



# Руководство по внедрению

Версия 2.0

# Оглавление

Од	окументе	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 Тробования к рабоним станциям	10
	треоования к расочим станциям	.10
	Гребования к программному обеспечению Требования к аппаратному обеспечению	10
3.	Технологии безопасности	.12
	Использование цифровых сертификатов и полный отказ от паролей	12
	Общие сведения Процедуры выдачи сертификатов Шаблоны сертификатов	12 12 13 26 28 41 41 44 45 46 46 47 49
	пастройка служо политики сети и доступа Настройка учётной записи пользователя	50 56
	пастроика рабочеи станции Подключение к удалённому рабочему столу	57 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 корреспонд	енции71
	Microsoft Outlook 2010 (из пакета Microsoft Office 2010)	71
	Цифровая подпись и шифрования при использовании OWA	
	Шифрование данных на жестком диске (ЕРS)	
	Общие сведения	76
	Запись сертификата EFS в память электронного ключа JaCarta	76
	Зашифрование данных на жёстком диске	
	шифрование диска вітьоскег с использованием засагта	81
	Общие сведения	81
	Системные требования	
	Дополнительная настроика шаблона сертификата Настройка компьютора пола поратора	2882 حە
	Пастроика компьютера пользователя	,
	Проверка предоставления доступа к зашифрованному диску	
	Известные проблемы при шифровании дисков средствами BitLocker с использо	ванием
	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: <u>www.aladdin-rd.ru/support/index.php.</u>

## 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 предназначается 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 электронновычислительных 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 гарантии

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 нелицензионным 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 понуждения 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 ложности.

Руководство по внедрению

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 **Вебсервер (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 cooтветствующей 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 OC 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 избрать 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 Пользовать 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 КВ958830, 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 отнеситесь 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.

- Загрузите с сайта Microsoft и установите средства удалённого администрирования сервера (обновление КВ958830).
- 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.

🔄 Программы и компоненты			
🕞 🗇 🖂 🔹 Все э Программ 🖅 Поиск: Программы и компоненты 👂			
	Панель управления - домашняя страница	Удаление или изменение программы	
	Просмотр установленных обновлений	Для удаления программы выберите ее в списке и щелкните "Удалить", "Изменить" или "Восстановить".	
8	Включение или отключение компонентов Windows	Упорядочить 🔻	:= • 🕡
	Установка новой программы из	Имя 🔶	• Издатель 🔺
	сети	🔀 Microsoft Exchange Server 2010	Microsoft C
		Microsoft Filter Pack 1.0	Microsoft C
		🔀 Microsoft Full Text Indexing Engine for Exchange	Microsoft C
		器 Microsoft Office профессиональный плюс 2010	Microsoft C
		🥮 Mozilla Firefox 4.0 (x86 en-US)	Mozilla
		🔀 Total Commander (Remove or Repair)	Ghisler Sof
		VMware Tools	VMware Ir
		Установленные программы	
		Установлено программ: 7	

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

🛃 Компоненты Windows					
Включение или отключение компонентов Windows 🕡					
Чтобы включить компонент, установите его флажок. Чтобы отключить компонент, снимите его флажок. Затененный флажок означает, что компонент включен частично.					
🗹 🎍 Службы XPS 📃					
🗄 🛨 📙 Службы для NFS					
🕀 🗹 🎍 Службы печати и документов					
📃 🖂 🔲 Средства удаленного администрирования сервер					
🔲 🍌 Диспетчер сервера					
🕀 🔳 🗋 Средства администрирования возможностей					
П. Средства администрирования ролей     П.     П.					
🗹 🍌 Средство просмотра XPS					
Удаленное разностное сжатие					
Фильто Windows TIFE IFilter					
ОК Отмена					

- 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.

🚟 Консоль1 - [Корень консоли]	
🚋 <u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>И</u> збранное <u>О</u> кно <u>С</u> правка	_ & ×
Корень консоли Имя	Действия
Нет элементов для отображения в этом виде.	Корень консоли 🔺
	Дополнитель 🕨

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

нтр сертификации		)
Выберите компьютер, которы	ым должна управлять эта оснастка.	
-Эта оснастка всегда управ	ляет:	
покальным компьютер	ом (тем, на котором выполняется эта консоль)	
С другим компьютером:		
		-
<u>Разрешается изменять выбранный для управления компьютер при запуске из комананой строки.</u> Применеется только при сохранении консоли.		
	< Назад <b>Готово Отмена Спра</b>	ska -

- 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 доступк 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.

Руководство по внедрению

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

🔚 Консоль1 - [Корень консоли\Центр сертификации (srv1.test.com)\EntCA]			
— Файл Действие Вид Избранное Окно Справка → → 2 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	B_X		
Корень консоли Центр сертификации (srv1.test.co EntCA Отозванные сертификаты Выданные сертификаты Запросы в ожидании Неудачные запросы Шаблоны сертификатов Управление Создать Новое окно отсюда Обновить Справка	Действия EntCA < Дополнительные дей >		
Запуск оснастки шаблонов сертификатов			

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

🖳 Консоль шаблонов сертификатов					
<u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка					
🗵 Шаблоны сертиф	🚇 Шаблоны сертиф Отображаемое имя шаблона 🔺 🔺 Действия				
	🚇 Пользователь Exchange	Шаблоны серт 🔺			
	🚇 Пользователь со смарт-картой				
	🚇 Почтовая репликация каталога	Скопировать шаблон			
	🚇 Проверенный сеанс	Все задачи			
	🚇 Проверка подлинности Kerberos				
	🚇 Проверка подлинности контрол	Свойства			
	🚇 Проверка подлинности рабочей	Справка			
	🚇 Только подпись Exchange				
При использовании данного шаблона в качестве б					

Руководство по внедрению



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

Свойства нового шаблона			
Требования выдачи Устаревшие шаблоны Расширения Безопасность Общие Обработка запроса Имя субъекта Сервер			
<u>О</u> тображаемое имя шаблона:			
Копия "Пользователь со смарт-картой"			
Минимально поддерживаемые ЦС: Windows Server 2003 Enterprise			
<u>И</u> мя шаблона:			
Копия "Пользователь со смарт-картой"			
Период действия: Период о <u>б</u> новления:			
<ul> <li>1 г. ▼</li> <li>6 нед. ▼</li> <li>Опубликовать сертификат в Active Directory</li> <li>Не использовать автоматическую перезаявку, если такой сертификат уже существует в Active Directory</li> <li>Если невозможно создать новый ключ, то для</li> <li>автоматического обновления сертификатов смарт-карт следует использовать существующий ключ</li> </ul>			
ОК Отмена Применить Справка			

- 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).

Свойства нового шаблона			
Требования выдачи Устаревшие ша Общие Обработка запроса	аблоны Расширения Безопасность Имя субъекта Сервер		
Цель: Подпись и шифрован	ие		
<ul> <li></li></ul>	ыбор CSP Выберите поставщики служб шифрования (CSP), которые могут быть использованы для запросов: О <u>П</u> юбые поставщики, имеющиеся на компьютере субъекта		
Минимальны <u>й</u> размер ключа: 2048 💌	Запросы должны использовать одного из следующих поставщиков:		
<ul> <li><u>Разрешить экспортировать зак</u></li> <li>При подаче заявки для субъекта и его сертификата следует:</li> <li><u>П</u>одавать заявку для субъекта</li> <li><u>З</u>апрашивать пользователя во</li> </ul>	Athena ASECard Crypto CSP Microsoft Base Smart Card Crypto Provider Microsoft DH SChannel Cryptographic Provider Microsoft Enhanced Cryptographic Provider v1.0 Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider Microsoft Enhanced RSA and AES Cryptographic Provider Microsoft RSA SChannel Cryptographic Provider Microsoft Strong Cryptographic Provider		
<ul> <li>Запрашивать пользователя и т использовании закрытого ключ</li> </ul>	ОК. Отмена		
Для выбора поставщиков служб шифрования (CSP) нажмите кнопку "Поставщики".			
ОК	Отмена Применить Справка		

### 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.

Стр. 20/121

Руководство по внедрению

- 14 В окне **Выбор СSP** 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.

Свойства нового шаблона	X		
Общие Обработка	а запроса Имя субъекта Сервер		
Требования выдачи Уста	ревшие шаблоны Расширения Безопасность		
<u>Г</u> руппы или пользователи:			
& Authenticated Users			
👗 a1			
Администраторы домен Администраторы домен	на (TEST\Администраторы домена)		
Администраторы предг	приятия (TEST Администраторы предприятия)		
Выбор	: "Пользователи", "Компьютеры", "Учетные запис	и служб" или " 🦹 🗙	
<u>В</u> ыбер	рите тип объекта:		
Пол	ьзователи", "Группы" или "Встроенные субъекты безопас	н Типы объектов	
, Bione	IVOULEM MECTE:		
Разрешения для гр test с	Разрешения для Гр. Трат сот		
Полный доступ Введи	Полный доступ Введите имена выбираемых объектов (примеры):		
Чтение Поль	Чтение Пользователи домена Проверить имена		
Запись	Запись		
Заявка			
Автоматическая		Отмена	
Чтобы задать особые разрешения или параметры, Дополнительно			
нажмите кнопку "Дополнительно".			
Подробнее об управлении доступом и разрешениях			
ОК	Отмена При <u>м</u> енить Справка		

- 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.

🚟 Консоль1 - [Корень консоли\Центр сертификации (srv1.test.com)\EntCA]			
<u>Файл Д</u> ействие <u>В</u> ид <u>И</u> збранное	<u>О</u> кно <u>С</u> правка	_8×	
🗢 🔿 🙋 🖬 🖬 🖬 🖉			
Корень консоли Корень консоли Бидантр сертификации (srv1.test.co Спозванные сертификаты Выданные сертификаты Запросы в ожидании Неудачные запросы Шаблоны сертификатов Спозванные сертификаты Спозванные сертификаты Спозвание сертификаты Спозвание сертификаты Спозвание серт	Имя Отозванные сертифика Выданные сертификать Запросы в ожидании Неудачные запросы Шаблоны сертификатов Иправление Создать Новое окно отсюда Обновить Справка	Действия EntCA        Дополнительные дей	
Запуск оснастки шаблонов сертификатов			

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

Руководство по внедрению

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 **OK**.

