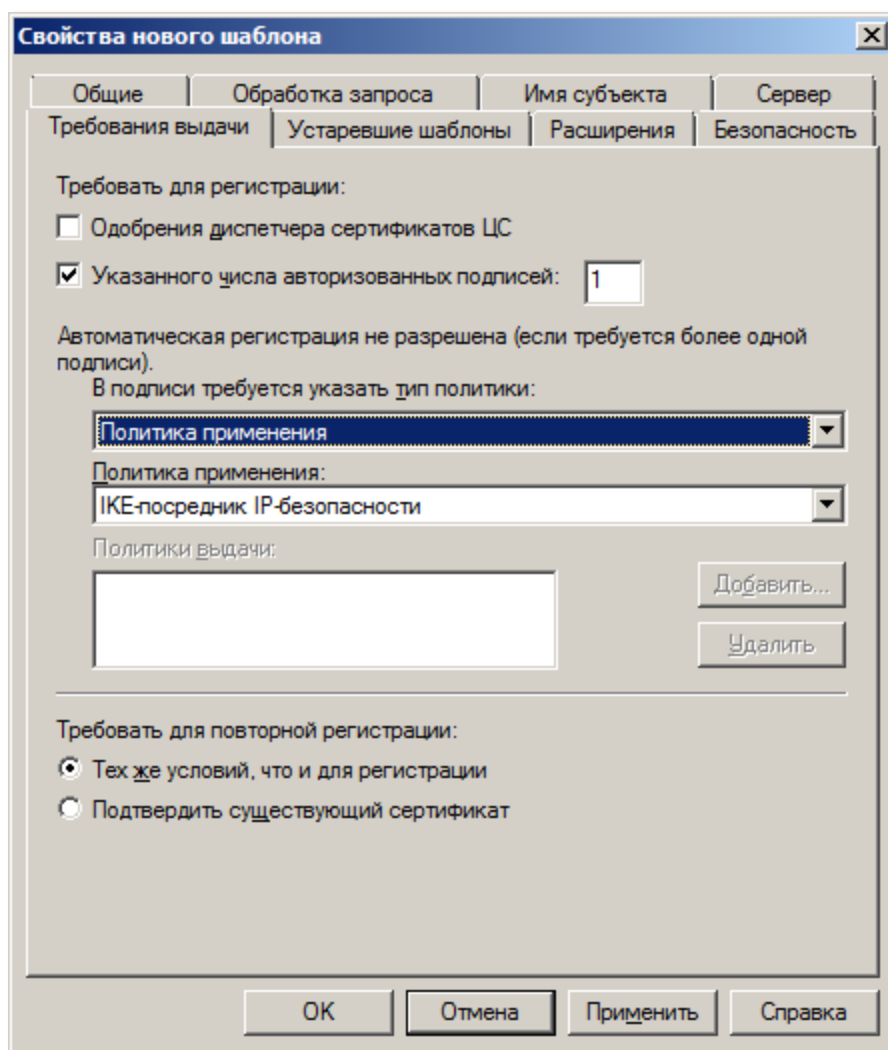
- 5 Выберите версию шаблона сертификата (в данном примере Windows Server 2003, что соответствует шаблону версии 2) и нажмите **ОК**.
- 6 Убедитесь в том, что в окне **Свойства нового шаблона** открыта вкладка **Общие**.
- 7 В поле **Отображаемое имя шаблона** введите **Пользователь JaCarta (централизованная процедура)**.
- 8 В поле **Период действия** введите срок действия сертификата.
- 9 Откройте вкладку **Обработка запроса**.
- 10 Нажмите **Поставщики**.
- 11 В окне **Выбор CSP** выберите **Запросы должны использовать одного из следующих поставщиков**.
- 12 В списке **Поставщики служб криптографии** выберите **Athena ASECard Crypto CSP**.

Примечание

Этот поставщик присутствует в списке только если на компьютере, с которого осуществляется настройка создаваемого шаблона, установлен JC-Client в режиме CSP. Если JC-Client установлен в режиме Minidriver, следует отметить Microsoft Base Smart Card Crypto Provider.

- 13 В окне **Выбор CSP** нажмите **ОК**.

- 14 В окне **Свойства нового шаблона** откройте вкладку **Требования выдачи**.

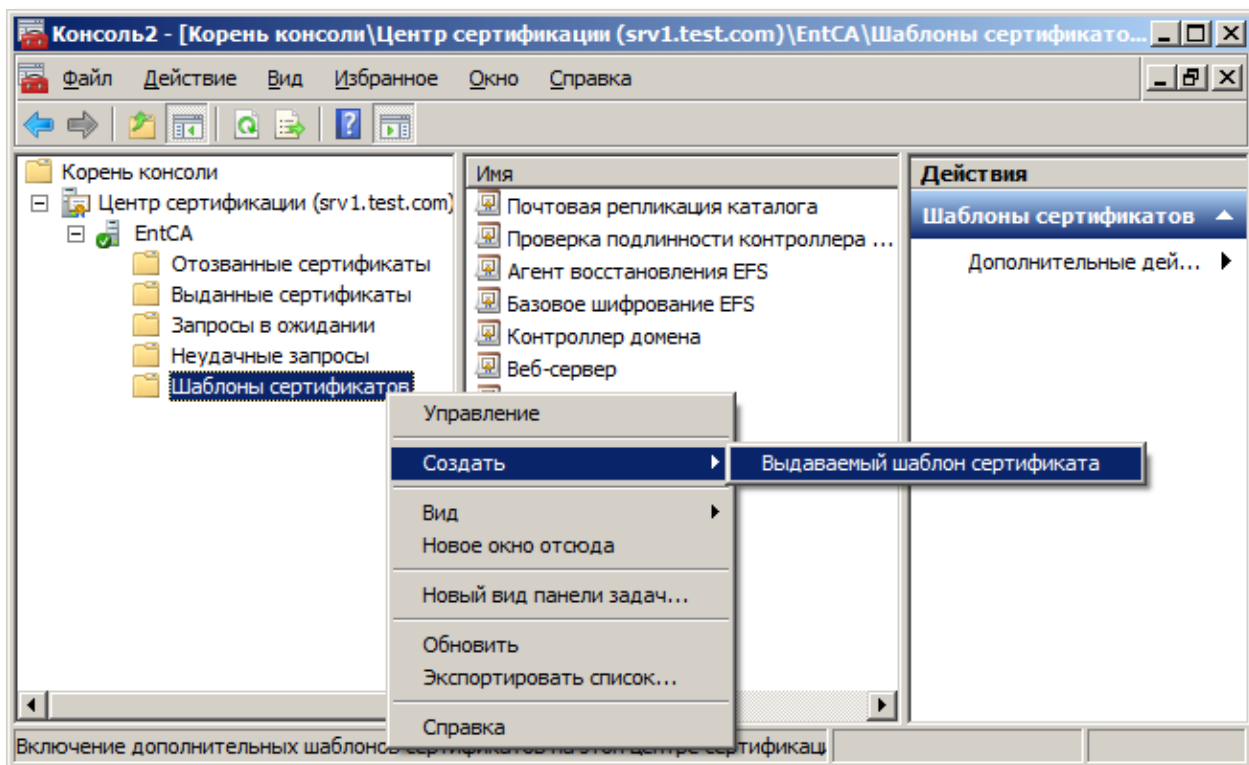


- 15 Поставьте флажок **Указанного числа авторизованных пользователей** и убедитесь, что этот параметр принимает значение **1**.
- 16 Убедитесь, что параметр **В подписи требуется указать тип политики** принимает значение **Политика применения**.
- 17 Из списка **Политика применения** выберите **Агент запроса сертификата**.
- 18 Откройте вкладку **Безопасность**.
- 19 Назначьте себе, а также группам и пользователям, которые будут выступать в качестве агентов подачи заявок, разрешение **Заявка, Чтение** и **Запись**. При необходимости нажмите кнопку **Добавить** и воспользуйтесь стандартным диалогом для выбора объектов.
- 20 В окне **Свойства нового шаблона** нажмите **ОК**.
- 21 Убедитесь в том, что шаблон **Пользователь JaCarta (централизованная процедура)** появился в списке **Шаблоны сертификатов**.
- 22 Назначьте себе, а также группам и пользователям, которые будут выступать в качестве агентов подачи заявок, разрешение **Заявка, Чтение** и **Запись** на шаблон **Агент регистрации**.
- 23 Закройте окно со списком шаблонов сертификатов.

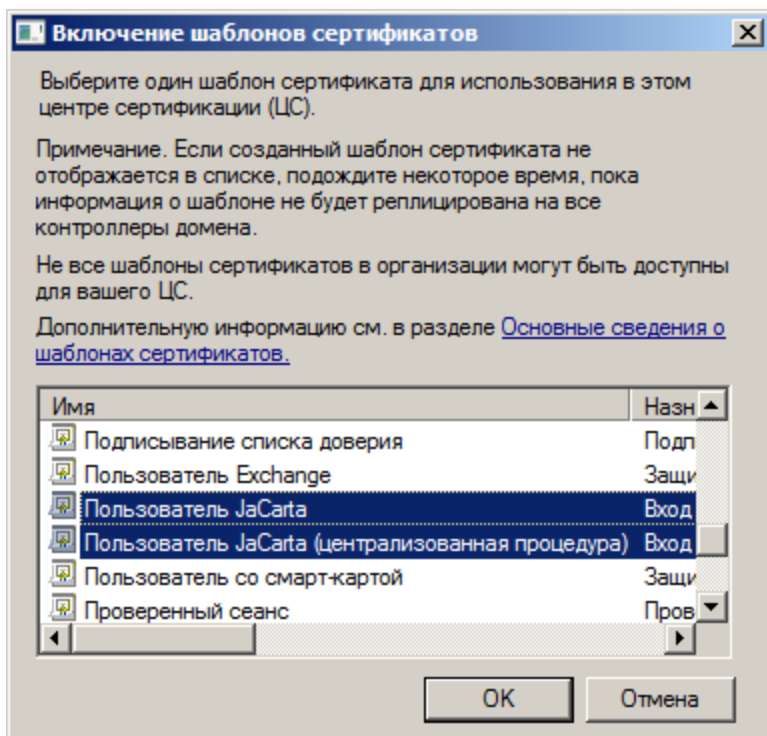
Включение шаблонов сертификатов

Для того чтобы включить необходимые шаблоны сертификатов, выполните следующее.

- 1 В дереве консоли центра сертификации разверните **Центр сертификации**.
- 2 Выберите центр сертификации, который вы настраиваете.
- 3 В дереве консоли щёлкните правой кнопкой мыши **Шаблоны сертификатов** и выберите **Создать**.
- 4 Щёлкните **Выдаваемый шаблон сертификата**.



- 5 В окне **Включение шаблонов сертификатов** выберите шаблоны:
 - **Пользователь JaCarta** — для децентрализованной процедур выдачи сертификатов;
 - **Пользователь JaCarta (централизованная процедура)** — для централизованной процедуры выдачи сертификатов;
 - **Агент регистрации** — для централизованной процедуры (если этот шаблон присутствует в списке).

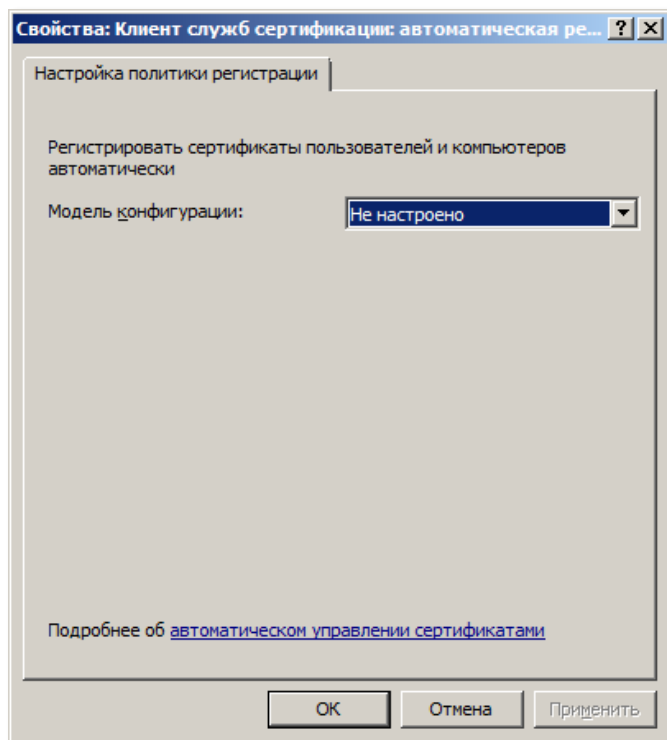


Отсутствие стандартного шаблона **Агент регистрации** в списке означает то, что этот шаблон уже включен.

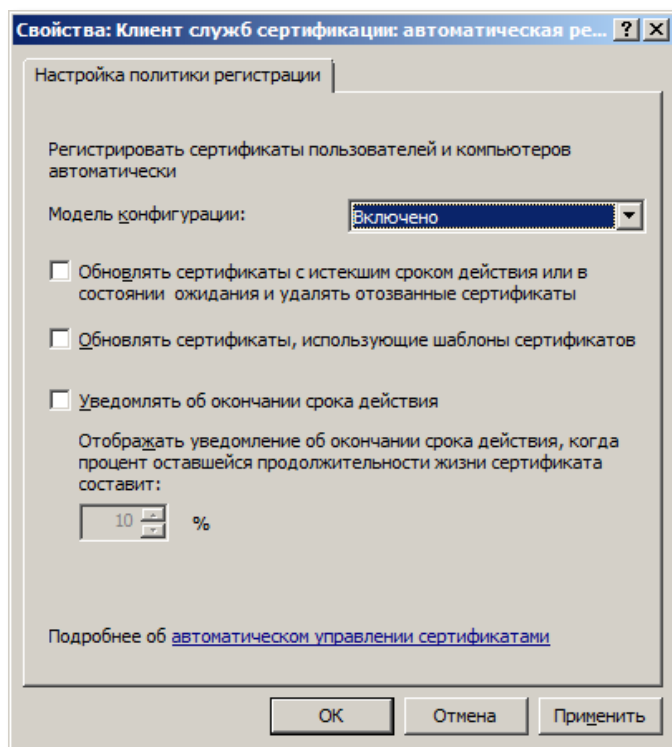
- 6 Нажмите **ОК**.
- 7 Для автоматической и децентрализованной процедуры выдачи сертификатов убедитесь в том, что шаблон **Пользователь JaCarta** появился в списке **Шаблоны сертификатов**. Для централизованной процедуры в этом списке должны присутствовать шаблоны **Агент регистрации** и **Пользователь JaCarta (централизованная процедура)**.

Объект групповой политики для автоматической выдачи сертификатов

Для того чтобы пользователи могли получать сертификаты автоматически, кроме настроек центра сертификации отредактируйте соответствующий объект групповой политики (**Конфигурация пользователя > Конфигурация Windows > Параметры безопасности > Клиент служб сертификации: автоматическая регистрация**.)



- 1 В списке Модель конфигурации выберите Включено.
Окно примет следующий вид.



- 2 Чтобы обеспечить автоматическую регистрацию по настроенному шаблону сертификата, установите флажок Обновлять сертификаты, использующие шаблоны сертификатов. Эта настройка будет действовать даже в том случае, если у пользователя ещё нет сертификатов.

- 3 При необходимости установите остальные настройки и нажмите ОК.

Примечание

После внесения изменений в настройки групповых политик необходимо в командной строке ввести команду `gpupdate /force`. Может потребоваться перезагрузка клиентских компьютеров.

Данный объект можно использовать как в доменных политиках, так и в политиках, применяемых к отдельным подразделениям.

Сертификат агента регистрации для централизованной выдачи сертификатов

О сертификате

Централизованная выдача сертификата проходит в отсутствие пользователя. Процедуру осуществляет агент регистрации. Для этого необходимо, чтобы на компьютере был установлен сертификат агента регистрации. Правом на установку такого сертификата обладают группы и пользователи, указанные в параметрах безопасности шаблона сертификатов *Агент регистрации*.

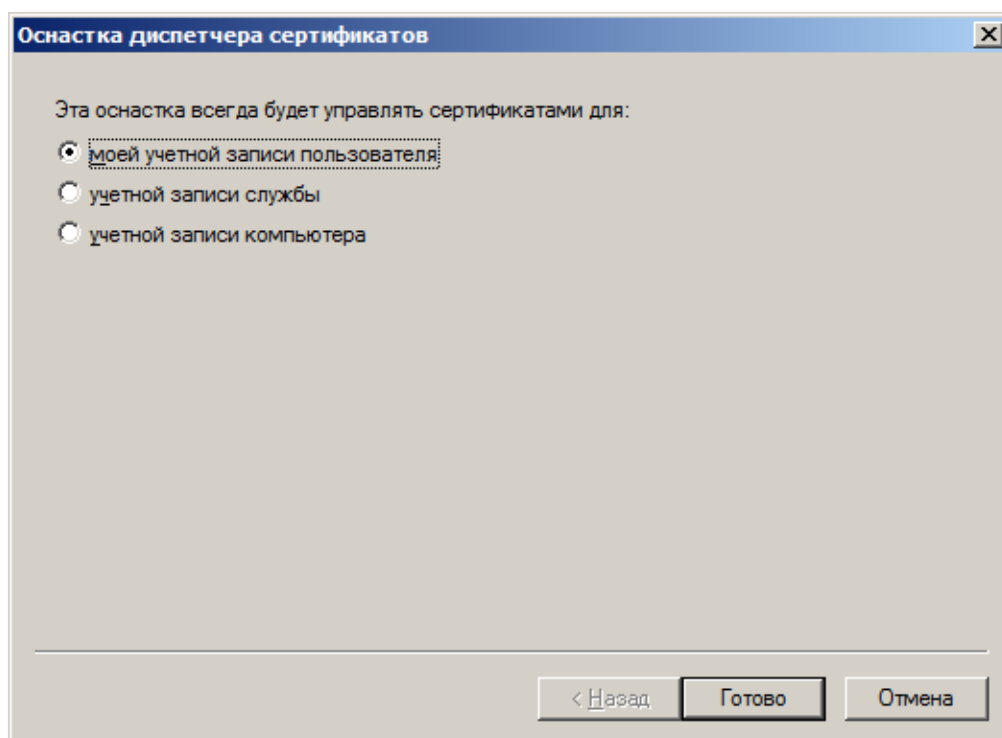
Для успешного получения сертификата агента регистрации необходимо, чтобы в центре сертификации шаблон *Агент регистрации* был включен.

Получение сертификата с помощью мастера запроса сертификата

Для того чтобы установить сертификат агента регистрации с помощью мастера запроса сертификата, выполните следующую последовательность действий.

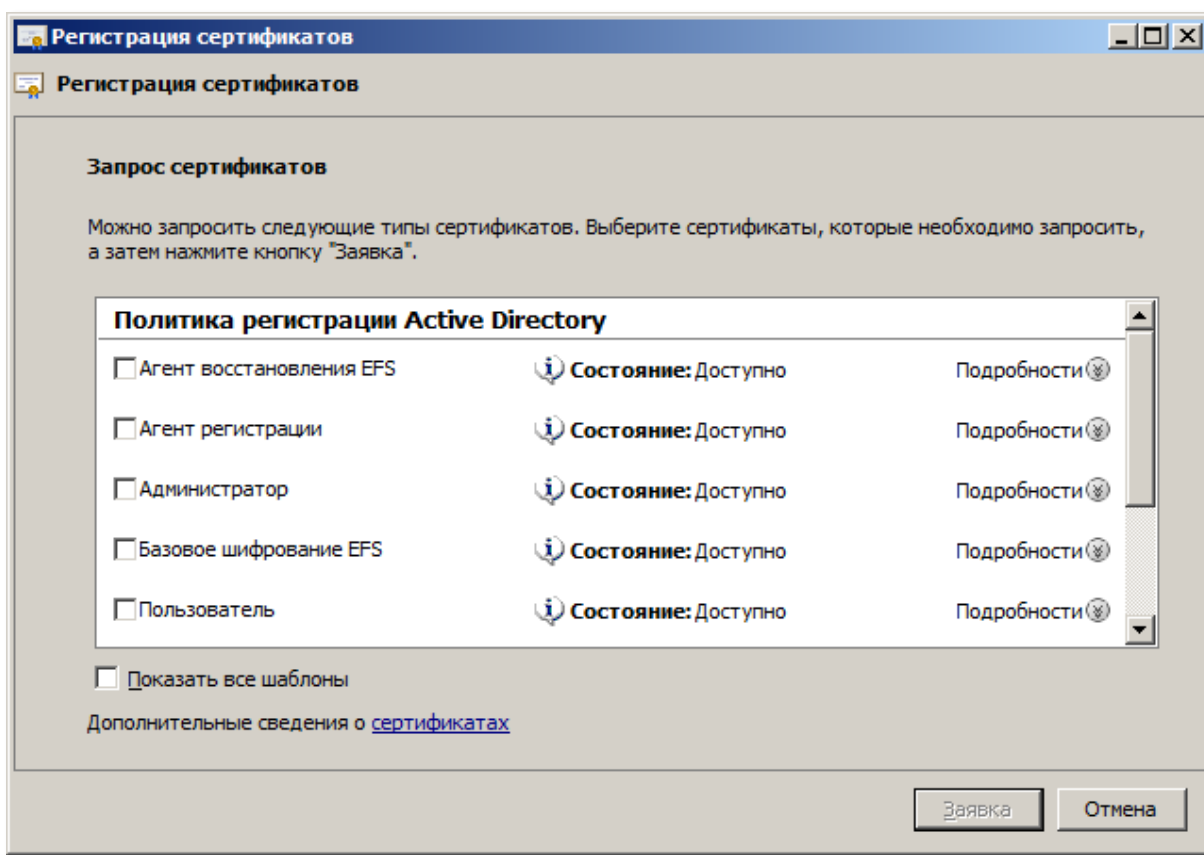
- 1 Выберите **Пуск > Все программы > Стандартные (Start > All Programs > Accessories)**, щёлкните правой кнопкой на пункте **Командная строка (Command Prompt)** и выберите **Запуск от имени администратора (Run as administrator)**.
- 2 В окне командной строки ведите **mmc** и нажмите клавишу **ВВОД (Enter)**.
- 3 В панели управления открывшегося окна выберите **Файл > Добавить или удалить оснастку (File -> Add/Remove Snap-In)**.
- 4 В окне **Добавление и удаление оснасток (Add/Remove Snap-In)** выберите **Сертификаты (Certificates)** и нажмите **Добавить (Add)**.

Отобразится следующее окно.



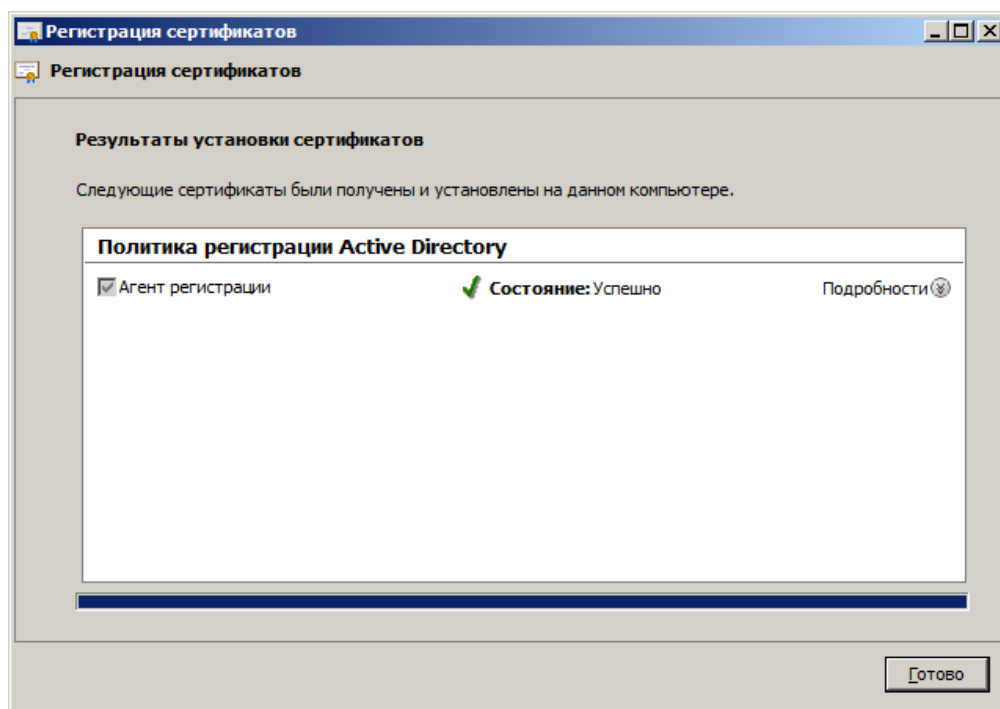
- 5 Выберите **моей учётной записи пользователя (my user account)** и нажмите **Готово (Finish)**.
- 6 В окне **Добавление и удаление оснасток (Add/Remove Snap-In)** нажмите **ОК**.
- 7 В дереве консоли разверните **Сертификаты – текущий пользователь (Certificates – Current User)**.
- 8 Щёлкните правой кнопкой мыши на пункте **Личное (Personal)**, выберите **Все задачи (All Tasks)** и щёлкните **Запросить новый сертификат (Request New Certificate)**.
- 9 На первой странице мастера запроса сертификатов нажмите **Далее (Next)**.
- 10 На странице **Выбор политики регистрации сертификатов (Select Certificate Enrollment Policy)** нажмите **Далее (Next)**.
- 11 На странице **Выбор политики регистрации сертификатов** нажмите **Далее (Next)**.

Отобразится страница **Запрос сертификатов**.



12 Установите флажок напротив **Агент регистрации** и нажмите **Заявка (Enroll)**.

При успешной записи сертификата в хранилище пользователя на компьютере отобразится следующее сообщение.



Получение сертификата пользователя и запись его в память электронного ключа JaCarta

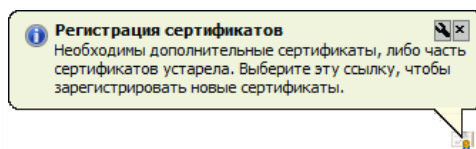
Параметры учётной записи пользователя

Для успешного получения сертификата необходимо выполнение условий:


- 1 Ключ JaCarta пользователя должен быть предварительно персонализирован администратором (см. документ "JC-Client. Руководство администратора");
- 2 Учётная запись пользователя должна содержать адрес электронной почты.

Автоматическая выдача сертификатов

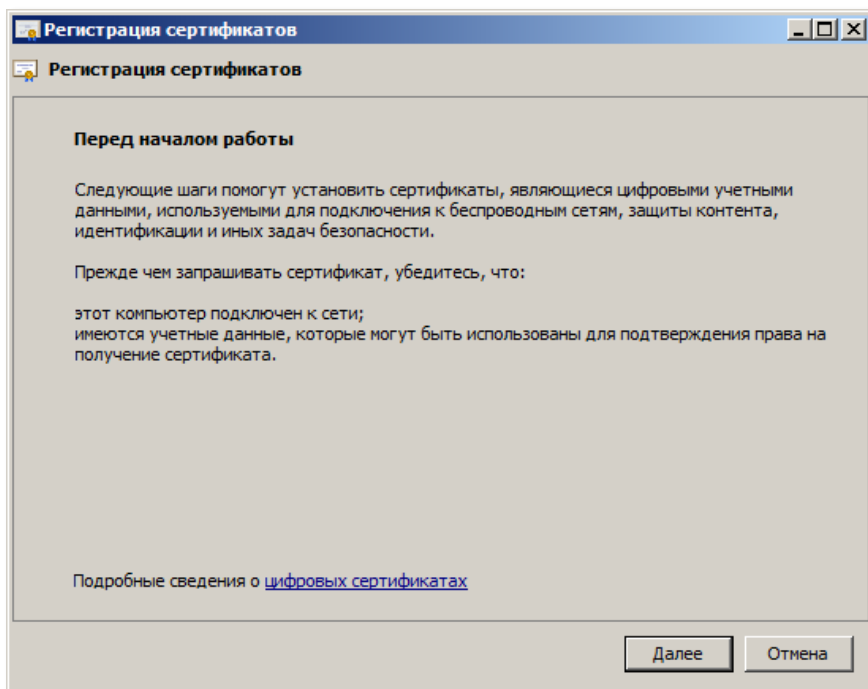
Если настройки шаблона сертификата **Пользователь JaCarta** предполагают для вас автоматическую выдачу сертификатов, при необходимости установить или обновить сертификат в области уведомлений появится значок **Регистрация сертификатов**.



Для получения сертификата:

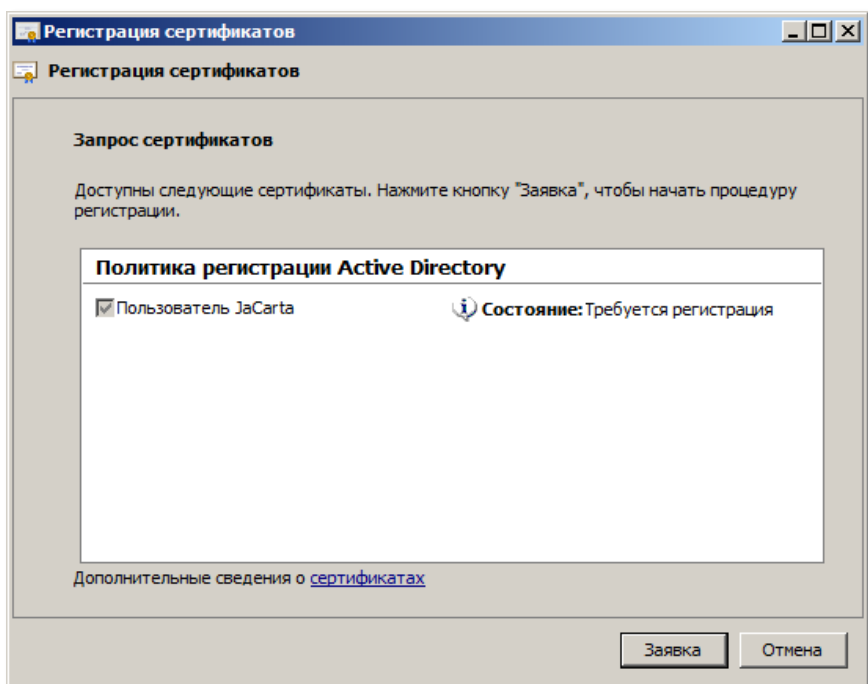
- 1 Убедитесь в том, что к компьютеру подключен электронный ключ JaCarta. На USB-токене JaCarta должен гореть световой индикатор.
- 2 Щёлкните на значке  в области уведомлений.

Отобразится следующее окно.



3 Нажмите **Далее**.

Отобразится следующее окно.

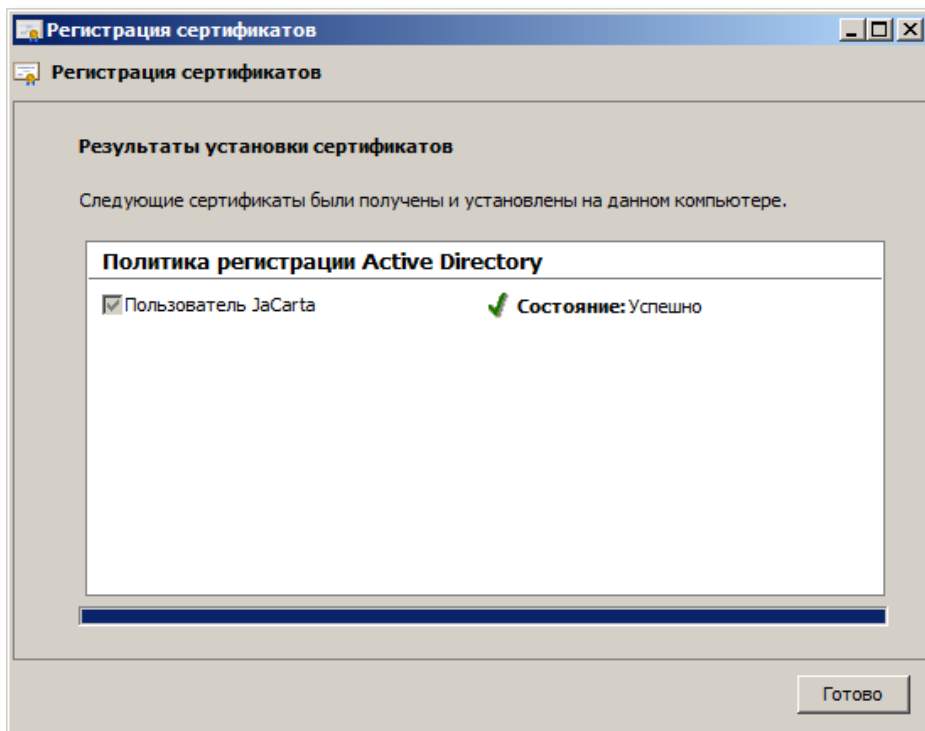


4 Нажмите **Заявка**.

5 Отобразится окно подтверждения доступа пользователя к электронному ключу JaCarta.

6 В зависимости от установленных настроек введите пароль пользователя или (и) приложите палец к сканеру отпечатков. Процедура генерации ключевой пары займет некоторое время.

7 При успешном завершении процедуры отобразится следующее сообщение.



8 Нажмите Готово для завершения процедуры.

Децентрализованная выдача сертификатов

Если настройки шаблона сертификата **Пользователь JaCarta** предполагают для вас децентрализованную выдачу сертификатов, для получения сертификата и записи его в память электронного ключа JaCarta вы можете воспользоваться мастером запроса сертификата.

Внимание!

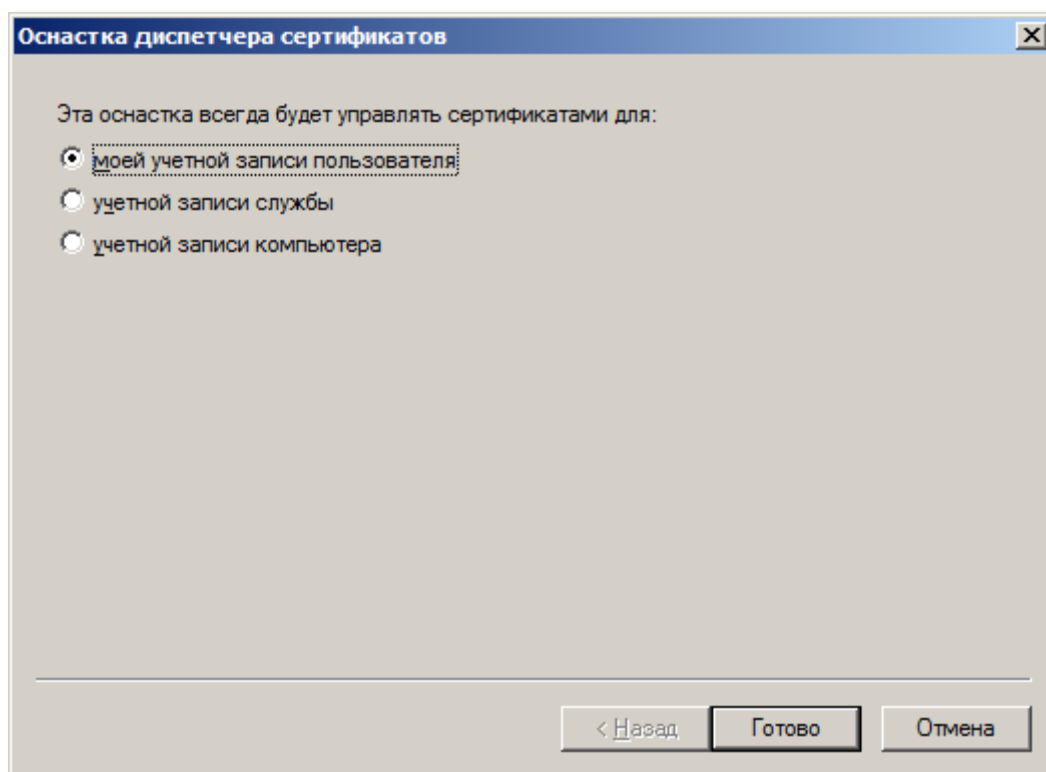
Предварительно электронный ключ JaCarta должен быть персонализирован с использованием одного из стандартных профилей. При этом устанавливаются пароли пользователя и администратора, соответствующие профилю.

Изменение установленного при персонализации стандартного пароля пользователя может привести к блокированию электронного ключа при выполнении действий, приведённых далее в этом пункте!

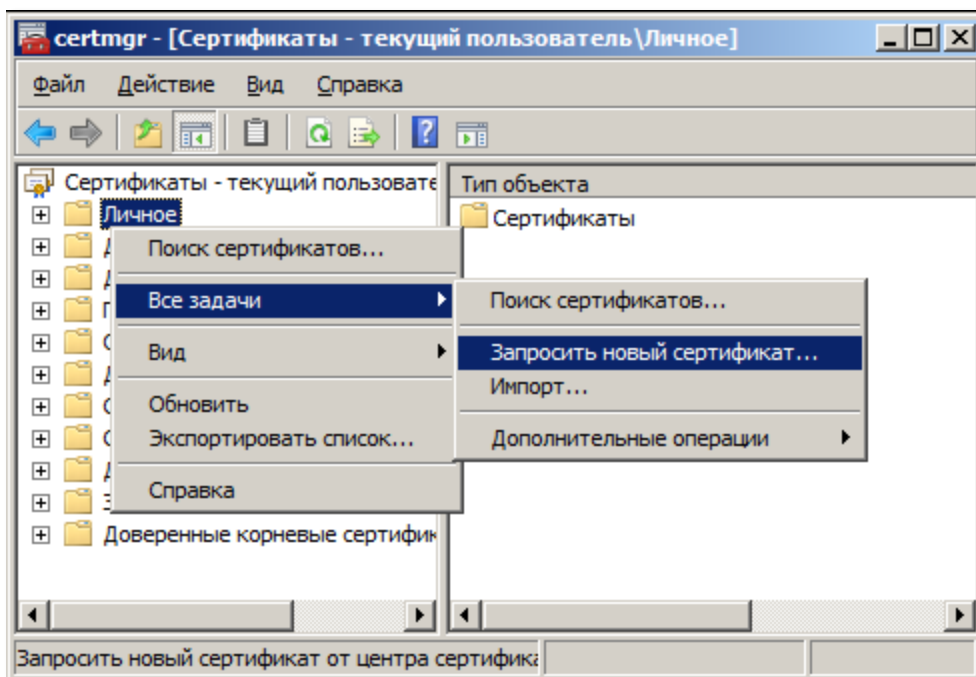
Для того чтобы получить сертификат с помощью мастера запроса сертификата, войдя с учётной записью пользователя, выполните следующую последовательность действий.

- 1 Щёлкните **Пуск > Все программы > Стандартные (Start > All Programs > Accessories)**, щёлкните правой кнопкой на пункте **Командная строка (Command Prompt)** и выберите **Запуск от имени администратора (Run as administrator)**.
- 2 В окне командной строки введите **mmc** и нажмите клавишу **ВВОД (Enter)**.
- 3 В панели управления открывшегося окна выберите **Файл > Добавить или удалить оснастку (File -> Add/Remove Snap-In)**.
- 4 В окне **Добавление и удаление оснасток (Add/Remove Snap-In)** выберите **Сертификаты (Certificates)** и нажмите **Добавить (Add)**.

Отобразится следующее окно.

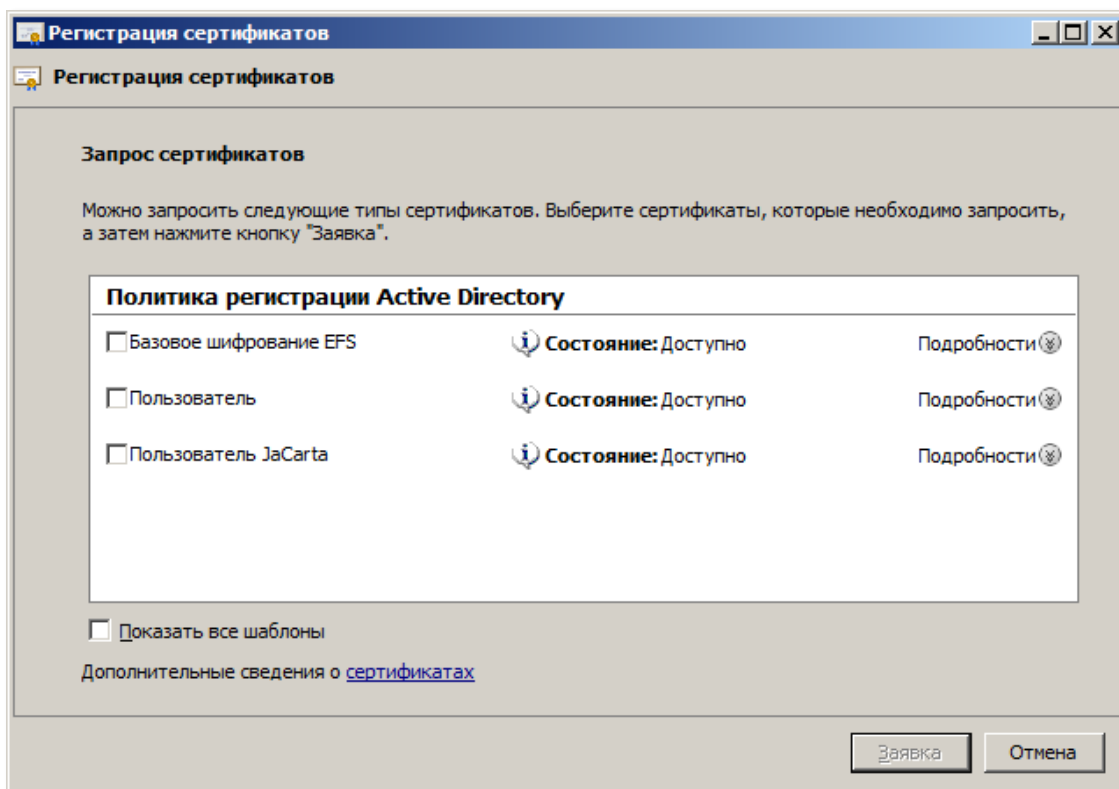


- 5 Выберите пункт **моей учётной записи пользователя (my user account)** и нажмите **Готово (Finish)**.
- 6 В окне **Добавление и удаление оснасток (Add/Remove Snap-In)** нажмите **ОК**.
- 7 Убедитесь в том, что к компьютеру подсоединен электронный ключ JaCarta. На USB-токене JaCarta должен гореть световой индикатор.
- 8 В дереве консоли разверните узел **Сертификаты – текущий пользователь (Certificates – Current User)**.
- 9 Щёлкните правой кнопкой мыши на пункте **Личное (Personal)**, выберите **Все задачи (All Tasks)** и щёлкните **Запросить новый сертификат (Request New Certificate)**.



- 10 На первой странице мастера запроса сертификатов нажмите **Далее (Next)**.
- 11 На странице **Выбор политики регистрации сертификатов (Select Certificate Enrollment Policy)** нажмите **Далее (Next)**.

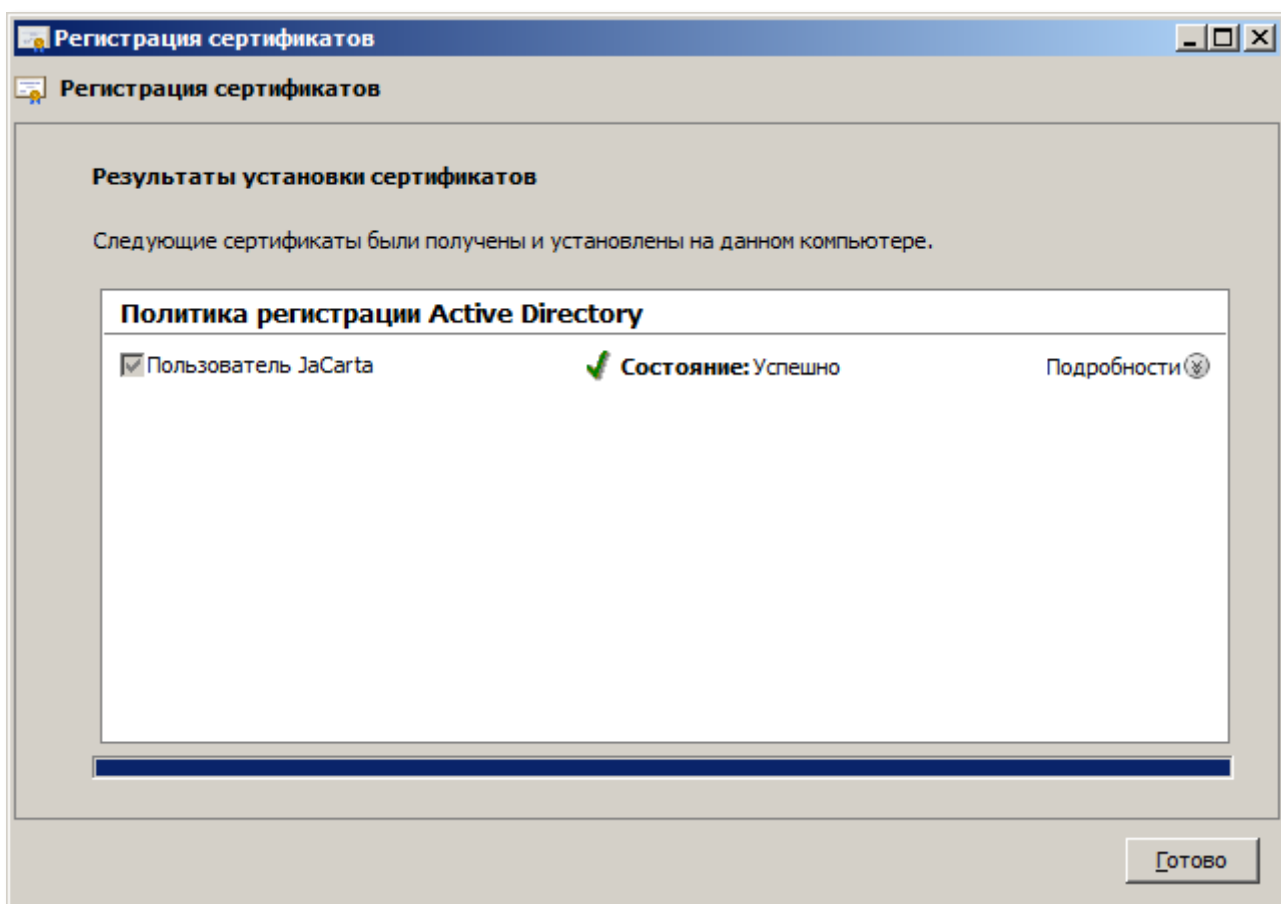
Отобразится следующее окно.



- 12 Установите флажок напротив **Пользователь JaCarta (User JaCarta)** и нажмите **Заявка (Enroll)**.
- 13 Отобразится окно подтверждения данных доступа пользователя.
- 14 Подтвердите доступ пользователя к электронному ключу JaCarta (введя пароль пользователя JaCarta или приложив палец к сканеру отпечатков).
- 15 Нажмите **Подтвердить**.

Операция генерации ключевой пары займёт некоторое время.

При успешной записи сертификата **Пользователь JaCarta (User JaCarta)** в память электронного ключа JaCarta отобразится следующее сообщение.



- 16 Нажмите **Готово (Finish)** для завершения процедуры.

Централизованная выдача сертификатов

Если вы являетесь агентом регистрации (в хранилище пользователей на вашем компьютере установлен соответствующий сертификат), вы можете подавать заявки на сертификат пользователя и записывать эти сертификаты в память электронных ключей JaCarta.

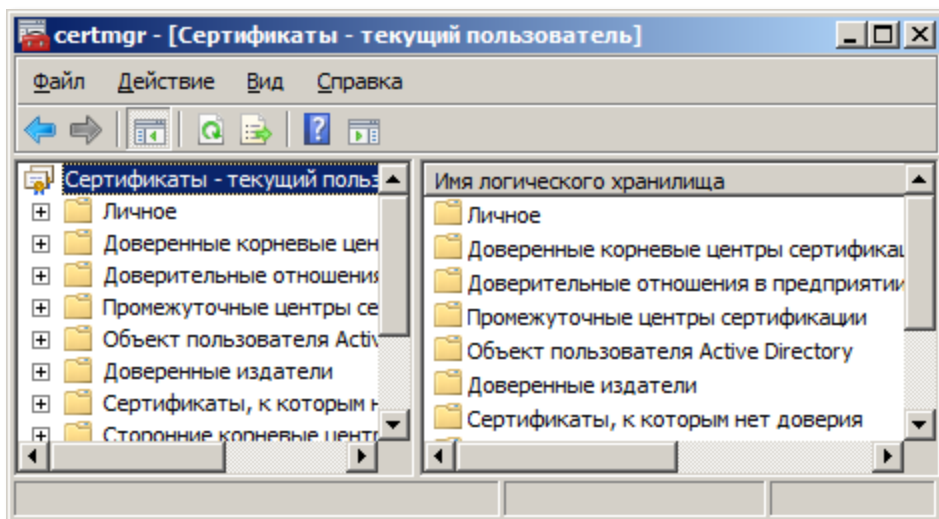
Внимание!

Предварительно электронный ключ JaCarta должен быть персонализирован с использованием одного из стандартных профилей. При этом устанавливаются пароли пользователя и администратора, соответствующие профилю.

Изменение установленного при персонализации стандартного пароля пользователя может привести к блокированию электронного ключа при выполнении действий, приведённых далее в этом пункте!

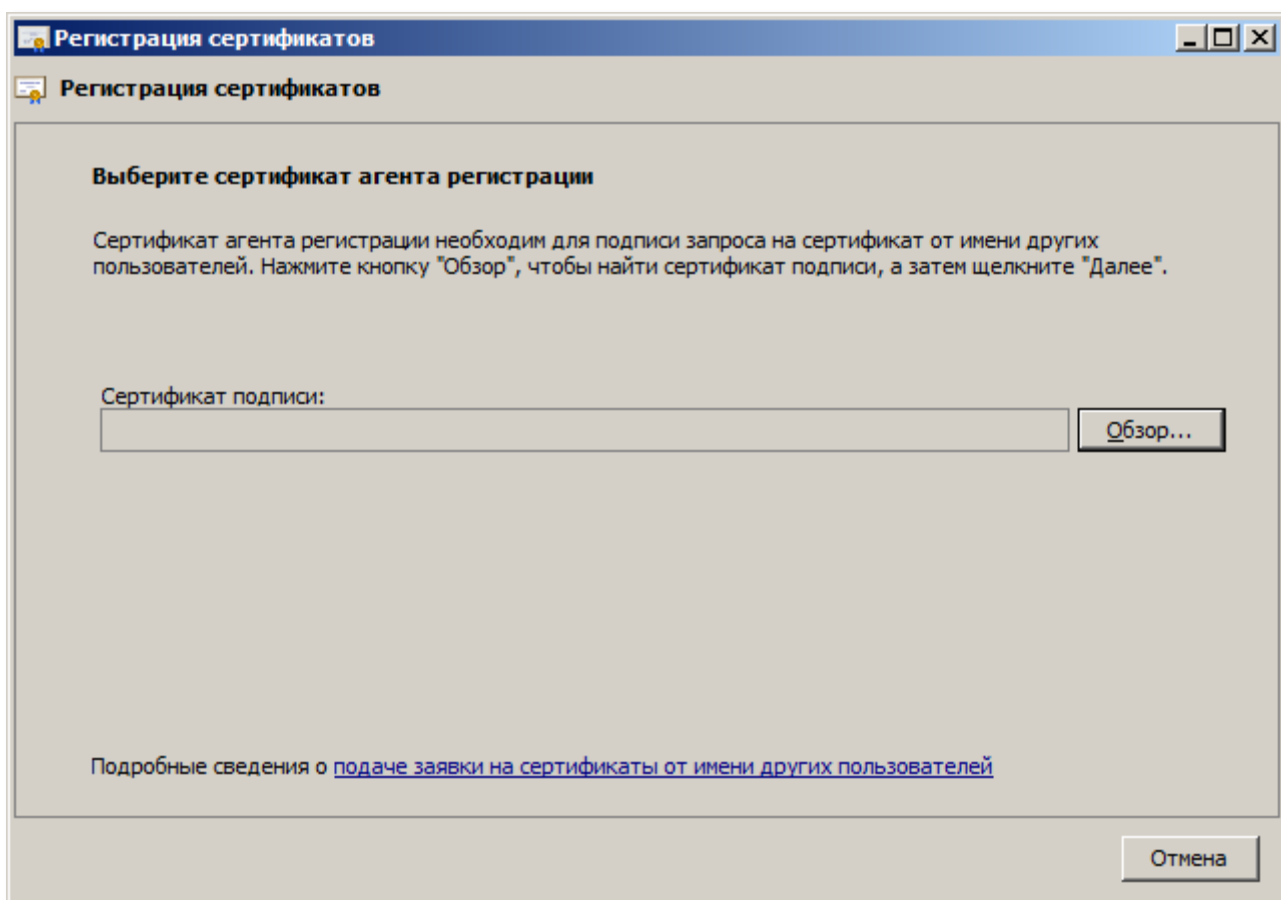
Для того чтобы подать заявку на сертификат пользователя, получить сертификат и записать его в память электронного ключа JaCarta, следуйте приведённой ниже инструкции.

- 17 Выберите **Пуск > Все программы > Стандартные (Start > All Programs > Accessories)**, щёлкните правой кнопкой на пункте **Командная строка (Command Prompt)** и выберите **Запуск от имени администратора (Run as administrator)**.
 - 18 В окне командной строке введите certmgr и нажмите клавишу **ВВОД (Enter)**.
- Отобразится следующее окно.



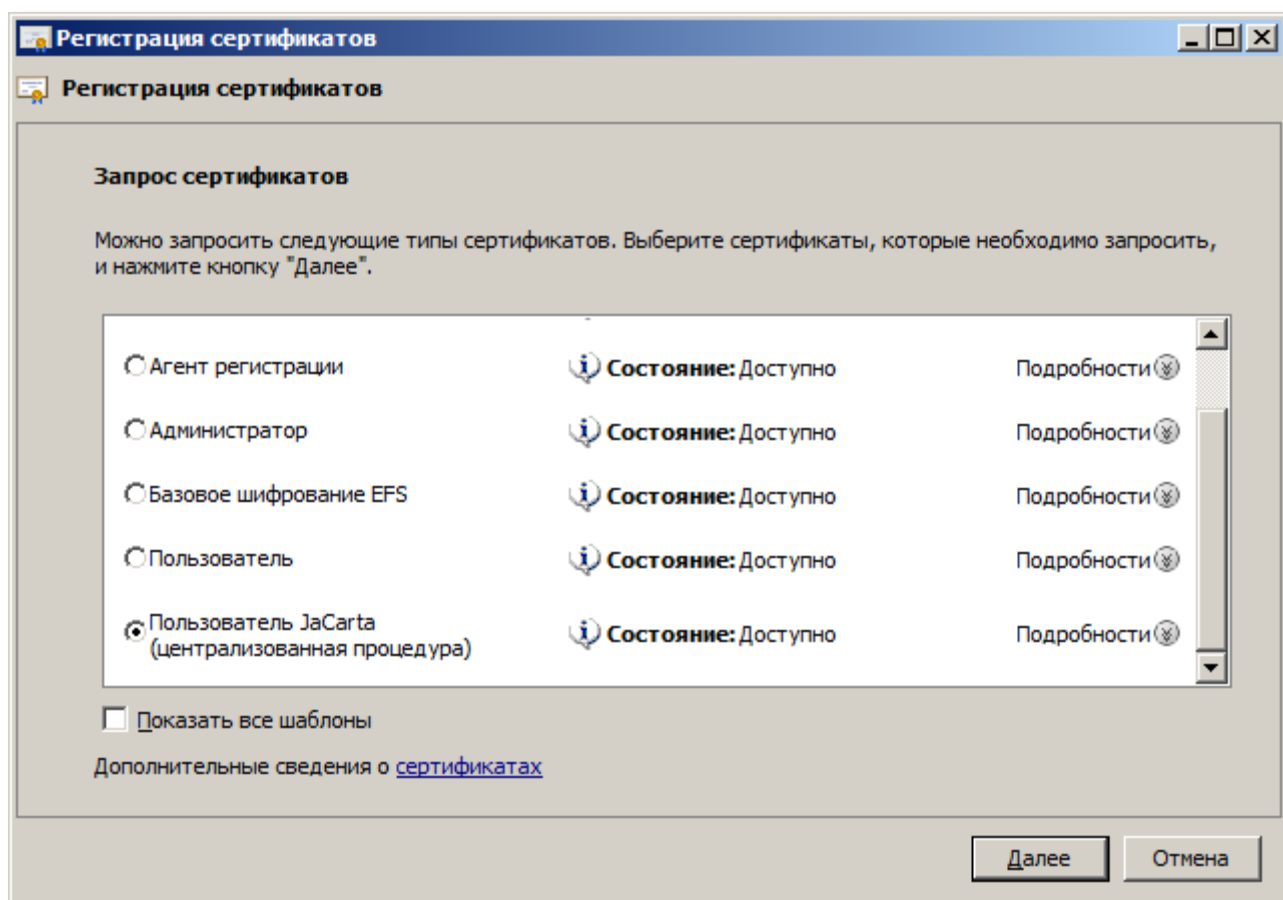
- 19 Щёлкните правой кнопкой на **Личное**, выберите **Все задачи > Дополнительные операции > Зарегистрироваться от имени**.
- 20 Отобразится окно мастера запросов сертификата.
- 21 На первой странице мастера запроса сертификатов нажмите **Далее**.
- 22 На странице **Выбор политики регистрации сертификатов** нажмите **Далее**.

Отобразится страница выбора сертификата агента регистрации.

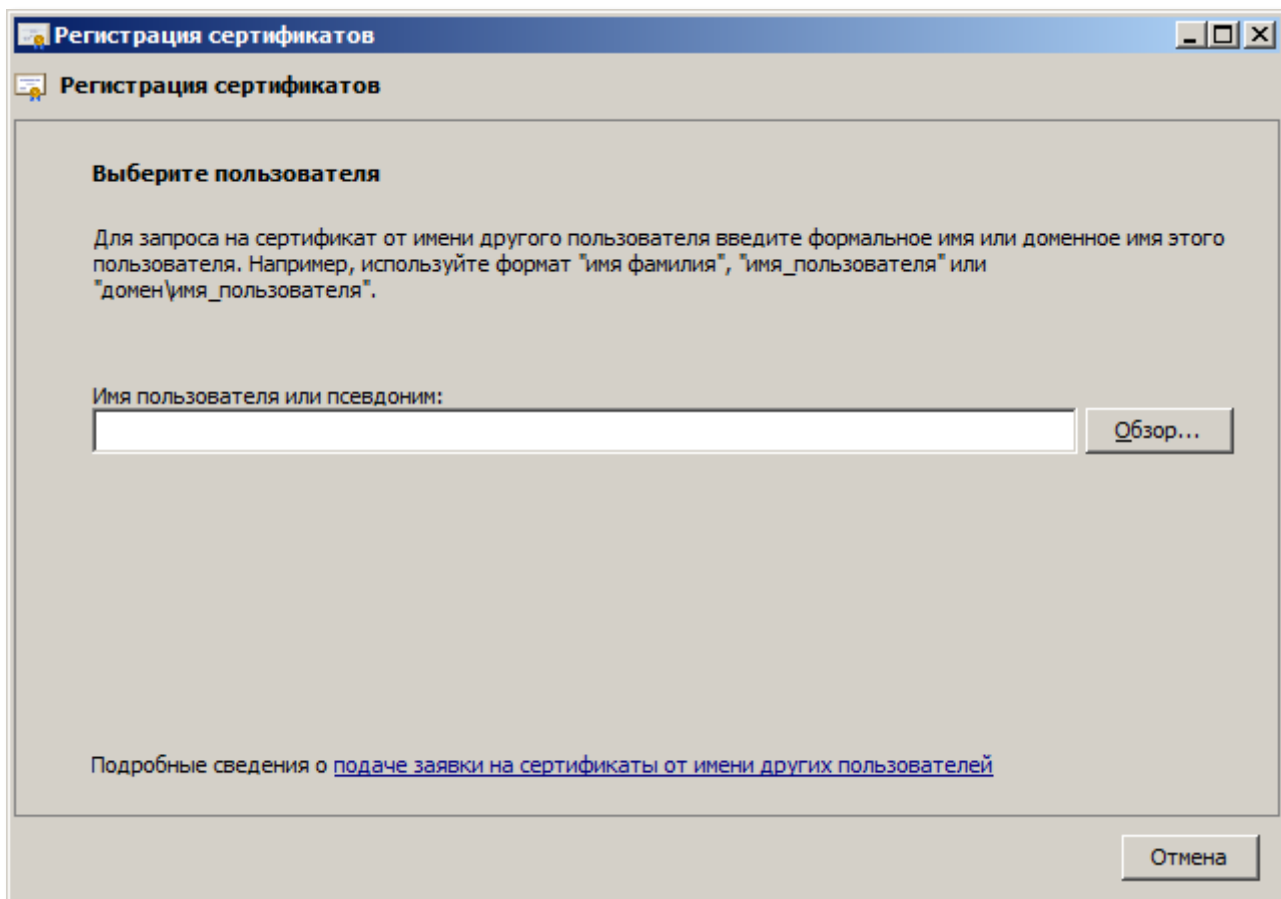


- 23 Воспользуйтесь кнопкой **Обзор**, чтобы выбрать свой сертификат агента регистрации.
- 24 После того как сертификат агента регистрации выбран, в окне мастера запроса сертификата будет доступна кнопка **Далее**. Нажмите на неё.

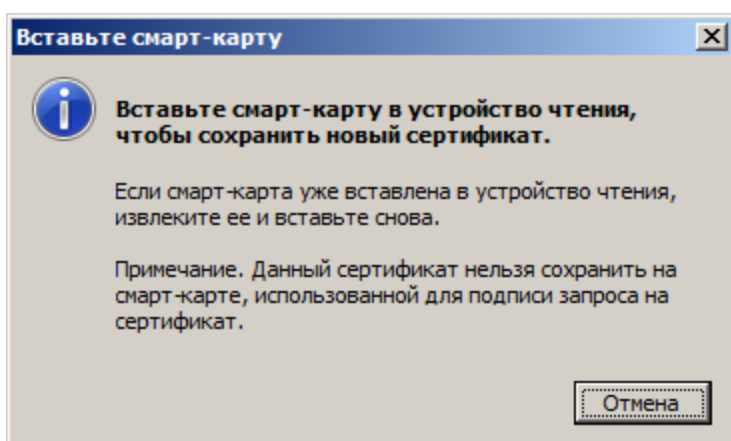
Отобразится окно запроса сертификатов.



25 Выберите **Пользователь JaCarta (централизованная процедура)** и нажмите **Далее**.
Отобразится окно выбора пользователя, от имени которого запрашивается сертификат.



- 26 Воспользуйтесь кнопкой **Обзор**, чтобы выбрать нужного пользователя.
 - 27 После того как пользователь, от чьего имени будет запрошен сертификат, выбран, станет доступной кнопка **Заявка**. Нажмите на эту кнопку.
- Отобразится следующее окно.

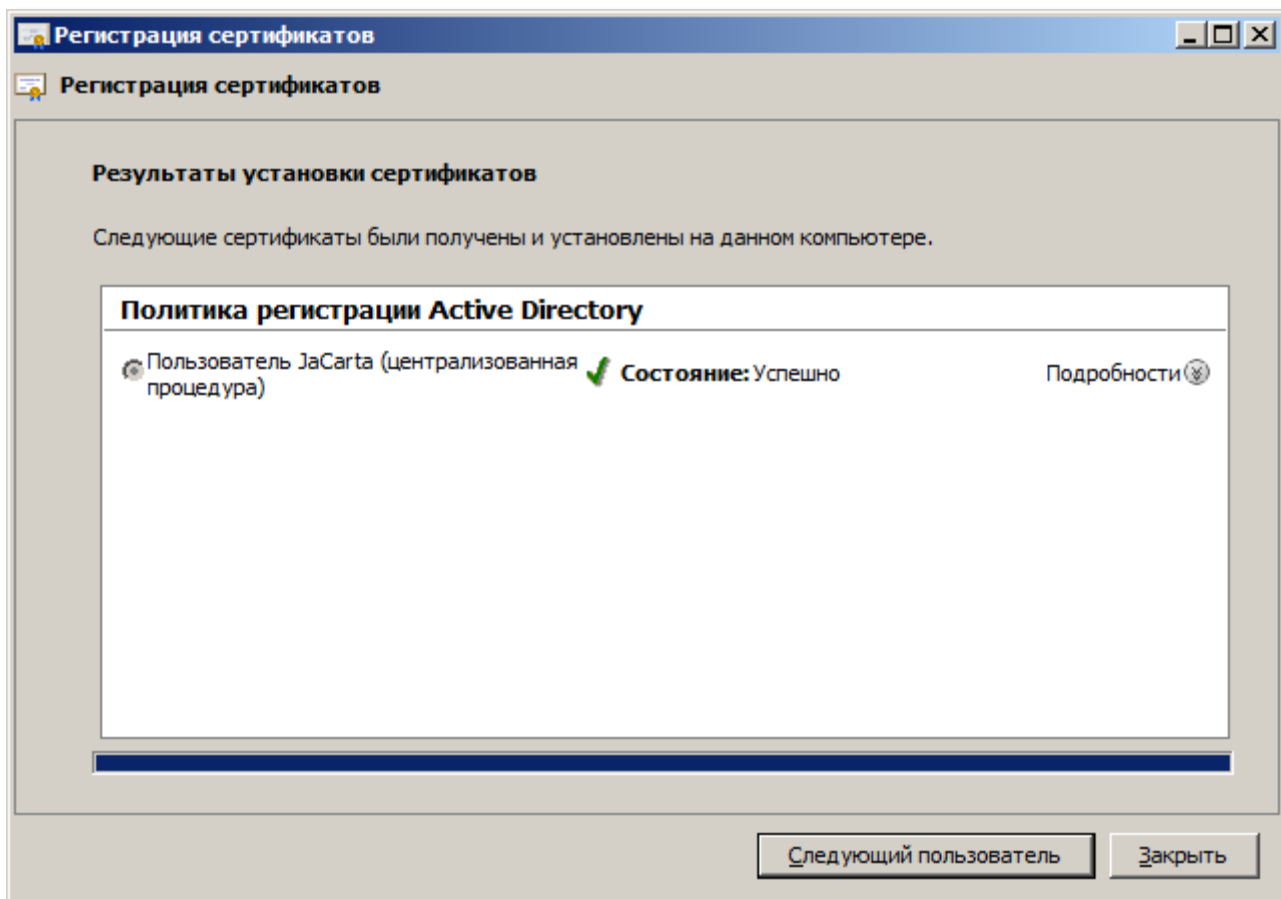


- 28 Подсоедините электронный ключ JaCarta к компьютеру. Если он подсоединён, отсоедините его и подсоедините вновь.
- Отобразится окно ввода пароля пользователя JaCarta.

- 29 Подтвердите доступ уровня пользователя к электронному ключу JaCarta и установите флажок В следующий раз сменить пароль (установка флажка нужна для того, чтобы пользователь сменил пароль после получения электронного ключа JaCarta на руки).
- 30 Нажмите Подтвердить.

Процесс генерации ключевой пары займёт некоторое время.

В случае успешной записи сертификата в память электронного ключа JaCarta отобразится следующее окно.



Вход в домен с электронным ключом JaCarta

Процедура входа (действия пользователя)

Чтобы войти в домен с помощью электронного ключа JaCarta.

- 1 После загрузки экрана приветствия Windows подсоедините электронный ключ JaCarta к компьютеру.

Отобразится экран ввода пароля пользователя JaCarta.



(Если экран не отобразился, щёлкните на значке  на экране приветствия Windows.)

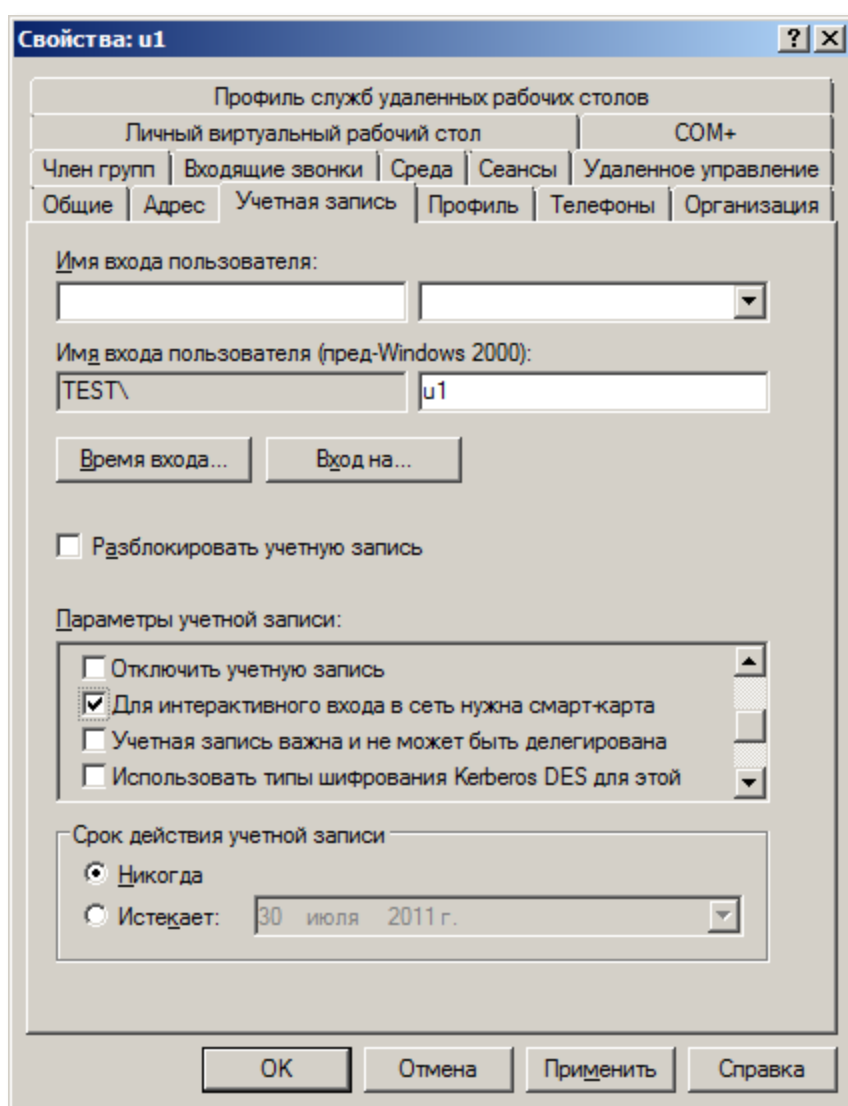
- 2 В отобразившемся поле для ввода пароля введите пароль пользователя JaCarta и нажмите клавишу ВВОД.

Отказ от использования паролей (инструкция для администратора)

Если вы успешно настроили возможность регистрации пользователя с помощью электронного ключа JaCarta, вы можете в целях безопасности запретить пользователю регистрацию в домене с использованием пароля.

Для того чтобы применить это требование к пользователю, выполните следующее.

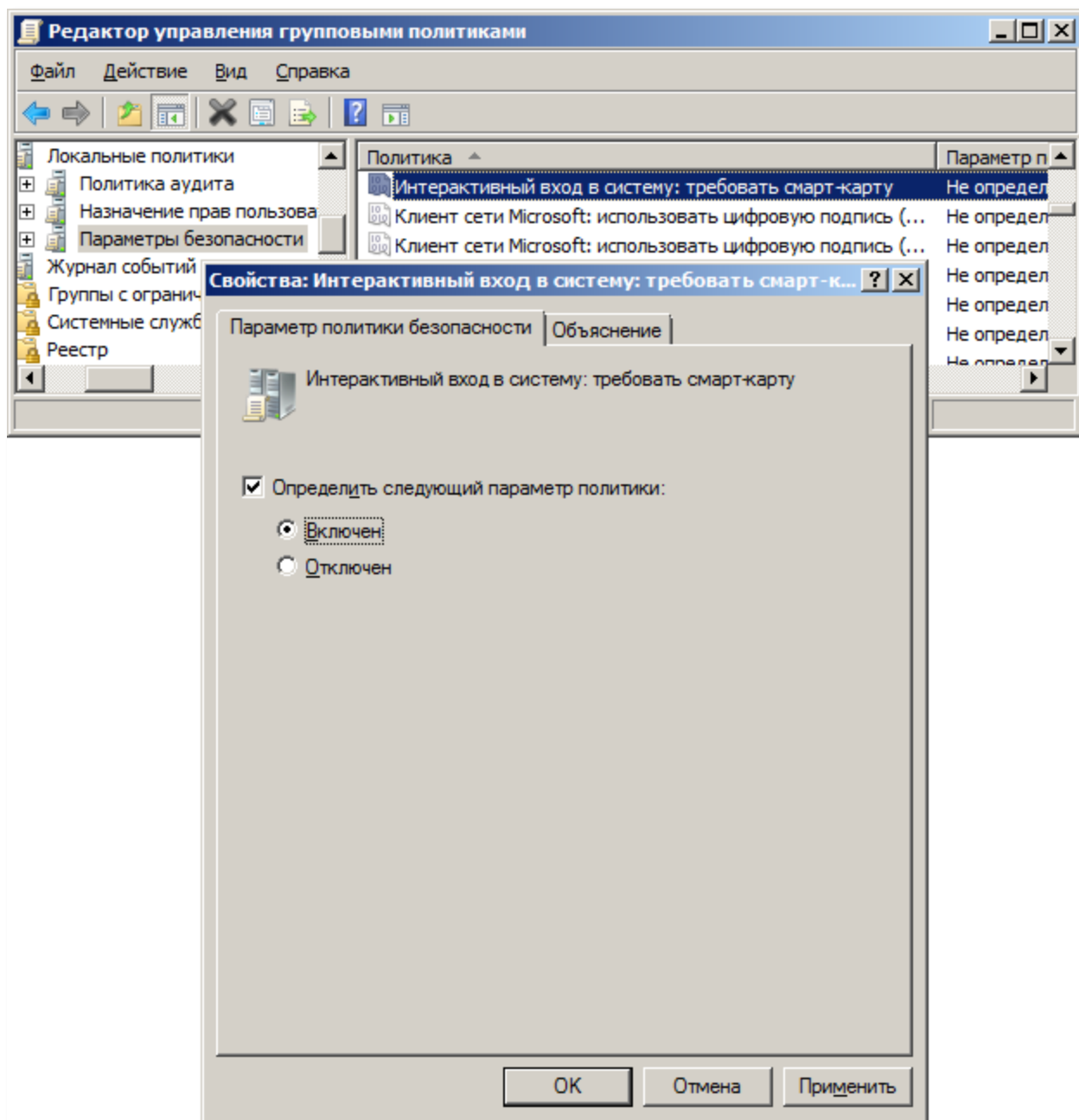
- 1 Откройте оснастку **Active Directory – пользователи и компьютеры**.
- 2 В дереве консоли, в узле с именем домена откройте **Users (Пользователи)**.
- 3 Дважды щёлкните по учётной записи пользователя в списке, чтобы открыть окно свойств учётной записи.
- 4 Откройте вкладку **Учётная запись**.



- 5 В списке **Параметры учётной записи** установите флажок **Для интерактивного входа в сеть нужна смарт-карта**.
- 6 Нажмите ОК.

Для того чтобы запретить группе пользователей вход в домен с использованием пароля, отредактируйте соответствующий объект групповой политики (**Конфигурация компьютера > Политики > Конфигурация Windows > Параметры безопасности > Локальные политики > Параметры безопасности > Интерактивный вход в систему: Требовать смарт-карту**):

- 7 Установите флажок **Определить следующий параметр политики**.
- 8 Выберите **Включен**.



Если вы хотите, чтобы обновлённая политика начала действовать немедленно, введите на контроллере домена команду `gpupdate /force`.

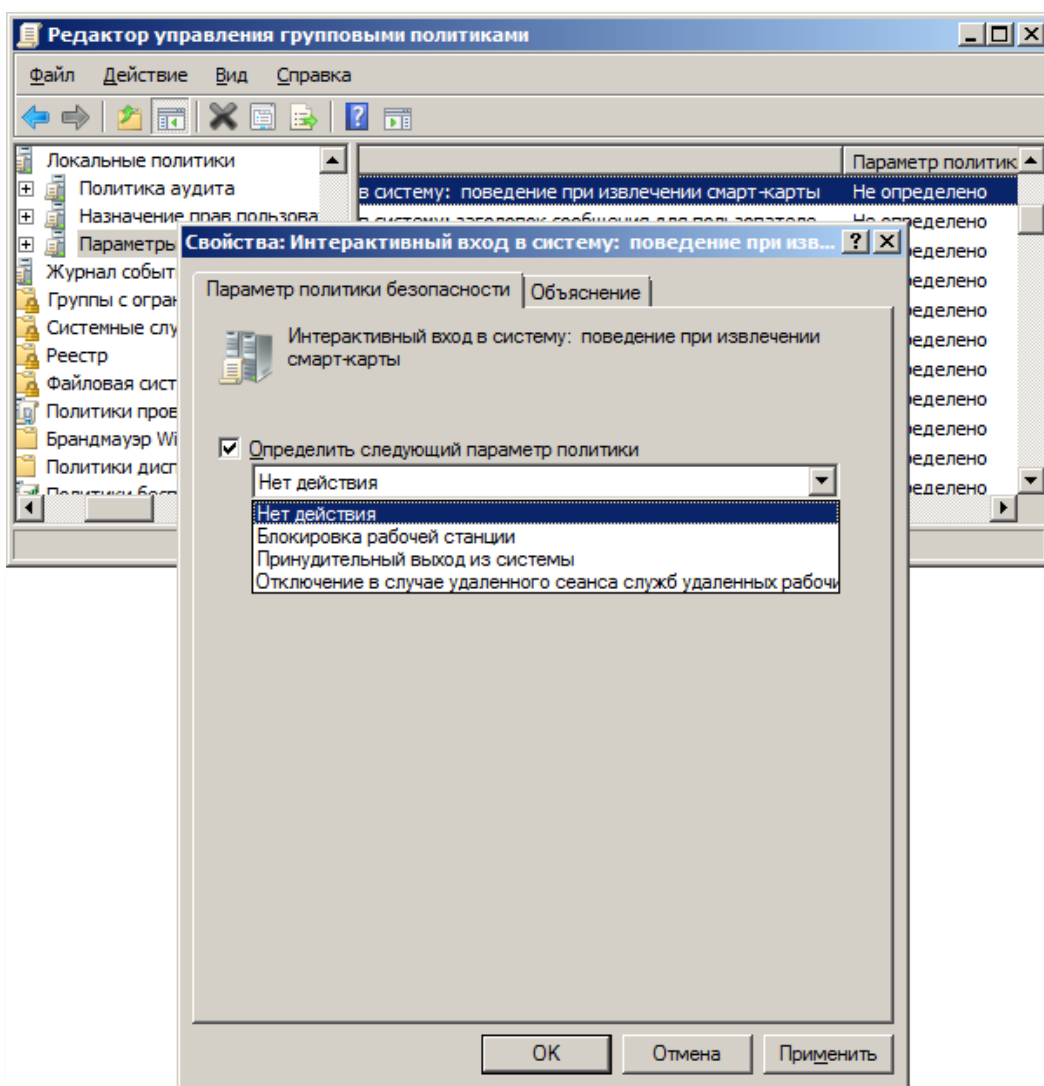
Блокирование компьютера и принудительный выход пользователя при отсоединении электронного ключа JaCarta

Действия администратора

Существует возможность в целях безопасности автоматически блокировать компьютер или осуществлять принудительный выход пользователя из системы при отсоединении электронного ключа JaCarta от компьютера.

Для этого выполните следующие действия.

- 1 Отредактируйте соответствующий объект групповой политики (**Конфигурация компьютера > Политики > Конфигурация Windows > Параметры безопасности > Локальные политики > Параметры безопасности > Интерактивный вход в систему: поведение при извлечении смарт-карты**):
 - Нет действия;
 - Блокировка рабочей станции;
 - Принудительный выход из системы;
 - Отключение в случае удалённого сеанса служб удаленных рабочих столов.



Данный объект можно использовать как в доменных политиках, так и в политиках, применяемых к отдельным подразделениям. Если вы хотите, чтобы обновлённая политика начала действовать немедленно, введите на контроллере домена команду `gpupdate /force`.

- 2 На каждом компьютере, к которому пользователи будут подключаться с использованием электронного ключа JaCarta, запустите службу `ScPolicySvc` и настройте её последующий автоматический запуск. Для этого из командной строки последовательно выполните следующие команды
 - `net start ScPolicySvc`
 - `sc config scpolicysvc start=auto`

Действия пользователя

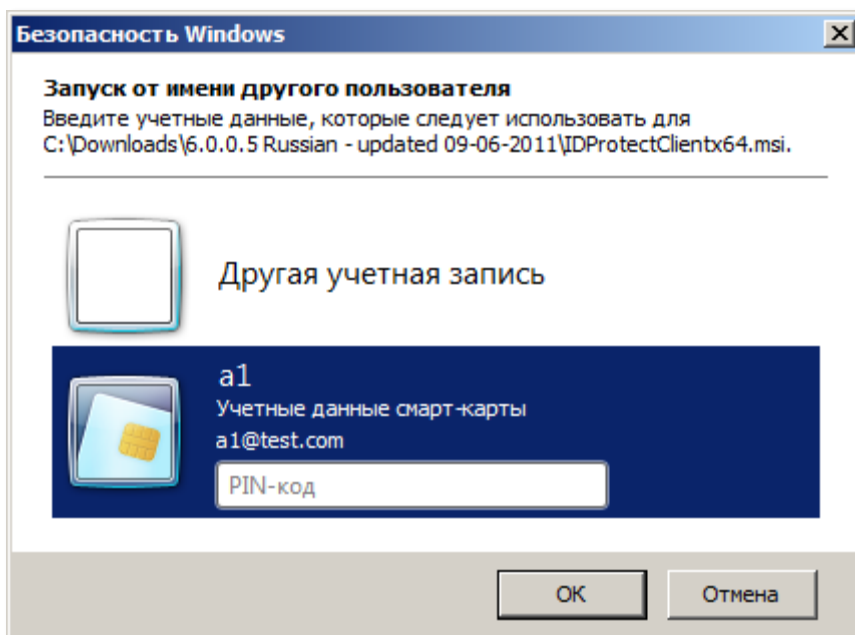
Если вы отсоединили электронный ключ JaCarta от компьютера, и произошёл принудительный выход, для возобновления работы повторно войдите в домен. Если при отсоединении электронного ключа JaCarta компьютер заблокировался, разблокируйте его. Процедура разблокирования полностью аналогична процедуре входа.

Запуск приложений от имени другого пользователя

Существует возможность использовать авторизацию с использованием электронного ключа JaCarta при запуске приложений от имени другого пользователя.

Для того чтобы запустить программу от имени другого пользователя, выполните следующую последовательность действий.

- 1 Убедитесь в том, что электронный ключ пользователя, от имени которого вы хотите запустить приложение, подключен к компьютеру. На USB-токене JaCarta должен гореть световой индикатор.
- 2 Зажмите клавишу **SHIFT**, щёлкните правой кнопкой мыши на ярлыке или значке исполняемого файла и выберите **Запуск от имени другого пользователя**.
- 3 В окне Запуск от имени другого пользователя выберите Учётные данные смарт-карты, введите пароль пользователя JaCarta, как показано на изображении ниже.

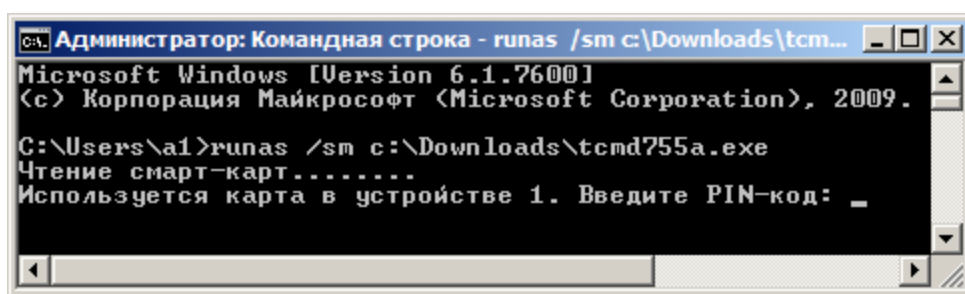


- 4 Нажмите **ОК**.