### 14 В окне Свойства нового шаблона откройте вкладку Требования выдачи.

войства нового шаблона
Общие Обработка запроса Имя субъекта Сервер Требования выдачи Устаревшие шаблоны Расширения Безопасность
Требовать для регистрации: □ Одобрения диспетчера сертификатов ЦС □ Указанного числа авторизованных подписей: 1 Автоматическая регистрация не разрешена (если требуется более одной подписи). В подписи требуется указать тип политики: Политика применения
Политика применения: IКЕ-посредник IP-безопасности Политики выдачи: Добавить Нладить
Требовать для повторной регистрации: <ul> <li> • Тех <u>ж</u>е условий, что и для регистрации </li> <li> ○ Подтвердить существующий сертификат </li> </ul>
ОК Отмена При <u>м</u> енить Справка

- 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).

🖪 Включение шаблонов сертификатов	×		
Выберите один шаблон сертификата для использования в этом центре сертификации (ЦС).			
Примечание. Если созданный шаблон сертификата не отображается в списке, подождите некоторое время, пока информация о шаблоне не будет реплицирована на все контроллеры домена.			
Не все шаблоны сертификатов в организации могут быть достуг для вашего ЦС.	тны		
Дополнительную информацию см. в разделе <u>Основные сведени</u> <u>шаблонах сертификатов.</u>	<u>я о</u>		
Имя Назн	•		
🖳 Подписывание списка доверия Подп			
🖳 Пользователь Exchange Защи			
💹 Пользователь JaCarta Вход			
💹 Пользователь JaCarta (централизованная процедура) Вход			
🖳 🖳 Пользователь со смарт-картой Защи			
🖳 Проверенный сеанс Пров	<b>_</b>		
ОК Отмена	a		

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.)

Руководство по внедрению

Настройка политики рег	истрации	
Регистрировать сертис автоматически	рикаты пользователей и компы	отеров
Модель <u>к</u> онфигурации:	Не настроено	<b>•</b>
Подробнее об <u>автомат</u>	ическом управлении сертифика	тами

1 В списке Модель конфигурации выберите Включено.

Окно примет следующий вид.

Свойства: Клиент служб сертификации: автоматическая ре 🏋 🗙			
Настройка политики регистрации			
Регистрировать сертификаты пользователей и компьютеров автоматически			
Модель конфигурации: Включено			
Обновлять сертификаты с истекшим сроком действия или в состоянии ожидания и удалять отозванные сертификаты			
Обновлять сертификаты, использующие шаблоны сертификатов			
Уведомлять об окончании срока действия			
Отобра <u>ж</u> ать уведомление об окончании срока действия, когда процент оставшейся продолжительности жизни сертификата составит:			
10 😴 %			
Подробнее об автоматическом управлении сертификатами			
ОК Отмена При <u>м</u> енить			

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.

Руководство по внедрению

3 При необходимости установите остальные настройки и нажмите OK.

### 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 *Areнm perucmpaцuu* 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).

настка диспетчера сертификатов		×
Эта оснастка всегда будет управлять сертифика	атами для:	
моей учетной записи пользователя		
О учетной записи службы		
О учетной записи компьютера		
	< Назад Готово Отмен	ia

- 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.

Запрос сертификатов		
Можно запросить следующие типы сер а затем нажмите кнопку "Заявка".	тификатов. Выберите сертификаты, кото	орые необходимо запросить,
Политика регистрации Activ	e Directory	
Aгент восстановления EFS	Остояние: Доступно	Подробности 🛞
Агент регистрации	Остояние: Доступно	Подробности 🛞
Администратор	Остояние: Доступно	Подробности 🛞 🔄
Базовое шифрование EFS	Остояние: Доступно	Подробности 🛞
Пользователь	Остояние: Доступно	Подробности 🛞 🗨
Показать все шаблоны		
Показать все шаблоны		

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

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

🟹 Регистрация сертификатов		
🔄 Регистрация сертификатов		
Результаты установки сертифи	катов	
Следующие сертификаты были пол	учены и установлены на данном компьютере.	
№ Агент регистрации	Состояние: Успешно	Подробности 🛞
		<u>Г</u> отово

# 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.

Руководство по внедрению



### 3 Нажмите **Далее**.

истрация сертификатов	
гистрация сертификатов	
Запрос сертификатов	
Доступны следующие сертификаты. регистрации.	. Нажмите кнопку "Заявка", чтобы начать процедуру
Политика регистрации Ас	tive Directory
₩Пользователь JaCarta	Осстояние: Требуется регистрация
ополнительные сведения о <u>сертиф</u>	икатах
	Заявка Отмена

- 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.

🔙 Pen	страция сертификатов		
📮 Per	истрация сертификатов		
	езультаты установки сертификато	8	
(	ледующие сертификаты были получены	и установлены на данном компьютере.	
	Политика регистрации Active	Directory	
	₩Пользователь JaCarta	✓ Состояние: Успешно	
			Готово

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 **BBOД** (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).

Оснастка диспетчера сертификатов	×
Эта оснастка всегда будет управлять сертификатами для:	
• моей учетной записи пользователя	
О учетной записи службы	
О учетной записи компьютера	
	-
< <u>Н</u> азад, <b>Готово Отмена</b>	

- 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).

🔚 certmgr - [Сертификаты - текущий пользователь\Личное]	×
<u>Ф</u> айл <u>Д</u> ействие <u>В</u> ид <u>С</u> правка	
🗢 🔿 🗾 📋 🙆 🗟 🗾 🖬	
🗊 Сертификаты - текущий пользоватє Тип объекта	
🕀 🧰 Личное	
Поиск сертификатов	
Вид     Вид     Запросить новый сертификат     Вид	
на н	
⊕ ☐ С Экспортировать список Дополнительные операции     ▶	
⊕ 4     ☐ 4     ☐ Справка     ☐ Справка     ☐	
Доверенные корневые сертифик	
Запросить новый сертификат от центра сертифика	

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

<mark>а</mark> Регистрация сертификатов				
🙀 Регистрация сертификатов				
Запрос сертификатов Можно запросить следующие типы серт а затем нажмите кнопку "Заявка".	гификатов. Выберите сертификаты, котор	рые необходимо запросить,		
Политика регистрации Active Directory				
Базовое шифрование EFS	(j) Состояние: Доступно	Подробности 🛞		
Пользователь	Остояние: Доступно	Подробности 🛞		
Пользователь JaCarta	Остояние: Доступно	Подробности 🛞		
Показать все шаблоны Дополнительные сведения о <u>сертифика</u>	Tax			
		<u>Заявка</u> Отмена		

- 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.

📑 Pen	истрация сертификатов истрация сертификатов		
F	Результаты установки сертифи	катов	
C	Следующие сертификаты были полу	учены и установлены на данном компьютере.	
	Политика регистрации Act	<b>Состояние:</b> Успешно	Подробности 🛞
			<u>Г</u> отово

### 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.

епистрация сертификатов	
🔄 Регистрация сертификатов	
Выберите сертификат агента регистрации	
Сертификат агента регистрации необходим для подписи запроса на сертификат от имени других пользователей. Нажмите кнопку "Обзор", чтобы найти сертификат подписи, а затем щелкните "Далее	e".
Сертификат подписи:	op
Подробные сведения о подаче заявки на сертификаты от имени других пользователей	
	Отмена

- 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.

V. 2.0

🟹 Регистрация сертификатов	
🔄 Регистрация сертификатов	
Выберите пользователя	
Для запроса на сертификат от имени другого пользователя введите формальное имя или доменн пользователя. Например, используйте формат "имя фамилия", "имя_пользователя" или "домен\имя_пользователя".	ое имя этого
Имя пользователя или псевдоним:	<u>О</u> бзор
Подробные сведения о <u>подаче заявки на сертификаты от имени других пользователей</u>	
	Отмена

- 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.

Вставы	ге смарт-карту	×
1	Вставьте смарт-карту в устройство чтения, чтобы сохранить новый сертификат.	
	Если смарт-карта уже вставлена в устройство чтения, извлеките ее и вставьте снова.	
	Примечание. Данный сертификат нельзя сохранить на смарт-карте, использованной для подписи запроса на сертификат.	
	Отмена	

28 Подсоедините электронный ключ JaCarta к компьютеру. Если он подсоединён, отсоедините его и подсоедините вновь.

Отобразится окно ввода пароля пользователя JaCarta.

V. 2.0

- 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).
- зо 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.)

Руководство по внедрению

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**.

Свойства: и1 ? 🔀			
Профиль служб удаленных рабочих столов Личный виртуальный рабочий стол СОМ+ Член групп Входящие звонки Среда Сеансы Удаленное управление Общие Адрес Учетная запись Профиль Телефоны Организация			
Имя входа пользователя:			
 Разблокировать учетную запись 			
<ul> <li>Отключить учетную запись</li> <li>Для интерактивного входа в сеть нужна смарт-карта</li> <li>Учетная запись важна и не может быть делегирована</li> <li>Использовать типы шифрования Kerberos DES для этой</li> </ul>			
Срок действия учетной записи • Никогда • Истекает: 30 июля 2011г.			
ОК Отмена При <u>м</u> енить Справка			

- 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.

Файл Лействие Вил Справка	
Tanu Wenerene Eud Cubana	
🗢 🔿 📶 💥 🖹 🛃 🚺	
Параметр Политика а Параметри Политика а Политика а Политика Клиент сети Містозоft: использовать инфровую подпись ( He опреде He	

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 смарткарты):
  - Нет действия;
  - Блокировка рабочей станции;
  - Принудительный выход из системы;
  - Отключение в случае удалённого сеанса служб удаленных рабочих столов.



#### Руководство по внедрению

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.

Безопасность Wi	indows	×
Запуск от имени другого пользователя Введите учетные данные, которые следует использовать для C:\Downloads\6.0.0.5 Russian - updated 09-06-2011\IDProtectClientx64.msi.		
	Другая учетная запись	
	a1 Учетные данные смарт-карты a1@test.com PIN-код	
	ОК Отмена	J

#### 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.

V. 2.0

## 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 раз	аличающегося имени	
Укажите данные, необходи быть указаны полные офиц	мые для сертификата. В полях "Область, край" и "Город" должны иальные названия без сокращений.	
Полное имя:		
Организация:		
Подразделение:		
Город		
О <u>б</u> ласть, край:		
Страна или регион:	RU	
	·	
	<u>Н</u> азад <u>Далее</u> <u>Г</u> отово <b>Отм</b>	ена

### 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.

н

Отобразится следующее окно.

Создать сертификат	<u>?</u> ×
Локальный центр сертификации	
Задайте в том же домене центр сертификации, который подпишет сертификат. Рекомендуется легко запоминающееся понятное имя.	
Докальный центр сертификации:	
Выбрать	
Пример: ИмяЦентраСертификации/ИмяСервера	
Пон <u>я</u> тное имя:	
Назад Лацее Готоро Отме	up [
<u>Н</u> азад Д <u>а</u> лее <u>Г</u> отово Отме	на

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.