Вы можете также запускать приложения и консольные утилиты от имени другого пользователя из командной строки. Для этого выполните следующее.

- 5 Убедитесь в том, что электронный ключ пользователя, от имени которого вы хотите запустить приложение, подключен к компьютеру. На USB-токене JaCarta должен гореть световой индикатор.
- 6 В командной строке введите `runas /sm <программа>`, где <программа> — путь к исполняемому файлу или имя утилиты.
- 7 Windows начнет перебор виртуальных и физических устройств чтения смарт-карт. Для каждого устройства, в котором Windows не обнаружит смарт-карту (электронный ключ JaCarta), будет выведено сообщение об ошибке Нет карты в устройстве чтения N/No card on reader N, где N – порядковый номер устройства. Для каждого устройства, в котором Windows обнаружит смарт-карту (электронный ключ JaCarta) без сертификата пользователя, будет выведено сообщение Ошибка при чтении смарт-карты в устройстве чтения N/Error reading smart card on reader N. В случае если Windows найдет несколько смарт-карт (электронных ключей JaCarta) с сертификатами пользователей, будет выведен список соответствующих устройств с указанием имён пользователя. Введите номер устройства, в котором хранится сертификат пользователя, от имени которого вы хотите запустить приложение.

Отобразится следующее сообщение.



- 8 Введите пароль пользователя соответствующего электронного ключа JaCarta и нажмите клавишу ВВОД.

Организация VPN-соединения для доступа к информационным ресурсам

Существует возможность использовать электронные ключи JaCarta для подключения по VPN. Процедура настройки состоит из двух этапов

- 1 Настройка сервера маршрутизации и удалённого доступа
- 2 Настройка рабочих станций

Необходимые действия приведены в подразделах ниже.

Настройка сервера маршрутизации и удалённого доступа

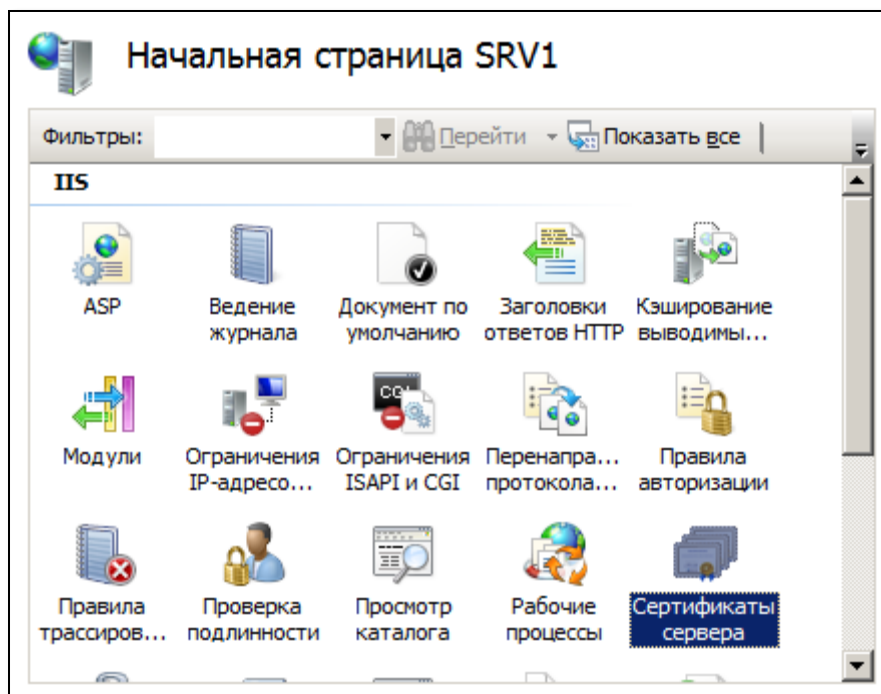
Для организации VPN-соединения необходим сервер маршрутизации и удалённого доступа. Перед тем как приступить к настройке, для сервера необходимо запросить сертификат.

Внимание:

Сертификат необходимо установить до того, как будет установлена роль Службы политики сети и доступа.

Установка сертификата сервера

- 3 Запустите консоль диспетчера служб IIS, выберите сервер и в центральной части окна сделайте двойной щелчок на иконке **Сертификаты сервера** (см. изображение ниже).



- 4 В колонке **Действия** справа щёлкните на ссылке **Создать сертификат домена**.

Отобразится следующая форма.

Создать сертификат

Свойства различающегося имени

Укажите данные, необходимые для сертификата. В полях "Область, край" и "Город" должны быть указаны полные официальные названия без сокращений.

Полное имя:

Организация:

Подразделение:

Город

Область, край:

Страна или регион:

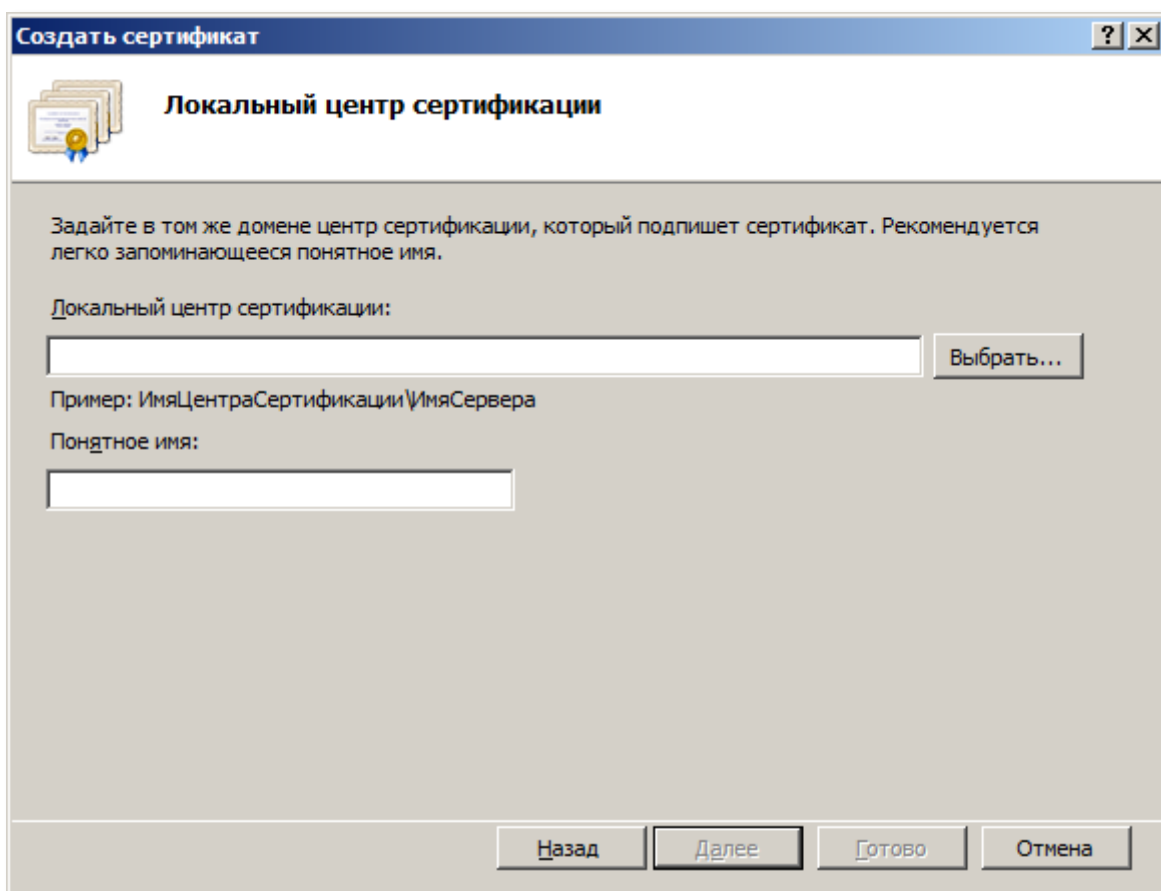
Назад Далее Готово Отмена

- 5 Заполните необходимые поля и нажмите **Далее**.

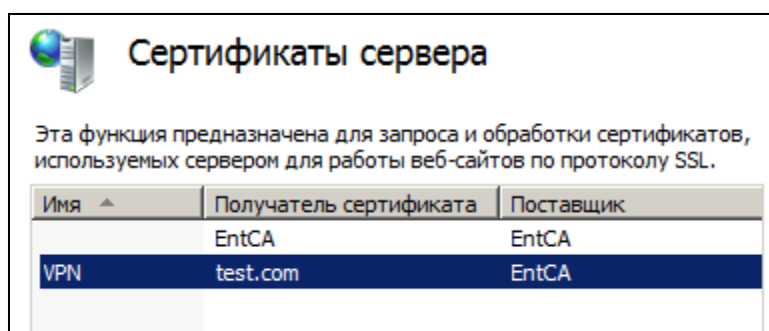
Внимание

Значение в поле Полное имя будет использоваться клиентом для соединения с VPN-сервером, рекомендуется использовать в данном поле полное имя сервера.

Отобразится следующее окно.



- 6 Воспользуйтесь кнопкой **Обзор**, чтобы выбрать используемый центр сертификации. При необходимости в поле **Понятное имя** введите понятное имя для сертификата и нажмите **Далее**. Сертификат появится в списке сертификатов сервера.

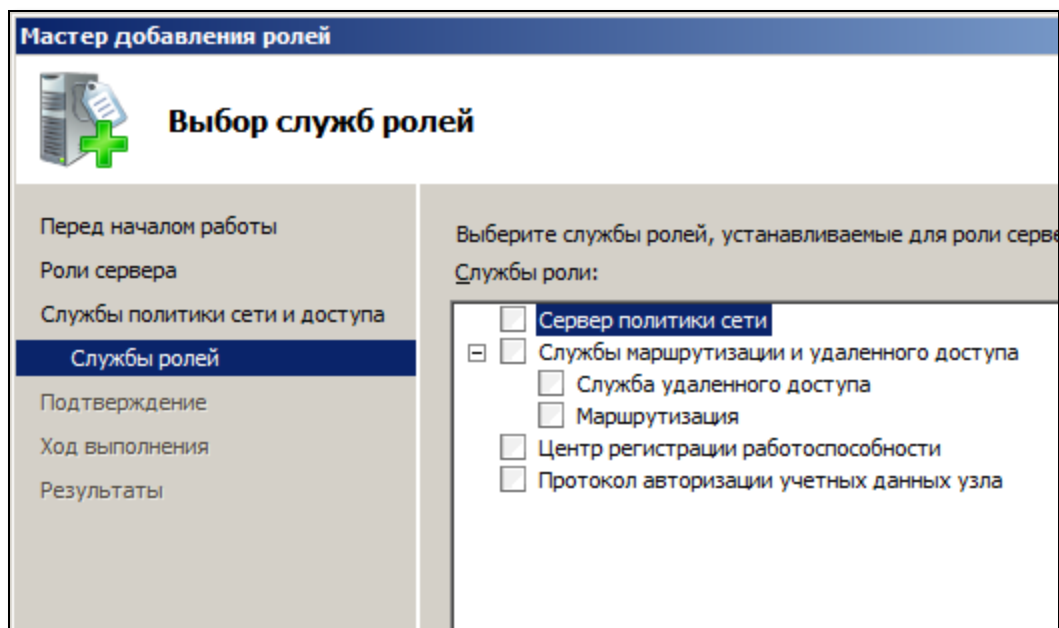


Установка роли Службы политики сети и доступа

Чтобы установить роль **Службы политики сети и доступа**, выполните следующие действия.

- 1 Запустите диспетчер сервера, выберите **Роли** и в правой части окна щёлкните на ссылке **Добавить роли**.
- 2 В окне **Выбор ролей** сервера отметьте к установке **Службы политики сети и доступа** и нажмите **Далее**.

- 3 В следующем окне отобразится информация об устанавливаемой роли. Нажмите **Далее**.
Отобразится следующее окно.



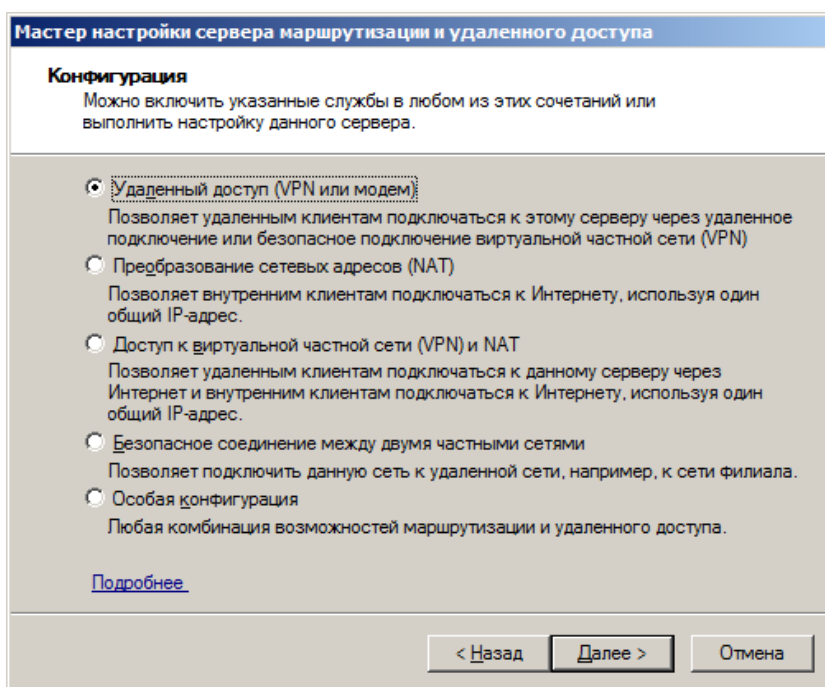
Отметьте к установке Служба удалённого доступа и Маршрутизация и нажмите **Далее**.

- 4 В окне подтверждения выбранных элементов для установки нажмите **Установить**.
- 5 После установки переходите к настройке установленных служб.

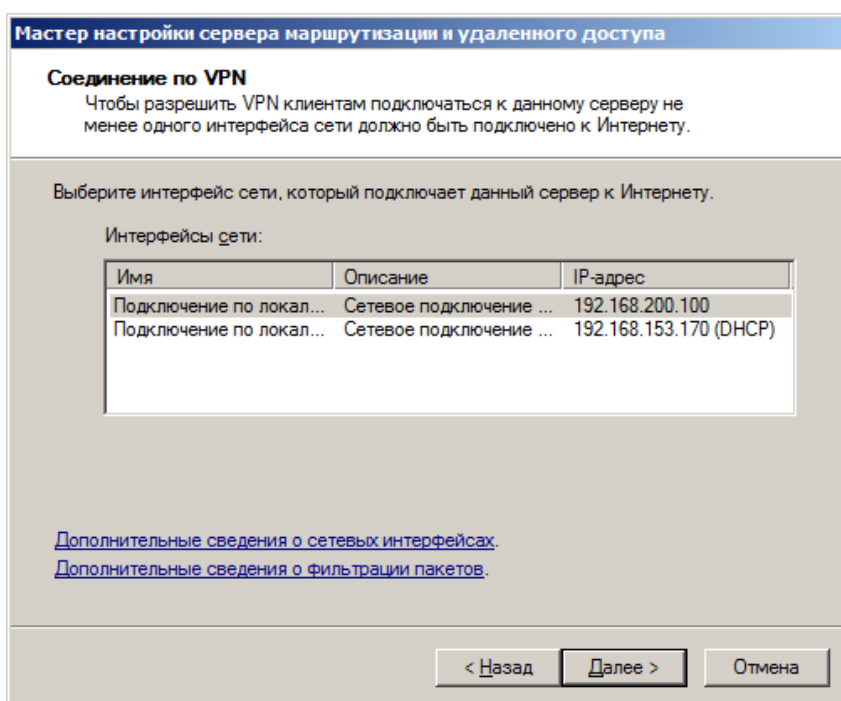
Настройка служб политики сети и доступа

- 1 В диспетчере сервера разверните узел Службы политики сети и доступа, щёлкните правой кнопкой на Маршрутизация и удалённый доступ и выберите Настроить и включить маршрутизацию и удалённый доступ.
- 2 В окне приветствия мастера настройки маршрутизация и удалённого доступа нажмите **Далее**.

Отобразится следующее окно.

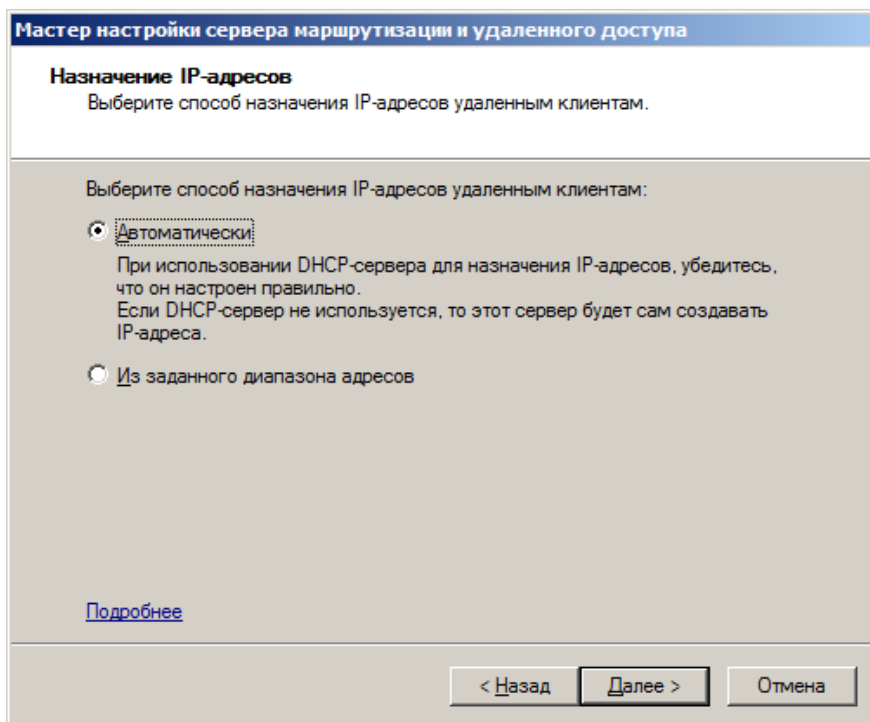


- 3 Выберите **Доступ к виртуальной частной сети (VPN) и NAT** и нажмите **Далее**.
Отобразится окно выбора сетевого адаптера.

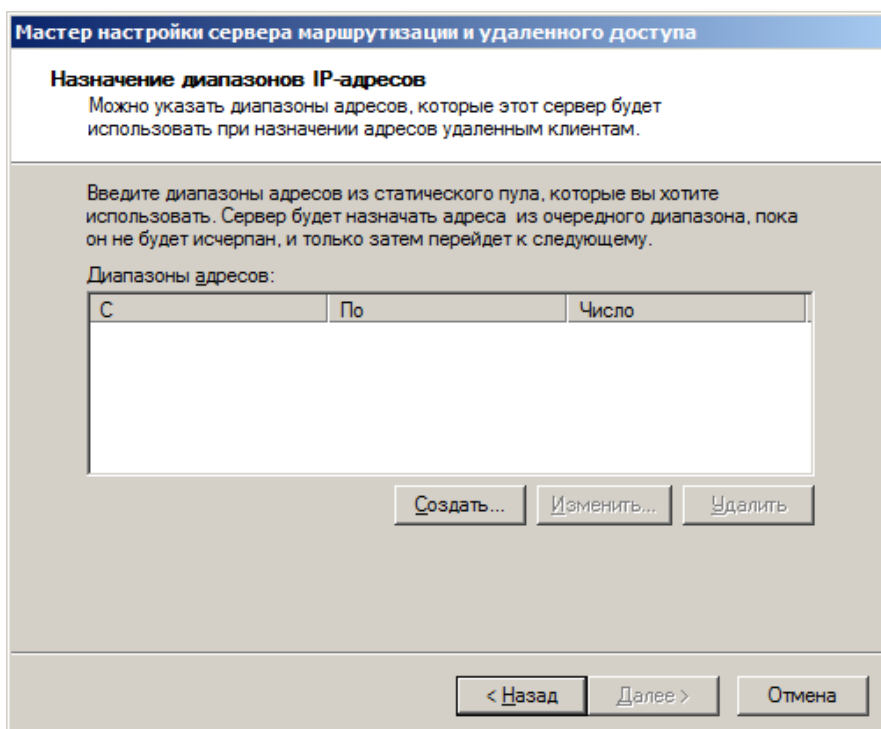


- 4 Выберите внешний (не доменный) сетевой адаптер и нажмите **Далее**.

Отобразится следующее окно.

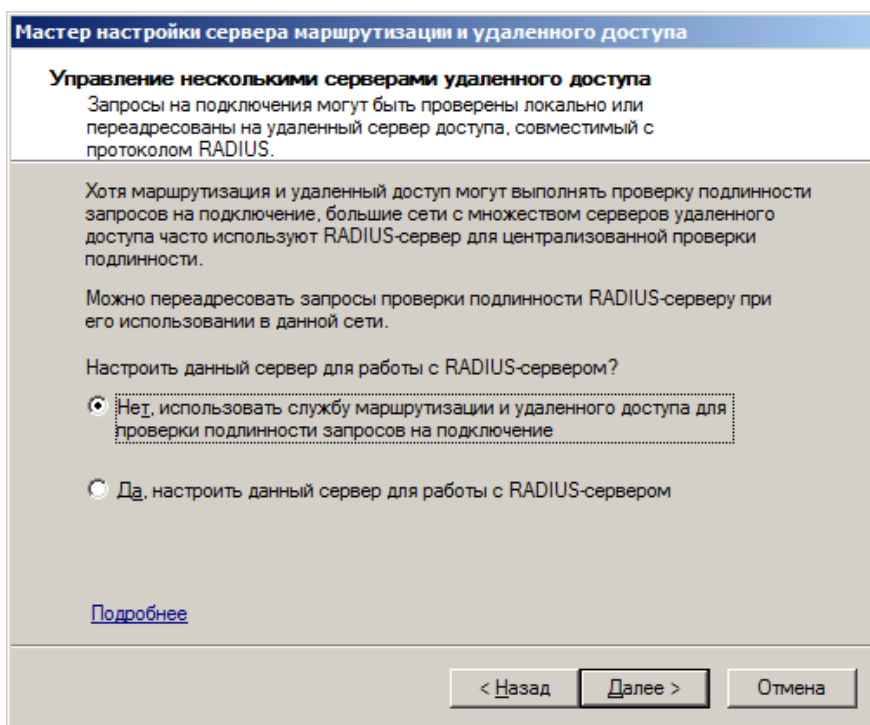


- 5 Выберите Из заданного диапазона адресов и нажмите Далее.
Отобразится следующее окно.



- 6 Нажмите **Создать** и укажите диапазон адресов, которые сервер будет назначать подключающимся пользователям. После назначения диапазона адресов нажмите **Далее**.

Отобразится следующее окно.

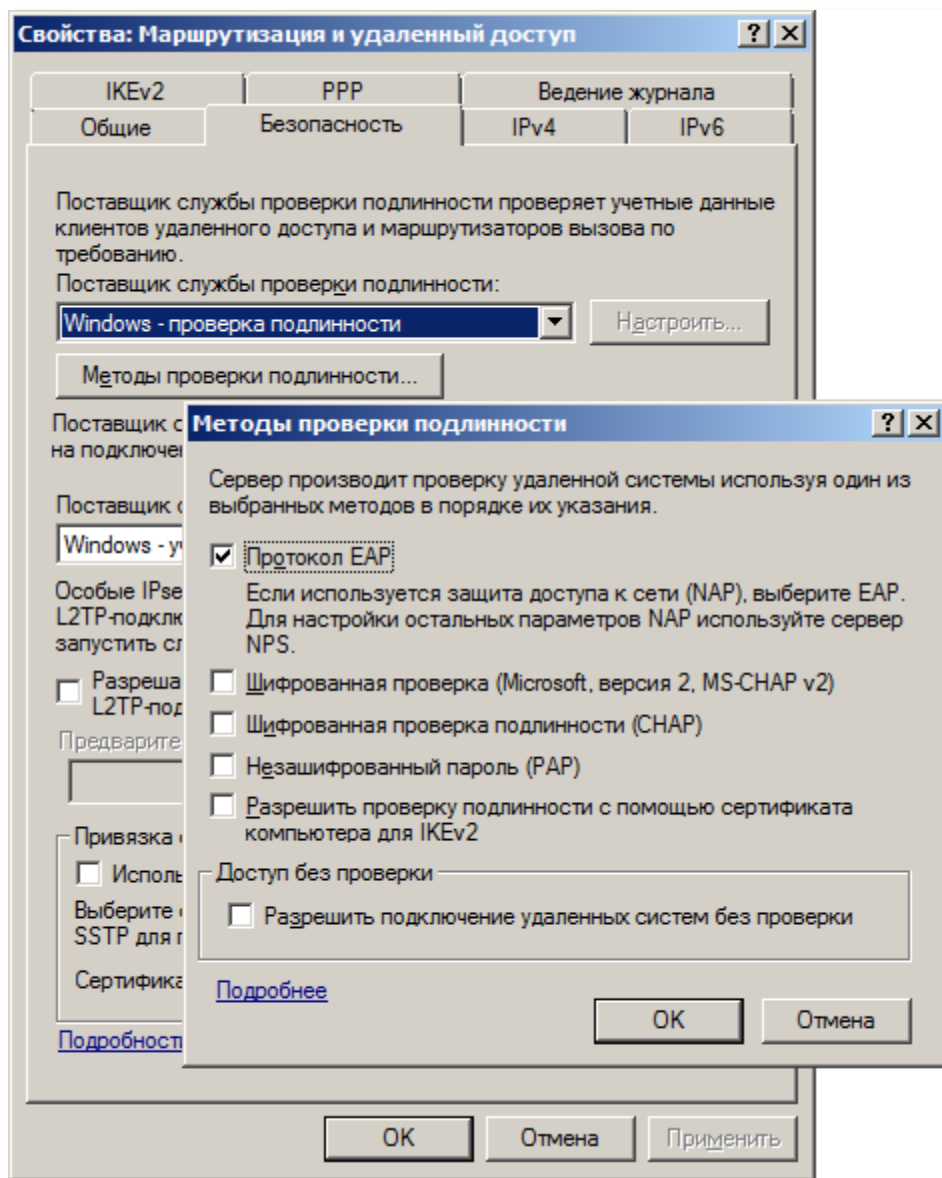


- 7 Оставьте отмеченным пункт Нет, использовать службу маршрутизации и удалённого доступа для проверки подлинности запросов на подключение и нажмите **Далее**.
- 8 В следующем окне нажмите **Готово**.

Конфигурирование сервера маршрутизации и удалённого доступа займёт некоторое время.

- 9 По завершении конфигурирования в консоли диспетчера сервера щёлкните правой кнопкой на **Маршрутизация и удалённый доступ** и нажмите **Свойства**.
- 10 В отобразившемся окне выберите вкладку **Безопасность**.

- 11 Нажмите **Методы проверки подлинности** и в открывшемся окне проверки подлинности оставьте отмеченным только пункт **Протокол EAP**, после чего нажмите **ОК** (см. изображение ниже).



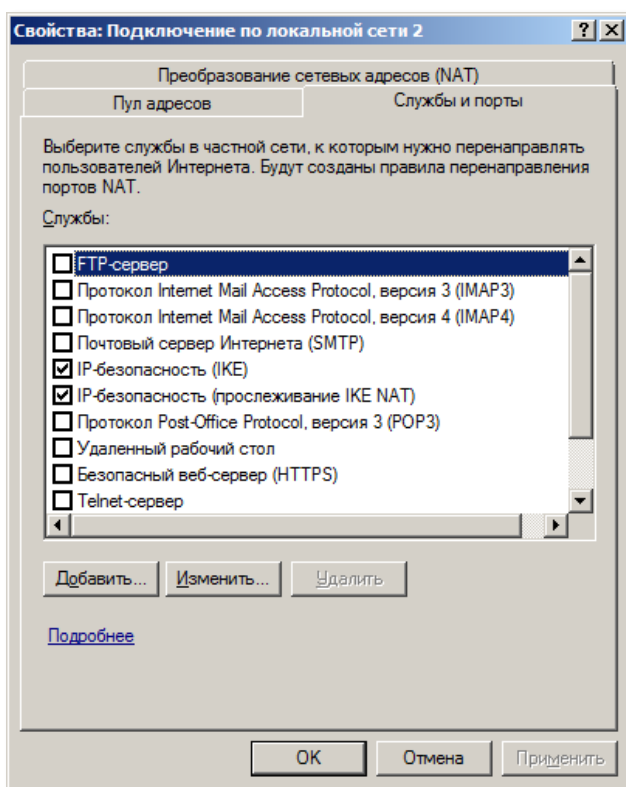
- 12 Нажмите **ОК**, чтобы закрыть окно свойств маршрутизации и удалённого доступа.
- 13 В консоли диспетчера сервера выберите **Роли > Услуги политики сети и доступа > Маршрутизация и удалённый доступ > IPv4 > Преобразование сетевых адресов (NAT)**.

Примечание

В данном руководстве подразумевается, что используются IP-адреса версии 4.

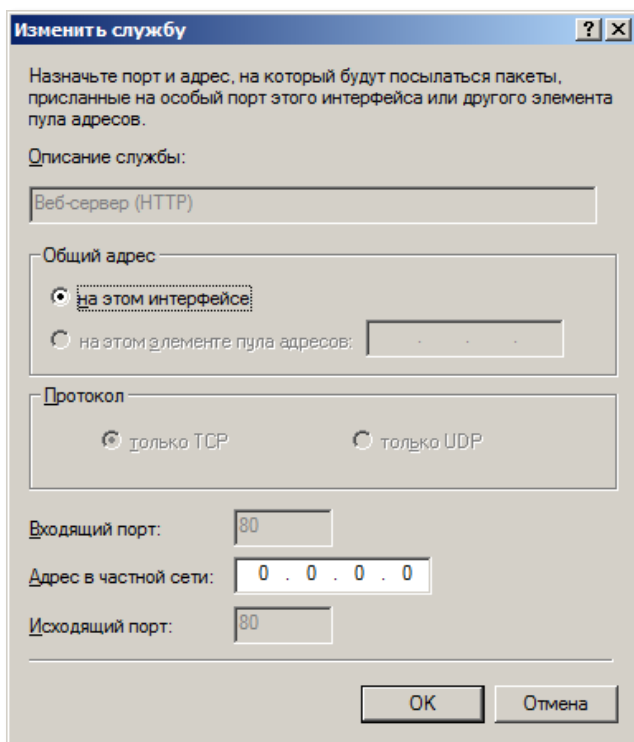
- 14 В центральной части окна щёлкните правой кнопкой на иконке внешнего соединения, выберите **Свойства** и в открывшемся окне выберите вкладку **Услуги и порты**.

Окно примет следующий вид.



15 Установите флажок **Веб-сервер (HTTP)**.

Отобразится следующее окно.

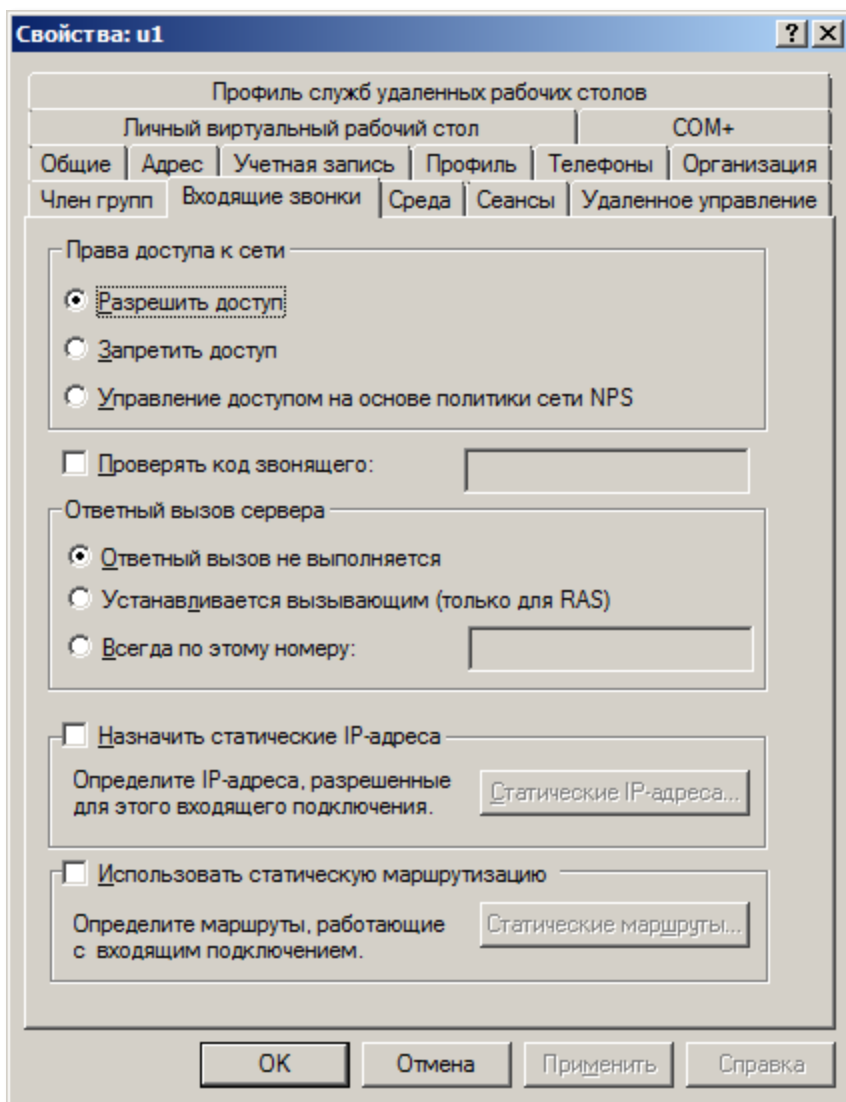


- 16 В поле **Адрес** в частной сети укажите IP-адрес вашего Web-сервера и нажмите **ОК**.

Настройка учётной записи пользователя

Подключаться к сети через VPN-соединения могут только те пользователи, учётные записи которых настроены для таких подключений. Для того чтобы настроить учётную запись пользователя, выполните следующие действия.

- 1 В окне свойств учётной записи откройте вкладку **Входящие звонки**.



- 2 Выберите **Разрешить доступ**.
- 3 Нажмите **ОК**.

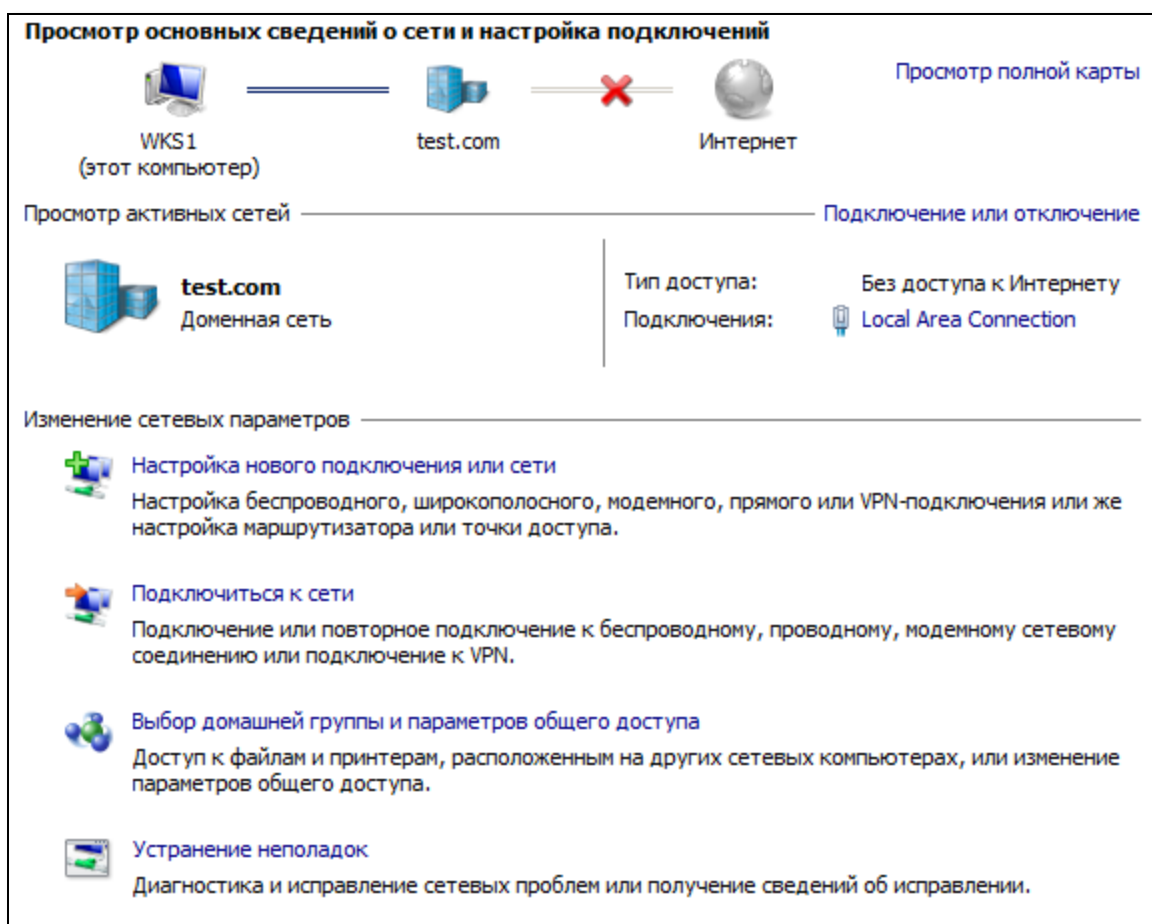
Для того чтобы настроить большое количество пользователей на подключение к виртуальной частной сети, рекомендуется использовать политики удалённого доступа, регулирующие доступ в зависимости от времени, дня недели, принадлежности пользователя к группам безопасности Windows Server 2008 R2 Enterprise или от типа подключения.

Настройка рабочей станции

Для того чтобы подключаться к сети через VPN-соединение, необходимо настроить соответствующее подключение на рабочей станции. Для VPN-подключения с использованием электронного ключа JaCarta на рабочей станции должен быть установлен JC-Client. Кроме того, в хранилище доверенных корневых центров сертификации данного пользователя должен содержаться сертификат центра сертификации, присутствующего в пути сертификации сертификата VPN-сервера. Для того чтобы настроить VPN-соединение на рабочей станции, выполните следующее.

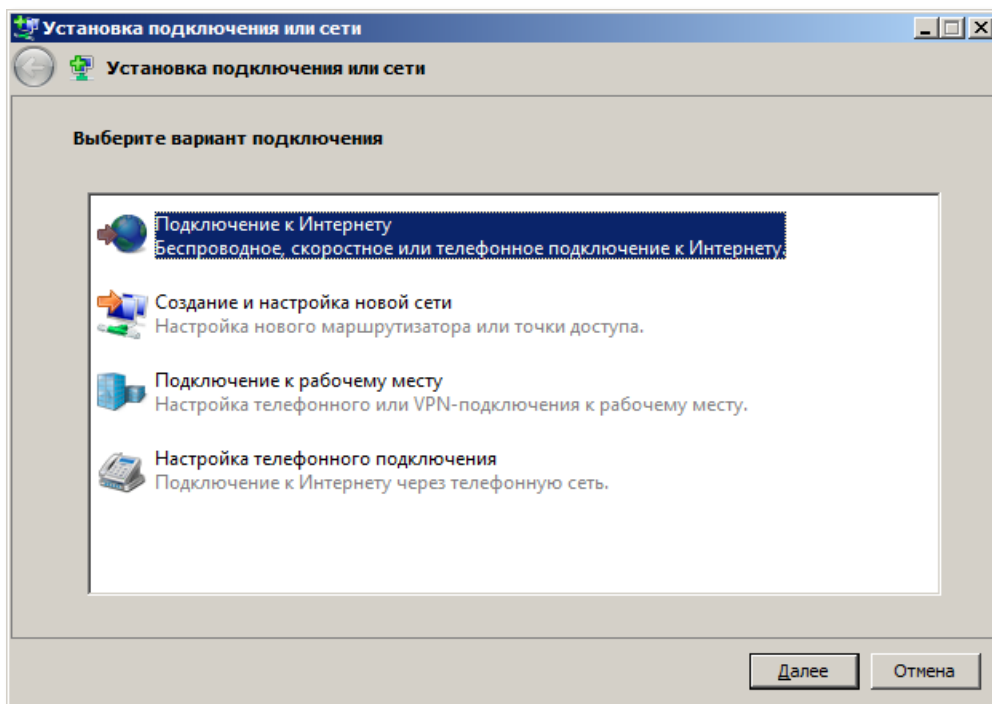
- 1 Убедитесь в том, что на компьютере установлен JC-Client.
- 2 Убедитесь в том, что в хранилище доверенных корневых центров сертификации данного пользователя содержится сертификат центра сертификации, присутствующего в пути сертификации сертификата VPN-сервера.
- 3 Выберите Пуск > Панель управления > Центр управления сетями и общим доступом.

Отобразится следующее окно.