Сертификаты сервера			
Эта функция предназначена для запроса и обработки сертификатов, используемых сервером для работы веб-сайтов по протоколу SSL.			
Имя 🔺	<ul> <li>Получатель сертификата Поставщик</li> </ul>		
	EntCA	EntCA	
VPN	test.com EntCA		

## 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**.

V. 2.0

3 В следующем окне отобразится информация об устанавливаемой роли. Нажмите **Далее**.

Отобразится следующее окно.

Мастер добавления ролей		
Выбор служб ро	лей	
Перед началом работы Роли сервера Службы политики сети и доступа Службы ролей	Выберите службы ролей, устанавливаемые для роли серве <u>С</u> лужбы роли: Сервер политики сети Службы маршрутизации и удаленного доступа	
Подтверждение Ход выполнения Результаты	<ul> <li>Служоа удаленного доступа</li> <li>Маршрутизация</li> <li>Центр регистрации работоспособности</li> <li>Протокол авторизации учетных данных узла</li> </ul>	

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.

Мастер настройки сервера маршрутизации и удаленного доступа			
Конфигурация Можно включить указанные службы в любом из этих сочетаний или выполнить настройку данного сервера.			
<ul> <li>Удаденный доступ (VPN или модем)</li> <li>Позволяет удаленным клиентам подключаться к этому серверу через удаленное подключение или безопасное подключение виртуальной частной сети (VPN)</li> <li>Преобразование сетевых адресов (NAT)</li> <li>Позволяет внутренним клиентам подключаться к Интернету, используя один общий IP-адрес.</li> <li>Доступ к виртуальной частной сети (VPN) и NAT</li> <li>Позволяет удаленным клиентам подключаться к данному серверу через Интернети внутренним клиентам подключаться к данному серверу через Интернети внутренним клиентам подключаться к данному серверу через Интернети внутренним клиентам подключаться к интернету, используя один общий IP-адрес.</li> <li>Безопасное соединение между двумя частными сетями</li> <li>Позволяет подключить данную сеть к удаленной сети, например, к сети филиала.</li> <li>Особая комбинация возможностей маршрутизации и удаленного доступа.</li> </ul>			
< <u>Н</u> азад Далее > Отмена			

3 Выберите Доступ к виртуальной частной сети (VPN) и NAT и нажмите Далее.

Отобразится окно выбора сетевого адаптера.

астерн Соеди Чт Ме	стер настройки сервера маршрутизации и удаленного доступа Соединение по VPN Чтобы разрешить VPN клиентам подключаться к данному серверу не менее одного интерфейса сети должно быть подключено к Интернету. Выберите интерфейс сети, который подключает данный сервер к Интернету.			
	Имя	Описание	IP-адрес 192 168 200 100	
	Подключение по локал	Сетевое подключение	192.168.153.170 (DHCP)	
<u>Допол</u> Допол	Дополнительные сведения о сетевых интерфейсах. Дополнительные сведения о фильтрации пакетов.			
		< <u>Н</u> азад	Далее > Отмена	

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

Отобразится следующее окно.

Мастер настройки сервера маршрутизации и удаленного доступа
Назначение IP-адресов Выберите способ назначения IP-адресов удаленным клиентам.
Выберите способ назначения IP-адресов удаленным клиентам: Фавтоматически При использовании DHCP-сервера для назначения IP-адресов, убедитесь, что он настроен правильно. Если DHCP-сервер не используется, то этот сервер будет сам создавать IP-адреса. Йз заданного диапазона адресов
<u>Подробнее</u>
< <u>Н</u> азад <u>Д</u> алее > Отмена

5 Выберите Из заданного диапазона адресов и нажмите Далее.

Отобразится следующее окно.

азначение диапа	зонов IP-адресов	_	
Можно указать ди использовать при	апазоны адресов, котор назначении адресов уда	ые этот сервер будет аленным клиентам.	
Введите диапазон использовать. Се он не будет исчер	ы адресов из статическо рвер будет назначать ад пан, и только затем пере	ого пула, которые вы хотите реса из очередного диапаз ейдет к следующему.	она, пока
Диапазоны адрес	0B:		
С	По	Число	
	<u>С</u> озда	ать	Ідалить

Руководство по внедрению

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

Отобразится следующее окно.

Мастер настройки сервера маршрутизации и удаленного доступа
Управление несколькими серверами удаленного доступа Запросы на подключения могут быть проверены локально или перезоверсявны на удаленный сервер постипа, совместичный с
протоколом RADIUS.
Хотя маршрутизация и удаленный доступ могут выполнять проверку подлинности запросов на подключение, большие сети с множеством серверов удаленного доступа часто используют RADIUS-сервер для централизованной проверки подлинности.
Можно переадресовать запросы проверки подлинности RADIUS-серверу при его использовании в данной сети.
Настроить данный сервер для работы с RADIUS-сервером?
Нет. использовать службу маршрутизации и удаленного доступа для проверки подлинности запросов на подключение
С Да, настроить данный сервер для работы с RADIUS-сервером
Подробнее
< <u>Н</u> азад <u>Д</u> алее > Отмена

- 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.

V. 2.0

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

Свойства: Марі	ирутизация и удаленны	ый доступ	? ×	1
IKEv2	PPP	Ведение	журнала	
Общие	Безопасность	IPv4	IPv6	
Поставщик сл клиентов удал требованию. Поставщик сл Windows - пр	тужбы проверки подлинно тенного доступа и маршру тужбы провер <u>к</u> и подлинно оверка подлинности	сти проверяет уч тизаторов вызов сти:	етные данные за по	
М <u>е</u> тоды про	оверки подлинности			
Поставщик с	Методы проверки под	линности		<u>? ×</u>
на подключен Поставщик (	Сервер производит пров выбранных методов в по	ерку удаленной рядке их указан	системы использ ия.	уя один из
Windows - y	Протокол ЕАР			
Особые IPse L2TP-подклк запустить сл	Если используется з Для настройки остал NPS.	ащита доступа к њных параметро	: сети (NAP), выбе юв NAP используй	рите EAP. те сервер
	Шифрованная провер	ока (Microsoft, ве	рсия 2, MS-CHAP	v2)
Предварите	Шифрованная провер	жа подлинности	(CHAP)	
	Незашифрованный п	ароль (РАР)		
, Привязка (	<u>Р</u> азрешить проверку компьютера для IKEv	подлинности с г /2	юмощью сертифи	ката
Исполь	– Доступ без проверки —			
Выберите SSTP для г	Разрешить подключ	чение удаленных	систем без пров	ерки
Сертифика	Подробнее	Г	ок	Отмена
Подробност				
		_		
	ОК	Отмена	При <u>м</u> енить	

- 12 Нажмите ОК, чтобы закрыть окно свойств маршрутизации и удалённого доступа.
- 13 В консоли диспетчера сервера выберите Роли > Службы 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 Службы и порты.

Окно примет следующий вид.

Свойства: Подключение по локальной сети 2	? ×
Преобразование сетевых адресов (NAT)	1
Пул адресов Службы и порты	
Выберите службы в частной сети, к которым нужно перенап пользователей Интернета. Будут созданы правила перенапр портов NAT. <u>С</u> лужбы:	равлять авления
FTP-сервер	
Протокол Internet Mail Access Protocol, версия 3 (IMAP3) Протокол Internet Mail Access Protocol, версия 4 (IMAP4) Почтовый сервер Интернета (SMTP) ИР-безопасность (IKE) ИР-безопасность (прослеживание IKE NAT) Протокол Post-Office Protocol, версия 3 (POP3) Удаленный рабочий стол Безопасный веб-сервер (HTTPS) Telnet-сервер ◀	 
Добавить <u>И</u> зменить <u>Ыдалить</u>	
Подробнее	
ОК Отмена Г	Три <u>м</u> енить

## 15 Установите флажок Веб-сервер (НТТР).

Отобразится следующее окно.

Изменить службу ? 🔀
Назначьте порт и адрес, на который будут посылаться пакеты, присланные на особый порт этого интерфейса или другого элемента пула адресов.
<u>О</u> писание службы:
Веб-сервер (НТТР)
Общий адрес
• на этом интерфейсе
О на этом <u>э</u> лементе пула адресов:
Протокол
© _олько ТСР С тол <u>ь</u> ко UDP
<u>В</u> ходящий порт: 80
Адрес в частной сети: 0.0.0.0
Исходящий порт: 80
ОК Отмена

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

## 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.

Свойства: и1	? ×
Профиль служб удаленных рабочих столов	1
Личный виртуальный рабочий стол СОМ-	+ İ
Общие Адрес Учетная запись Профиль Телефоны Орга	анизация
Член групп Входящие звонки Среда Сеансы Удаленное упр	равление
Права доступа к сети Разрешить доступ <u>З</u> апретить доступ <u>У</u> правление доступом на основе политики сети NPS	
Проверять код звонящего:     Ответный вызов сервера     Ответный вызов не выполняется     Устанавдивается вызывающим (только для RAS)     Всегда по этому номеру:	
<ul> <li>Назначить статические IP-адреса</li> <li>Определите IP-адреса, разрешенные для этого входящего подключения.</li> <li><u>И</u>спользовать статическую маршрутизацию</li> <li>Определите маршруты, работающие с входящим подключением.</li> </ul>	
ОК Отмена При <u>м</u> енить С	Справка

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.

Просмотр основных сведений о сети и настройка подключений Просмотр полной карты WKS1 Интернет (этот компьютер) Просмотр активных сетей Подключение или отключение Тип доступа: Без доступа к Интернету test.com Доменная сеть Подключения: Local Area Connection Изменение сетевых параметров Настройка нового подключения или сети Настройка беспроводного, широкополосного, модемного, прямого или VPN-подключения или же настройка маршрутизатора или точки доступа. Подключиться к сети Подключение или повторное подключение к беспроводному, проводному, модемному сетевому соединению или подключение к VPN. Выбор домашней группы и параметров общего доступа Доступ к файлам и принтерам, расположенным на других сетевых компьютерах, или изменение параметров общего доступа. Устранение неполадок Диагностика и исправление сетевых проблем или получение сведений об исправлении.

Отобразится следующее окно.

4 Щёлкните на ссылке Настройка нового подключения или сети.

Отобразится следующее окно.

🍚 🐏 Установка подключения или сети	
Выберите вариант подключения	
Подключение к Интернету Беспроводное, скоростное или телефонное подключение к Интернету.	
Создание и настройка новой сети Настройка нового маршрутизатора или точки доступа.	
Подключение к рабочему месту Настройка телефонного или VPN-подключения к рабочему месту.	
Кастройка телефонного подключения Подключение к Интернету через телефонную сеть.	
Janee	тмена

5 Выберите Подключение к рабочему месту и нажмите Далее.

Отобразится следующее окно.

🛃 Подключение к рабочему ме	сту	
🌀 🗽 Подключение к рабоч	ему месту	
Введите Интернета-адре	с для подключения	
Этот адрес можно получит	ъ у сетевого администратора.	
<u>И</u> нтернете-адрес:	Пример: Contoso.com либо 157.54.0.1 либо 3ffe:1234:	
Имя местоназна <u>ч</u> ения:	VPN-подключение	
Использовать <u>с</u> мар	эт-карту	
🛞 🔲 <u>Р</u> азрешить исполь:	зовать это подключение другим пользователям	
Этот параметр позв компьютеру, испол	оляет любому пользователю, имеющему доступ к этому ызовать это подключение.	
🔽 Н <u>е</u> подключаться с	ейчас, только выполнить установку для подключения в будущем	
	Далее	Отмена

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

V. 2.0

Руководство по внедрению

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

Отобразится окно следующего вида.

📴 Сетевые по	одключения	
<b>G</b> O- <b>!</b>	🖣 👻 Панель управления 👻 Сеть и Инте	рнет 👻 Сетевые подключения 👻
Упорядочить	•	
Loca Unid Inte	al Area Connection dentified network el(R) PRO/1000 MT Network Conn	VPN-подключение Отключено WAN Miniport (IKEv2)

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.

VPN - c	войства
Общие	Параметры Безопасность Сеть Доступ
<u>Т</u> ип VPI	N:
Автома	атически
	Лополнительные параметры
Шифрон	Свойства смарт-карты или другого сертификата
обязат	При подключении:
Пров	использовать мою <u>смарт карту</u>
• <u> </u>	С использовать сертификат на этом компьютере
Mi	Использовать выбор простого сертификата (рек.)
C Pa	Проверять сертификат сервера
	Подключение к серверам:
Д) EA	
лю	
	Доверенные корневые центры сертификации
	Class 3 Public Primary Certification Authority     EntCA
	Microsoft Root Authority
	Microsoft Root Certificate Authority
	Thawte Timestamping CA
	UTN-USERFIRST-Object
	Просмотреть сертификат
	Не запрашивать пользователя авторизовать новые серверы
	или доверенные Центры Сертификации.
	Использовать для подключения другое имя пользователя
	ОК Отмена

- 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.

Имя компьюте	epa	Оборудование
Дополнительно	Защита системы	Удаленный доступ
Удаленный помощни	κ	
Разрешить подкли компьютеру	очения удаленного по	мощника к этому
Об удаленном помощ	нике	
		Дополнительно
D. cf		
Выберите вариант и з	затем укажите, кому р	разрешено
Выберите вариант и с подключение, если ну	затем укажите, кому ; /жно.	разрешено
Выберите вариант и : подключение, если ну <u>Н</u> е разрешать под	затем укажите, кому ( /жно. цключения к этому ко	разрешено мпьютеру
Выберите вариант и с подключение, если ну © <u>Н</u> е разрешать под С Разрешать подкли удаленного рабоч	затем укажите, кому ( ужно. аключения к этому ко ючения от компьютер его стола (опаснее)	разрешено мпьютеру ов с любой версией
Выберите вариант и з подключение, если ну С <u>Н</u> е разрешать подкли удаленного рабоч С Разрешить подкли которых работает подлинности на ур	затем укажите, кому р ужно. аключения к этому кол очения от компьютер его стола (опаснее) очаться только с ком удаленный рабочий с ровне <u>с</u> ети	разрешено мпьютеру ов с любой версией пьютеров, на тол с проверкой
Выберите вариант и з подключение, если ну С <u>Н</u> е разрешать подкли удаленного рабоч Разрешить подкли которых работает подлинности на ур <u>Помочь выбрать</u>	затем укажите, кому ( ужно. аключения к этому кол ючения от компьютер его стола (опаснее) ючаться только с ком удаленный рабочий с ровне <u>с</u> ети	разрешено мпьютеру ов с любой версией пьютеров, на этол с проверкой обрать пользователей
Выберите вариант и з подключение, если ну Разрешать подкли удаленного рабоч Разрешить подкли которых работает подлинности на ур Помочь выбрать	затем укажите, кому ( /жно. цключения к этому ко ючения от компьютер его стола (опаснее) ючаться только с ком удаленный рабочий с ровне <u>с</u> ети	разрешено мпьютеру ов с любой версией пьютеров, на этол с проверкой юбрать пользователей

- 3 В секции Удалённый рабочий стол выберите один из двух пунктов
  - Разрешать 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

Руководство по внедрению

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.

Свойства систе	мы
Имя компьютер	ра Оборудование Дополнительно Удаленный доступ
-Удаленный	Пользователи удаленного рабочего стола
Разреші компью	Пользователи из списка ниже, а также члены группы "Администраторы", могут подключаться к этому компьютеру.
	TEST\a1 TEST\a2
	TEST/u2
Удаленный	
Выберите в подключени	TEST\a1 уже имеет доступ.
О <u>Н</u> е разр	Добавить Удалить
Разреша удаленн	Чтобы создать новую учетную запись или добавить пользователей в другие группы, откройте панель управления <u>Учетные записи</u> пользователей.
Разреши которых подлинн	ОК Отмена
<u>Помочь выб</u>	<u>Выбрать пользователей</u>
	ОК Отмена При <u>м</u> енить

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.

Руководство по внедрению

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

🖫 Подключение	к удаленному рабоч	ему столу	
Поди раб	олючение к удален очему столу	ному	
<u>К</u> омпьютер: srv1	test.com	•	
При подключении данные.	не задано необходимо будет указа	ать учетные	
💽 Пара <u>м</u> етры		Подкл <u>ю</u> чить	<u>С</u> правка

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

🕞 Подключение к удаленному рабочему столу
Подключение к удаленному рабочему столу
Общие Экран Локальные ресурсы Программы Дополнительн • • Удаленный звук Настроить параметры удаленного звука. Параметры
Клавиатура Использовать сочетания клави <u>ш</u> Windows: Только в полноэкранном режиме Пример: ALT+TAB
Локальные устройства и ресурсы Выберите устройства и ресурсы, которые следует использовать во время удаленного сеанса. ГПринтеры ГУ Буфер обмена Подробнее
Параметры Подключить Справка

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

🎩 Подключение к удаленному рабочему столу	×
Подключение к удаленному рабочему столу	
Покальные устройства и ресурсы	
Выберите устройства и ресурсы этого компьютера, которые следует использовать во время удаленного сеанса.	
🔽 Смарт-карты	
Порты	
<ul> <li>Эругие поддерживаемые самонастраивающиеся устройства</li> </ul>	
Какие самонастраивающиеся устройства можно использовать во время удаленного сеанса?	
ОК Отмена	

- 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.

Руководство по внедрению

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

Безопасность W	indows	×
Введите учет Эти учетные да srv1.test.com.	ные данные нные будут использоваться при подключении к	_
	TEST\a1	
	Другая учетная запись	
	a1 Учетные данные смарт-карты a1@test.com PIN-код	
🗌 Запомн	нить учетные данные	
	ОК Отмена	

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.

<b>i</b>	Сертификаты сервера					
Эта функц работы ве	ия предназначена д 6-сайтов по протоко	ля запрос лу SSL.	а и обработки сертиф	икатов, используемых сервером для		
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**.

Проверка подлинности					
Сгруппировать по: Без группировани	19 -				
Имя 🔺	Состояние	Тип ответа			
Анонимная проверка подлинности	Включен				
Дайджест-проверка подлинности	Отключен	Вызов НТТР 401			
Обычная проверка подлинности	Отключен	Вызов НТТР 401			
Олицетворение ASP.NET	Отключен				
Проверка подлинности Windows	Отключен	Вызов НТТР 401			
Проверка подлинности клиента Ас	Отключен	Вызов НТТР 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

- 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.

ривязки	і сайта				<u>? ×</u>
Тип http	Имя узла	Порт 80	IP-адреса *	Сведен	<u>До</u> бавить Изменить Удалить О <u>б</u> зор
•				Þ	<u>З</u> акрыть

## 3 Нажмите **Добавить**.

Отобразится следующее окно.

Добавление привя	зки сайта	<u>? ×</u>
<u>Т</u> ип: https	IP- <u>а</u> дрес: Все неназначенные	П <u>о</u> рт: <b>4</b> 43
Имя <u>уз</u> ла:		
, Сертификат <u>ы</u> SSL:		
Не выбрано	<u> </u>	Вид
	OK	Отмена

- 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).

Руководство по внедрению

В центральной части окна станут доступны настройки данного сайта.



7 Сделайте двойной щелчок на иконке Параметры SSL.

Страница примет следующий вид.

📄 Параметры SSL
Эта страница позволяет изменить параметры SSL для содержимого веб-сайта или приложения.
🗌 Требовать SSL
Сертификаты клиента:
О Игнорировать
С Принимать
Требовать

- 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 "Hacmpoйкa 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.

V. 2.0

Руководство по внедрению

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://test.com).
- 4 В окне Безопасность Windows выберите сертификат пользователя и нажмите ОК.

Безопасность V	Vindows	×		
Подтверждение сертификата Подтвердите этот сертификат, нажав кнопку "ОК". Если это неправильный сертификат, нажмите кнопку "Отмена".				
	a1 Издатель: EntCA Действителен с: 30.06.2011 по 29.0 Просмотреть свойства сертификата			
	ОК Отмена			

- 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 подставятся автоматически.