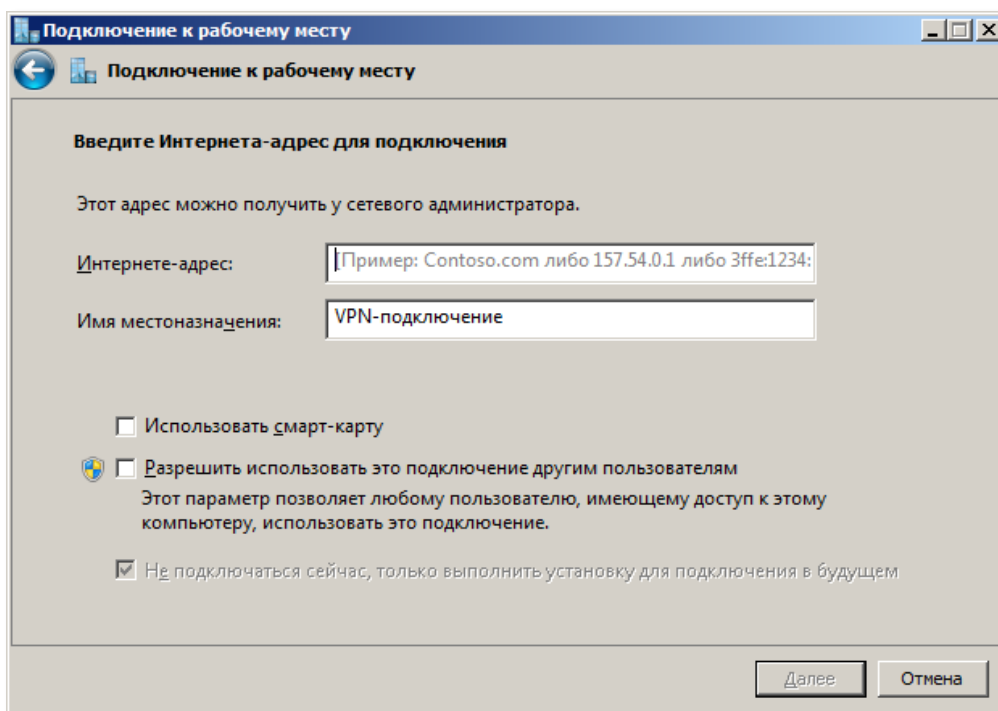
- 4 Щёлкните на ссылке **Настройка нового подключения или сети**.

Отобразится следующее окно.



5 Выберите Подключение к рабочему месту и нажмите Далее.

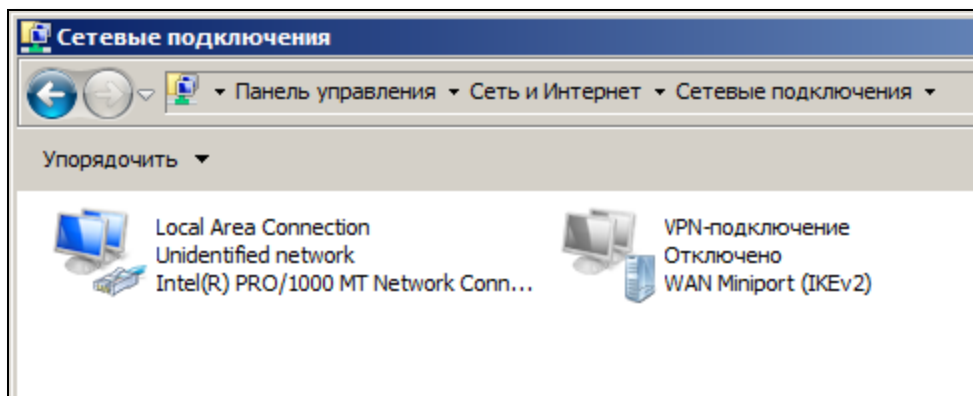
Отобразится следующее окно.



6 В поле **Интернет адрес** введите IP-адрес VPN-сервера, через который будет осуществляться VPN-соединение и установите флажок **Использовать смарт-карту**. (При необходимости введите свое значение в поле **Имя местоназначения**.)

- 7 Нажмите **Создать**.
- 8 После того как подключение будет создано, нажмите **Заккрыть**.
- 9 В окне центра управления сетями и общим доступом щёлкните на ссылке **Изменение параметров адаптера**.

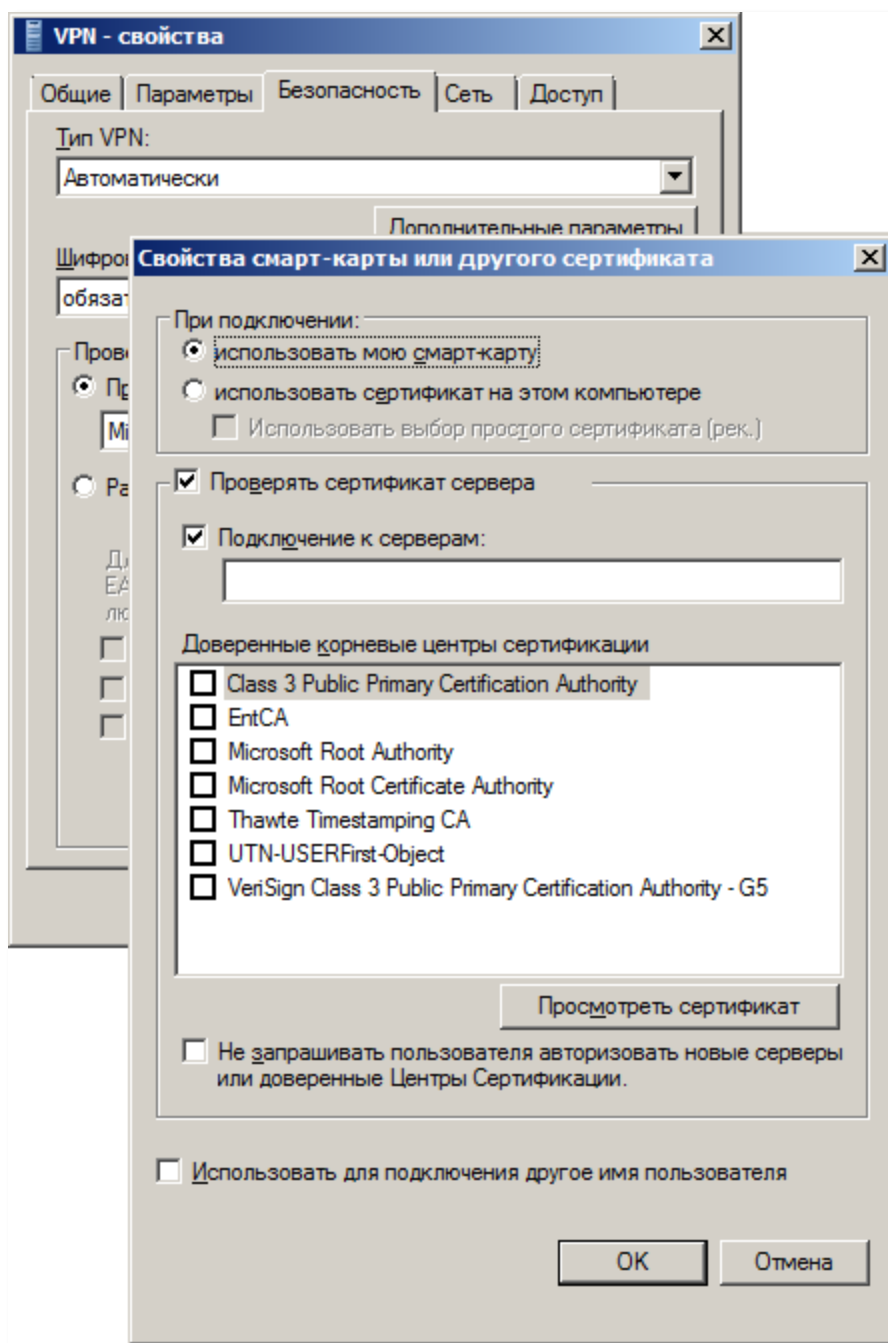
Отобразится окно следующего вида.



Щёлкните правой кнопкой на созданном VPN-соединении и выберите **Свойства**.

- 10 В отобразившемся окне выберите вкладку **Безопасность**.
- 11 Выберите пункт **Протокол расширенной проверки подлинности** и в соответствующем списке выберите **Microsoft: Смарт-карта или иной сертификат (шифрование включено)**.
- 12 Нажмите **Свойства**.

Отобразится окно Свойства смарт-карты или другого сертификата.



- 13 В поле **Подключение к серверам** введите имя сервера, на котором установлены службы политики сети и доступа (оно должно совпадать с полным именем, указанным в сертификате сервера/домена).
- 14 В списке **Доверенные корневые центры сертификации** установите флажок напротив центра сертификации вашей организации.
- 15 Последовательно нажмите **ОК**, чтобы закрыть данное окно и окно свойств VPN-подключения.

Подключение к удалённому рабочему столу

Электронные ключи JaCarta позволяют использовать аутентификацию при подключении к удалённому рабочему столу.

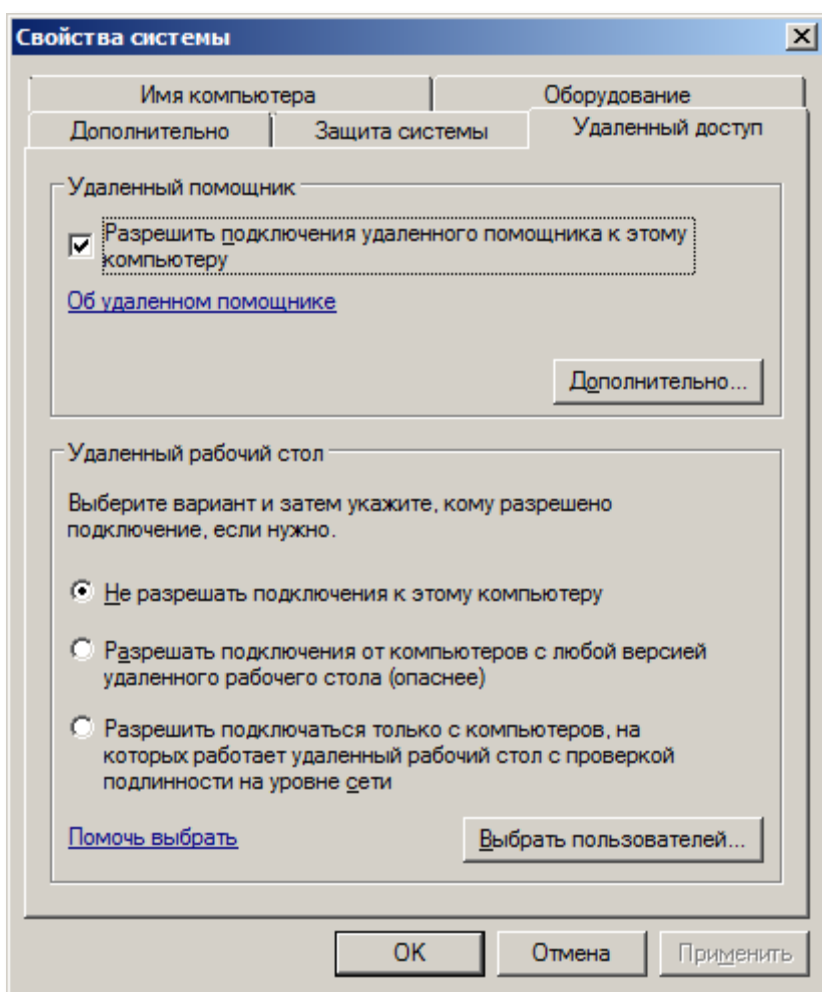
Настройка рабочих станций и серверов

Для соответствующей настройки компьютера необходимы полномочия локального администратора.

Для того чтобы к рабочему столу компьютера можно было подключаться удалённо, выполните следующее.

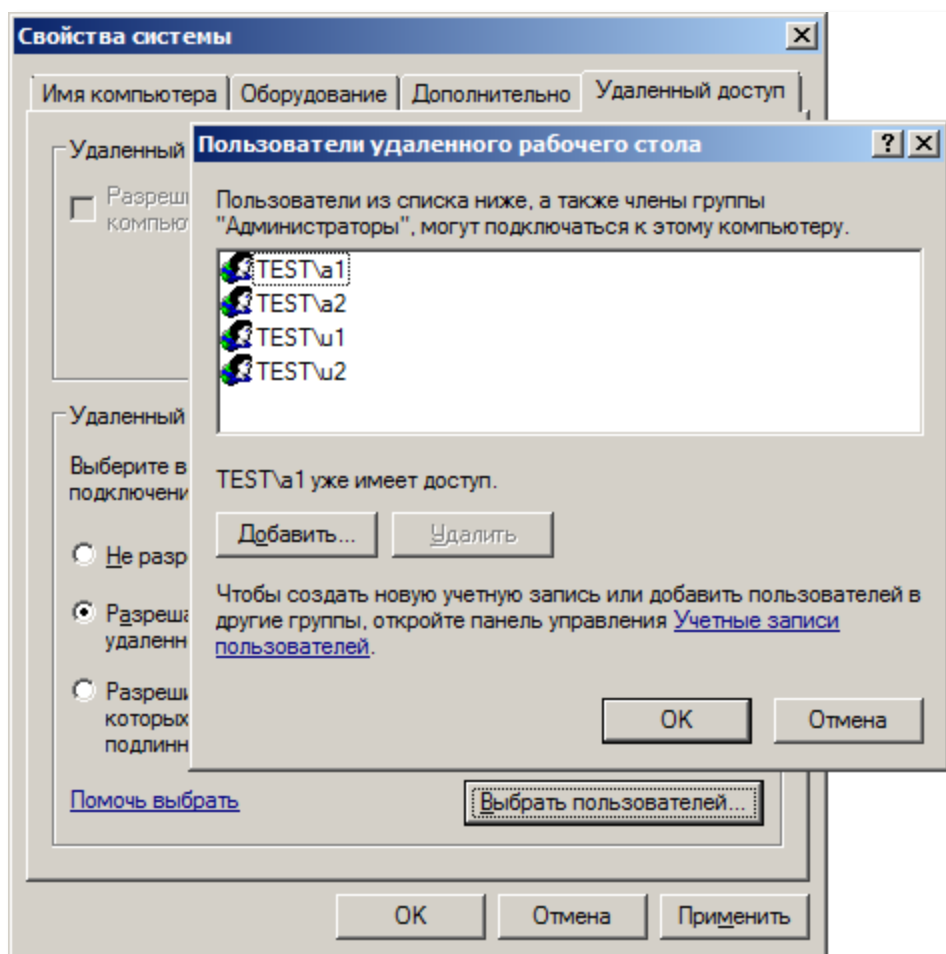
- 1 Выберите **Пуск**, щёлкните правой кнопкой на **Компьютер** и выберите **Свойства**.
- 2 В окне **Система** щёлкните на ссылке **Настройка удалённого доступа**.

Отобразится окно **Свойства системы**.



- 3 В секции **Удалённый рабочий стол** выберите один из двух пунктов
 - Разрешить подключения от компьютеров с любой версией удалённого рабочего стола
 - Разрешить подключаться только с компьютеров, на которых работает удалённый рабочий стол с проверкой подлинности на уровне сети

- 4 Если вы хотите, чтобы к компьютеру могли подключаться пользователи, не имеющие полномочий локального администратора, нажмите **Выбрать пользователей** и выберите этих пользователей или (и) группы.



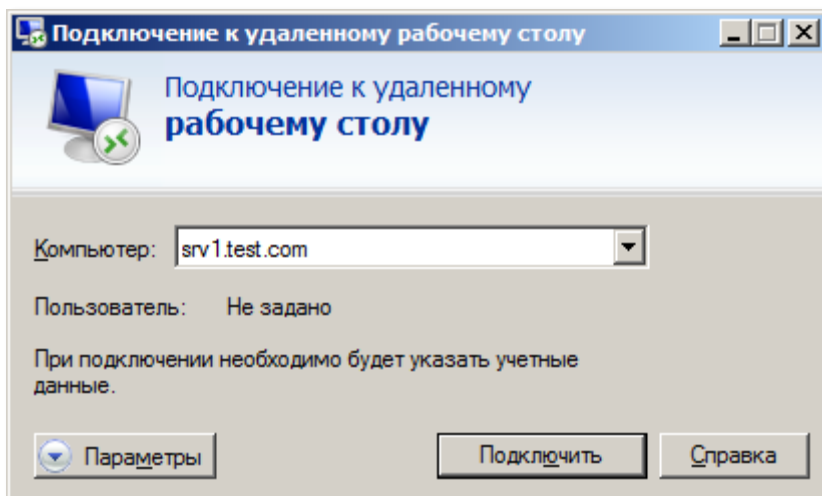
- 5 Закройте все окна нажатием на кнопки **ОК**.

Действия пользователя

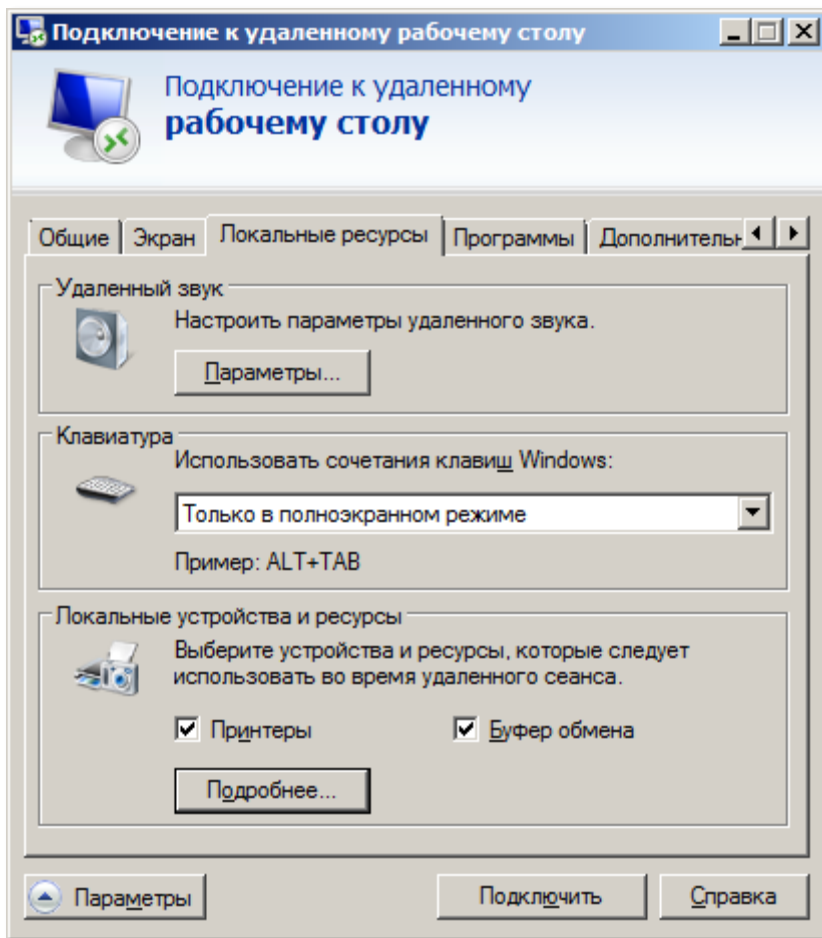
Для того чтобы подключиться к удалённому рабочему столу, выполните следующее.

- 1 Убедитесь в том, что вы располагаете электронным ключом JaCarta с сертификатом пользователя, имеющего право на подключение к удалённому рабочему столу соответствующего компьютера.

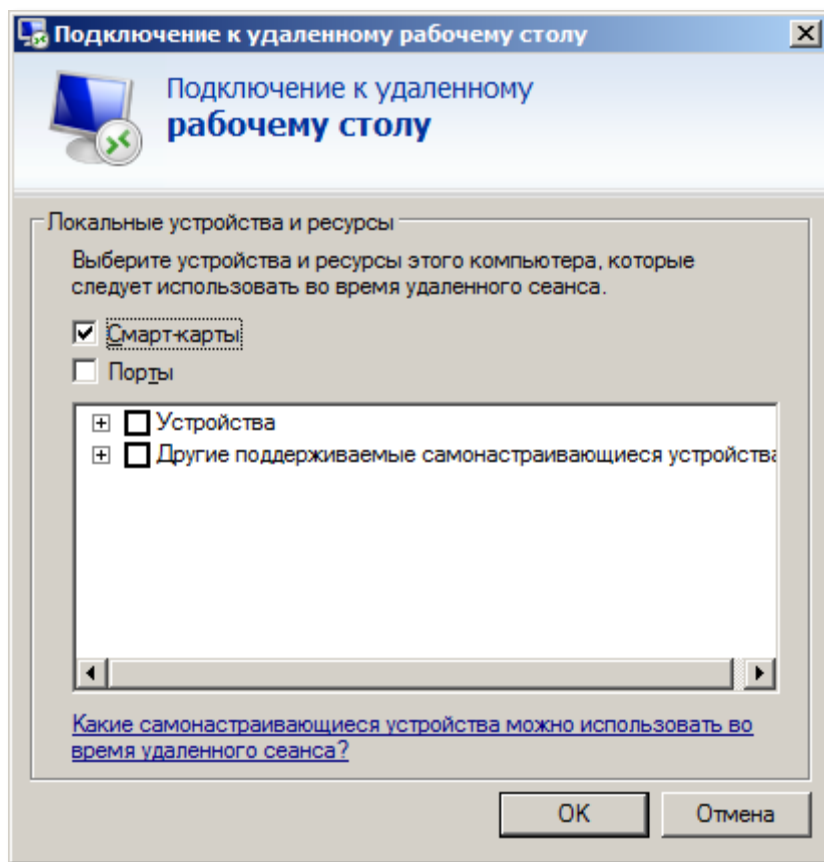
- Щёлкните **Пуск > Все программы > Стандартные > Подключение к удалённому рабочему столу**.



- В окне **Подключение к удалённому рабочему столу** в поле **Компьютер** введите имя или IP-адрес компьютера, к рабочему столу которого вы хотите подключиться.
- Нажмите **Параметры**.
- Откройте вкладку **Локальные ресурсы**.

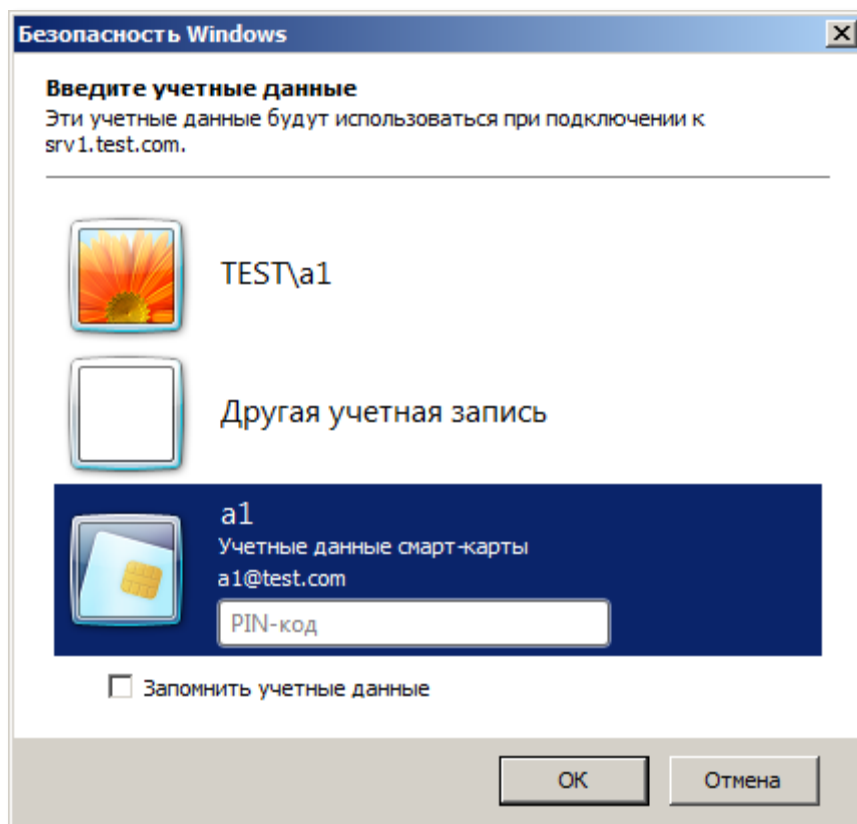


- 6 В секции **Локальные устройства** и ресурсы нажмите **Подробнее**.



- 7 Убедитесь, что флажок **Смарт-карты** установлен, и нажмите **ОК**.
- 8 Убедитесь в том, что ваш электронный ключ JaCarta подсоединен к компьютеру. На USB-токене JaCarta должен гореть световой индикатор.
- 9 Нажмите Подключить.

- 10 В окне **Безопасность Windows** выберите **Учётные данные смарт-карты** и введите пароль пользователя JaCarta.



- 11 Нажмите **ОК**.

Доступ к информационным ресурсам по HTTPS

Общие сведения

Существует возможность аутентифицироваться с использованием электронного ключа JaCarta при получении доступа к информационным ресурсам по протоколу HTTPS. Аутентификация по протоколу HTTPS может использоваться не только для доступа к защищённому Web-сайту, но и в следующих технологиях доступа к различным службам.

Outlook Web Access / Outlook Web App (OWA)	OWA представляет собой Web-приложение, которое даёт пользователям доступ к службам Exchange с использованием соединения Web-браузера по протоколу HTTPS.
Microsoft Exchange	Microsoft Outlook в сети предприятия при обращении к серверу Microsoft Exchange использует вызовы MAPI, которые основаны на технологии RPC (Вызов удалённой процедуры). Если пользователь находится за пределами интрасети предприятия, существует возможность передавать вызовы RPC через Интернет. В этом случае RPC-вызовы инкапсулированы в HTTP-туннеле и могут быть зашифрованы с помощью протокола SSL (HTTPS).
Шлюз служб терминалов	Вместо того чтобы включить полный сетевой доступ для разрешения удалённого доступа к серверу терминалов или операционной системе компьютера в корпоративной сети, вы можете воспользоваться преимуществами шлюза служб терминалов, которые позволяют инкапсулировать соединения RDP в HTTP-туннеле, а затем зашифровать его с помощью протокола SSL (HTTPS).

Внедрение аутентификации пользователя с использованием сертификата в памяти JaCarta позволит усилить защищённость указанных служб и предотвратить несанкционированный доступ.

Примечание

В качестве примера в настоящем документе рассматривается доступ к защищённому сайту.

Настройка сервера

Общие рекомендации и последовательность действий

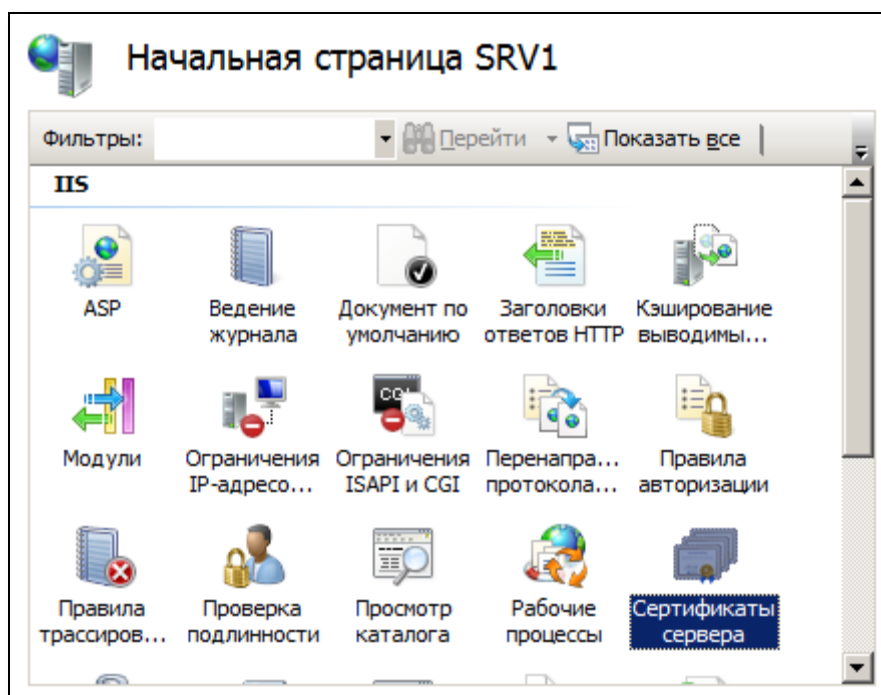
При настройке Web-сервера для исключения несанкционированного доступа к нему рекомендуется максимально ограничить возможности аутентификации пользователя, исключив анонимную аутентификацию, а также другие стандартные способы аутентификации. В целях безопасности развертывать центр сертификации на Web-сервере не рекомендуется.

Общие настройки сервера

Для того чтобы настроить Web-сервер, выполните следующую последовательность действий.

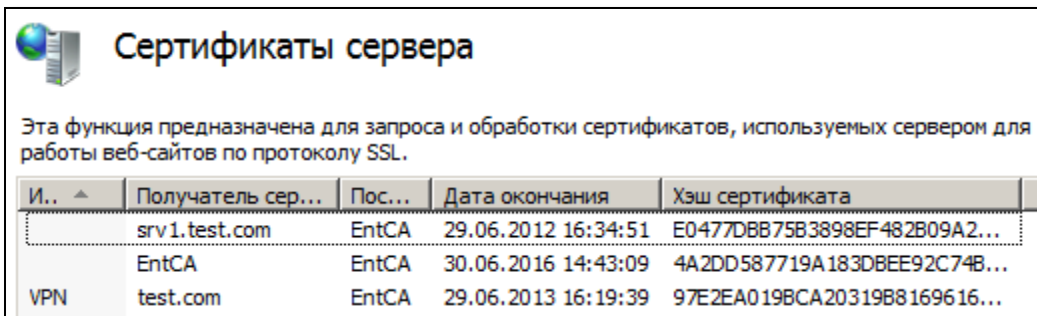
- 1 Убедитесь в том, что сервер удовлетворяет системным требованиям. В частности, на нём должна быть установлена роль **Веб-сервер (IIS)**.
- 2 Запустите **Диспетчер служб IIS**.

В дереве консоли выберите имя сервера – в центральной части окна отобразятся доступные возможности.



- 3 В секции **IIS** сделайте двойной щелчок на **Сертификаты сервера**.

Центральная область окна будет выглядеть следующим образом.



И.. ^	Получатель сер...	Пос...	Дата окончания	Хэш сертификата
	srv1.test.com	EntCA	29.06.2012 16:34:51	E0477DBB75B3898EF482B09A2...
	EntCA	EntCA	30.06.2016 14:43:09	4A2DD587719A183DBEE92C74B...
VPN	test.com	EntCA	29.06.2013 16:19:39	97E2EA019BCA20319B8169616...

- 4 В колонке **Действия** справа щёлкните на ссылке **Создать сертификат домена**.

Отобразится окно мастера создания сертификата.

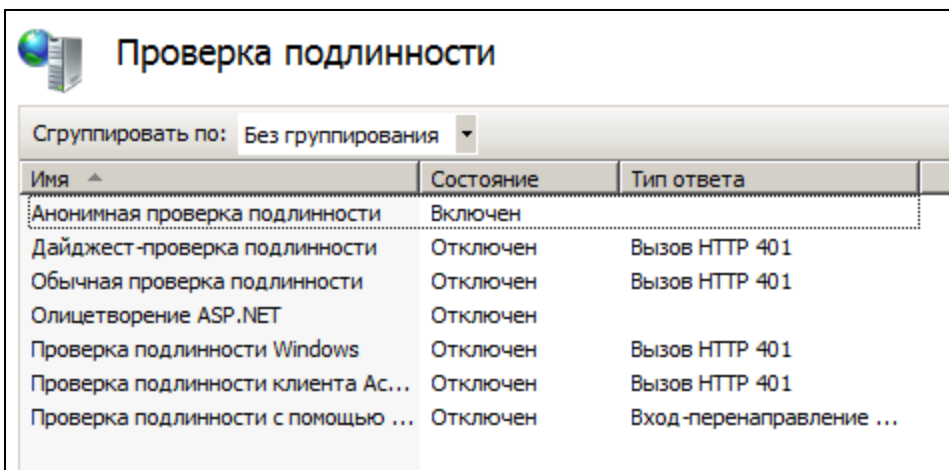
- 5 В окне мастера создания сертификата заполните необходимые поля и нажмите **Далее**.

Примечание

Значение в поле Полное имя должно совпадать с адресом сайта, который пользователь будет вводить в браузере.

- 6 На следующей странице мастера создания сертификата в поле **Локальный центр сертификации** выберите используемый центр сертификации (при необходимости воспользуйтесь кнопкой **Обзор**), в поле **Понятное имя** введите дополнительное имя сертификата.
- 7 Нажмите **Готово**, чтобы закрыть окно мастера создания сертификата.
- 8 Снова выберите Web-сервер, щёлкнув на его имени в окне диспетчера служб IIS.

В центральной части окна в секции **IIS** сделайте двойной щелчок на значке **Проверка подлинности**.



Имя ^	Состояние	Тип ответа
Анонимная проверка подлинности	Включен	
Дайджест-проверка подлинности	Отключен	Вызов HTTP 401
Обычная проверка подлинности	Отключен	Вызов HTTP 401
Олицетворение ASP.NET	Отключен	
Проверка подлинности Windows	Отключен	Вызов HTTP 401
Проверка подлинности клиента Ac...	Отключен	Вызов HTTP 401
Проверка подлинности с помощью ...	Отключен	Вход-перенаправление ...

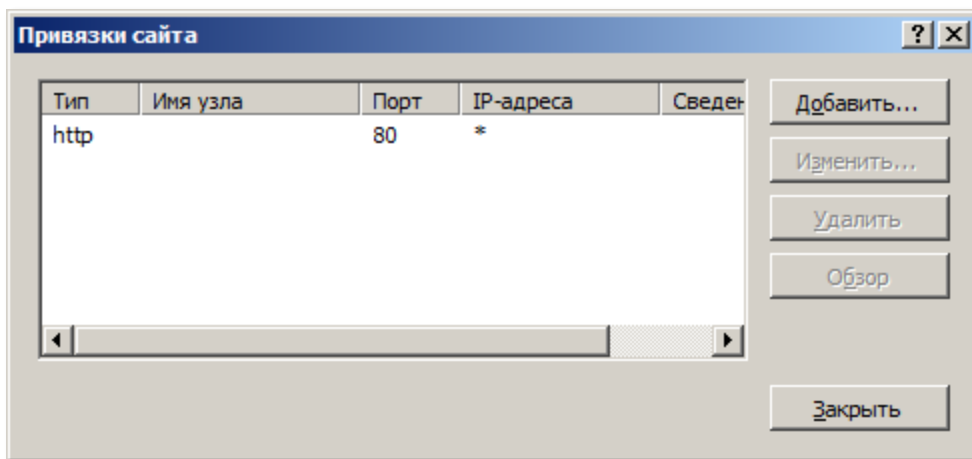
Окно примет следующий вид.

- 9 Отключите все способы проверки подлинности, кроме **Проверка подлинности клиента Active Directory с помощью сертификата**. Для этого, выбрав способ проверки подлинности, в колонке **Действия** щёлкните на ссылке **Отключить** или **Включить** соответственно.

Настройка сайта

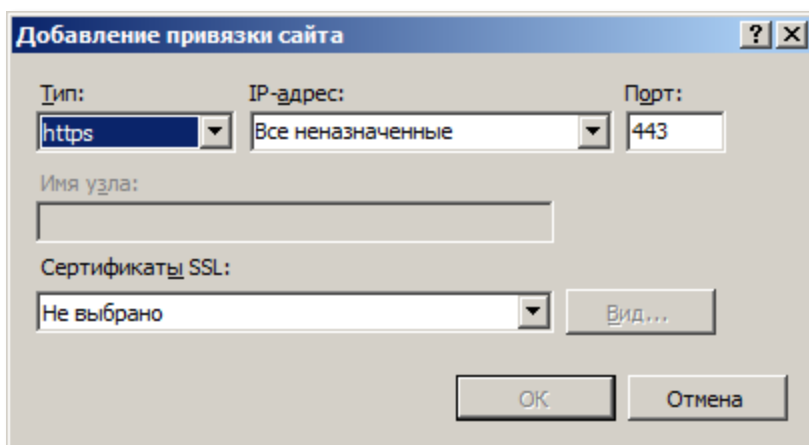
- 1 В окне диспетчера служб IIS разверните ветвь с именем сервера и выберите **сайты > Default Web Site**.
- 2 В правой части окна щёлкните на ссылке **Привязка**.

Отобразится следующее окно.



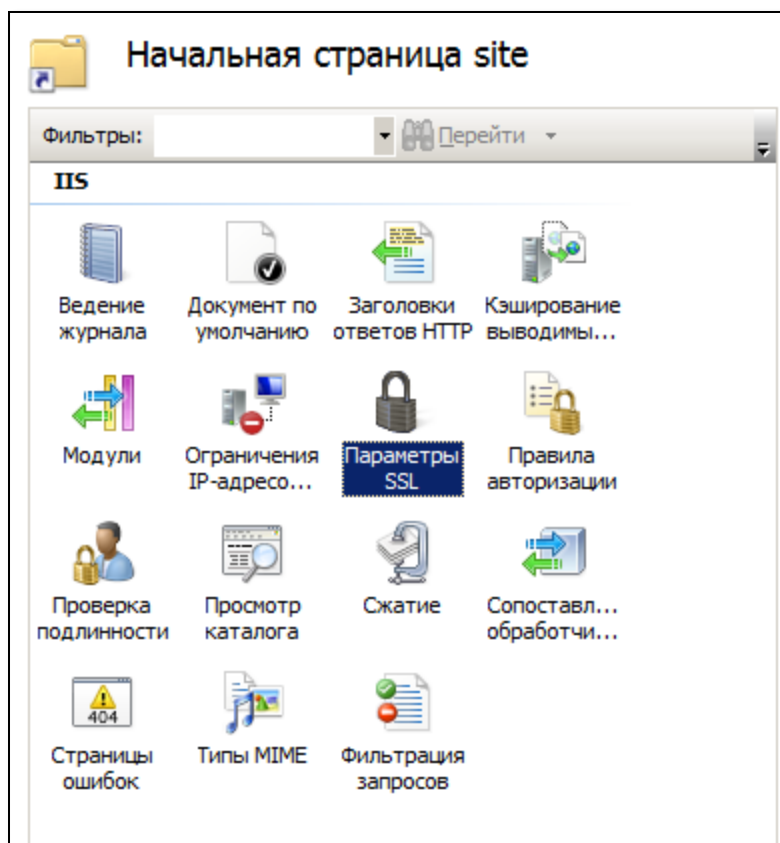
- 3 Нажмите **Добавить**.

Отобразится следующее окно.



- 4 В списке Тип выберите https, и в списке Сертификаты SSL выберите сертификат сервера.
- 5 Нажмите ОК.
- 6 В окне диспетчера служб IIS щёлкните на сайте или виртуальном каталоге, доступ к которому вы хотите сделать защищённым (например, сайты > Default Web Site > site).

В центральной части окна станут доступны настройки данного сайта.



7 Сделайте двойной щелчок на иконке **Параметры SSL**.

Страница примет следующий вид.



8 Установите флажок **Требовать SSL**, и в секции **Сертификаты клиента** выберите **Требовать**.

9 В колонке **Действия** нажмите **Применить**.

Примечание

Существует возможность использовать для доступа к защищённому сайту с электронным ключом JaCarta браузер Mozilla Firefox. Необходимые действия представлены в приложении "Настройка Mozilla Firefox" в конце данного документа.

Настройка доступа к Outlook Web Access / Outlook Web App

Существует возможность использовать электронные ключи JaCarta для доступа к Outlook Web Access / Outlook Web App (OWA) из внешней сети. Для этого необходимо включить для виртуального каталога OWA проверку подлинности с сопоставлением SSL-сертификатов клиентов. Чтобы обеспечить возможность использования электронных ключей JaCarta для доступа к OWA, выполните следующие действия.

- 1 В диспетчере IIS установите требование на использование SSL-сертификатов для виртуального каталога OWA (Имя сервера > сайты > Default Web Site > owa.)
- 2 Данная процедура аналогична процедуре, описанной в предыдущем разделе ("Общие настройки сервера").
- 3 Используйте утилиту командной строки AppCmd.exe, чтобы включить проверку подлинности с сопоставлением SSL-сертификатов клиентов (данная утилита находится в папке C:\Windows\System32\inetsrv). Для этого
 - Выберите Пуск > Все программы > Стандартные, щёлкните правой кнопкой на Командная строка и выберите Запуск от имени администратора.
 - Из командной строки выполните последовательно следующие команды:

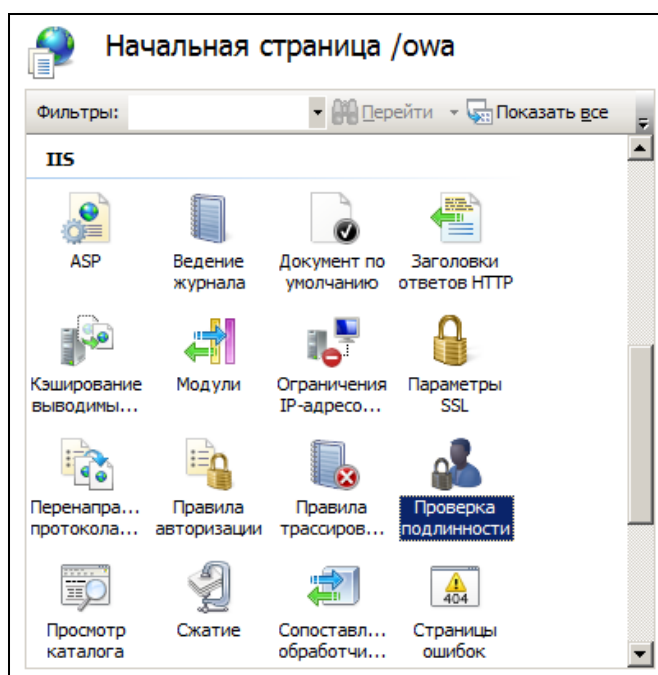
```
C:\Windows\System32\inetsrv\appcmd unlock config /section:clientCertificateMappingAuthentication
```

```
C:\Windows\System32\inetsrv\appcmd set config "Default Web Site/OWA"
```

```
-section:clientCertificateMappingAuthentication /enabled:true
```

- 4 В диспетчере IIS выберите Имя сервера > сайты > Default Web Site > owa.

Отобразится следующее окно.



- 5 Сделайте двойной щелчок на иконке **Проверка подлинности**.

- 6 В отобразившемся окне отключите все включенные способы проверки подлинности.