Изменение настройки безог	асности	×
Настройка безопасности		
<u>И</u> мя конфигурации:		
Установки S/MIME (a1@tes	st.com)	•
Формат криптографии:	S/MIME	7
Настройка безопасности	и по умолчанию для этого формата	
Настройка по умолчанию	о для всех сообщений	
Метки безопасности	<u>С</u> оздать Удалит <u>ь</u>	Пароль
Сертификаты и алгоритмы		
Сертификат подписи:	a1	<u>В</u> ыбрать
Алгоритм хеширования:	SHA1	
Сертификат шифрования:	al	В <u>ы</u> брать
Алгоритм шифрования:	3DES 💌	
Передавать сертификат	гы с сообщением	
	ОК	Отмена

- 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

Шифров	анная электронная почта
<b>?</b>	<ul> <li>Шифровать содержимое и вложения исходящих сообщений</li> <li>Добавлять цифровую подпись к исходящим сообщениям</li> <li>Отправлять подписанные сообщения открытым текстом</li> <li>Запрашивать уведомление S/MIME для всех подписанных сообщений S/MIME</li> <li>По умолчанию: Установки S/MIME (a1@test.com)</li> </ul>
Использование Microsoft Outlook 2010 для отправки подписанных и зашифрованных сообщений

- 1 Чтобы удостовериться в том, что исходящие 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)

👔 🛃 🕫 🔍 🔶 👻 🖃			Без имени
Файл Сообщение Встан	вка Параметры	Формат текста	Рецензир
Аа А Шрифты т Темы темы Ф Эффекты т страницы	СК От	Разрешения 🛃 Под	фровать писать г
Темы	Показать поля	Разрешение	
Ко <u>м</u> у Отправит <u>ь</u> <u>Т</u> ема:			

## 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).

Учетная запись Упорядочивание электронной почты	Гочта Правописание К
Группы	Подпись электронной поч
Параметры	Tahoma 💌 10 💌
Телефон	≇ ≢ <u>*</u> • <u>A</u> • ⊘ <b>≜</b> •
Блокировать или разрешить	



6 Щёлкните на иконке **S/MIME** 

Отобразится следующая страница.

X	ABC		000	9	R	
Почта	Правописание	Календарь	Общие	Региональные	Пароль	S/MIME
Безопасно Протокол электронн зашифрова подписи от На этом ко загрузить з "Выполнит Загрузи	ЭСТЬ ЭЛЕКТРОНІ S/MIME позволя ой почты шифр анное содержим тправителей. Эмпьютере не ус этот элемент, щ ъ" в диалоговой	ной почты ет использов ование и циф юе получаеми тановлен эле целкните ссыл и окне Interne	ать в отпр ровую под ых сообщен емент упра аку ниже, а et Explorer. ME	авляемых сообще пись, просматрие ний и проверять с вления S/MIME. Ч а затем нажмите к	ниях зать цифровые тобы кнопку	

7 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.



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

Руководство по внедрению

- 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).

🖃 Отправить	9	11 <b>S</b> /	9 I	<u>84</u>	à 😽 - 😽	🗈 Параметры	0
🕮 Кому							
🕮 Копия							
Тема:							
Tahoma	<b>~</b> 1	0 🕶 В ј	t <u>U</u>	i≡ i≡ i≡	🛊 👱 - 🛕	* *	

2

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.

Шифрующая файловая система (EFS)
 Шифрующая файловая система (EFS)
 Какой тип сертификата вы хотите создать?
 Выберите подходящий вариант для автоматического создания и хранения сертификата шифрования файлов.
 Самозаверяющий сертификат на этом компьютере Используйте этот вариант, если у вас нет смарт-карты или центра сертификации.
 Самозаверяющий сертификат на смарт-карте Вставьте смарт-карту в устройство чтения.
 Сертификат, выданный центром сертификации моего домена Убедитесь, что компьютер имеет доступ к домену. Если сертификат хранится на смарт-карте, вставьте ее в устройство чтения.

- 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.

Руководство по внедрению

Через некоторое время отобразится следующее окно.

📒 Шифрующая файлова	я система (EFS)	
💮 🔬 Шифрующая ф	айловая система (EFS)	
Обновить ранее за	шифрованные файлы	
Выберите папки, связать с новым позволяет избех утраты прежнего	, содержащие зашифрованные файлы, которые следует сертификатом и ключом. Немедленное обновление кать потери доступа к зашифрованным файлам в случае о сертификата или ключа.	
<u>П</u> апки:		
<ul> <li>Все логич</li> <li>Локаль</li> <li>Воот</li> <li>Воот<th>еские диски ный диск (C:) cycle.Bin uments and Settings nloads ypted angeSetupLogs ub iCache</th><th></th></li></ul>	еские диски ный диск (C:) cycle.Bin uments and Settings nloads ypted angeSetupLogs ub iCache	

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 Закрыть.

## Зашифрование данных на жёстком диске

1 Чтобы зашифровать данные, выполните следующую последовательность действий.

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

Убедитесь в том, что в окне свойств папки открытка вкладка Общие.

🐌 Свойства: Заш	ифрованная папка	×
Предыду. Общие	цие версии Настройка Доступ Безопасность	
]. 3	ашифрованная папка	
Тип:	Папка с файлами	
Расположение:	C:\	
Размер:	0 байт	
На диске:	0 байт	
Содержит:	Файлов: 0; папок: 0	
Создан:	17 июня 2011 г., 18:14:15	
Атрибуты:	<ul> <li>✓ Только для чтения (применимо только к файлам в папке)</li> <li>Г Скрытый Другие</li> </ul>	
	ОК Отмена Примени	ть

3 Нажмите **Другие**.

Отобразится следующее окно.

Дополн	ительные атрибуты	×
<b>1</b>	Установите подходящие параметры для этой папки. При изменении этих параметров будет задан вопрос, следует ли затрагивать вложенные папки и файлы.	
Атриб П Па В	буты индексирования и архивации апка готова для архивирования азрешить индексировать содержимое файлов в этой папке дополнение к свойствам файла	
Атриб С <u>С</u>	буты сжатия и шифрования кимать содержимое для экономии места на диске ифровать содержимое для защиты данных Подро <u>б</u> но	
	ОК Отмена	

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

Отобразится следующее окно.

ᆀ

- 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 OC Windows и позволяет защитить данные, хранящиеся на дисках компьютера. BitLocker противостоит атакам с выключением, которые проводятся путём отключения или обхода установленной OC либо путём физического удаления жёсткого диска с компьютера для автономного взлома данных.

Texнология 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. <u>http://technet.microsoft.com/ru-ru/library/ee424307)</u>.

## Системные требования

#### Требования к центру сертификации

Центр сертификации должен работать под управлением OC 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.

• → 2 📅 🗙 🗅 📄	General	Request Ha	inding	Subject Name	Issuance F	lequirements		
Console Root	Supersec	ied Template	6	Extensions	Security	Server	i Inter 🛃	Actions
Certificate Templates (D)	To modify Extension	an extension	, select i	t, and then click E	ide.			Certificate Te
स्य हम हम हम हम	Applic Basic Cetth Issuar Key U	ation Policie Constraints cate Templa noe Policies Isage	Edit Ke Spec exten Sig	ry Usage Extensi fy the required sig sion. nature Digital signature Signature is proof	on nature and se of origin (none	cutty options for	a key usage	ACarta Vore Act
the first first first first	Description of Key Us Signature requiremer Digital signature Allow key exchange	n of Key Usa requirement nature exchange c	Erx O	1				
		ОК	EM	ake this extension	ortical	ОК	Cancel	

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.

#### Руководство по внедрению

nap-in	Vendor	*		Console Root	Edit Extensions
ActiveX Control Authorization Manager	Microsoft Cor Microsoft Cor			Certificate Templates	Remove
Certificate Templates Certificates	Microsoft Cor Microsoft Cor	III			Move Up
Certification Authority Component Services	Microsoft Cor Microsoft Cor		Add >		Move <u>D</u> own
Computer Managem Device Manager	Microsoft Cor Microsoft Cor				
Disk Management	Microsoft and Microsoft Cor				
Event Viewer Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor	Ŧ			Ad <u>v</u> anced
cription:					

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.

e Acuon view Pavonies	window nep				
ertificate Templates (WIN-VO8D3	Template Display Name 🔺	Minimum Supported CAs	Version	Intended Purposes	Actions
	Administrator	Windows 2000	4.1		Certificate Templates (WIN
	Authenticated Session	Windows 2000	3.1		
	Basic EFS	Windows 2000	3.1		More Actions
	CA Exchange	Windows Server 2003 Ent	106.0	Private Key Archiva	liser JaCarta
	CEP Encryption	Windows 2000	4.1		User Jacarta
	🖳 Code Signing	Windows 2000	3.1		More Actions
	Computer	Windows 2000	5.1		
	Cross Certification Authority	Windows Server 2003 Ent	105.0		
	Directory Email Replication	Windows Server 2003 Ent	115.0	Directory Service E	
	Domain Controller	Windows 2000	4.1		
	Domain Controller Authentication	Windows Server 2003 Enterpr	rise 0.0	<b>Client Authenticatic</b>	
	EFS Recovery Agent	Windows 2000	6.1		
	Enrollment Agent	Windows 2000	4.1		
	Enrollment Agent (Computer)	Windows 2000	5.1		
	Rechange Enrollment Agent (Offline request)	Windows 2000	4.1		
	Exchange Signature Only	Windows 2000	6.1		
	🚇 Exchange User	Windows 2000	7.1		
	🖳 IPSec	Windows 2000	8.1		
	IPSec (Offine request)	Windows 2000	7.1		
	Kerberos Authentication	Windows Server 2003 Ent	110.0	Client Authenticatic	
	Key Recovery Agent	Windows Server 2003 Ent	105.0	Key Recovery Ager	
	OCSP Response Signing	Windows Server 2008 Ent	101.0	OCSP Signing	
	RAS and IAS Server	Windows Server 2003 Ent	101.0	Client Authenticatic	
	Root Certification Authority	Windows 2000	5.1		
	Router (Offline request)	Windows 2000	4.1		
	Smartcard Logon	Windows 2000	6.1		
	B Smartcard User	Windows 2000	11.1		
	Subordinate Certification Authority	Windows 2000	5.1		
	P Trust List Signing	Windows 2000	3.1		
	2 User	Windows 2000	3.1		
	🖉 User JaCarta	Windows Server 2003 Ent	100.4	BitLocker Drive Enc	
	User Signature Only	Windows 2000	4.1		
	Web Server	Windows 2000	4.1		
	Workstation Authentication	Windows Server 2003 Ent	101.0	Client Authenticatic	

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

ə 🖄 🛅 🔀 🗐 🗄	s 🛛 🖬			
onsole Root	Template Display Name 🔺	Minimum Supported CAs	Version 🔺	Actions
Certificate Templates (W	Recross Certification Authority	Windows Server 2003 Ent	105.0	Certificate Templates
	Replication	Windows Server 2003 Ent	115.0	
	🕮 Domain Controller	Windows 2000	4.1	More Actions
	Domain Controller Authentication	Windows Server 2003 Ent	110.0	User JaCarta
	💹 EFS Recovery Agent	Windows 2000	6.1	USET Jacarta
	🕮 Enrollment Agent	Windows 2000	4.1	More Actions
	Brollment Agent (Computer)	Windows 2000	5.1	
	Rechange Enrollment Agent (Offline request)	Windows 2000	4.1	
	Rechange Signature Only	Windows 2000	6.1	
	Rechange User	Windows 2000	7.1	
	IPSec	Windows 2000	8.1	
	IPSec (Offline request)	Windows 2000	7.1	
	Rerberos Authentication	Windows Server 2003 Ent	110.0	
	Rey Recovery Agent	Windows Server 2003 Ent	105.0	
	R OC Duplicate Template	Windows Server 2008 Ent	101.0	
	RA Reenroll All Certificate Holders	Windows Server 2003 Ent	101.0	
	Roy Change Names	Windows 2000	5.1	
	Ro	Windows 2000	4.1	
	Sm All Tasks	Windows 2000	6.1	
	🕮 Sm Delete	Windows 2000	11.1	
	🖳 Sut	Windows 2000	5.1	
	Tru Properties	Windows 2000	3.1	
	B Use Help	Windows 2000	3.1	
	🚇 User Jacarta	Windows Server 2003 Ent	100.4	
	B User Signature Only	Windows 2000	4.1	
	Reb Server	Windows 2000	4.1	
	B Workstation Authentication	Windows Server 2003 Ent	101.0 -	1

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

User JaCarta Properties
General         Request Handling         Subject Name         Issuance Requirements           Superseded Templates         Extensions         Security         Server           To modify an extension, select it, and then click Edit.         Security         Server
Extensions included in this template: Application Policies Basic Constraints Certificate Template Information Issuance Policies Key Usage
Edit  Description of Application Policies:  Smart Card Logon Client Authentication
OK Cancel Apply Help

- 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).

Edit Application Policies Extension
An application policy defines how a certificate can be used.
Application policies:
Any Purpose Client Authentication Secure Email Smart Card Logon
Add <u>E</u> dit <u>R</u> emove
Make this extension critical
OK Cancel

- 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 ОК 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.

Add Application Policy
An application policy (called enhanced key usage in Windows 2000) defines how a certificate can be used. Select the application policy required for valid signatures of certificates issued by this template.
Application policies:
Any Purpose Certificate Request Agent Code Signing CTL Usage Digital Rights Directory Service Email Replication Disallowed List Document Signing Domain Name System (DNS) Server Trust Embedded Windows System Component Verification Encrypting File System File Recovery IP security end system
<u>N</u> ew
OK Cancel

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.

New Application Policy
Type a name for the new application policy, and if necessary change the object identifier.
Name:
BitLocker
Object identifier:
1.3.6.1.4.1.311.67.1.1
OK Cancel

10 Нажмите кнопку ОК.

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

🖳 Certificate Templates Console					l×
File Action View Favorites Wind	ow Help			_12	×
🗇 🔿 📅 💥 🖬 🔒 🔽 🖬					
Rertificate Templates (WIN-VO8D3 Tem	plate Display Name 🔺	Minimum Supported CAs Version	Intended Purposes	Actions	
A 19	Administrator	Windows 2000 4.1		Certificate Templates (WIN	
A	Authenticated Session	Windows 2000 3.1		More Actions	
	Basic EFS	Windows 2000 3.1		More Actions	2003
	CR Exchange	Windows Server 2003 Ent 106.0	Private Key Archiva	User JaCarta	
	Ode Signing User JaCarta Propertie	25	? ×	More Actions	•
	Computer	Frank Frank			
	Cross Certification General Request Ha	andling   Subject Name   Issuance Re	quirements		
	Directory Email Re	es Excensions Security	Server   rvice E		
	omain Controller To modify an extension	, select it, and then click Edit.			
	Oomain Controller		Inticatic		
	FS Recovery Age Extensions included in	this template:			
E E	nrollment Agent Application Policies	3			
	nrollment Agent ( Basic Constraints	56 :			
	xchange Enrollme Certificate Templat	e Information			
	xchange Signatui				
	Exchange User				
	PSec DEac (Offling rag				
	erberos Authenti		Inticatio		
	er Beroverv Age		I I I Ager		
	CSP Response Si		Edit		
I F	AS and IAS Serve Down to the term		inticatic		
R F	Root Certification	on Policies:			
R P	Router (Offline rec Smart Lard Logon	otion	<u> </u>		
🖳 S	Ginart Card Logon Client Authentication				
🖳 S	Smartcard User				
🖳 s	Subordinate Certif				
	rust List Signing		<u> </u>		
। 	Jser				
	Jser JaCarta		ive Enc		
	Jser Signature On				
	Veb Server				
	Vorkstation Authe OK	Cancel Apply	Help Inticatic		
			4	1	_

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).

Руководство по внедрению

Local Group Policy Editor						
Eile Action View Help						
🗢 🄿 🙋 🗔 📄 👔 👘 🐬						
Windows Components ActiveX Installer Service	*	BitLocker Drive Encryption				
Application Compatibility		Validate smart card certificate		Setting	State	Comment
AutoPlay Policies		usage rule compliance		Fixed Data Drives		
Backup Biometrics		Edit policy setting	Â	Operating System Drives		
BitLocker Drive Encryption				Removable Data Drives		
Fixed Data Drives		Requirements:		Store BitLocker recovery information in Active Directory Do	Not configured	No
Operating System Drives		windows / ramity		Choose default folder for recovery password	Not configured	No
Removable Data Drives		Description:		E Choose how users can recover BitLocker-protected drives (	Not configured	No
🧮 Credential User Interface	al User Interface This policy setting allows you to	This policy setting allows you to		E Choose drive encryption method and cipher strength	Not configured	No
🚞 Desktop Gadgets		associate an object identifier from		E Provide the unique identifiers for your organization	Not configured	No
Desktop Window Manager		a smart card certificate to a		Prevent memory overwrite on restart	Not configured	No
Digital Locker	Ξ	policy setting is applied when you		Validate smart card certificate usage rule compliance		No
Event Forwarding		turn on BitLocker.				

Откроется одноимённое окно.

Validate smart card certificate usage rule compliance       Previous Setting       Next Setting         Not Configured       Comment:       Image: Comment:       Image: Comment:         Enabled       Disabled       Image: Comment:       Image: Comment:       Image: Comment:         Options:       Windows 7 family       Image: Comment:       Image: Comment:       Image: Comment:       Image: Comment:         Options:       Help:       Image: Comment:       Image: Comment:	Validate smart card certificate usag	e rule compliance	3
Not Configured       Comment:	Validate smart card certificate usa	ge rule compliance Previous Setting <u>N</u> ext Setting	
Disabled       Supported on:       Windows 7 family         Options:       Help:         Object identifier:       This policy setting allows you to associate an object identifier from a smart card certificate to a BitLocker-protected drive. This policy setting is applied when you turn on BitLocker.         13.6.1.4.1.311.67.1.1       The object identifier is specified in the enhanced key usage (EKU) of a certificate. BitLocker can identify which certificates may be used to authenticate a user certificate to a BitLocker-protected drive by matching the object identifier in the certificate with the object identifier that is defined by this policy setting.         Default object identifier is 1.3.6.1.4.1.311.67.1.1         Note: BitLocker does not require that a certificate have an EKU attribute, but if one is configured for the certificate it must be set	<ul> <li>Not <u>Configured</u> Comment:</li> <li><u>Enabled</u></li> </ul>		*
Options:       Help:         Object identifier:       This policy setting allows you to associate an object identifier from a smart card certificate to a BitLocker-protected drive. This policy setting is applied when you turn on BitLocker.         The object identifier is specified in the enhanced key usage (EKU) of a certificate. BitLocker can identify which certificates may be used to authenticate a user certificate to a BitLocker-protected drive by matching the object identifier in the certificate with the object identifier that is defined by this policy setting.         Default object identifier is 1.3.6.1.4.1.311.67.1.1         Note: BitLocker does not require that a certificate have an EKU attribute, but if one is configured for the certificate it must be set	Disabled Supported on:	Windows 7 family	*
Object identifier:         1.3.6.1.4.1.311.67.1.1         This policy setting allows you to associate an object identifier from a smart card certificate to a BitLocker-protected drive. This policy setting is applied when you turn on BitLocker.         The object identifier is specified in the enhanced key usage (EKU) of a certificate. BitLocker can identify which certificates may be used to authenticate a user certificate to a BitLocker-protected drive by matching the object identifier in the certificate with the object identifier that is defined by this policy setting.         Default object identifier is 1.3.6.1.4.1.311.67.1.1         Note: BitLocker does not require that a certificate have an EKU attribute, but if one is configured for the certificate it must be set	Options:	Help:	
to an object identifier (OID) that matches the OID configured for BitLocker. If you enable this policy setting, the object identifier specified in the "Object identifier" has must match the object identifier in the	Object identifier:	This policy setting allows you to associate an object identifier         from a smart card certificate to a BitLocker-protected drive. This         policy setting is applied when you turn on BitLocker.         The object identifier is specified in the enhanced key usage (EKU)         of a certificate. BitLocker can identify which certificates may be         used to authenticate a user certificate to a BitLocker-protected         drive by matching the object identifier in the certificate with the         object identifier is 1.3.6.1.4.1.311.67.1.1         Note: BitLocker does not require that a certificate have an EKU         attribute, but if one is configured for the certificate it must be set         to an object identifier (OID) that matches the OID configured for         BitLocker.         If you enable this policy setting, the object identifier specified in         the "Object identifier" how must match the object identifier in the	A III

- 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).

[] Local Group Policy Editor				
<u>File</u> <u>Action</u> <u>View</u> <u>H</u> elp				
🗢 🔿 🖄 📰 🗟 🖬 🛛 🍸				
Windows Components     ActiveX Installer Service	📋 Fixed Data Drives			
Application Compatibility	Configure use of smart cards on	Setting	State	Comment
AutoPlay Policies	fixed data drives	Configure use of smart cards on fixed data drives	Enabled	No
Biometrics	Edit policy setting	E Deny write access to fixed drives not protected by BitLocker	Not configured	No
Bitl ocker Drive Encountion	Can policy secting	Allow access to BitLocker-protected fixed data drives from e	Not configured	No
Fixed Data Drives	Requirements:	Configure use of passwords for fixed data drives	Not configured	No
Operating System Drives	Windows 7 family	E Choose how BitLocker-protected fixed drives can be recover	Not configured	No
Removable Data Drives	Description:			

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).