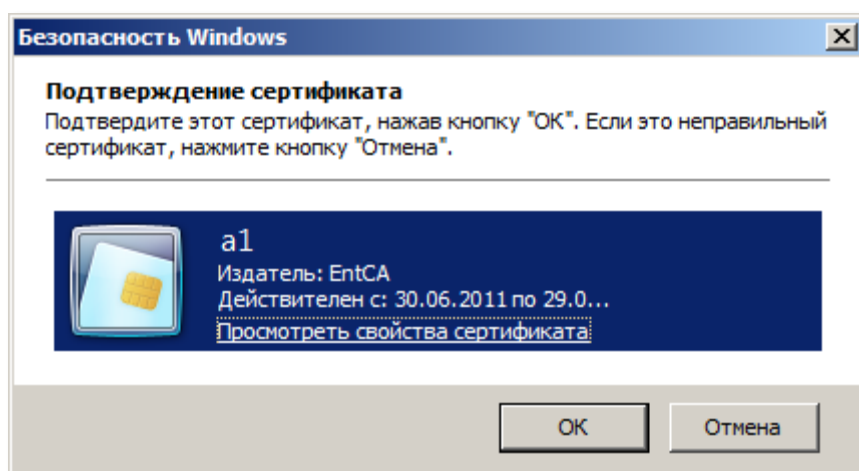
Примечание


Данный шаг нужен для того, чтобы пользователь автоматически попадал в свой почтовый ящик после ввода пароля пользователя JaCarta. В противном случае пользователь будет должен также вводить своё имя пользователя и пароль учётной записи.

Действия пользователя

Для получения доступа к защищённому сайту выполните следующее.

- 1 Запустите Microsoft Internet Explorer.
- 2 Убедитесь в том, что ваш электронный ключ JaCarta с сертификатом, дающим право на доступ к сайту, подсоединён к компьютеру. На USB-токене JaCarta должен гореть световой индикатор.
- 3 Введите адрес защищённого сайта, начинающийся с https: (например, https://test.com).
- 4 В окне Безопасность Windows выберите сертификат пользователя и нажмите ОК.



- 5 При необходимости введите пароль пользователя JaCarta.
- 6 Признаком установления защищённого соединения служит появление значка  рядом с адресной строкой Internet Explorer.

Защита электронной почты

Возможности электронных ключей JaCarta по защите электронной корреспонденции

Существует возможность использовать сертификаты, хранящиеся в памяти электронного ключа JaCarta для электронных подписей и шифрования электронных писем. В иллюстрациях к настоящему разделу фигурируют сертификаты, получение которых описано в разделе "Использование цифровых сертификатов и полный отказ от паролей" настоящего документа.

Microsoft Outlook 2010 (из пакета Microsoft Office 2010)

Настройка Microsoft Outlook 2010

Для того чтобы настроить Microsoft Outlook 2010 для работы с электронным ключом JaCarta, выполните следующую последовательность действий.

- 7 Запустите Microsoft Outlook.
- 8 В меню **Файл** выберите **Параметры**.
- 9 В открывшемся окне **Параметры Outlook** выберите **Центр управления безопасностью**.

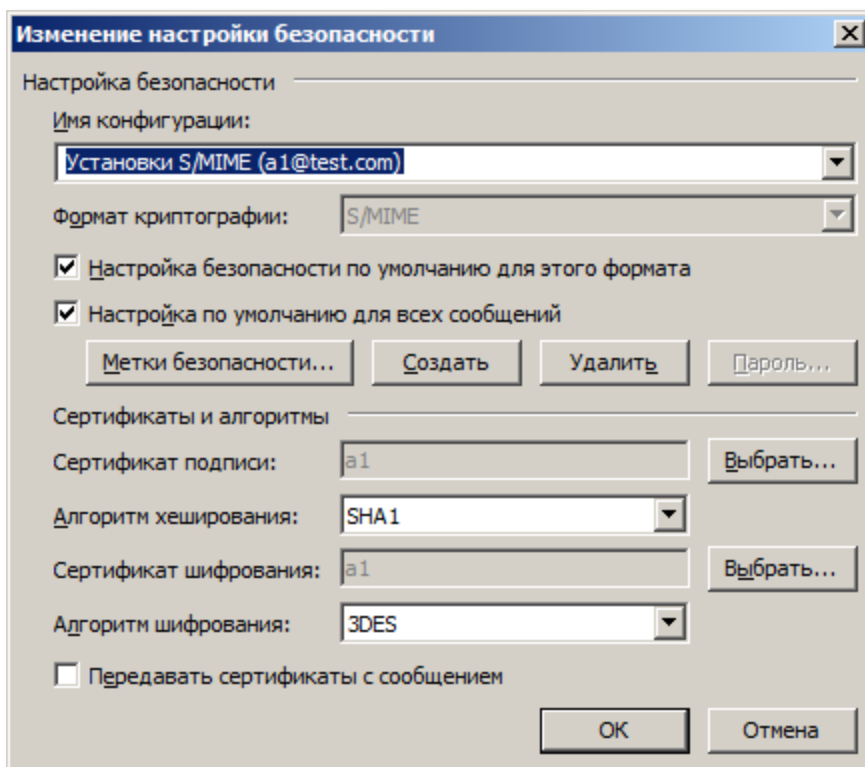
10 В правой части окна нажмите **Параметры центра управления безопасностью**.

Откроется окно Центр управления безопасностью.

11 Убедитесь в том, что ваш электронный ключ JaCarta подсоединён к компьютеру. На USB-токене JaCarta должен гореть световой индикатор.

12 В окне **Центр управления безопасностью** в меню слева выберите **Защита электронной почты** и в секции **Шифрованная электронная почта** нажмите **Параметры**.

Отобразится окно **Изменение настройки безопасности**, необходимые данные подставляются автоматически.

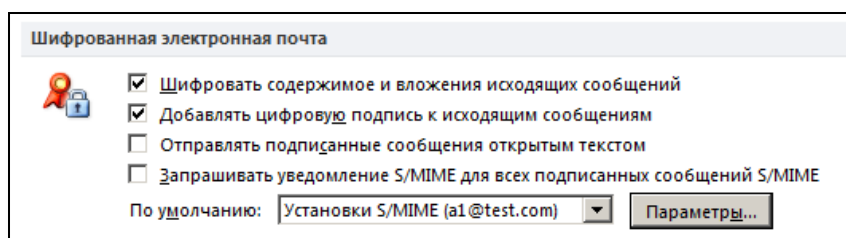


13 При необходимости можно выбрать другие учётные данные, нажав кнопку **Выбрать** напротив поля **Сертификат подписи** и (или) **Сертификат шифрования**.

14 Нажмите **ОК**.

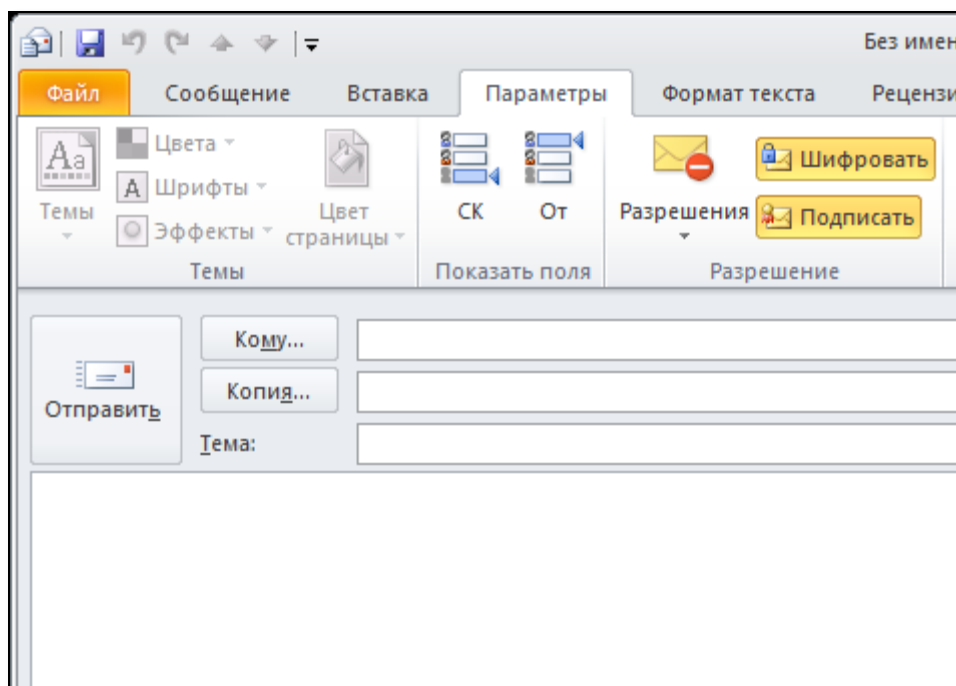
15 В окне **Центр управления безопасностью** установите флажки

- Шифровать содержимое и вложения исходящих сообщений - для шифрования сообщений
- Добавлять цифровую подпись к исходящим сообщениям – для использования цифровой подписи



Использование Microsoft Outlook 2010 для отправки подписанных и зашифрованных сообщений

- 1 Чтобы удостовериться в том, что исходящее письмо будет зашифровано и (или) к нему будет присоединена цифровая подпись, в окне сообщения выберите вкладку **Параметры**.
- 2 На вкладке **Параметры** в секции **Разрешение** отметьте пункты
 - **Шифровать** (для шифрования сообщения)
 - **Подписать** (для присоединения цифровой подписи)



Цифровая подпись и шифрования при использовании OWA

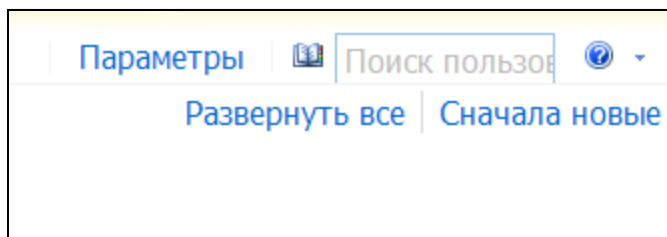
Чтобы отправить зашифрованное электронное сообщение и (или) сообщение с цифровой подписью, используя сайт Outlook Web Access / Outlook Web App, выполните следующую последовательность действий.

Примечание:

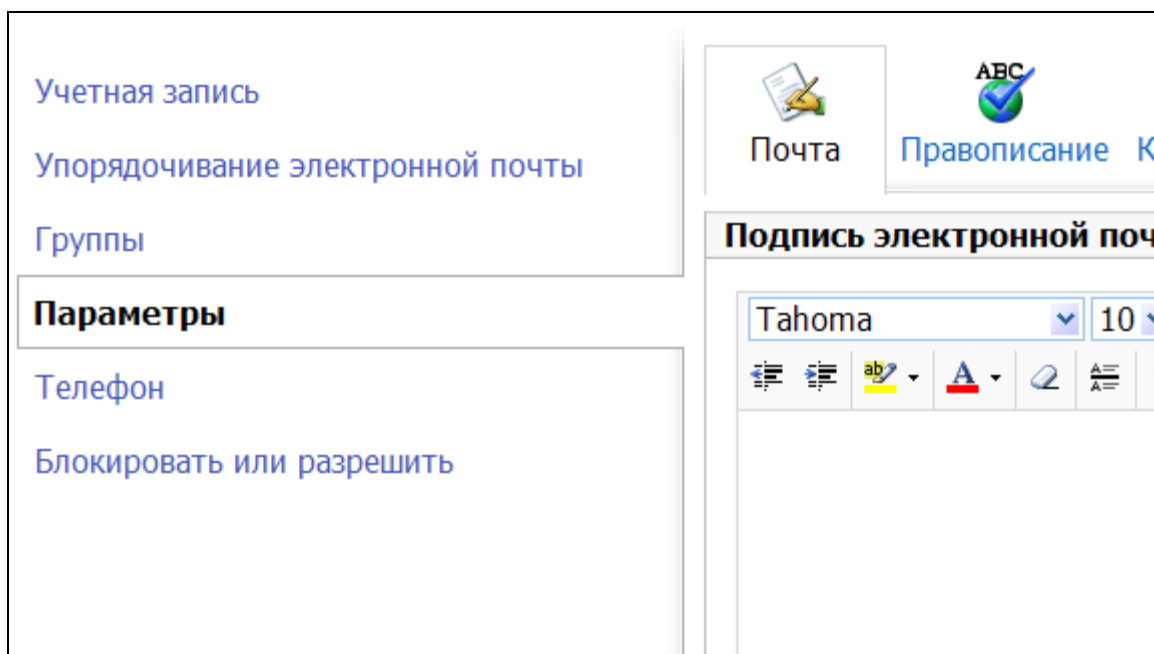
Возможность шифрования и использования цифровой подписи в OWA доступна только в том случае, если вы используете браузер Internet Explorer 7 или более поздней версии под управлением операционной системы Microsoft Windows.


- 1 Запустите Microsoft Internet Explorer.
- 2 Убедитесь в том, что ваш электронный ключ JaCarta с сертификатом, дающим право на доступ к сайту, подсоединён к компьютеру. На USB-токене JaCarta должен гореть световой индикатор.
- 3 Зайдите на сайт OWA с использованием электронного ключа JaCarta.

- 4 В правом верхнем углу страницы выберите Параметры (см. изображение ниже).

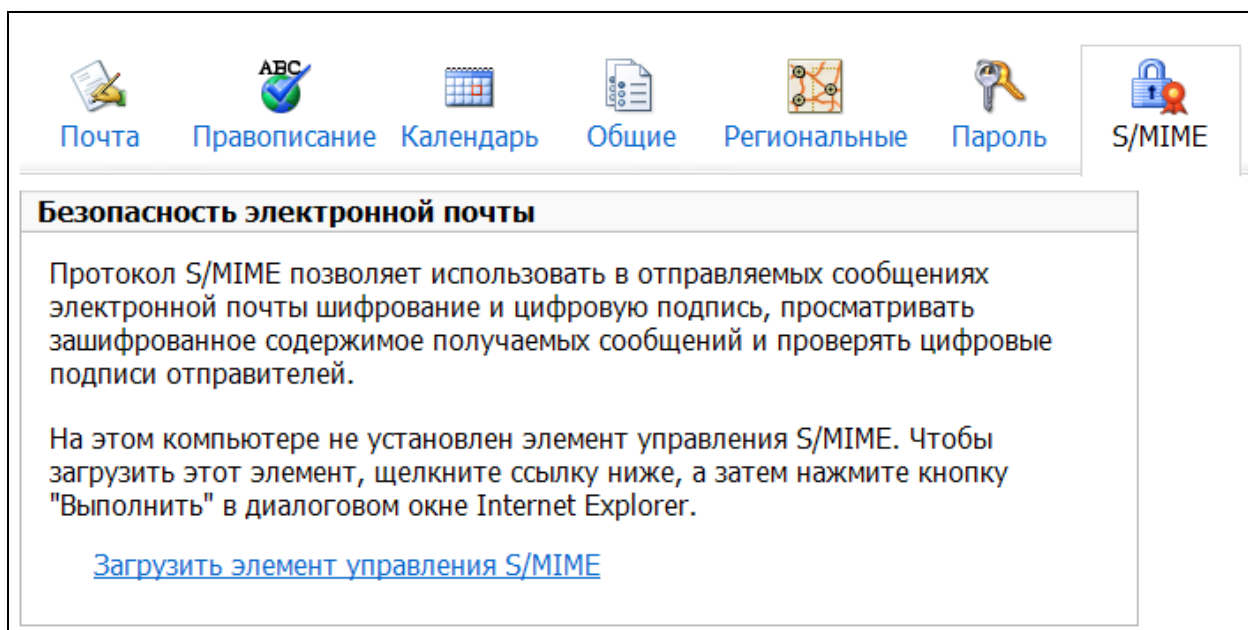


- 5 На отобразившейся странице снова выберите **Параметры** (см. изображение ниже).



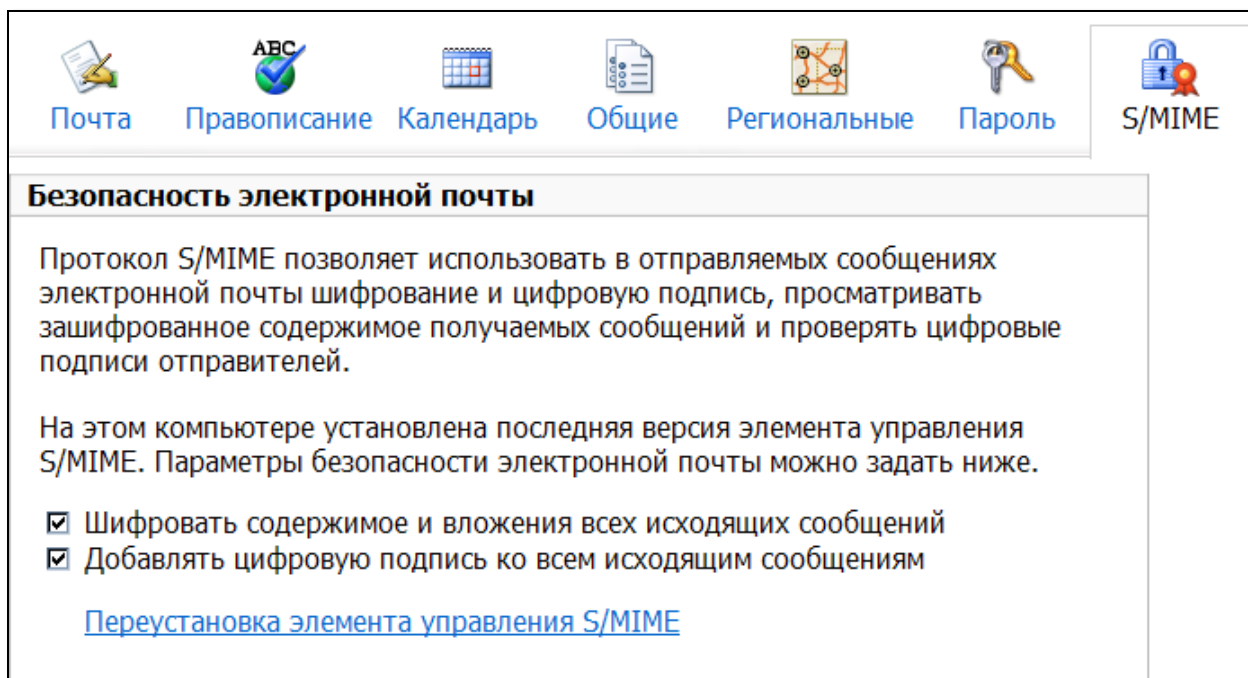
- 6 Щёлкните на иконке  S/MIME.

Отобразится следующая страница.



- Щёлкните на ссылке **Загрузить элемент управления S/MIME**, сохраните установочный файл на локальном компьютере и установите элемент управления S/MIME.

После установки элемента управления S/MIME страница на сайте OWA будет выглядеть следующим образом.

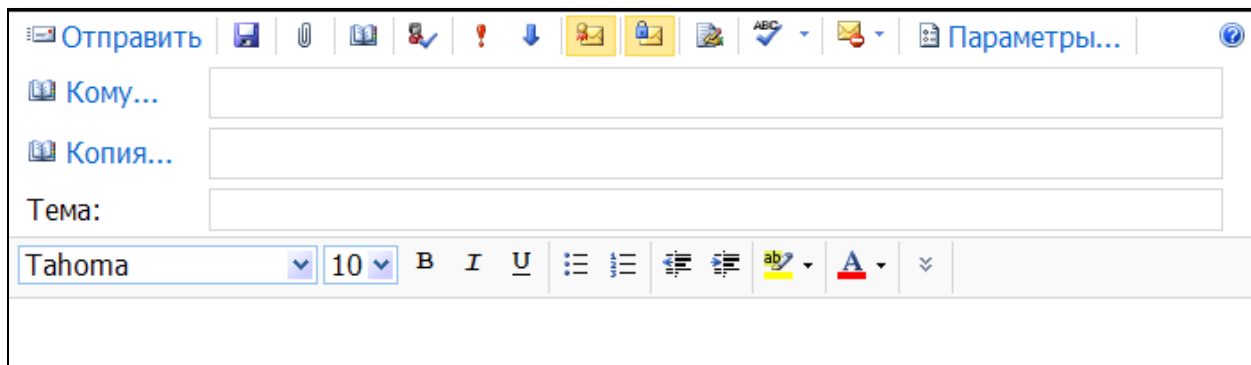




- Установите необходимые флажки
 - Шифровать содержимое и вложения всех исходящих сообщений

- Добавлять цифровую подпись ко всем исходящим сообщениям

9 Нажмите **Сохранить** в правом нижнем углу страницы, чтобы сохранить сделанные настройки.

После этого при отправке электронных сообщений с использованием сайта OWA будут автоматически отмечены соответствующие иконки (см. изображение ниже).



-  означает, что к отправленному сообщению будет присоединена цифровая подпись.
-  означает, что отправленное сообщение и содержащиеся в нём вложения будут зашифрованы.

При отправке электронного сообщения в зависимости от установленных настроек кэширования может потребоваться ввести пароль пользователя JaCarta.

Шифрование данных на жёстком диске (EFS)

Общие сведения

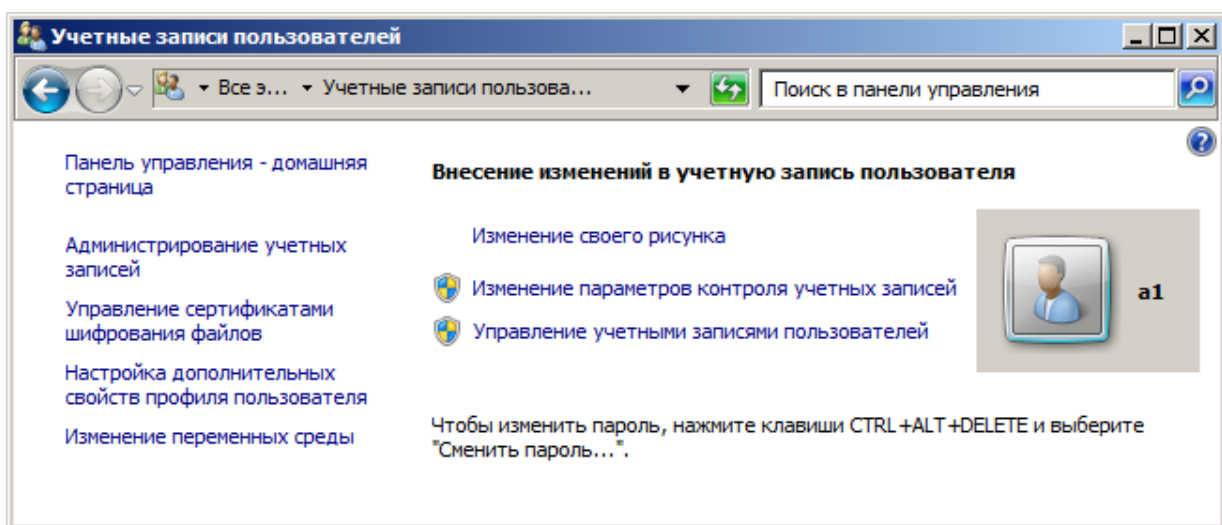
Существует возможность записывать в память электронных ключей JaCarta сертификаты, позволяющие шифровать данные на жёстком диске. В данном документе рассматривается вариант создания и записи в память электронного ключа JaCarta самозаверяющего сертификата шифрования.

Запись сертификата EFS в память электронного ключа JaCarta

Чтобы записать сертификат EFS в память электронного ключа JaCarta, выполните следующую последовательность действий.

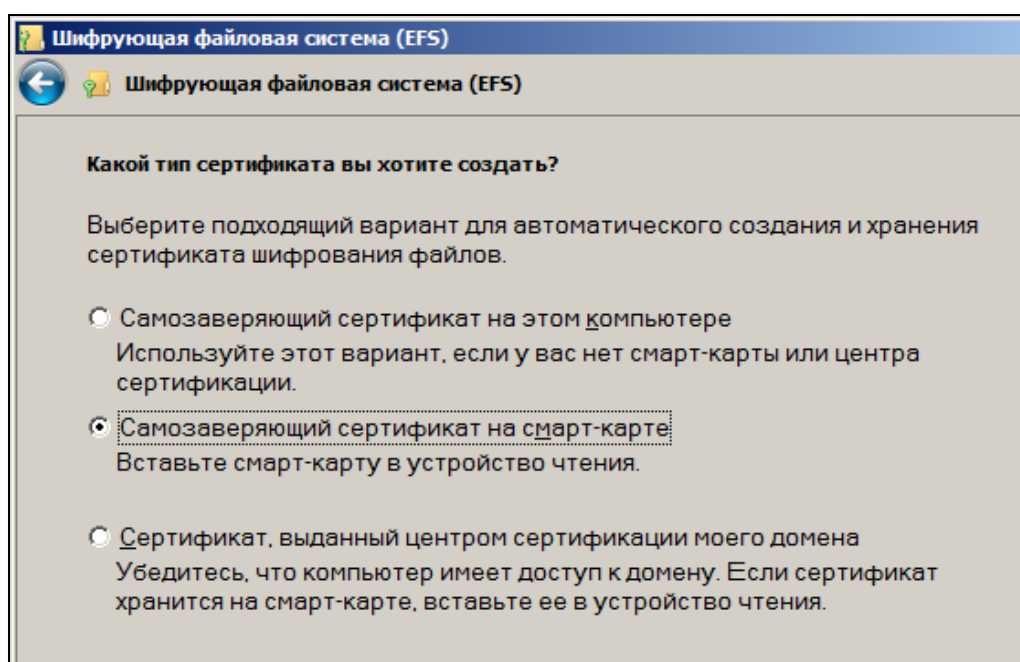
- 1 Выберите Пуск > Панель управления > Учётные записи пользователей.

Окно должно выглядеть следующим образом.



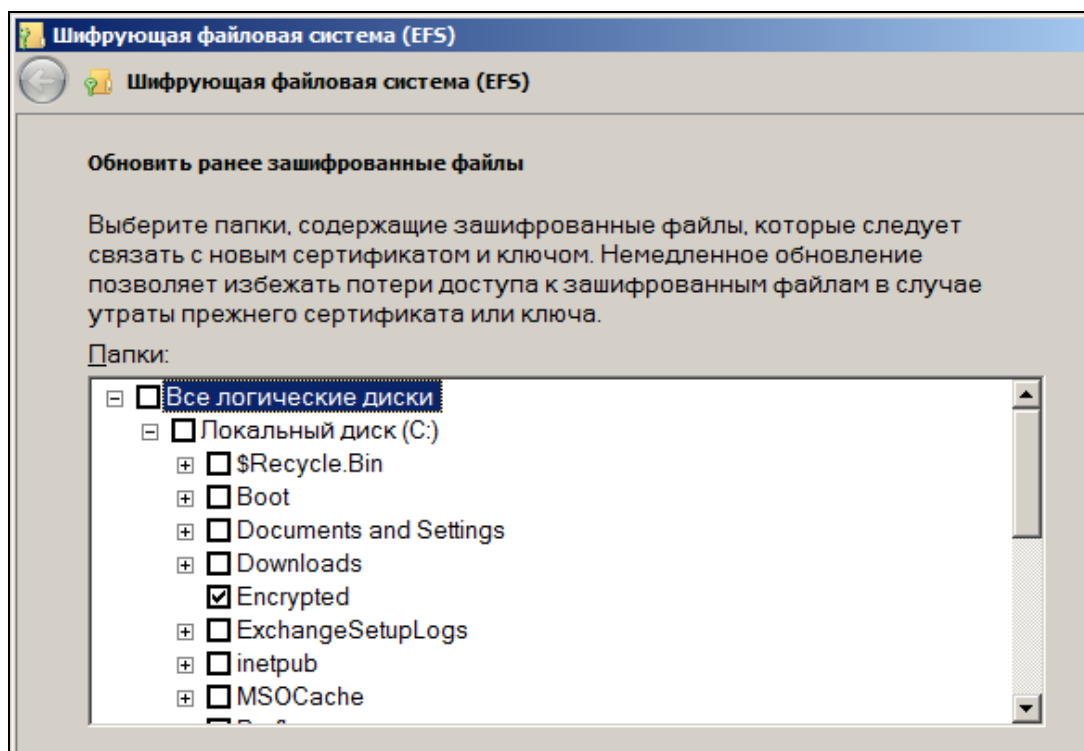
- 2 Щёлкните на ссылке **Управление сертификатами шифрования файлов**.
- 3 В окне приветствия мастера управления сертификатами EFS нажмите **Далее**.
- 4 В следующем окне выберите **Создать новый сертификат** и нажмите **Далее**.

Отобразится следующее окно.



- 5 Выберите **Самозаверяющий сертификат на смарт-карте**.
- 6 Убедитесь в том, что ваш электронный ключ JaCarta подсоединён к компьютеру. На USB-токене JaCarta должен гореть световой индикатор.
- 7 Нажмите **Далее**.
- 8 Когда появится соответствующее окно, введите пароль пользователя JaCarta и нажмите клавишу **ВВОД**.

Через некоторое время отобразится следующее окно.



- 9 Установите флажок напротив папок, которые можно будет расшифровать созданным сертификатом (также можно выбрать папки, которые были зашифрованы ранее), и нажмите **Далее**.

Примечание

Собственно зашифрования данных, если они не были до этого зашифрованы, на данном этапе не происходит.

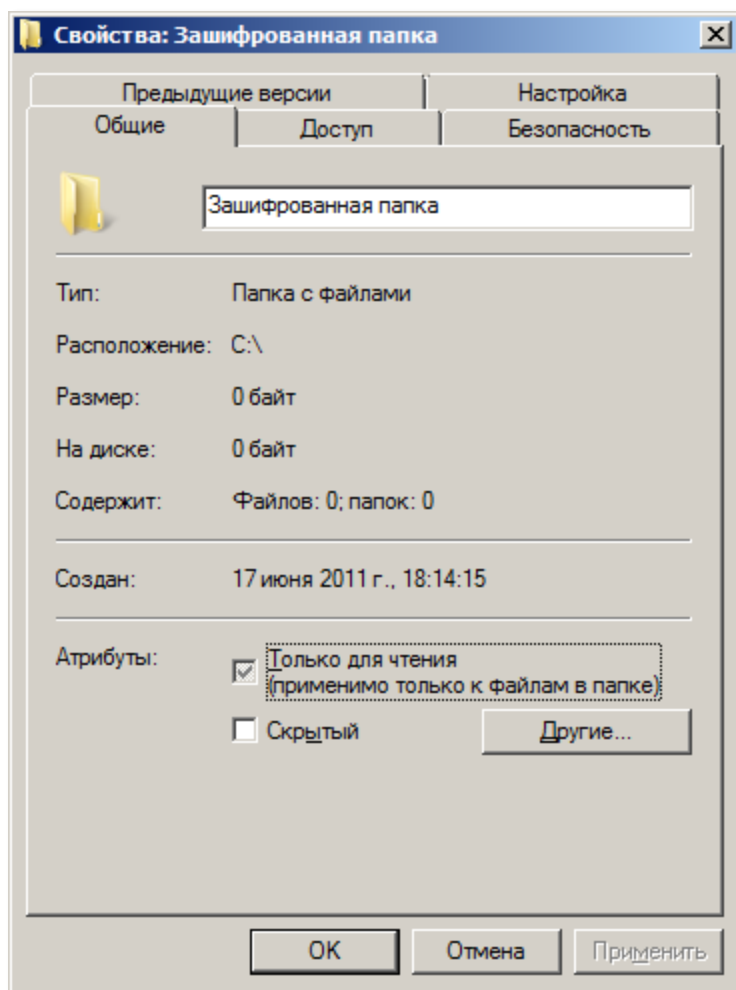
- 10 Появится окно ввода учётных данных смарт-карты. Введите необходимые данные и нажмите **ВВОД**.
- 11 В окне окончания создания сертификата шифрования нажмите **Заккрыть**.

Зашифрование данных на жёстком диске

- 1 Чтобы зашифровать данные, выполните следующую последовательность действий.

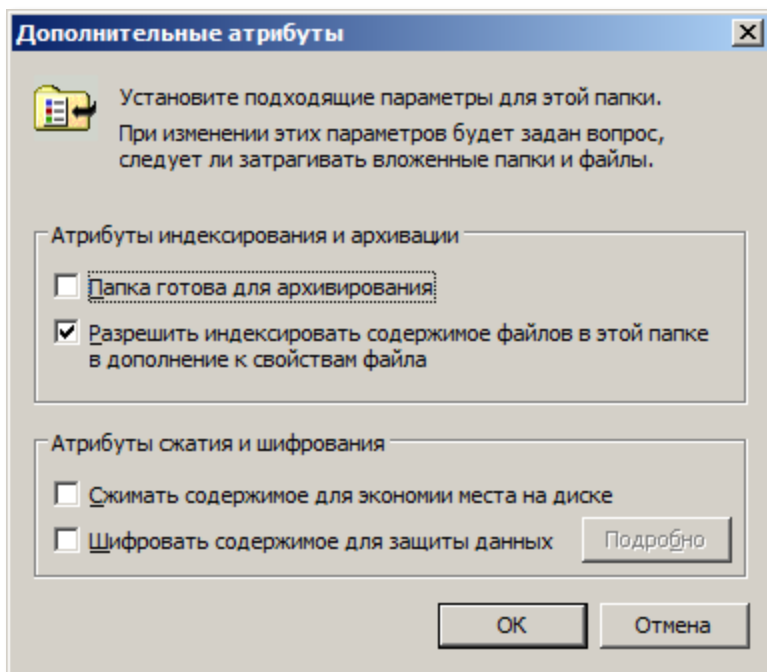
- Щёлкните правой кнопкой на папке, содержимое которой необходимо зашифровать, и выберите Свойства.

Убедитесь в том, что в окне свойств папки открыта вкладка **Общие**.



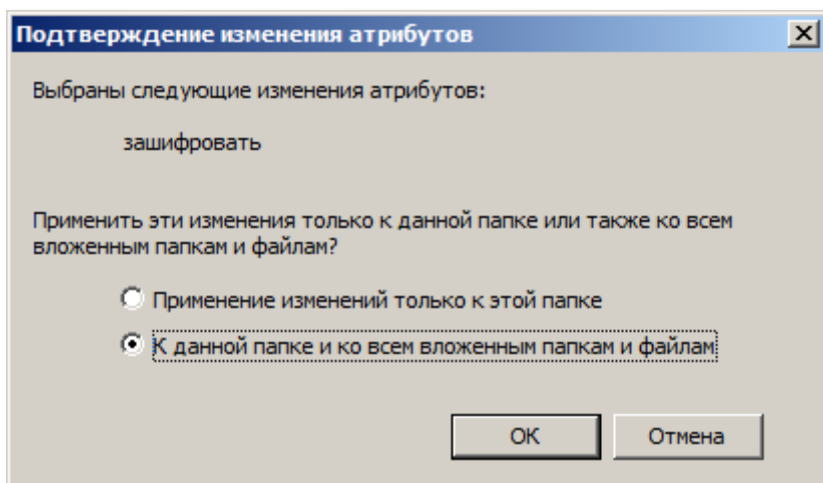
- Нажмите **Другие**.

Отобразится следующее окно.



- 4 Установите флажок Шифровать содержимое для защиты данных и нажмите ОК.
- 5 В окне свойств выбранной папки нажмите ОК.

Отобразится следующее окно.



- 6 Чтобы зашифровать папку и все вложенные папки и файлы, выберите **К данной папке и ко всем вложенным папкам и файлам** и нажмите **ОК**.
- 7 После того как папка будет зашифрована, её можно будет расшифровать только с использованием сертификата, хранящегося в памяти электронного ключа JaCarta.

Шифрование диска BitLocker с использованием JaCarta

Общие сведения

Средство шифрования диска BitLocker входит в состав некоторых редакций ОС Windows и позволяет защитить данные, хранящиеся на дисках компьютера. BitLocker противостоит атакам с выключением, которые проводятся путём отключения или обхода установленной ОС либо путём физического удаления жёсткого диска с компьютера для автономного взлома данных.

Технология BitLocker основана на использовании криптографических преобразований с ключевой парой и сертификатом открытого ключа. Этот сертификат может быть как самоподписанным, так и выпущенным центром сертификации.

Примечание

Использование самоподписанных сертификатов не рекомендовано Microsoft, за исключением случаев тестирования. Если использовать самоподписанные сертификаты при шифровании BitLocker всё же необходимо, обратитесь к статье "Руководство по настройке BitLocker для работы с использованием самоподписанных сертификатов" (см. <http://technet.microsoft.com/ru-ru/library/ee424307>).

Системные требования

Требования к центру сертификации

Центр сертификации должен работать под управлением ОС Windows Server 2008 R2 Enterprise и быть настроен согласно п. о настоящего документа.

Требования к компьютеру пользователя

Компьютер пользователя должен работать под управлением одной из следующих ОС:

- Windows 7 Enterprise/Ultimate;
- Windows Server 2008 R2.

Примечание:

Технология шифрования диска BitLocker входит в состав Windows Server 2008 R2 в качестве дополнительного компонента.

Кроме того, на компьютере пользователя должен быть установлен поставщик службы криптографии Athena ASECard Crypto CSP.

Требования к JaCarta

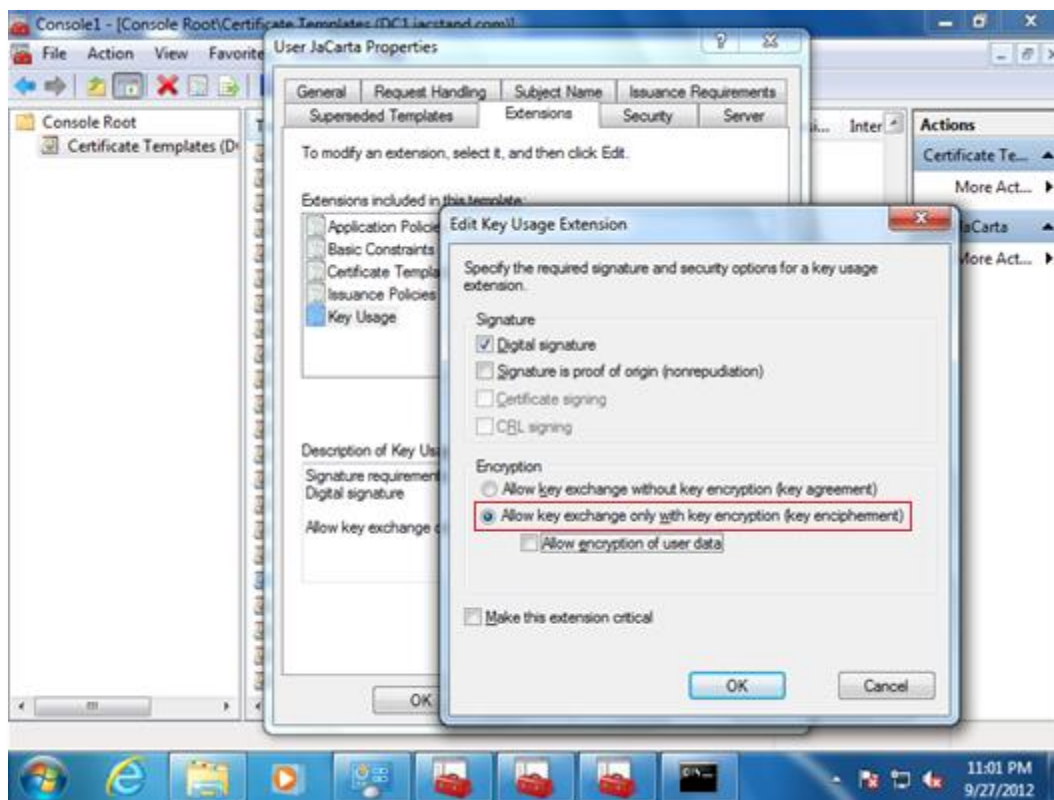
Для работы с BitLocker используется устройство JaCarta с апплетом Laser.

Ограничение

При использовании устройства JaCarta с апплетом Laser защита BitLocker не может быть установлена на системный раздел.

Дополнительная настройка шаблона сертификата

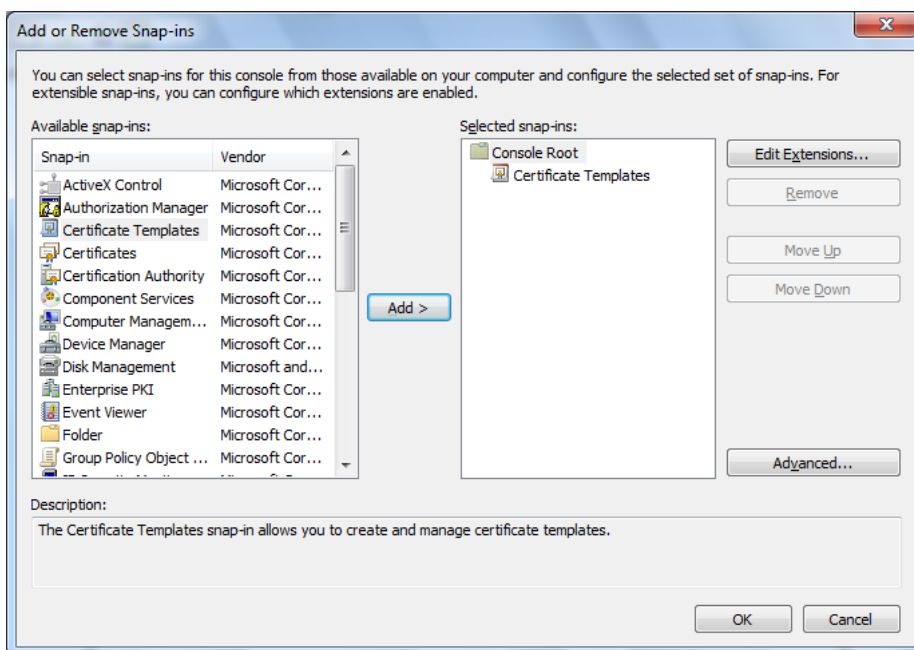
Шаблон сертификата (в нашем примере – User JaCarta) должен быть предварительно создан и включён (см. пп. о – о) при настройке ЦС. При этом расширение сертификата "использование ключа" может задавать любой из способов шифрования — согласование ключей (key agreement), шифрование ключей (key encipherment) и шифрование данных пользователя.