Local Group Policy Editor           Eile         Action         View         Help						
🗢 🤿 🗾 🖬 🔒 🛛 🖬 🍸						
Windows Components ActiveX Installer Service	^	Removable Data Drives				
Application Compatibility		Configure use of smart cards on		Setting	State	Comment
AutoPlay Policies		removable data drives		E Control use of BitLocker on removable drives	Not configured	No
Biometrics	_	Edit policy setting	1	Configure use of smart cards on removable data drives	Enabled	No
Bitl ocker Drive Encountion		Lan policy secting		Deny write access to removable drives not protected by BitL	Not configured	No
Fixed Data Drives		Requirements:		🖹 Allow access to BitLocker-protected removable data drives f	Not configured	No
Operating System Drives		Windows 7 family		🖹 Configure use of passwords for removable data drives	Not configured	No
📔 Removable Data Drives		Description:		E Choose how BitLocker-protected removable drives can be r	Not configured	No
Credential User Interface		This policy setting allows you to				

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



Руководство по внедрению

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



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).

Руководство по внедрению

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

📴 Все элементы панели управления			×
🚫 🌍 🗢 🛤 🔹 Панель управления 🔹 Все	элементы панели управления 👻	<ul> <li>Поиск в панели управления</li> </ul>	2
Настройка параметров компьютера		Просмотр: Мелкие значки 🔻	
📑 Windows CardSpace	📑 Автозапуск	😨 Администрирование	
🐌 Архивация и восстановление	🗬 Брандмауэр Windows	🜮 Восстановление	- 1
📑 Гаджеты рабочего стола	👚 Дата и время	ಶ Датчик расположения и другие датч	- 1
🚔 Диспетчер устройств	🧕 Диспетчер учетных данных	輚 Домашняя группа	- 1
🕍 Защитник Windows	🗸 Звук	📟 Значки области уведомлений	- 1
🕮 Клавиатура	🕜 Мышь	🛄 Панель задач и меню "Пуск"	- 1
🚨 Параметры индексирования	📔 Параметры папок	🖉 Персонализация	- 1
🐻 Подключения к удаленным рабочим с	📲 Приступая к работе	🕎 Программы и компоненты	- 1
🗑 Программы по умолчанию	🖶 Распознавание речи	🧓 Родительский контроль	- 1
🐑 Свойства обозревателя	🕎 Система	Счетчики и средства производитель	- 1
📰 Телефон и модем	💶 Управление цветом	📧 Устранение неполадок	- 1
📾 Устройства и принтеры	🎎 Учетные записи пользователей	🖑 Центр обновления Windows	- 1
陀 Центр поддержки	🔞 Центр синхронизации	🕲 Центр специальных возможностей	- 1
鞋 Центр управления сетями и общим д	🏘 Шифрование диска BitLocker	] Шрифты	- 1
💆 Экран	ЭлектропитШифрование диска BitLocker Защитите компьютер при по программы шифрования диск BitLocker.	Язык и региональные стандарты ка	

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:

#### JaCarta для Microsoft Windows Руководство по в недрению

• 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.

🕞 🎭 BitLocker Drive Encryption (E:)
Change how want to walk this drive
Choose now you want to unlock this drive
Use a <u>p</u> assword to unlock the drive
Passwords should contain upper and lowercase letters, numbers, spaces, and symbols.
Type your password:
Retype your password:
Use my smart card to unlock the drive
You will need to insert your smart card. The smart card PIN will be required when you unlock the drive.
How do I use these options?
Next Cancel

- 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.

Руководство по внедрению

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 OK.



- 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.

#### Руководство по внедрению

Выберите вариант сохранения ключа восстановления.

BitLocker Drive Encryption (E:)
How do you want to store your recovery key? If you forget your password or lose your smartcard, you can use your recovery key to access your drive. We recommended that you save your recovery key to a file and print it.
<ul> <li>Save the recovery key to a <u>file</u></li> <li><u>Print the recovery key</u></li> </ul>
Some settings are managed by your system administrator.
What is a recovery key?

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).



Руководство по внедрению

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

BitLocke	r Drive Encryption		
	Encrypting		
6-	Drive E: 2.8% Completed		
	-		
	Pause		
Pause encryption before removing the drive or files on the drive could be damaged.			

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

🎨 Шифрование диска BitLocker	×	×				
\Re Шифрование Е: завершено.						
DOCC FOR DODINCHING.	Закрыть	но использовать ключ				
Рекомендуется сохранить ключ восстановлени	ия в отдельный файл и распечатать	ero.				
Сохранить ключ восстановления в ф	райле					
Напечатать ключ восстановления	Напечатать ключ восстановления					
🕦 Ключ восстановления сохранен.						
Нто такое ключ восстановления?						
		Далее Отмена				

Руководство по внедрению

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

👫 Шифрование диска BitLocker						
О Каралария и безопасни	ость 🔻 Шифрование диска BitLocker	<ul> <li>Поиск в панели управления</li> </ul>				
Панель управления - домашняя страница	Защитите файлы и папки путем шифров Программа шифрования диска BitLocker помог указанных ниже дисках. Вы сиожете использ пользователи не сиотут открывать и исполы. Что необходимо знать перед включением пр	ения дисков ает предотвратить несанкционированный доступ к файлам на овать компьютер как обычно, однако неавторизованные юзвать ваши файлы. ограммы шифрования диска BitLocker?				
	Шифрование диска BitLocker - жесткие диски С: Откл.	🛞 Включить BitLocker				
	Новый том (Е:) Вкл.	😵 Выключить BitLocker 🎯 Управление BitLocker				
	Шифрование диска BitLocker - BitLocker To Go F: Откл.	Включить BitLocker				
См. также						
Администрирование доверенного платформенного модуля						
🌍 Управление дисками						
Ознакомътесъ с заявлением о конфиденциальности в Интернете						

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

Проверка предоставления доступа к зашифрованному диску

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

1 Выполните одно из действий:

V. 2.0

JaCarta для Microsoft Windows Руководство по в недрению

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

🔾 🖉 – 🌆 🕨 Computer	•	1 1	•	49	Search Con	puter			× P
Organize  Properties  Favorites  Desktop	System properties <ul> <li>Hard Disk Drives (2)</li> <li>Local Disk (C)</li> </ul>	Uninstall or change a program 2)		Map n	network drive	>>			0
<ul> <li>Downloads</li> <li>Recent Places</li> <li>Libraries</li> <li>Documents</li> <li>Music</li> <li>Pictures</li> <li>Videos</li> <li>Computer</li> </ul>	<ul> <li>2.51 GB free o</li> <li>Devices with Remo</li> <li>Floppy Disk D</li> </ul>	f 19.7 GB ovable Storage (2) rive (A:)	S	Unio Oper Share Resto Inclu Сино Form	ock Drive n n in new wind e with ore previous v ide in library хронизация о nat	ow ersions бщих п	апок	•	
📬 Network				Copy Crea Rena Prop	y te shortcut ame erties				
Local Disk (E:) B Local Disk	litLocker status: Locked								
📀 🙆 📋	0					- 😼	12 📢	9:4 3 9/28	6 PM 3/2012

 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).

This drive is p	protected by E	BitLocker Drive	e Encryption	
Use your smart can You will need to ins	d to unlock this drive sert your smart card a	and type your smart (	ard PIN.	
Automatically ur	nlock on this comput	er from now on		
I don't have my sm	art card			
Why do I have to u	inlock the drive?			

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



Откроется окно проводника с файлами, записанными на защищённый диск.

Руководство по внедрению

4 Откройте любой из файлов.

Organize 👻 AutoPlay	Properties System properties Uninstall or change a pro	ogram » 🚛 🔹 🚺 🔞
☆ Favorites ■ Desktop ↓ Downloads ★ Recent Places	A Hard Disk Drives (2) Local Disk (C:) Local Disk (C:)	Disk (E:)
Libraries	Goo 🖗 > Computer > Local Disk (E:) - 49	Search Local Disk (E:)
Pictures	Organize 👻 🦳 Open 👻 Print New folder	III • 🔲 🔞
H Videos	☆ Favorites	Date modified Type
🖳 Computer	Desktop	9/28/2012 8:27 PM Text Do
🗣 Network	Commission Comments	elp
	E Pictures Videos	* *

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.

Выберите спосо	бы снятия блокировки диска
Использовать	пароль для снятия блокировки диска
Пароли должны	і содержать прописные и строчные буквы, цифры, пробелы и символы.
Введите паро	ль:
Введите паро	ль еще раз:
Использовать	дчарт-карту для снятия блокировки диска
Необходимо вс	тавить смарт-карту. ПИН-код смарт-карты потребуется при снятии блокировки с диска
🐼 На смарт-карт	ге не удается найти сертификат, подходящий для BitLocker.

#### 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.

👯 Шı	ифрование диска BitLocker (E:)	X				
	🎭 Шифрование диска BitLocker (E:)					
	Как сохранить ключ восстановления?					
	В случае утраты пароля или смарт-карты для возобновления доступа к диску можно использовать ключ восстановления.					
	Рекомендуется сохранить ключ восстановления в отдельный файл и распечатать его.					
	Сохранить ключ восстановления на флэш-накопителе USB					
	Сохранить ключ восстановления в файле					
	Напечатать ключ восстановления					
	😢 Не удалось сохранить ключ восстановления в этом расположении. Сохраните ключ восстановления в					
	другом месте.					
	Что такое ключ восстановления?					
		1				
	Далее Отмена					

#### 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.

JaCarta для Microsoft Windows Руководство по внедрению

#### Проблема з

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

	×
💬 💱 Шифрование диска BitLocker (E:)	
Запуск BitLocker	
Подождите, пока BitLocker выполнит инициализацию диска.	
🔇 Отказано в доступе.	
<u>Какие требования к системе предъявляет программа BitLocker?</u>	
	Отмена

#### 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.

Мастер добавления ролей				
Выбор ролей сервера				
Перед началом работы Роли сервера Подтверждение Ход выполнения Результаты	Выберите одну или несколько ролей для установки на сервер. Роли:			

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

Отобразится следующее окно.