В приведённом в настоящем документе примере используется шаблон сертификата, задающий в расширении сертификата "использование ключа" в качестве способа шифрования (key encipherment).

Для использования сертификатов с BitLocker необходима дополнительная настройка шаблона, для чего на компьютере с установленным центром сертификации от имени учётной записи пользователя, обладающего правами администратора, выполните следующие действия.

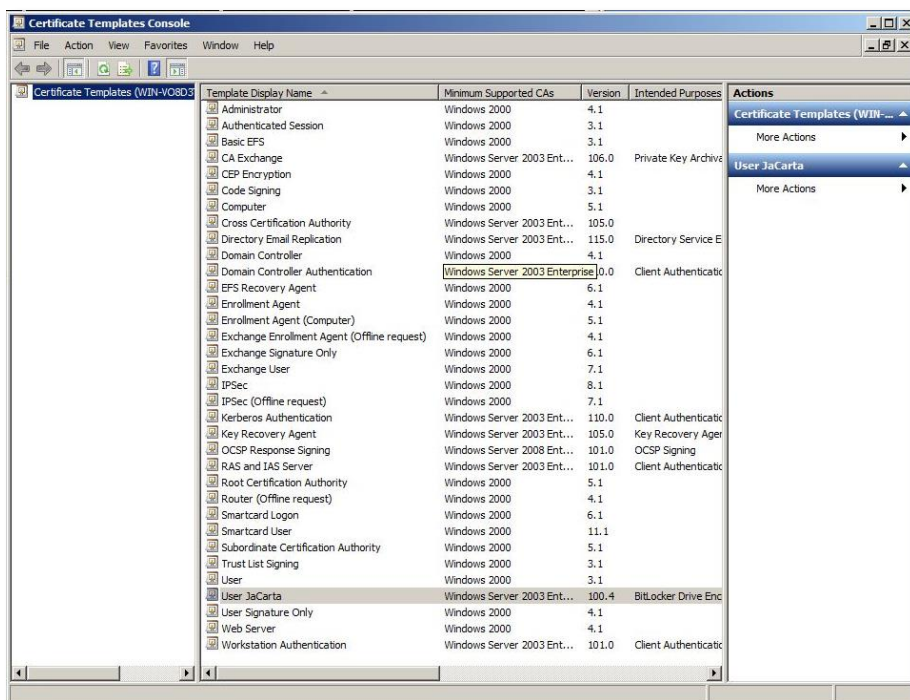
- 1 Откройте оснастку управления шаблонами сертификатов (**Certificate Templates**). Для этого: Выполните команду **mmc**. В открывшемся окне последовательно выберите **Файл -> Добавить или удалить оснастку (File -> Add/Remove Snap-In)**. Далее в левой панели открывшегося окна **Добавление и удаление оснасток (Add or Remove Snap-ins)**, содержащей список доступных оснасток, выберите **Шаблоны сертификатов (Certificate Templates)** и нажмите кнопку **Добавить (Add)**, расположенную в центре окна. После этого оснастка **Шаблоны сертификатов (Certificate Templates)** появится в правой панели окна.



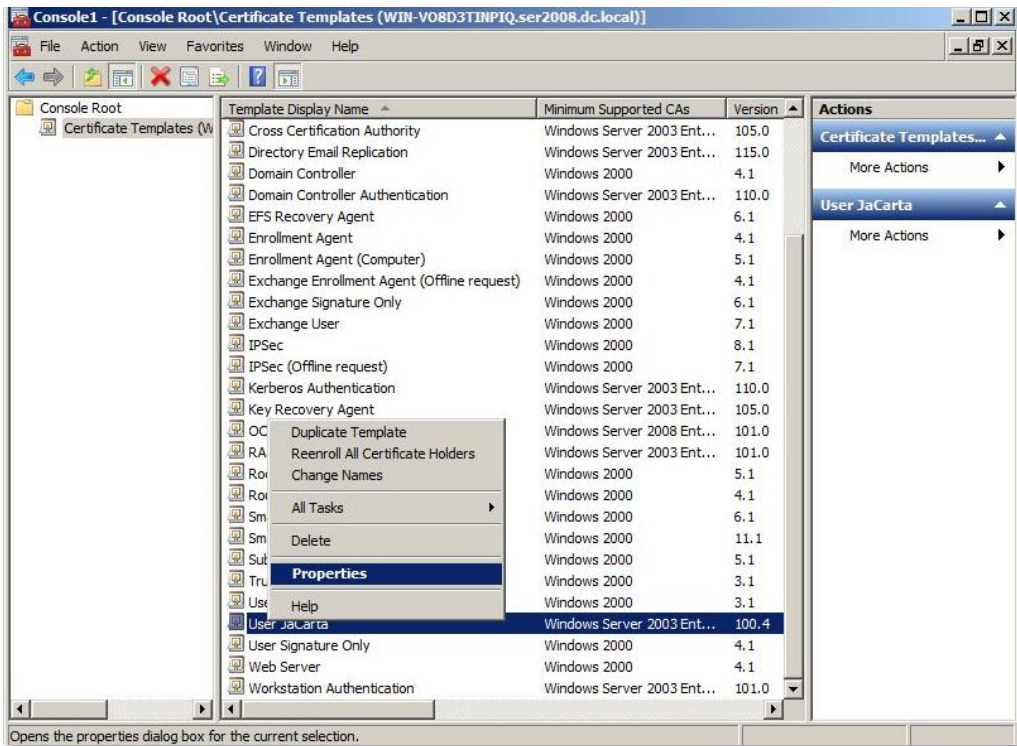
- 2 Нажмите кнопку **ОК** и закройте окно.

Добавленная оснастка управления шаблонами сертификатов (**Certificate Templates**) появится в дереве консоли.

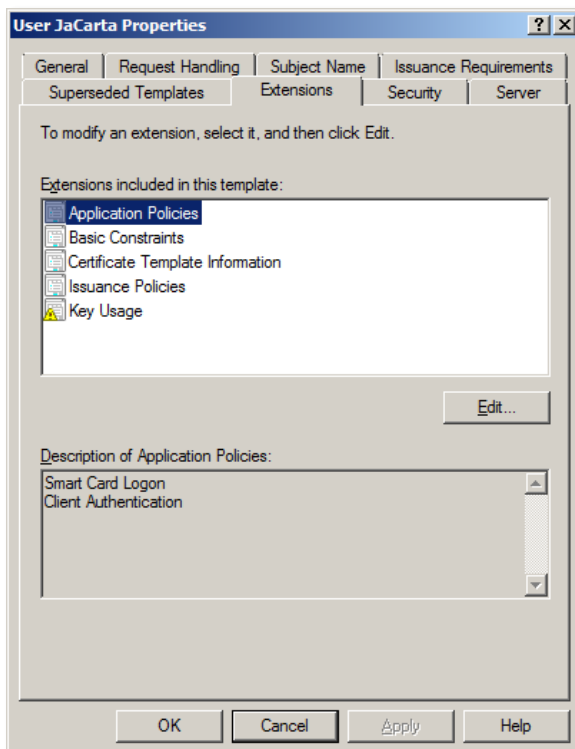
- 3 В дереве консоли разверните узел **Certificate Templates (Шаблоны сертификатов)** и выберите в правой панели в списке шаблон, созданный и включённый в соответствии с п. о – о. На рисунке выделен созданный для примера шаблон **User JaCarta**.



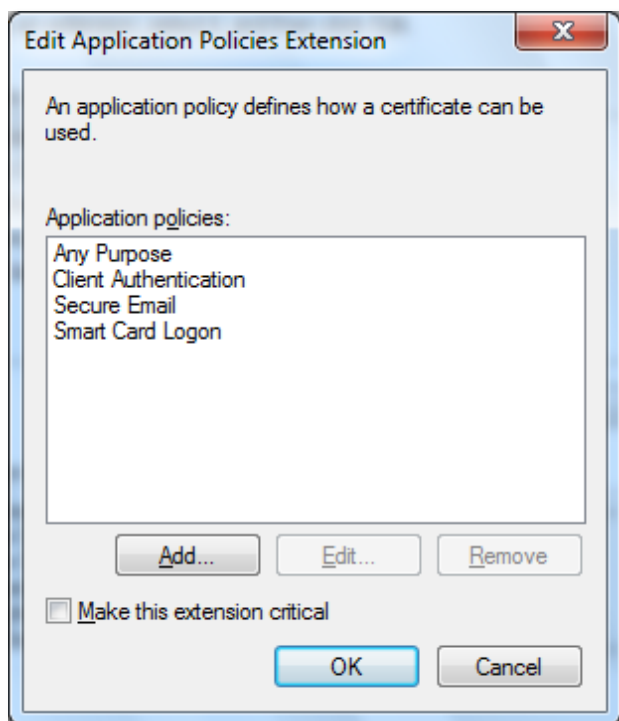
- 4 Дважды щёлкните по шаблону сертификата или выберите пункт **Properties (Свойства)** из контекстного меню, чтобы открыть окно свойств шаблона.



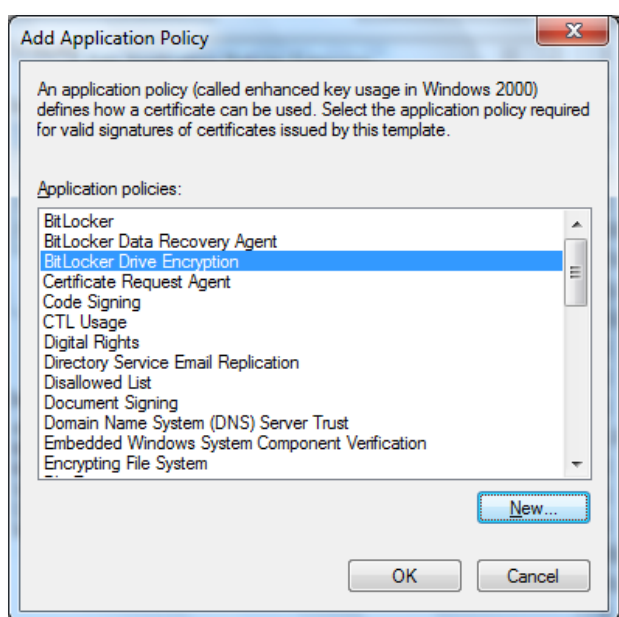
- 5 В открывшемся окне перейдите на вкладку **Extensions (Расширения)**.



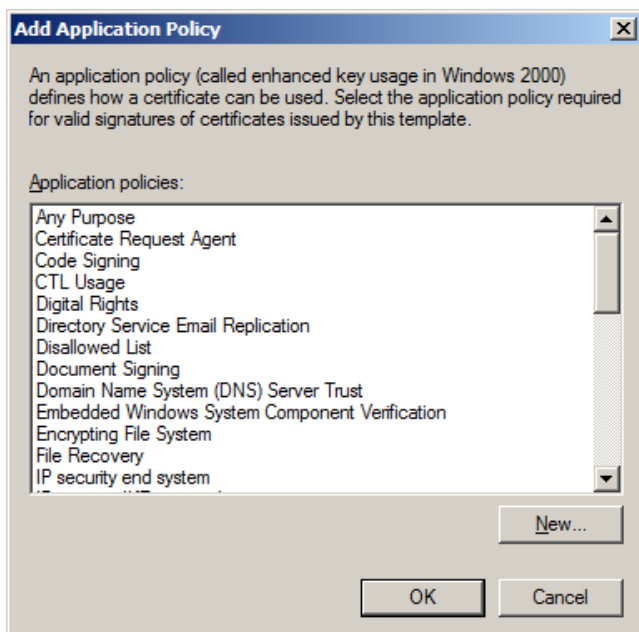
- 6 Выберите в списке **Application Policies (Политики приложения)** и нажмите кнопку **Edit (Редактировать)**.
- 7 В открывшемся окне **Edit Application Policies Extension (Редактирование расширений политик приложения)** нажмите кнопку **Add (Добавить)**.



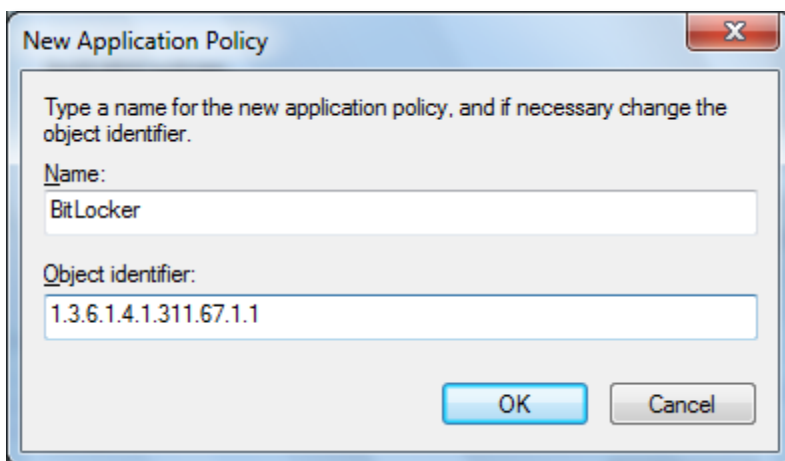
- 8 В открывшемся окне **Add Application Policy (Добавить политику приложения)**:
 - если политика **BitLocker Drive Encryption (Шифрование диска BitLocker)** находится в списке **Application Policies (Политики приложения)**, выделите её, нажмите **OK** и перейдите к шагу 11;



- если политика **BitLocker Drive Encryption (Шифрование диска BitLocker)** в списке отсутствует, нажмите кнопку **New (Новая)** и перейдите к шагу 9.

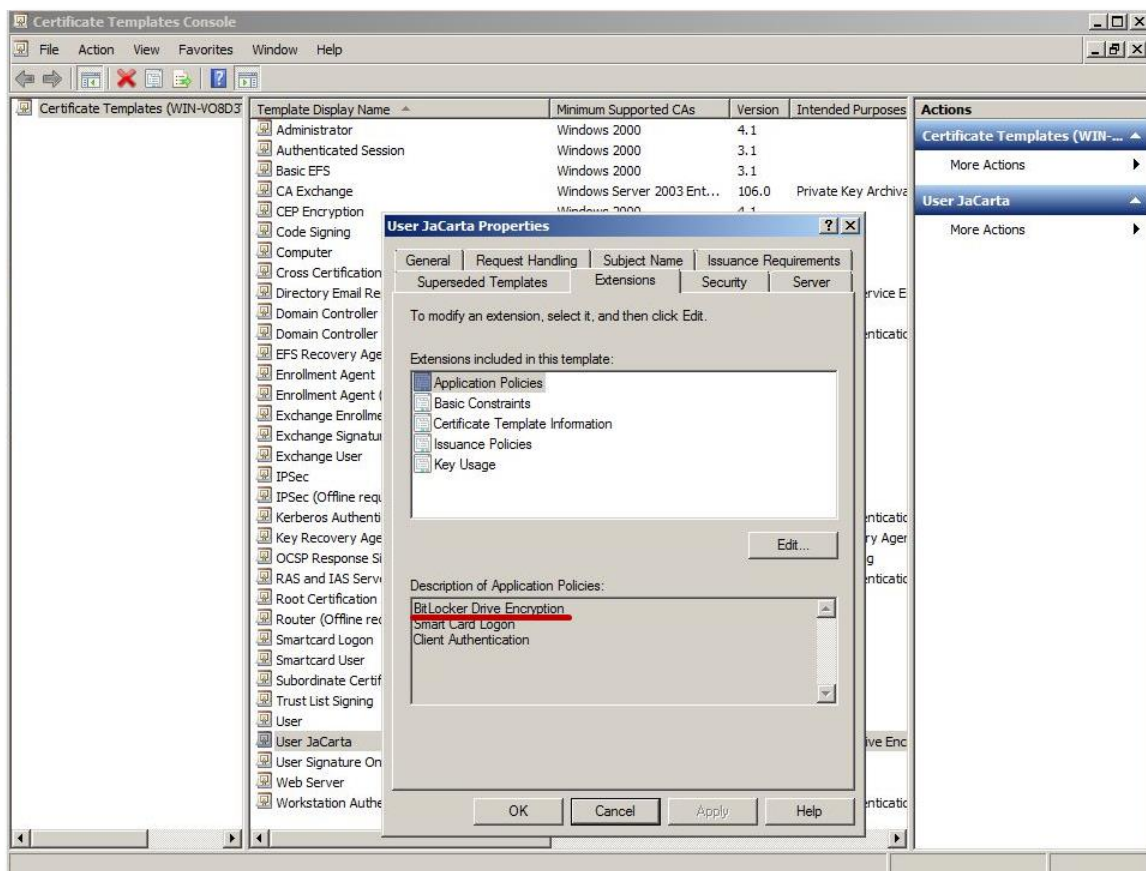


- 9 В открывшемся окне укажите в поле **Name (Имя)** название политики, например, **BitLocker**, а в поле **Object identifier (Идентификатор объекта)** укажите стандартный OID BitLocker – **1.3.6.1.4.1.311.67.1.1**, как показано на рисунке ниже.



- 10 Нажмите кнопку **OK**.

- 11 Убедитесь, что новая политика добавлена в список **Description of Application Policies (Описание политик приложения)** для **Application Policies (Политики приложения)**.



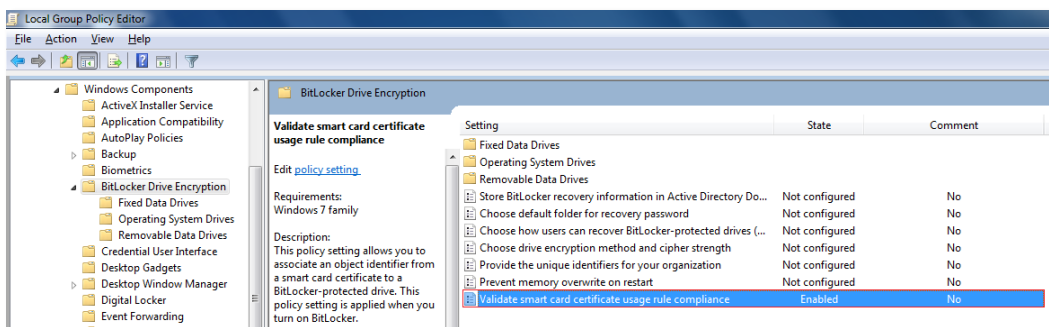
- 12 Закройте окно свойств шаблона сертификата, нажав кнопку **ОК**.

Выпустите сертификат пользователя и запишите его в память электронного ключа JaCarta для использования при защите дисков средствами BitLocker. Описание действий см. в п. о.

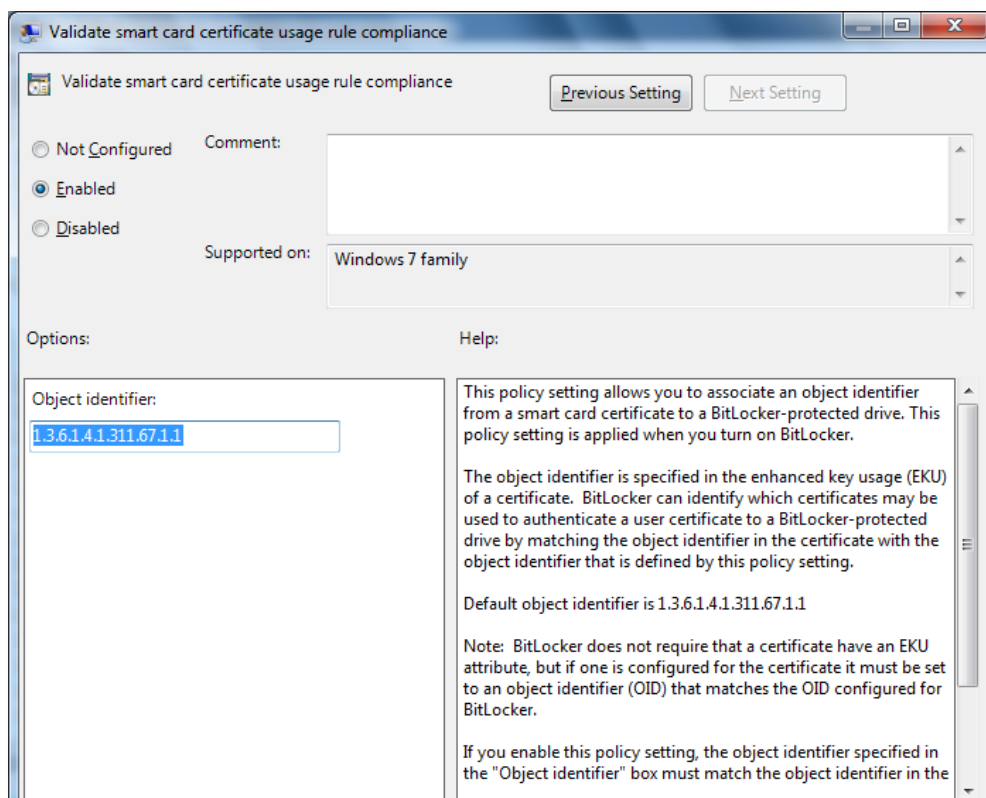
Настройка компьютера пользователя

Чтобы установить защиту BitLocker на жёсткие и съёмные диски с использованием электронного ключа JaCarta, необходимо выполнить конфигурацию групповых политик. Для выполнения описанных ниже действий необходимо наличие полномочий администратора на компьютере пользователя.

- 1 Откройте консоль управления групповыми политиками. Для этого запустите утилиту командной строки с правами администратора системы и в её окне введите **gpedit.msc**. Откроется окно редактора групповых политик.
- 2 В дереве объектов окна редактора групповых политик разверните узлы **Local Computer Policy -> Computer Configuration -> Administrative Templates -> Windows Components -> BitLocker Drive Encryption (Политика «Локальный компьютер», Конфигурация Компьютера, Административные шаблоны, Компоненты Windows, Шифрование диска BitLocker)** и выделите узел **BitLocker Drive Encryption (Шифрование диска BitLocker)**.
- 3 В правой панели окна **Setting** дважды щёлкните пункт **Validate smart card certificate usage rule compliance (Проверить согласованность правил использования сертификатов смарт-карт)**.

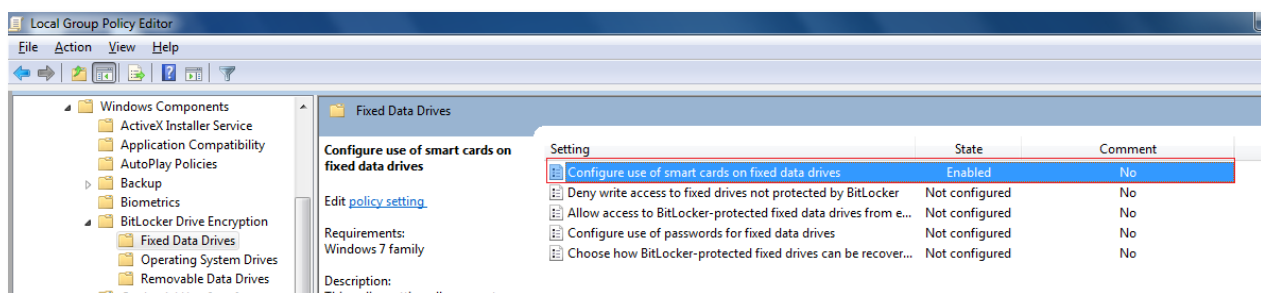


Откроется одноимённое окно.



- 4 Установите переключатель в значение **Enable (Включить)**. Убедитесь, что в поле **Object identifier (Идентификатор объекта)** указано значение OID BitLocker (**1.3.6.1.4.1.311.67.1.1**). Если это не так, исправьте значение OID на указанное.
- 5 Нажмите **ОК**.

6. Перейдите в подраздел **Fixed Data Drives (Жёсткие диски с данными)** и дважды щёлкните **Configure use of smart cards on fixed data drives (Настроить использование смарт-карт на фиксированных дисках данных)**.

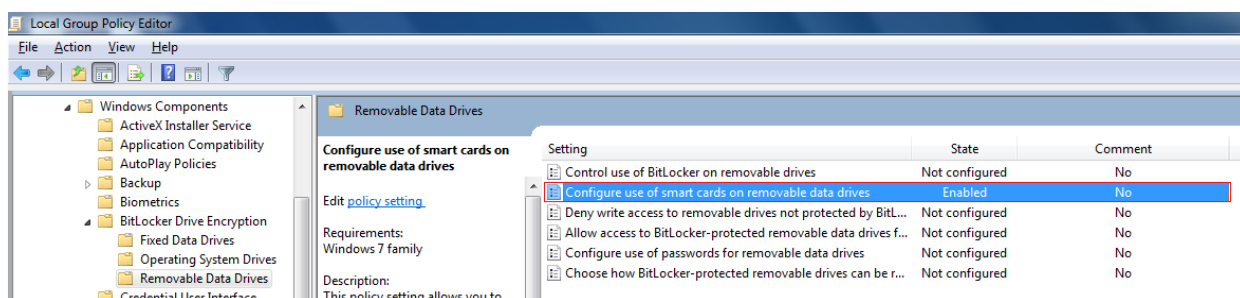


- В открывшемся окне выберите значение **Enable (Включить)**.



7. Нажмите **ОК**.

- 8 Перейдите в узле **BitLocker Drive Encryption** в подраздел **Removable Data Drives (Съёмные диски с данными)** и дважды щёлкните пункт **Configure use of smart cards on removable data drives (Настроить использование смарт-карт на съёмных дисках с данными)**.

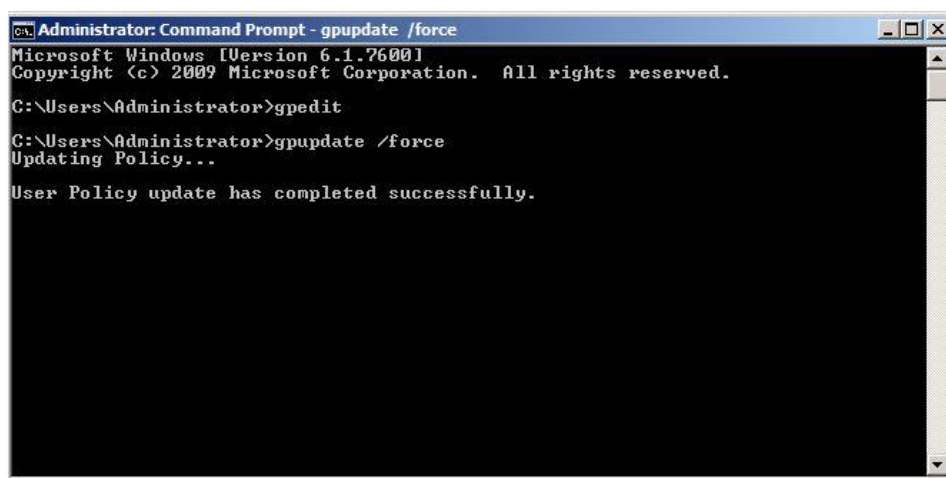


- 9 В открывшемся окне **Configure use of smart cards on removable data drives (Настроить использование смарт-карт на съёмных дисках с данными)** выберите значение **Enable (Включить)**.



- 10 Нажмите **ОК**.

- 11 Закройте консоль управления групповыми политиками и для немедленного применения политики выполните команду **gpupdate /force** и дождитесь сообщения об успешном завершении обновления политики.



```
Administrator: Command Prompt - gpupdate /force
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpedit
C:\Users\Administrator>gpupdate /force
Updating Policy...

User Policy update has completed successfully.
```

В результате выполненных действий настройка групповых политик для использования BitLocker на компьютере пользователя будет закончена.

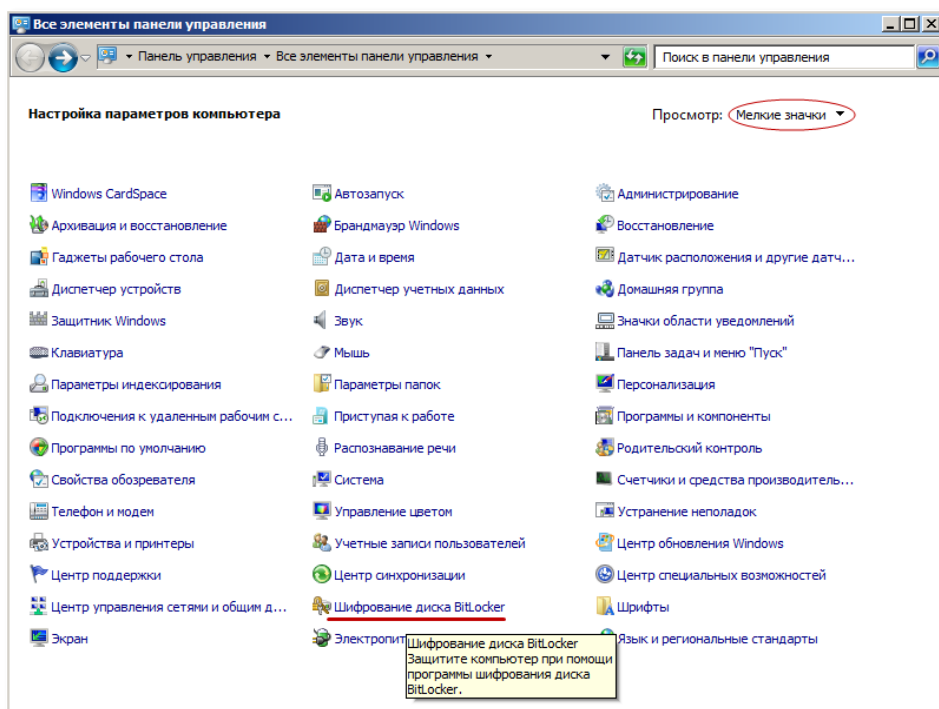
Шифрование дисков

Для включения BitLocker на фиксированных жёстких дисках с данными необходимо наличие полномочий администратора. Для включения BitLocker на съёмных дисках таких полномочий не требуется.

Чтобы зашифровать данные на дисках, расположенных на компьютере с установленной операционной системой Windows 7, выполните следующие действия.

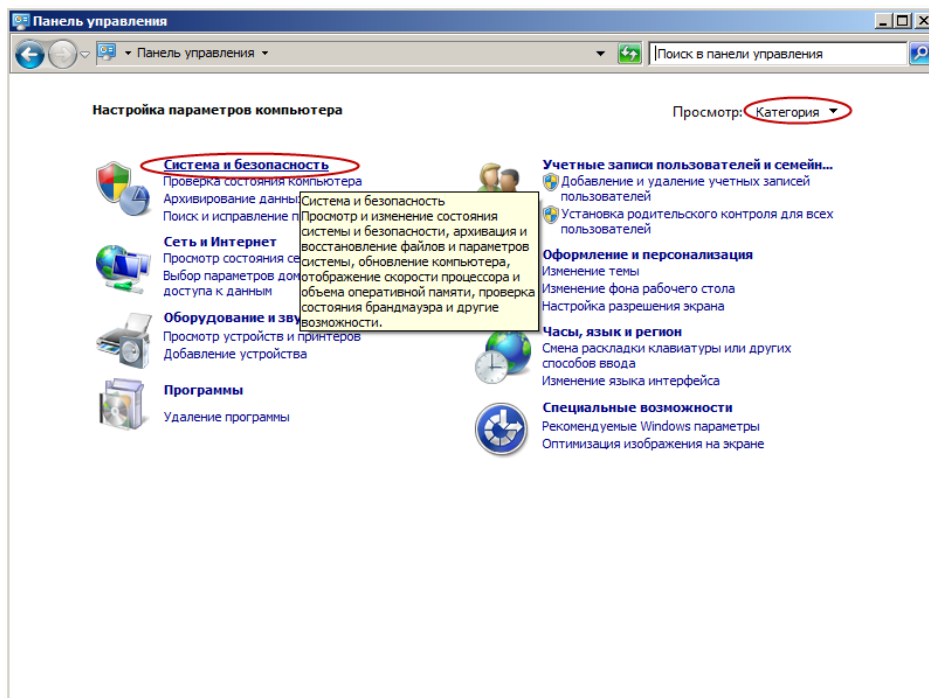
- 1 Нажмите кнопку Start (Пуск), выберите Control Panel (Панель управления).

- 2 Если окно находится в режиме просмотра **Мелкие значки**, выберите пункт **BitLocker Drive Encryption (Шифрование диска BitLocker)** и перейдите к шагу 3.

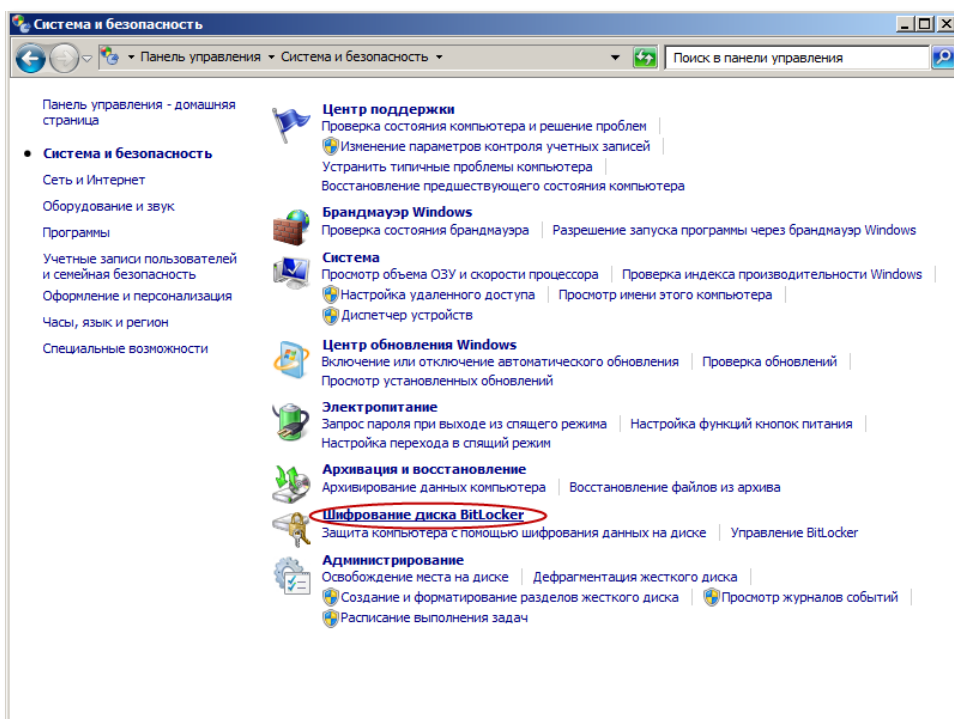


Если окно находится в режиме просмотра **Категория**:

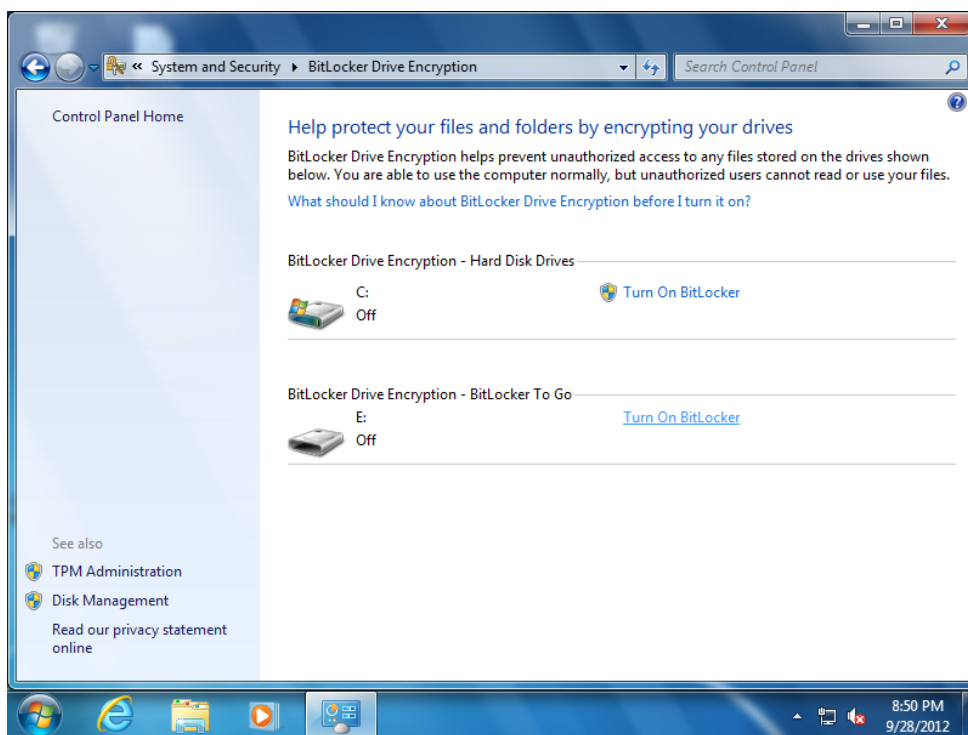
- щёлкните System and Security (Система и Безопасность);



- в открывшемся окне System and Security (Система и Безопасность) щёлкните BitLocker Drive Encryption (Шифрование диска BitLocker).



- 3 В открывшемся окне BitLocker Drive Encryption (Шифрование диска BitLocker) выберите диск и



- 4 справа от него щёлкните Turn On BitLocker (Включить BitLocker).

В открывшемся окне **BitLocker Drive Encryption (Шифрование диска BitLocker)** укажите способы разблокирования диска:

- если хотите настроить пароль для разблокирования диска, выберите **Use a password to unlock the drive (Использовать пароль для снятия блокировки диска)** введите пароль и его подтверждение;

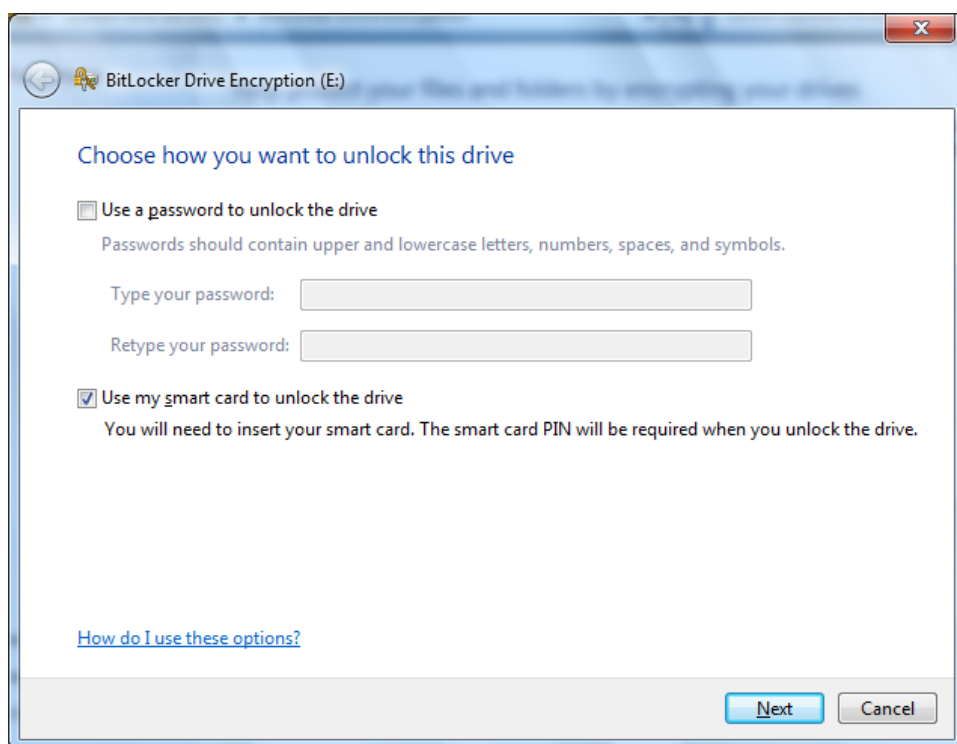
Важно

Фиксированные диски можно настроить на автоматическую разблокировку при шифровании диска операционной системы, на разблокировку при предоставлении пароля или после вставки электронного ключа JaCarta.

Съёмные диски по умолчанию можно настроить на разблокировку после предоставления пароля или после вставки электронного ключа JaCarta.

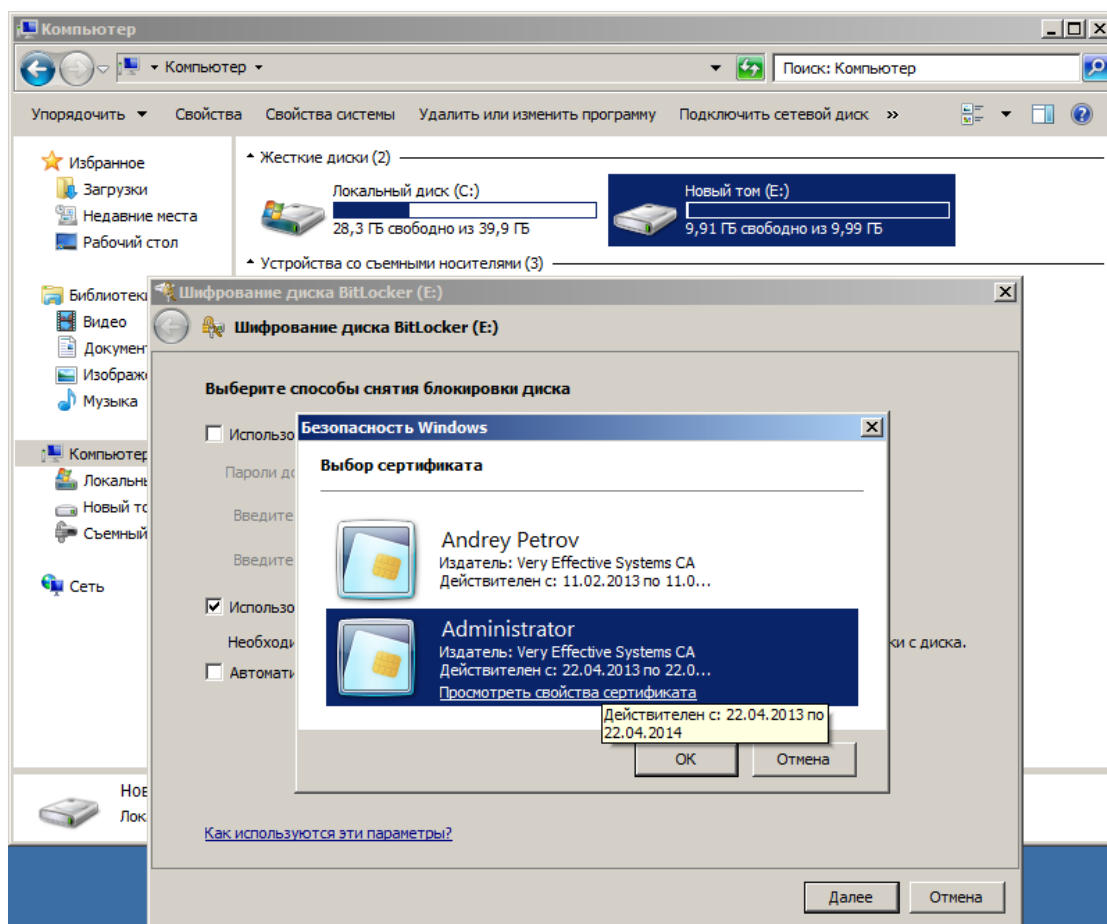
Для того чтобы съёмный диск разблокировался автоматически, необходимо настроить эту возможность после шифрования. Для этого щёлкните элемент Управление BitLocker в окне панели управления Шифрование диска BitLocker или установите флажок В дальнейшем автоматически снимать блокировку с этого компьютера при разблокировке диска.

- щёлкните Use my smart card to unlock the drive (Использовать смарт-карту для снятия блокировки диска) и подключите JaCarta к компьютеру.



- 5 Нажмите Next (Далее).
- 6 Если вы отметили пункт **Use my smart card to unlock the drive (Использовать смарт-карту для снятия блокировки диска)** и в памяти вашего электронного ключа JaCarta содержится только один сертификат, перейдите к п. 7.

Если вы отметили пункт **Use my smart card to unlock the drive (Использовать смарт-карту для снятия блокировки диска)** и в памяти вашего электронного ключа JaCarta содержится несколько сертификатов, в открывшемся окне выбора сертификатов укажите сертификат, по которому будет предоставляться доступ к зашифрованному диску и нажмите кнопку **ОК**.



7 В окне BitLocker Drive Encryption (Шифрование диска BitLocker) нажмите кнопку Next (Далее).

8 Откроется окно выбора варианта для сохранения ключа восстановления:

- сохранить ключ восстановления на флеш-накопителе USB (предусматривается, если такой накопитель подключён к компьютеру);
- сохранить ключ восстановления в файле;
- напечатать ключ восстановления.

Примечание

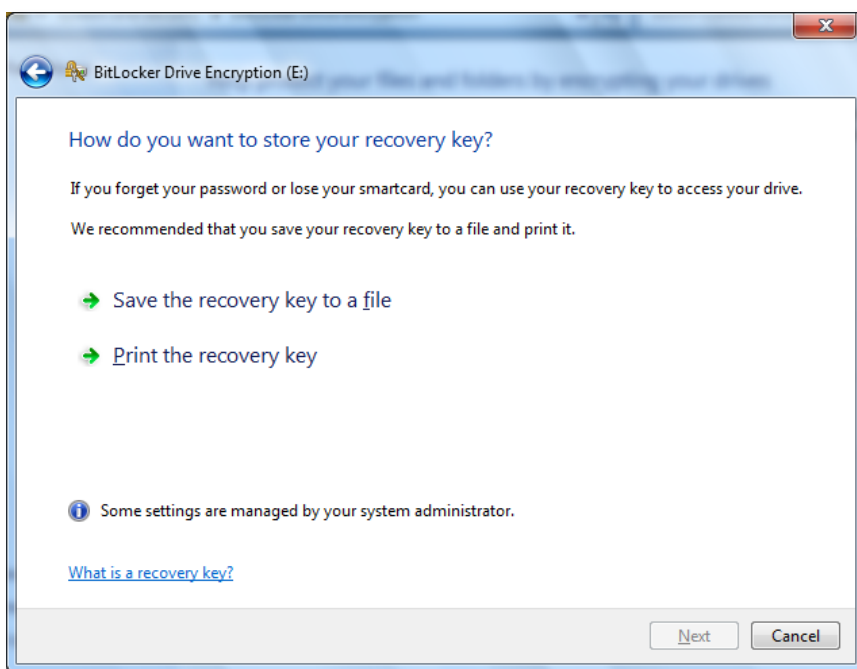
Ключ восстановления необходим при перемещении автоматически разблокируемого фиксированного диска с защитой BitLocker на другой компьютер или при недоступности пароля или электронного ключа JaCarta для разблокировки фиксированного или съёмного диска (например, при их утере).

Ключ восстановления необходим для разблокировки зашифрованных данных при переходе BitLocker в заблокированное состояние.

Ключ восстановления уникален для каждого диска и не подходит для восстановления зашифрованных данных с другого диска с защитой BitLocker.

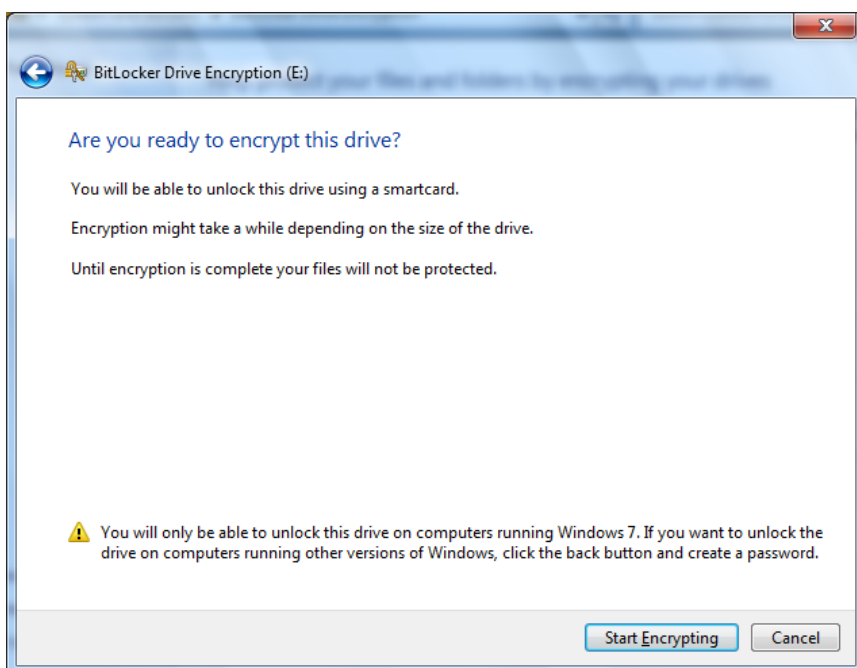
Для обеспечения должного уровня безопасности необходимо хранить ключи восстановления отдельно от связанных с ними дисков.

Выберите вариант сохранения ключа восстановления.



При выборе варианта сохранения ключа восстановления в файле появится окно проводника, в котором необходимо выбрать расположение и указать имя файла.

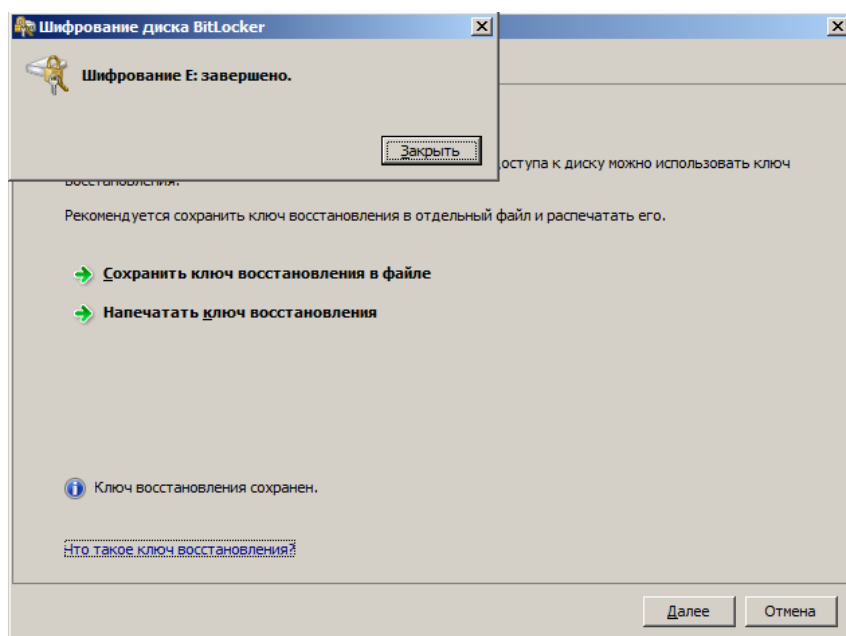
- 9 После выбора варианта нажмите **Next (Далее)**. При этом ключ будет сохранён или напечатан, о чём в нижней части страницы появится сообщение.
- 10 Для запуска процесса зашифрования выбранного диска в следующем окне нажмите кнопку **Start Encrypting (Начать шифрование)**.



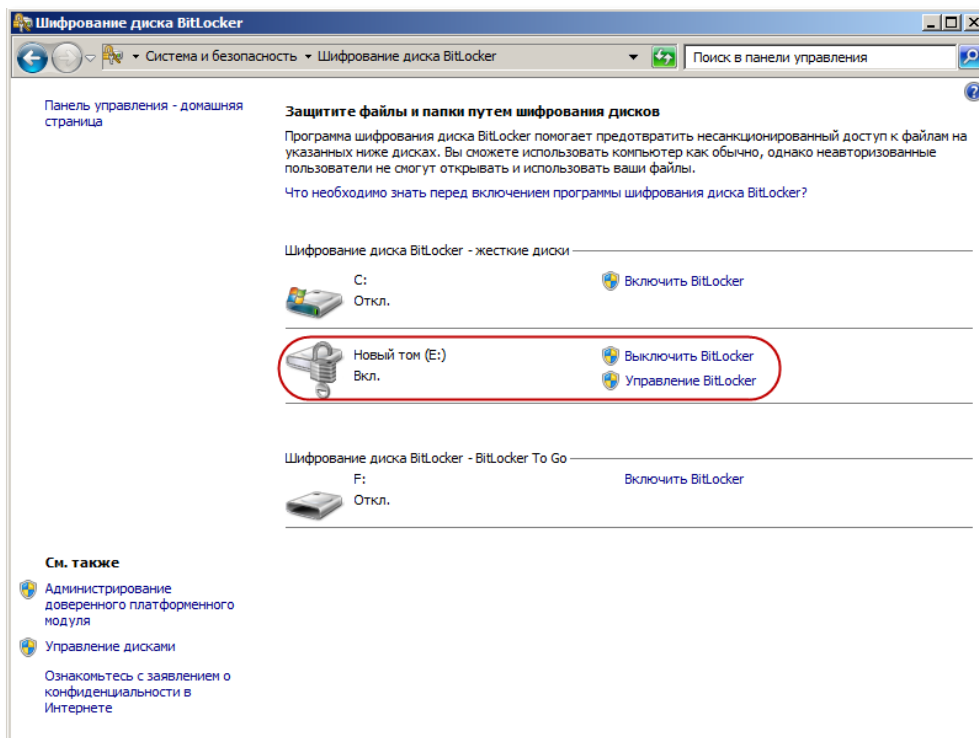
После выполненных действий появится окно с индикацией процесса шифрования и начнётся шифрование диска.



11 Дождитесь сообщения о завершении шифрования и в окне этого сообщения щёлкните **Заккрыть**.



Диск с установленной защитой BitLocker будет отображаться в окне Шифрование диска BitLocker, как показано на рисунке ниже.



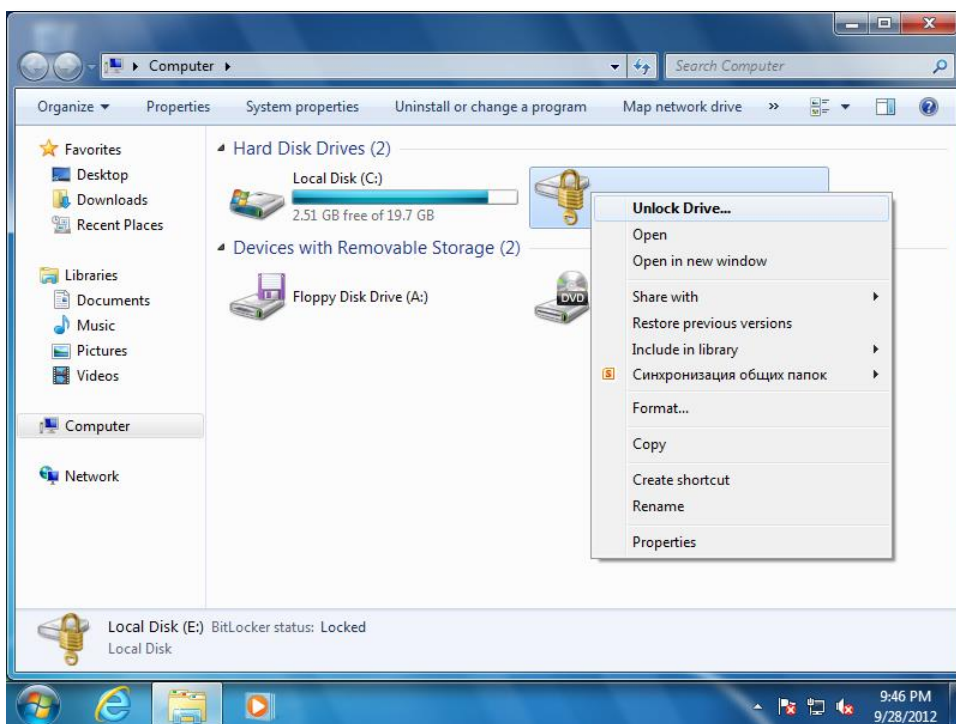
Для корректного проведения проверки предоставления доступа к зашифрованному BitLocker диску перезагрузите компьютер.

Проверка предоставления доступа к зашифрованному диску

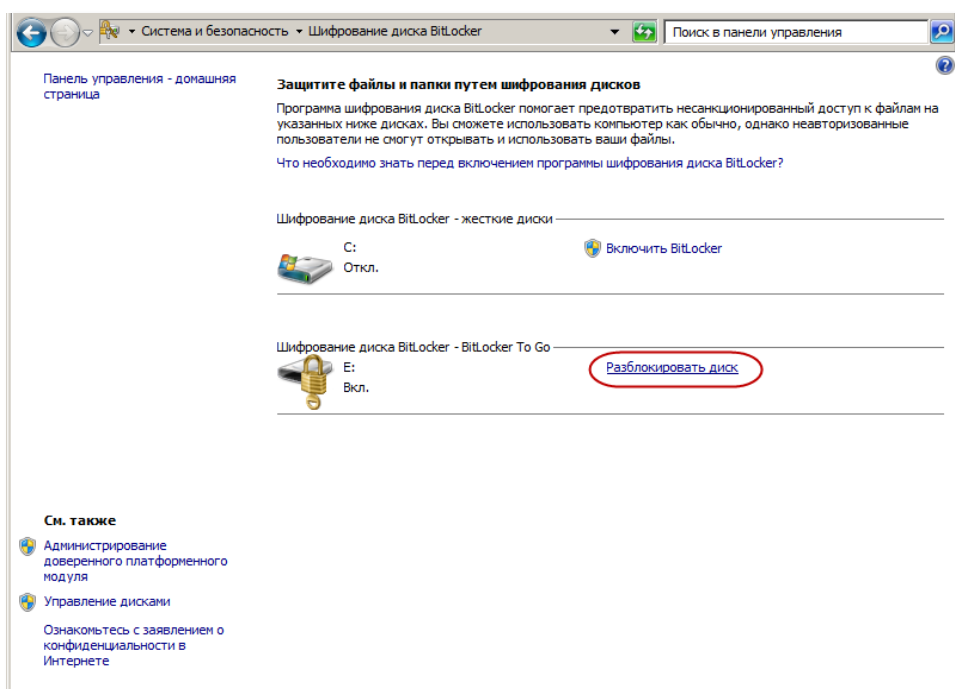
После завершения процесса шифрования необходимо проверить корректность предоставления доступа к зашифрованному диску. Для этого выполните следующие действия.

- 1 Выполните одно из действий:

- выберите **Start -> Computer (Пуск -> Компьютер)**, щёлкните правой кнопкой мыши по изображению зашифрованного диска и из открывшегося контекстного меню выберите пункт **Unlock Drive (Разблокировать диск)**;

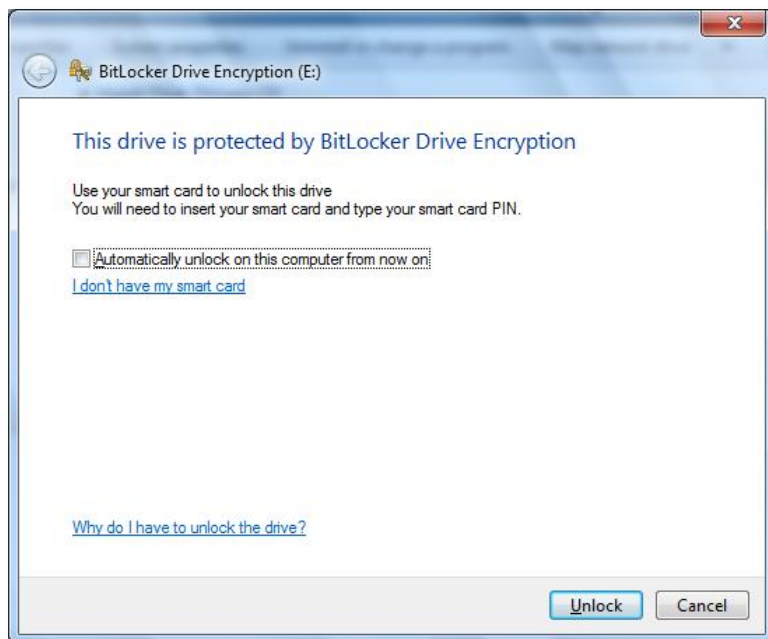


- или откройте окно **BitLocker Drive Encryption (Шифрование диска BitLocker)**, выполнив шаги 1 – 2 п. о, и щёлкните рядом с нужным диском **Разблокировать диск**.

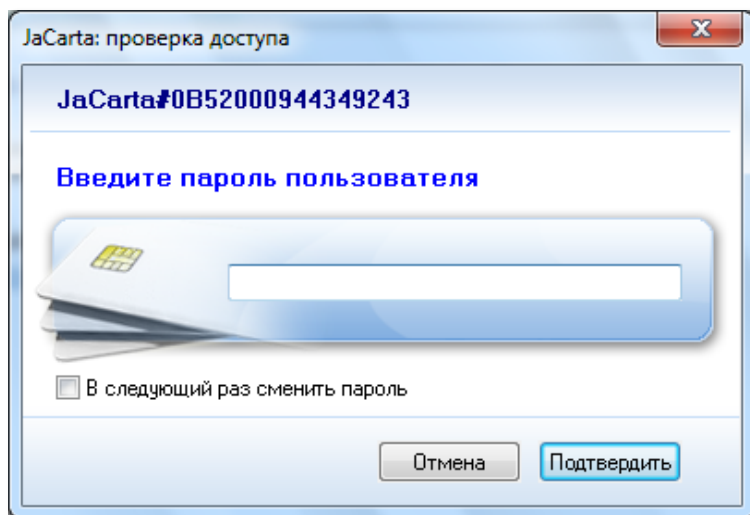


Появится окно BitLocker Drive Encryption (Шифрование диска BitLocker).

- 2 Подключите JaCarta и нажмите кнопку **Unlock** (Разблокировать).

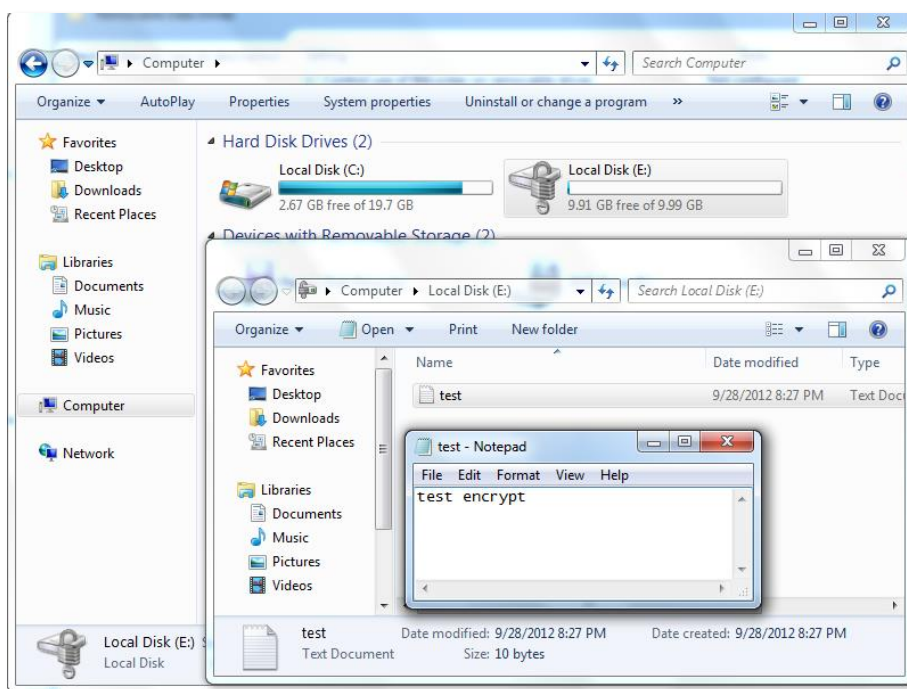


- 3 В открывшемся окне **JaCarta: проверка доступа** введите пароль ключа JaCarta и нажмите **Подтвердить**.



Откроется окно проводника с файлами, записанными на защищённый диск.

4 Откройте любой из файлов.

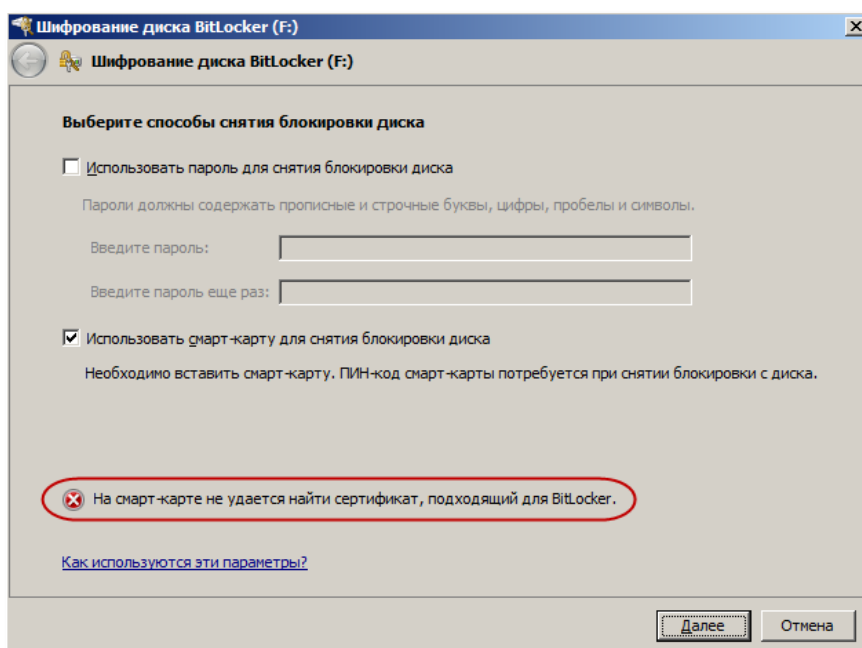


Успешное подключение к защищённому диску и открытие файла означает, что доступ к диску получен.

Известные проблемы при шифровании дисков средствами BitLocker с использованием JaCarta и их решение

Проблема 1:

При попытке установить на диск защиту BitLocker появилось сообщение об ошибке.



Возможная причина

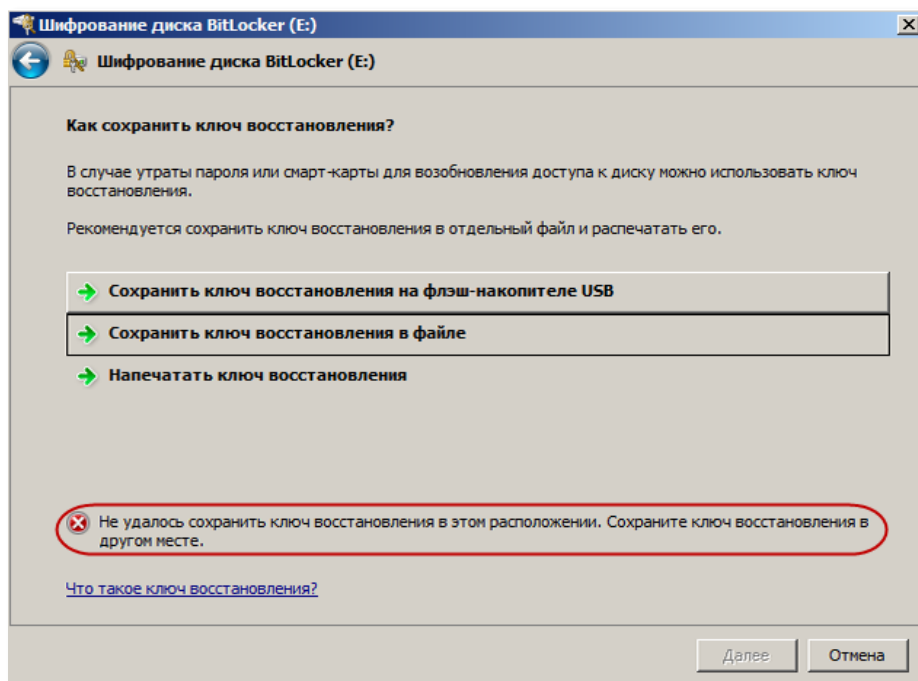
В памяти JaCarta нет сертификата, выпущенного для использования с BitLocker.

Решение

Используйте при установке защиты BitLocker ключ JaCarta с подходящим сертификатом.

Проблема 2

При попытке установить защиту BitLocker диска появилось сообщение об ошибке.



Возможная причина

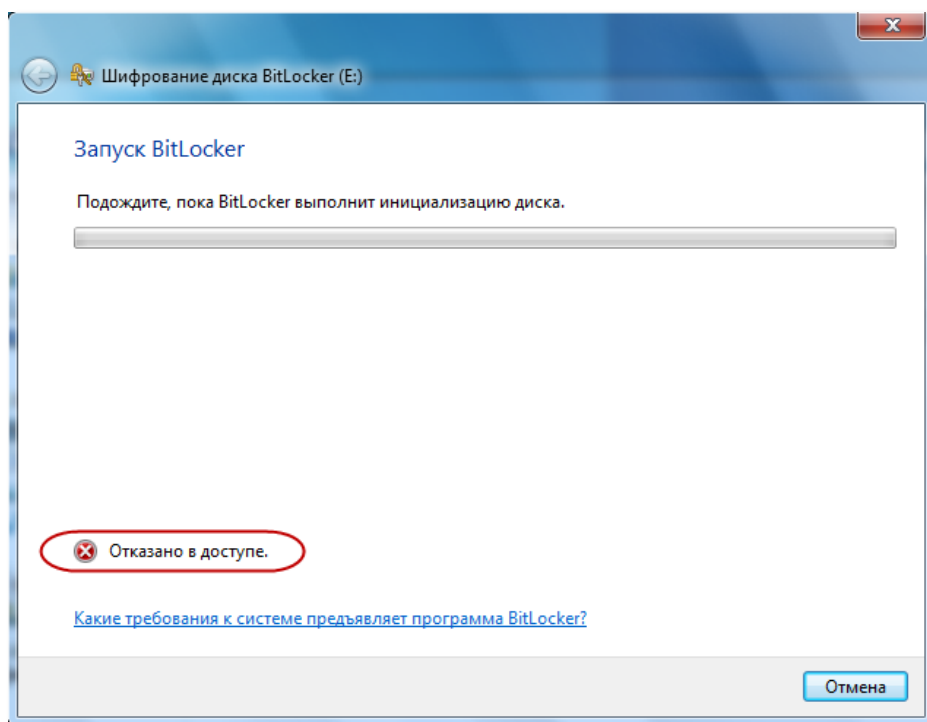
Вы указали некорректное расположение для сохранения ключа восстановления.

Решение

Укажите для этой цели доступное расположение. Для обеспечения должного уровня безопасности храните ключи восстановления отдельно от связанных с ними дисков.

Проблема 3

При попытке установить защиту BitLocker внутреннего жёсткого диска появилось сообщение об ошибке.



Возможная причина

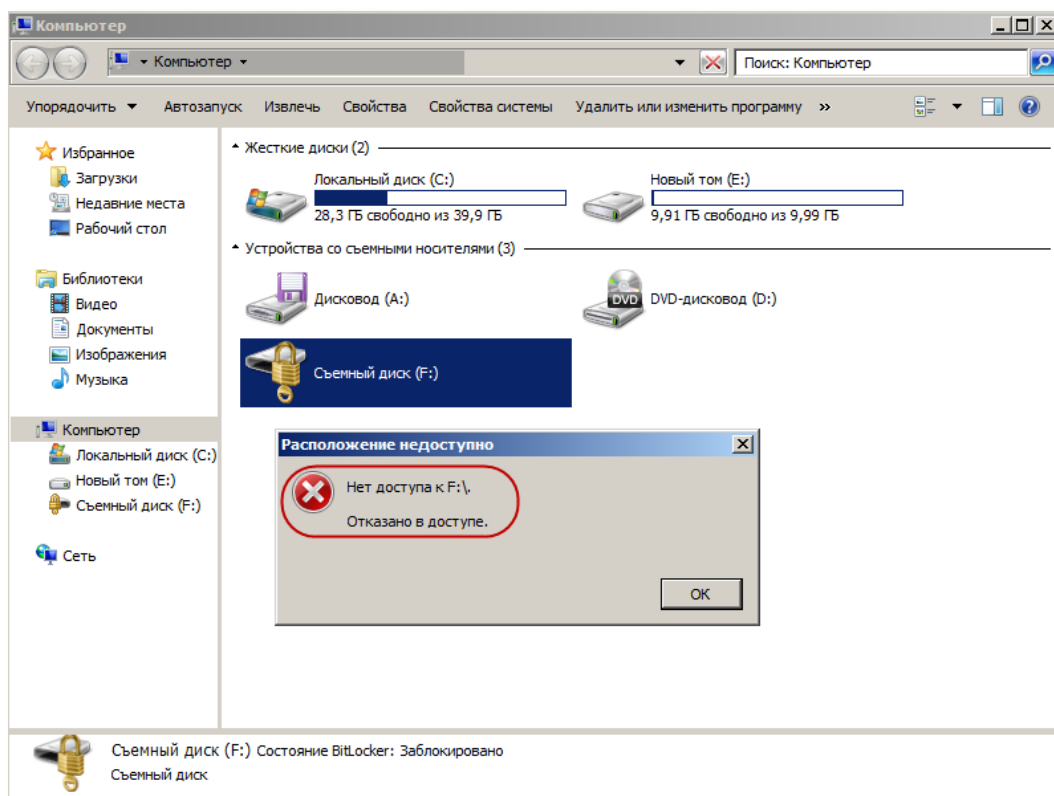
У Вас нет прав администратора на этом компьютере.

Решение

При необходимости установки защиты жёстких дисков обратитесь к администратору для получения прав администратора на этом компьютере.

Проблема 4

При попытке расшифровать диск с установленной защитой BitLocker появилось сообщение об ошибке.



Возможная причина

В памяти устройства JaCarta, подключенного к компьютеру, нет сертификата, использованного при установке защиты BitLocker на указанный диск.

Решение

Используйте для расшифрования диска ключ JaCarta с тем сертификатом, который был использован при установке защиты BitLocker на указанный диск.

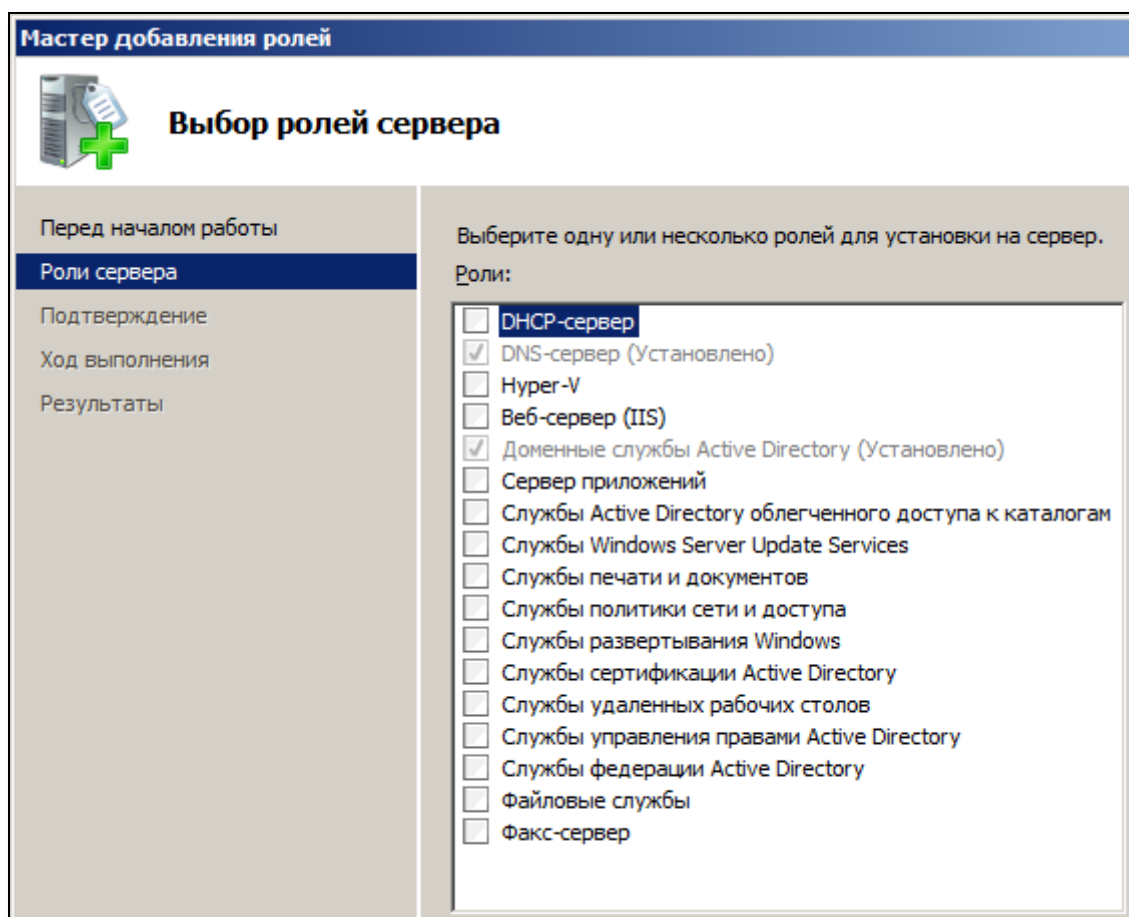
4. Установка служб сертификации (Windows Server 2008)

В данном приложении представлена процедура установки роли **Службы сертификации Active Directory** на сервере Windows Server 2008 R2 Enterprise. Процедура представлена на примере установки корневого центра сертификации предприятия. Подразумевается, что роль **Веб-сервер (IIS)** на сервере не установлена.

Чтобы установить роль **Службы сертификации Active Directory**, выполните следующие действия.

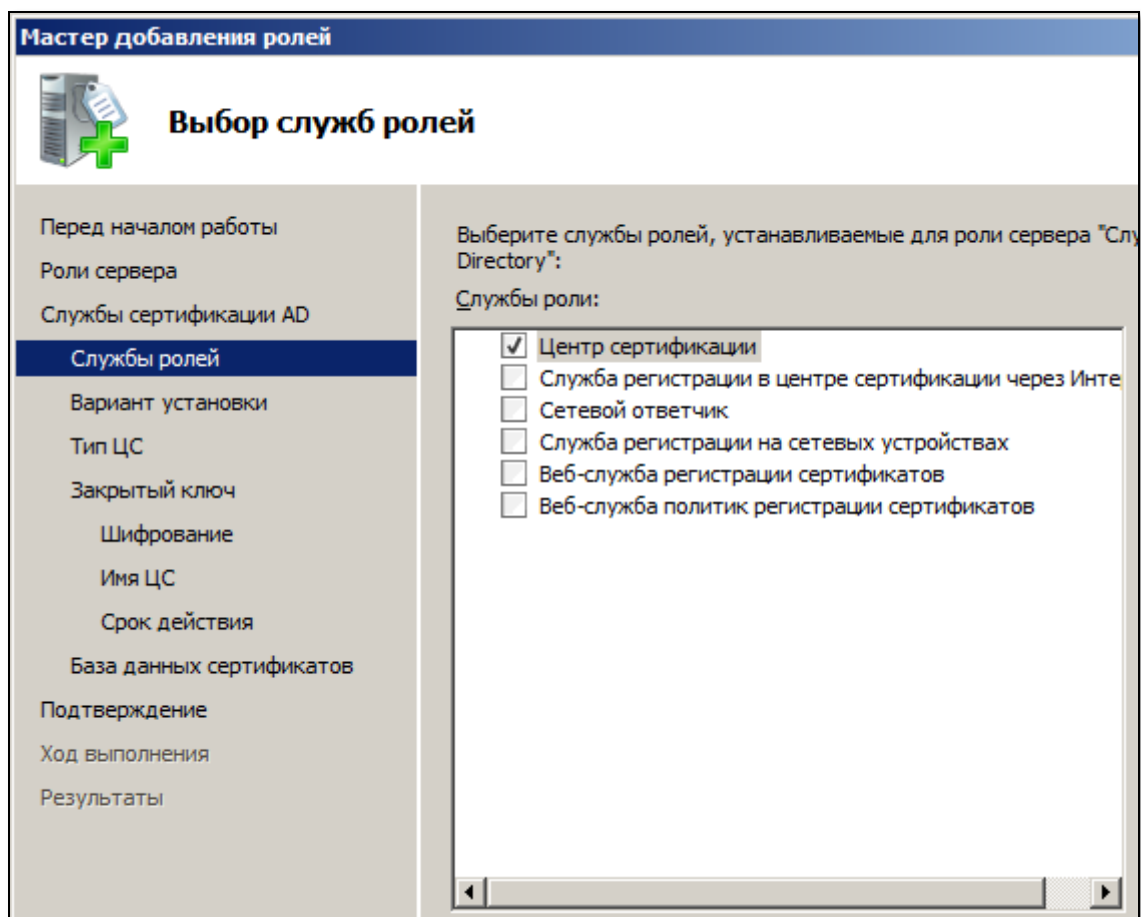
- 1 Запустите Диспетчер сервера, в левой части окна выберите **Роли**, затем в центральной части окна щёлкните на ссылке **Добавить роли**.
- 2 В окне приветствия мастера добавления ролей нажмите **Далее**.

Отобразится следующее окно.



- 3 Установите флажок Службы сертификации Active Directory и нажмите **Далее**.
- 4 В окне Знакомство со службами сертификации Active Directory нажмите **Далее**.

Отобразится следующее окно.

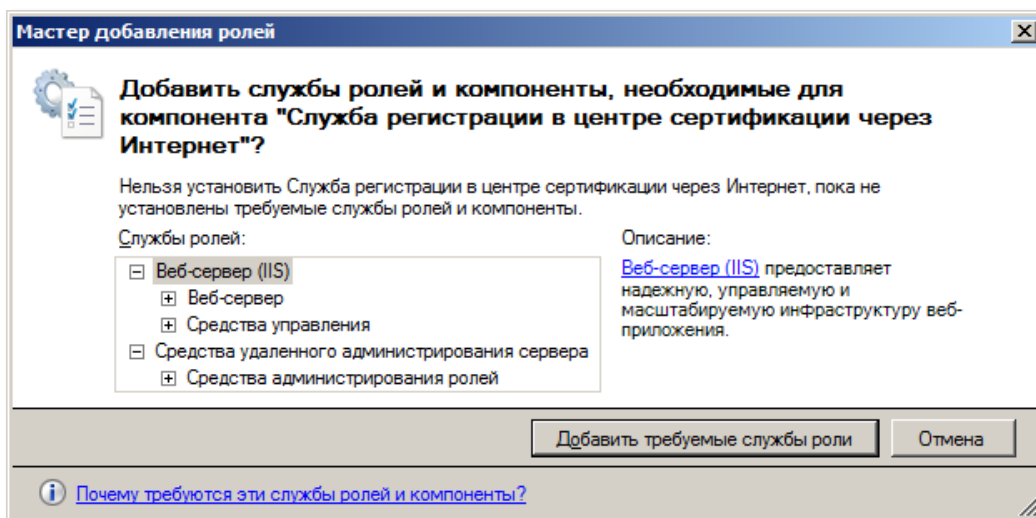


- 5 Отметьте необходимые пункты и нажмите **Далее**.

Примечание

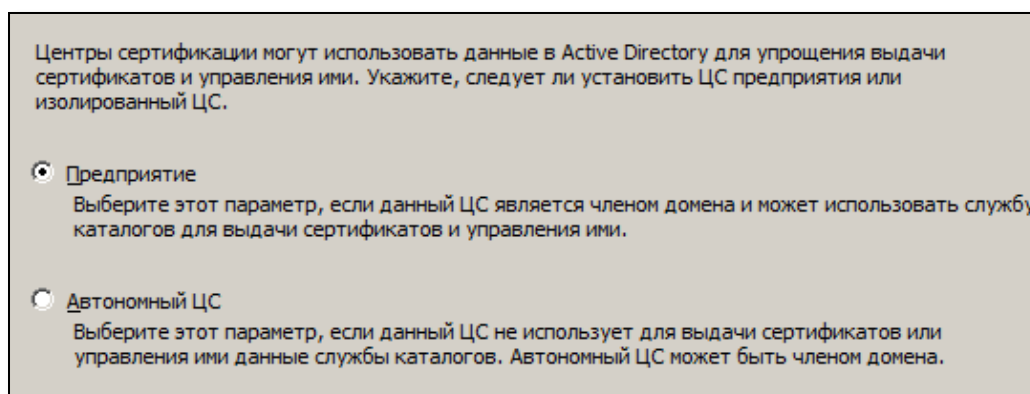
Чтобы обеспечить возможность записи сертификатов с использованием Web-интерфейса, необходимо отметить пункт Служба регистрации в центре сертификации через Интернет.

Если вы отметили пункт **Служба регистрации в центре сертификации через Интернет** и на сервере не установлена роль Веб-сервер (IIS), отобразится следующее окно.



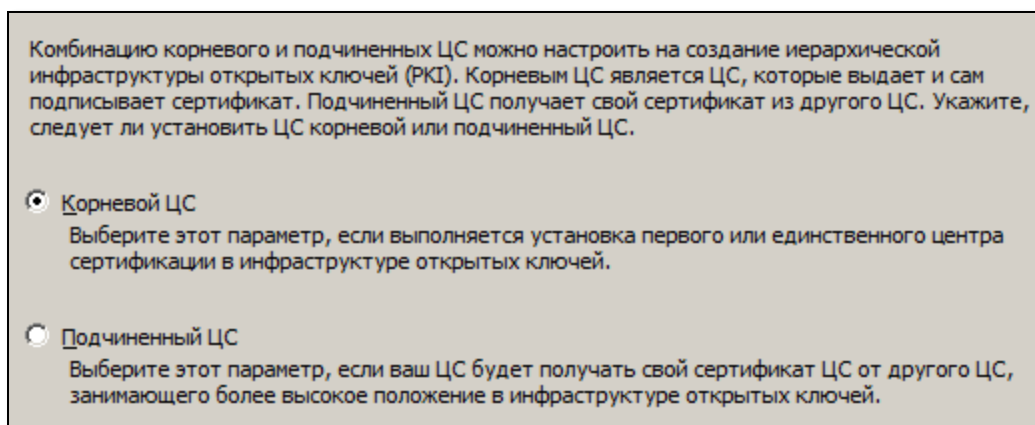
6 В этом случае нажмите **Добавить требуемые службы ролей** и в окне выбора служб ролей нажмите **Далее**.

Отобразится следующее окно.



7 Выберите один из двух вариантов (**Предприятие** или **Автономный ЦС**) и нажмите **Далее**. (В данном примере рассматривается установка центра сертификации предприятия.)

Отобразится следующее окно.

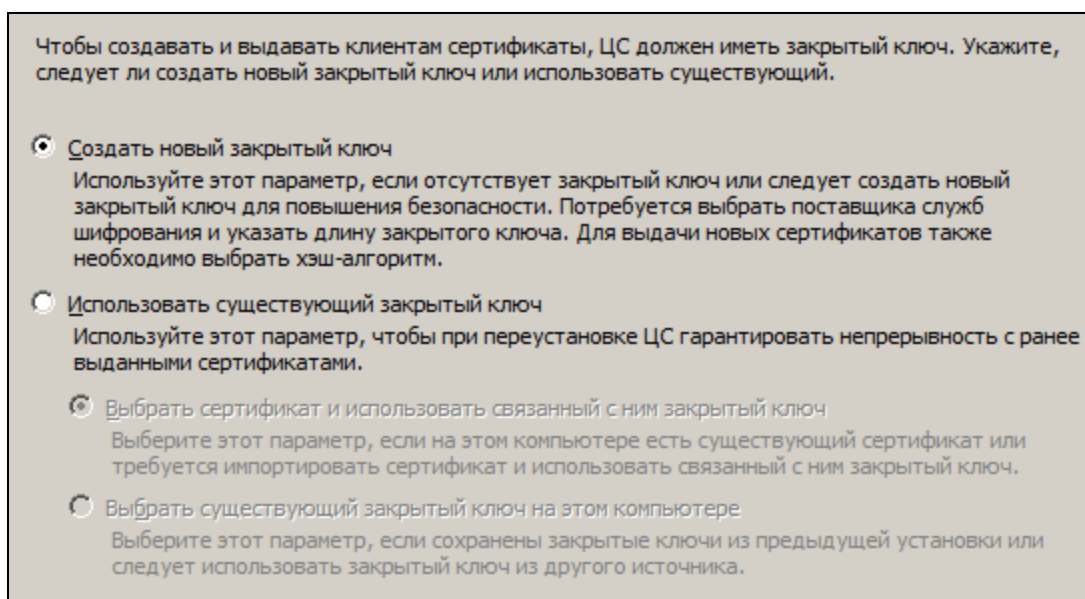


- 8 Выберите один из двух типов ЦС (Корневой ЦС или Подчиненный ЦС) и нажмите **Далее**. (В данном примере рассматривается установка корневого центра сертификации).

Примечание

Если это первый центр сертификации в вашей организации, необходимо выбрать пункт Корневой ЦС.

Отобразится следующее окно.



- 9 Выберите Создать новый закрытый ключ и нажмите **Далее**.

Отобразится следующее окно.

Для создания нового закрытого ключа необходимо выбрать [поставщика служб шифрования, хэш-алгоритм](#) и длину ключа в соответствии с назначением выдаваемых сертификатов. Выбор большей длины ключа повышает уровень безопасности, но увеличивает время, необходимое для выполнения операций подписания.

Выберите поставщика служб шифрования (CSP): RSA#Microsoft Software Key Storage Provider Длина ключа (знаков): 2048

Выберите алгоритм хеширования для подписывания сертификатов, выдаваемых этим ЦС:

- SHA256
- SHA384
- SHA512
- SHA 1

Разрешить взаимодействие с администратором, если центр сертификации обращается к закрытому ключу.

10 Выберите параметры формирования закрытого ключа.

Примечание

В поле *Выберите поставщика служб шифрования (CSP)* рекомендуется указывать CSP от компании Microsoft.

Если вы не уверены, какие настройки следует указать, оставьте настройки по умолчанию и нажмите **Далее**.

Отобразится следующее окно.

Введите общее имя, определяющее ЦС. Это имя добавляется во все сертификаты, выдаваемые данным ЦС. Значения суффикса различающегося имени генерируются автоматически, но не могут быть изменены.

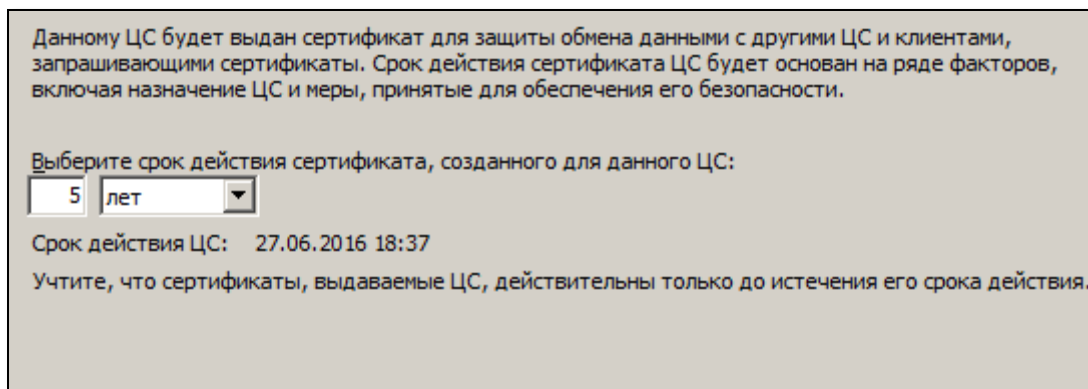
Общее имя для этого ЦС:
EntCA

Суффикс различающегося имени:
DC=test,DC=com

Предпросмотр различающегося имени:
CN=EntCA,DC=test,DC=com

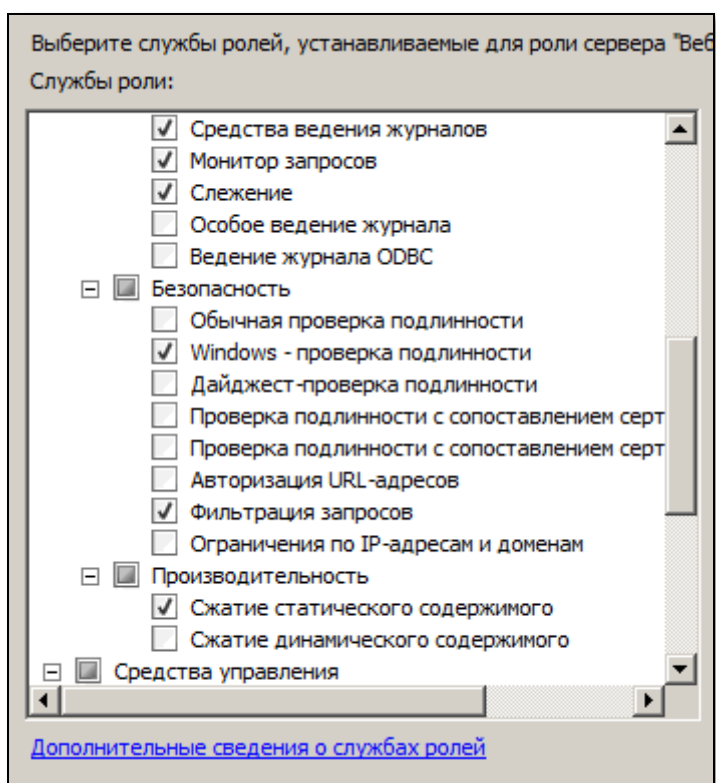
11 Введите необходимые данные и нажмите **Далее**.

Отобразится следующее окно.



- 12 Установите срок действия сертификата для создаваемого центра сертификации и нажмите **Далее**.
- 13 В окне **Настройка базы данных сертификатов** нажмите **Далее**.
- 14 Если вы отмечали службу роли **Служба регистрации** в центре сертификации через Интернет, отобразится окно установки службы Веб-сервер (IIS).
- 15 Нажмите **Далее**.

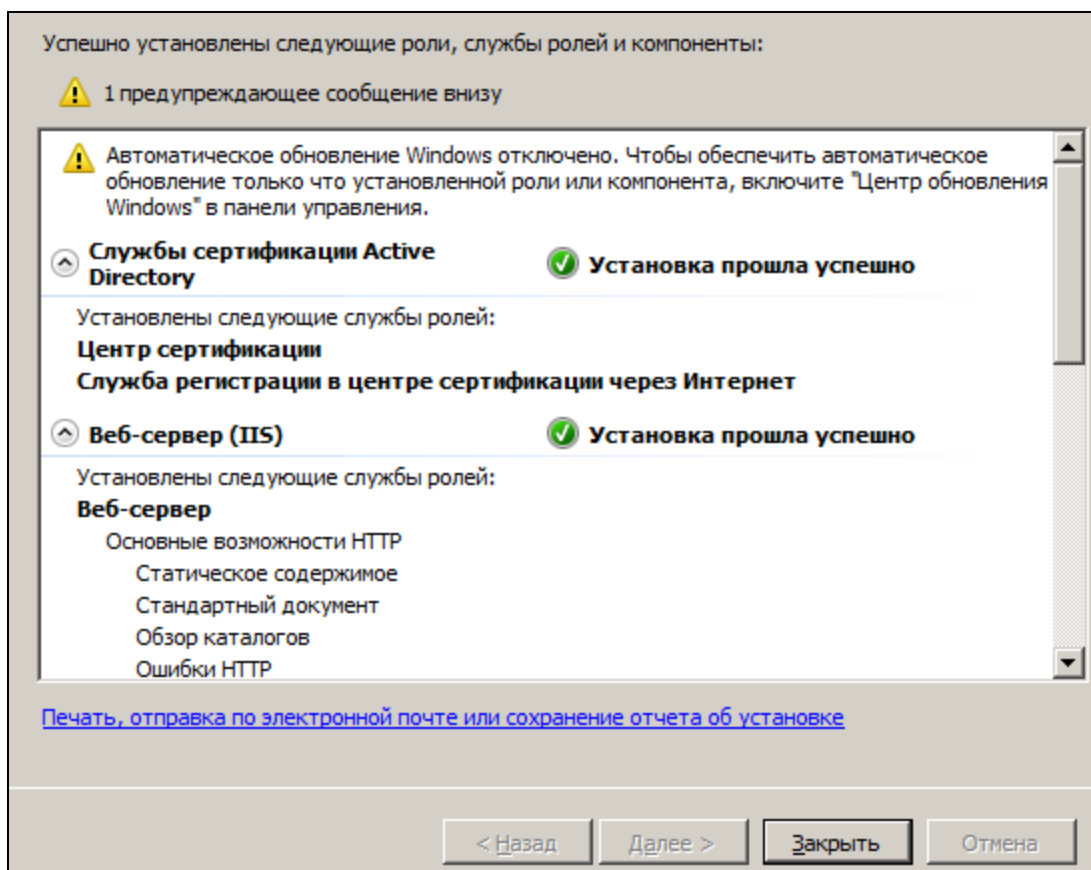
Отобразится окно выбора служб ролей веб-сервера (IIS).



- 16 Отметьте все пункты в секции **Безопасность** и нажмите **Далее**.
- 17 В окне подтверждения выбранных элементов для установки нажмите **Установить**.

Установка займёт некоторое время.

По окончании установки отобразится следующее окно.



При установке центра сертификации вы можете сделать его корневым или подчинённым, а также определить, будет ли он центром сертификации предприятия (интегрированным с Active Directory) - или автономным центром сертификации. Далее в таблице приведены основные различия между ЦС предприятия и автономным ЦС.

Особенность	Автономный ЦС	ЦС предприятия
Интеграция с Active Directory	Не интегрирован	Интегрирован
Публикация сертификатов	ЦС выдает сертификат по запросу пользователя через Web-сайт. Вы можете автоматически публиковать списки аннулированных сертификатов (CRL) и сертификаты в AD.	Зависит от шаблона сертификата — можно настроить автоматическую публикацию сертификата в профиль пользователя, публикацию в AD, либо и то, и другое.
Одобрение запроса на выдачу сертификата	Решение принимается автоматически или вручную. CA имеет единственную настройку, которая распространяется на все типы сертификатов.	Решение принимается автоматически или вручную. Вы можете настроить принятие решения на глобальном уровне (уровне CA), либо для каждого сертификата, используя шаблоны сертификатов.
Область применимости изданных	Extranet и Internet PKI.	Intranet PKI.

Требования к платформе	Можно устанавливать на контроллер домена Windows 2003 и Windows 2008, сервер в составе домена, автономный сервер (не являющийся членом домена).	Можно устанавливать на контроллер домена Windows 2003 и Windows 2008, сервер в составе домена.
Поддерживаемые типы сертификатов	Может выпускать ограниченное количество типов сертификатов и сертификаты, требующие особые OID в расширении EKU. Не поддерживает шаблоны сертификатов.	Может выпускать все сертификаты Windows 2008, шаблоны которых определены в соответствующей оснастке (Шаблоны сертификатов). Поддерживает шаблоны сертификатов: версии 1 (Win2K PKI), версии 2 (Windows 2003 PKI) и версии 3 (Windows 2008 PKI)
Идентификация пользователя	Пользователь должен сам вводить идентификационную информацию во время запроса сертификата. Используется для выделения перекрестных ссылок	ЦС автоматически получает информацию о пользователе из AD. Выпуск сертификатов пользователей осуществляется с помощью Web-интерфейса или оснастки Сертификаты. также можно использовать возможность автоматической выдачи сертификатов или утилиту certreq.exe в режиме командной строки.
Управление пользователями		

При установке центра сертификации предприятия вы должны обладать правами администратора предприятия или правами администратора домена (корневого домена леса AD). Кроме того, сервер, на который устанавливается ЦС предприятия, должен быть членом домена, на котором развёрнута служба каталогов AD. При невыполнении этих условий возможность установки ЦС предприятия будет затенена в мастере установки СА и вы сможете установить только автономный ЦС.

Для установки автономного ЦС наличие Active Directory не требуется. Вы можете установить центр сертификации на автономный сервер, сервер в составе домена или на контроллер домена. При установке автономного ЦС наличие прав администратора предприятия или администратора домена не требуется — для этого достаточно прав локального администратора. Если же вы обладаете правами администратора предприятия, то в ЦС будут включены дополнительные возможности. Например, если администратор предприятия устанавливает автономный ЦС на сервер, который присоединён к домену, то ЦС будет публиковать в Active Directory сертификаты, которые он выпускает.

Шаблоны сертификатов

ЦС предприятия использует шаблоны предприятия, которые хранятся в Active Directory. Шаблоны сертификатов определяют их содержание и характеристики. Кроме того, шаблоны сертификатов также определяют:

- какие типы сертификатов может выпускать ЦС предприятия;
- какие пользователи могут запрашивать сертификаты (и какого типа).

Windows 2008 PKI поддерживает вторую и третью версию (version 2, version 3) шаблонов сертификатов. В отличие от первой версии (version 1) вторая является полностью настраиваемой, в третьей версии шаблонов также добавлена поддержка CNG. Настройку шаблонов сертификатов можно осуществлять с помощью оснастки консоли управления mmc — Шаблоны сертификатов.

- Автономный ЦС не может использовать шаблоны сертификатов. Как следствие, вы не можете управлять пользователями, запрашивающими сертификаты таких типов из ЦС. По умолчанию автономный ЦС может выпускать только сертификаты для:
- Web-аутентификации по протоколам SSL или TLS;
- защиты электронной почты (S/MIME);
- аутентификации серверов (server authentication);
- подписывания кода (code signing);
- подписывания штампов времени (timestamp signing);
- IPSec;
- других областей применения (используя значения OID, хранящихся в расширении сертификатов ECU X.509).

5. Настройка Mozilla Firefox

Для доступа к защищённому сайту с электронным ключом JaCarta можно использовать браузер Mozilla Firefox. Для этого необходимо выполнить следующие действия:


- установить сертификат (или цепочку сертификатов) центра сертификации в Mozilla Firefox;
- в настройках Mozilla Firefox указать путь к библиотеке PKCS11 из состава JC-Client (если путь не был указан автоматически в процессе установки JC-Client);
- включить настройку, позволяющую согласование SSL-соединения (требуется для Firefox, начиная с версии 4.0 и выше).

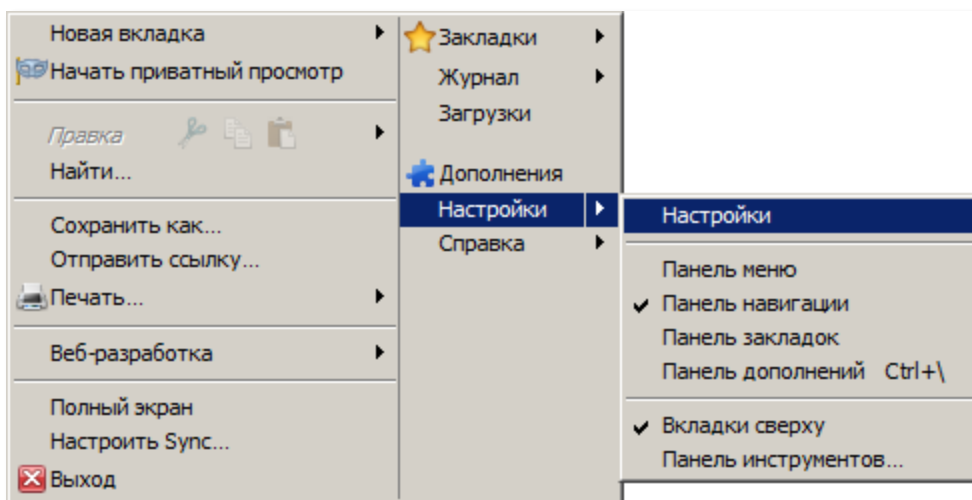
Примечание:


Все настройки приведены на примере Mozilla Firefox 5.0

Установка сертификата центра сертификации в Mozilla Firefox

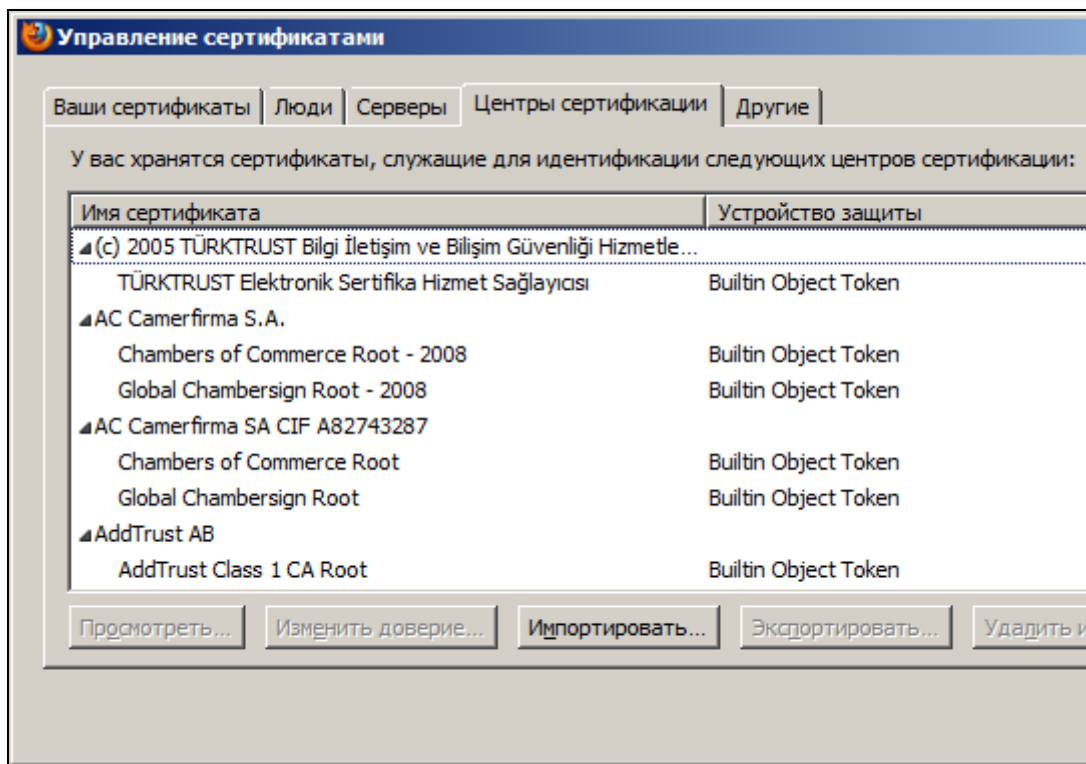
Чтобы при использовании JaCarta для доступа к защищённому сайту в браузере пользователя не отображалось предупреждение, необходимо установить сертификат или (и) цепочку сертификатов центра сертификации в Mozilla Firefox. Для этого выполните следующие действия.

- 1 Запустите Mozilla Firefox, щёлкните на значке  и выберите **Настройки > Настройки**, как показано на изображении ниже.



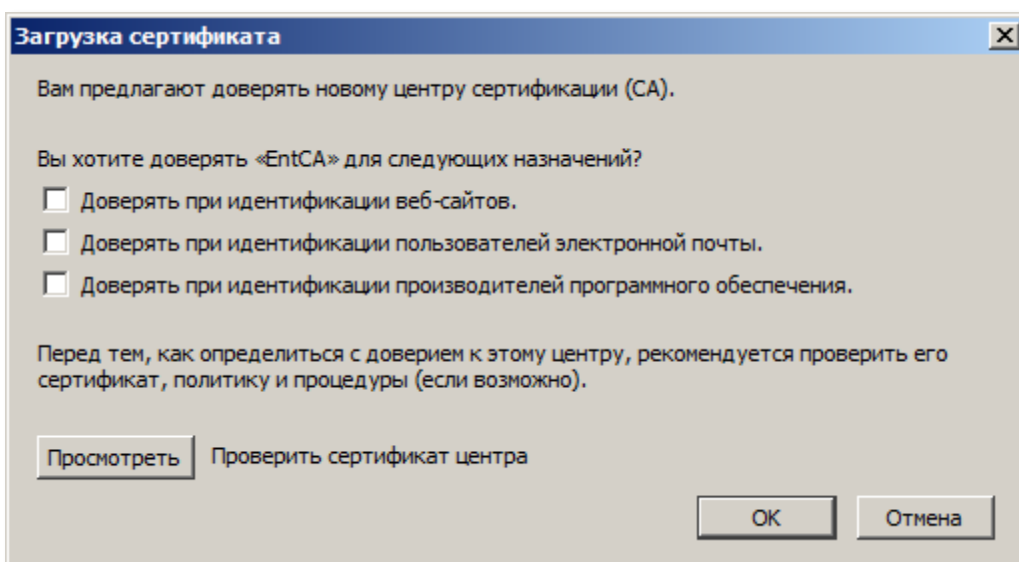
- 2 В отобразившемся окне щёлкните на значке  (**Дополнительные**), выберите вкладку **Шифрование**, нажмите **Просмотр сертификатов** и выберите вкладку **Центры сертификации**.

Окно настроек примет следующий вид.



- 3 Нажмите **Импортировать** и укажите путь к файлу сертификата или цепочки сертификатов центра сертификации.

Отобразится следующее окно.




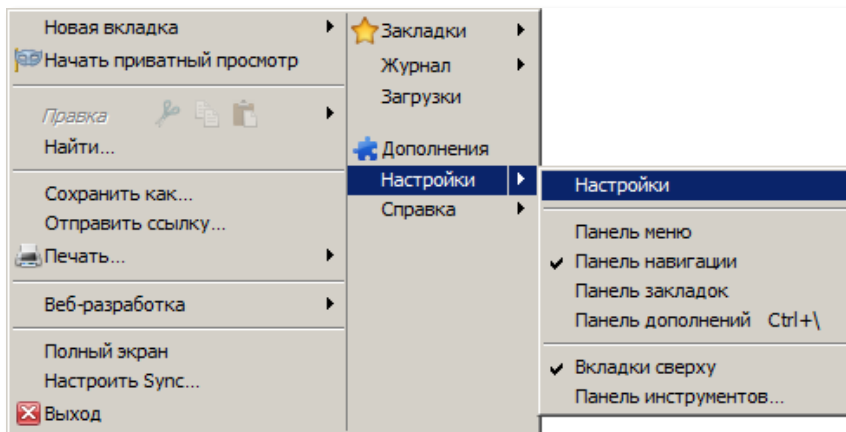
- 4 Отметьте необходимые пункты и нажмите **ОК**.


Настройка Mozilla Firefox

Чтобы использовать электронные ключи JaCarta с Mozilla Firefox, в настройках браузера необходимо указать путь к библиотеке PKCS11 из состава JC-Client. Если браузер Mozilla Firefox был установлен на компьютер до установки JC-Client и если при установке JC-Client была отмечена соответствующая опция, путь к библиотеке прописывается в настройках Mozilla Firefox автоматически.

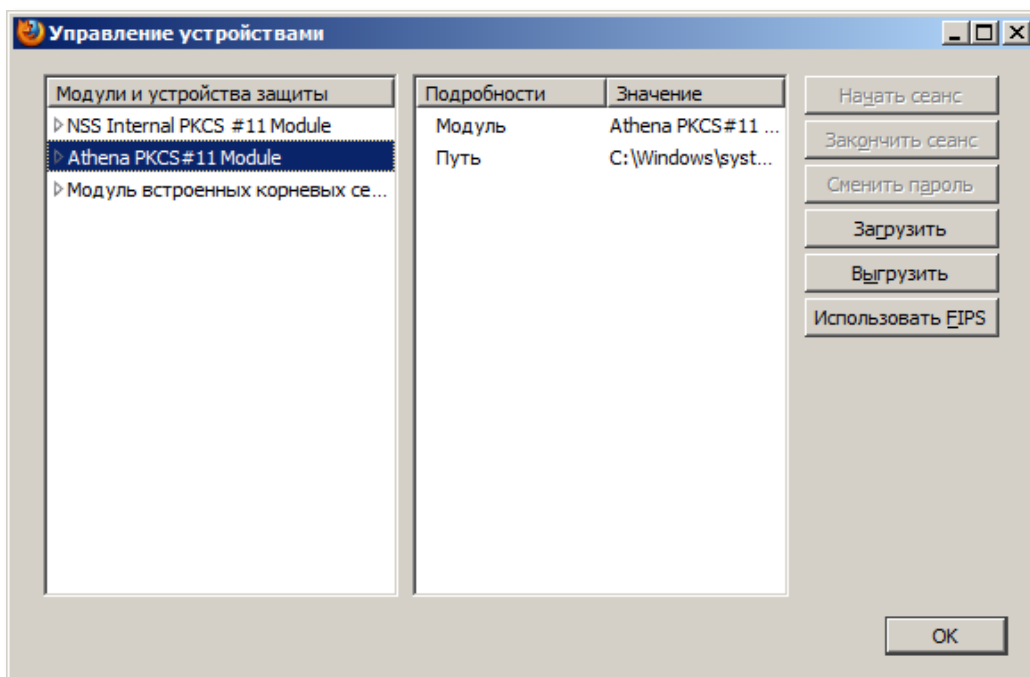
Чтобы указать путь к PKCS11 из состава JC-Client вручную, выполните следующие действия.

- 1 Запустите Mozilla Firefox, щёлкните на значке  и выберите **Настройки > Настройки**, как показано на изображении ниже.



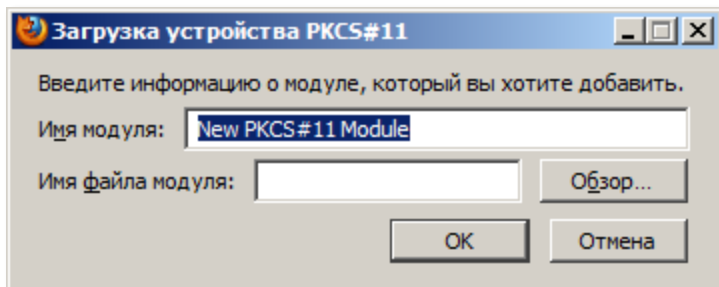
- 2 В отобразившемся окне щёлкните на значке  (**Дополнительные**), выберите вкладку **Шифрование** и нажмите **Устройства защиты**.

Отобразится следующее окно.



- 3 Если путь к библиотеке PKCS#11 был прописан автоматически в процессе установки JC-Client, в списке **Модули и устройства защиты** будет значиться **Athena PKCS#11 Module**. В противном случае нажмите **Загрузить**.

Отобразится следующее окно.

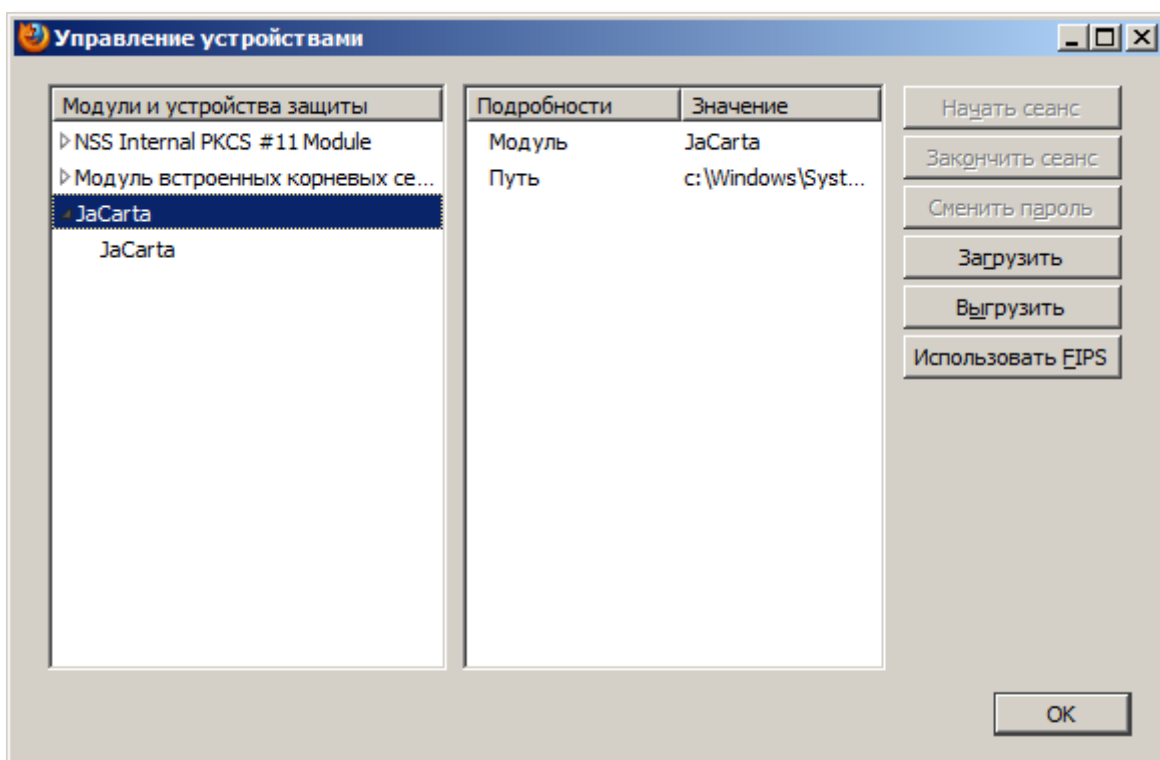


- 4 В поле **Имя модуля** введите имя нового модуля (например, JaCarta), в поле **Имя файла модуля** укажите путь к библиотеке PKCS11 из состава JC-Client (при необходимости воспользуйтесь кнопкой **Обзор**).

Файл библиотеки PKCS11 из состава JC-Client находится по следующему пути:

C:\Windows\System32\asepkcs.dll

- 5 Нажмите **OK**.
- 6 Добавленная библиотека отобразится в списке **Модули и устройства защиты**.



Настройка конфигурации Mozilla Firefox

Чтобы обеспечить SSL-доступ к защищённому сайту с использованием цифрового сертификата в памяти JaCarta, необходимо включить соответствующую настройку в конфигурации Mozilla Firefox. Для этого выполните следующие действия.

Примечание

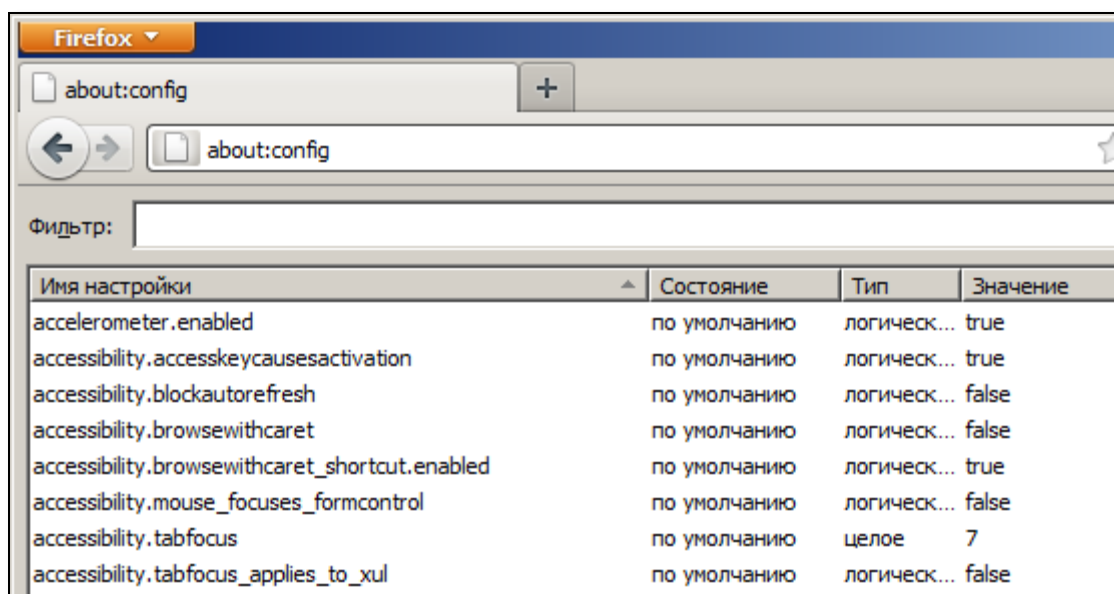
Данные действия необязательны для Firefox версий до 4.0.

- 7 Запустите Mozilla Firefox.
- 8 В адресной строке наберите `about:config` и нажмите клавишу ВВОД.

В окне браузера отобразится предупреждающее сообщение.

- 9 Нажмите Я обещаю, что буду осторожен.

Окно браузера примет следующий вид



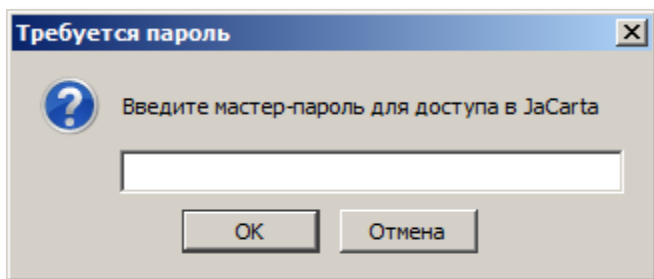
- 10 Двойным щелчком измените значение настройки `security.ssl.allow_unrestricted_renego_everywhere__temporarily_available_pref` на `true` (истина).
(Для быстрого поиска настройки введите или скопируйте ее в поле **Фильтр**).

Действия пользователя

Чтобы получить доступ к защищённому сайту с использованием браузера Mozilla Firefox и электронного ключа JaCarta, выполните следующие действия.

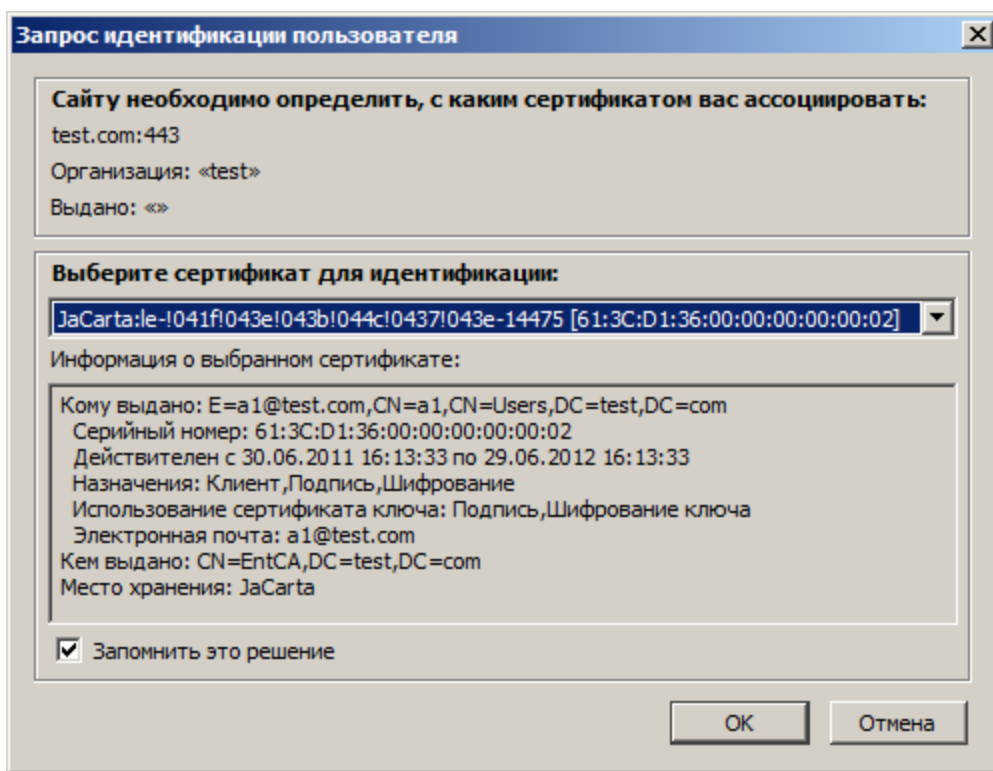
- 1 Убедитесь в том, что к компьютеру подключен электронный ключ JaCarta. На USB-токене JaCarta должен гореть световой индикатор.
- 2 Запустите браузер Mozilla Firefox, в адресной строке введите адрес защищённого сайта (адрес должен начинаться с `https://`) и нажмите клавишу ВВОД.

Отобразится следующее окно.



3 Введите пароль пользователя JaCarta и нажмите **ОК**.

Отобразится следующее окно.



4 Установите флажок **Запомнить это решение** и нажмите **ОК**.

После этого вы попадете на защищённый сайт.

Регистрация изменений

Версия	Изменения
2.0	Документ сверстан в новом корпоративном шаблоне
1.3	Добавлен раздел Шифрование BitLocker
1.2	Добавлен раздел Шифрование электронной почты
1.1	Добавлен раздел Установка служб сертификации
1.0	Исходная версия документа

Коротко о компании

Основанная в апреле 1995 года компания "Аладдин Р. Д." — российский разработчик (вендор) средств защиты информации.

Компания является признанным экспертом и лидером российского рынка средств двухфакторной аутентификации пользователей, электронной подписи и защиты данных.

Основные направления:

- обеспечение безопасного доступа к информационным ресурсам предприятия, Web-порталам и облачным сервисам (строгая двух- и трёхфакторная аутентификация);
- электронная подпись (ЭП с неизвлекаемым закрытым ключом, формируемая в защищённом чипе), PKI;
- защита персональных данных, данных на дисках компьютеров, серверов, баз данных.

Все основные продукты имеют необходимые сертификаты ФСТЭК, ФСБ и Министерства обороны (включая работу с гостайной до уровня секретности СС).

Лицензии:

- компания имеет все необходимые лицензии ФСТЭК России, ФСБ России и Министерства обороны России для проектирования, производства и поддержки СЗИ и СКЗИ, включая работу с гостайной и производство продукции в рамках гособоронзаказа;
- система менеджмента качества продукции в компании с 2012 г. соответствует стандарту ГОСТ ISO 9001-2011 и имеет соответствующие сертификаты;
- система проектирования, разработки, производства и поддержки продукции соответствует требованиям российского военного стандарта ГОСТ РВ 15.002-2012, необходимого для участия в реализации гособоронзаказа.



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 3442 от 10.11.2017
Лицензии ФСБ России № 12632 Н от 20.12.12, № 30419 от 16.08.17
Лицензия Министерства обороны РФ № 1384 от 22.08.16
Система менеджмента качества компании соответствует требованиям ISO/ИСО 9001-2011
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15
© ЗАО «Аладдин Р. Д.», 1995—2018. Все права защищены
Тел. +7 (495) 223-00-01 Email: aladdin@aladdin-rd.ru Web: www.aladdin-rd.ru