Мастер добавления ролей						
Выбор служб ро	лей					
Перед началом работы Роли сервера Службы сертификации AD Службы ролей Вариант установки Тип ЦС Закрытый ключ Шифрование Имя ЦС Срок действия База данных сертификатов Подтверждение Ход выполнения Результаты	Выберите службы ролей, устанавливаемые для роли сервера "Слу Directory": 					

#### 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.

Мастер д	обавления ролей	X					
	Добавить службы ролей и компоненты, необходимые для компонента "Служба регистрации в центре сертификации через Интернет"?						
	Нельзя установить Служба регистрации в центре сертификации через Интернет, пока не установлены требуемые службы ролей и компоненты.						
	<u>С</u> лужбы ролей:	Описание:					
	<ul> <li>Веб-сервер (IIS)</li> <li>Веб-сервер</li> <li>Средства управления</li> <li>Средства удаленного администрирования сервера</li> <li>€ Средства администрирования ролей</li> </ul>	Веб-сервер (IIS) предоставляет надежную, управляемую и масштабируемую инфраструктуру веб- приложения.					
	Добавить требуемые службы роли Отмена						
<u>і Поч</u>	ему требуются эти службы ролей и компоненты?	li					

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

Отобразится следующее окно.

Центры сертификации могут использовать данные в Active Directory для упрощения выдачи сертификатов и управления ими. Укажите, следует ли установить ЦС предприятия или изолированный ЦС.
Предприятие Выберите этот параметр, если данный ЦС является членом домена и может использовать службу каталогов для выдачи сертификатов и управления ими.
О <u>А</u> втономный ЦС Выберите этот параметр, если данный ЦС не использует для выдачи сертификатов или управления ими данные службы каталогов. Автономный ЦС может быть членом домена.

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

Отобразится следующее окно.

Комбинацию корневого и подчиненных ЦС можно настроить на создание иерархической инфраструктуры открытых ключей (РКІ). Корневым ЦС является ЦС, которые выдает и сам подписывает сертификат. Подчиненный ЦС получает свой сертификат из другого ЦС. Укажите, следует ли установить ЦС корневой или подчиненный ЦС.

Корневой ЦС

Выберите этот параметр, если выполняется установка первого или единственного центра сертификации в инфраструктуре открытых ключей.

О Подчиненный ЦС

Выберите этот параметр, если ваш ЦС будет получать свой сертификат ЦС от другого ЦС, занимающего более высокое положение в инфраструктуре открытых ключей.

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.

Чтобы создавать и выдавать клиентам сертификаты, ЦС должен иметь закрытый ключ. Укажите, следует ли создать новый закрытый ключ или использовать существующий.
Создать новый закрытый ключ Используйте этот параметр, если отсутствует закрытый ключ или следует создать новый закрытый ключ для повышения безопасности. Потребуется выбрать поставщика служб шифрования и указать длину закрытого ключа. Для выдачи новых сертификатов также необходимо выбрать хэш-алгоритм.
О Использовать существующий закрытый ключ Используйте этот параметр, чтобы при переустановке ЦС гарантировать непрерывность с ранее выданными сертификатами.
Выбрать сертификат и использовать связанный с ним закрытый ключ Выберите этот параметр, если на этом компьютере есть существующий сертификат или требуется импортировать сертификат и использовать связанный с ним закрытый ключ.
Выбрать существующий закрытый ключ на этом компьютере Выберите этот параметр, если сохранены закрытые ключи из предыдущей установки или следует использовать закрытый ключ из другого источника.

9 Выберите Создать новый закрытый ключ и нажмите **Далее**.
#### Руководство по внедрению

Отобразится следующее окно.

Для создания нового закрытого ключа необходимо выбрать <u>поставщика служб шифрования, хэш- алгоритм</u> 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): Длина ключа (знаков):			
Выберите алгоритм хеширования для подписывания сертификатов, выдаваемых этим ЦС:			
SHA256			
SHA384			
SHA512			
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 отличающегося имени генерируются автоматически, но не могут быть изменены.
<u>О</u> бщее 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.

### Руководство по внедрению

Отобразится следующее окно.

Данному ЦС будет выдан сертификат для защиты обмена данными с другими ЦС и клиентами, запрашивающими сертификаты. Срок действия сертификата ЦС будет основан на ряде факторов, включая назначение ЦС и меры, принятые для обеспечения его безопасности.
Выберите срок действия сертификата, созданного для данного ЦС: 5 лет
Срок действия ЦС: 27.06.2016 18:37
Учтите, что сертификаты, выдаваемые ЦС, действительны только до истечения его срока действия.

- 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.

#### Руководство по в недрению

По окончании установки отобразится следующее окно.



18 Нажмите Закрыть для завершения процедуры.

## Основные отличия между автономным ЦС и ЦС предприятия

При установке центра сертификации вы можете сделать его корневым или подчинённым, а также определить, будет ли он центром сертификации предприятия (интегрированным c 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. СА имеет единственную настройку, которая распространяется на все типы сертификатов.	Решение принимается автоматически или вручную. Вы можете настроить принятие решения на глобальном уровне (уровне СА), либо для каждого сертификата, используя шаблоны сертификатов.
Область применимости изданных	Extranet и Intarnet PKI.	Intranet PKI.
© ЗАО "Аладдин Р. Д.", 1995—2018	Шаблон_документов_с_180214	Стр. 111 /

JaCarta для Microsoft Windows Руководство по в недрению		V. 2.0
сертификатов		
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.	Может выпускать все сертификаты Windows 2008, шаблоны которых определены в соответствующей оснастке (Шаблоны сертификатов).
	Не поддерживает 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.	ЦС автоматически получает информацию о пользователе из AD.
	Используется для выделения перекрестных ссылок	Выпуск сертификатов пользователей осуществляется с помощью Web-интерфейса или оснастки Сертификаты. также можно
Управление пользователями		использовать возможность автоматической выдачи сертификатов или утилиту certreq.exe в режиме командной строки.

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. JaCarta для Microsoft Windows

Руководство по внедрению

- 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 ЕКU 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.

- Запустите Mozilla Firefox, щёлкните на значке и выберите Настройки > Настройки, как показано на изображении ниже.
- Новая вкладка ۲ Закладки 💷 Начать приватный просмотр Журнал Загрузки 🎾 🖻 🗖 ۲ Найти... Дополнения Настройки ٠ Настройки Сохранить как... Справка Отправить ссылку... Панель меню 👝 Печать... ۲ Панель навигации Панель закладок Þ Веб-разработка Панель дополнений Ctrl+\ Полный экран Вкладки сверху Настроить Sync... Панель инструментов.. 🗟 Выход
- 2 В отобразившемся окне щёлкните на значке <sup>2000</sup> (Дополнительные), выберите вкладку Шифрование, нажмите Просмотр сертификатов и выберите вкладку Центры сертификации.

JaCarta для Microsoft Windows

Руководство по внедрению

Окно настроек примет следующий вид.

Управление сертификатами				
Ваши сертификаты Люди Серверы Центры сертифика	ции Другие			
У вас хранятся сертификаты, служащие для идентификац	У вас хранятся сертификаты, служащие для идентификации следующих центров сертификации:			
Имя сертификата	Устройство защиты			
₄(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetle	2			
TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı	Builtin Object Token			
▲AC Camerfirma S.A.				
Chambers of Commerce Root - 2008	Builtin Object Token			
Global Chambersign Root - 2008	Builtin Object Token			
▲AC Camerfirma SA CIF A82743287				
Chambers of Commerce Root	Builtin Object Token			
Global Chambersign Root	Builtin Object Token			
⊿AddTrust AB				
AddTrust Class 1 CA Root	Builtin Object Token			
Просмотреть Изменить доверие Импортироват	ъ Экспортировать Удадити			

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

Отобразится следующее окно.

Загрузка сертификата	×		
Вам предлагают доверять новому центру сертификации (СА).			
Вы хотите доверять «EntCA» для следующих назначений?			
🔲 Доверять при идентификации веб-сайтов.			
🔲 Доверять при идентификации пользователей электронной почты.			
🔲 Доверять при идентификации производителей программного обеспечения.			
Перед тем, как определиться с доверием к этому центру, рекомендуется проверить его сертификат, политику и процедуры (если возможно).			
Просмотреть Проверить сертификат центра			
ОК Отмена			

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

## Hастройка 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.

Firefox **\*** 

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

Запустите Mozilla Firefox, щёлкните на значке 1 как показано на изображении ниже.

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

Отобразится следующее окно.

🕗 Управление устройствами			<u>_</u> _×
Модули и устройства защиты	Подробности	Значение	На <u>ч</u> ать сеанс
▷NSS Internal PKCS #11 Module	Модуль	Athena PKCS#11	Закончить сеанс
▷ Athena PKCS#11 Module	Путь	C:\Windows\syst	
Модуль встроенных корневых се			Сменить пароль
			Загрузить
			В <u>ы</u> грузить
			Использовать <u>F</u> IPS
	I		
ОК			

ивыберите Настройки > Настройки,

JaCarta для Microsoft Windows

Руководство по внедрению

3 Если путь к библиотеке PKCS11 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.

🍪 Загрузка устройства РКС5#11 📃 🗆 🗙				
Введите информацию о модуле, который вы хотите добавить.				
И <u>м</u> я модуля: New PKCS#11 Module				
Имя файла модуля: Обзор				
ОК Отмена				

4 В поле Имя модуля введите имя нового модуля (например, JaCarta), в поле Имя файла модуля укажите путь к библиотеке РКСS11 из состава JC-Client (при необходимости воспользуйтесь кнопкой Обзор).

Файл библиотеки РКСS11 из состава JC-Client находится по следующему пути:

C:\Windows\System32\asepkcs.dll

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

Управление устройствами			_ [] >
Модули и устройства защиты	Подробности	Значение	На <u>ч</u> ать сеанс
▷NSS Internal PKCS #11 Module	Модуль	JaCarta	Bakonutte caanc
• Модуль встроенных корневых се	Путь	c:\Windows\Syst	раколчить сеанс
⊿ JaCarta			Сменить пароль
JaCarta			Загрузить
			В <u>ы</u> грузить
			Использовать <u>F</u> IPS
			UK

### 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

Firefox 🔨				
about:config	+			
♦ → about:config				ŕ
Фидьтр:				
Имя настройки	A	Состояние	Тип	Значение
accelerometer.enabled		по умолчанию	логическ	true
accessibility.accesskeycausesactivation		по умолчанию	логическ	true
accessibility.blockautorefresh		по умолчанию	логическ	false
accessibility.browsewithcaret		по умолчанию	логическ	false
accessibility.browsewithcaret_shortcut.enabled		по умолчанию	логическ	true
accessibility.mouse_focuses_formcontrol		по умолчанию	логическ	false
accessibility.tabfocus		по умолчанию	целое	7
accessibility.tabfocus_applies_to_xul		по умолчанию	логическ	false

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 доступк 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 chttps://) и нажмите клавишу ВВОД.

Руководство по внедрению

Отобразится следующее окно.

Требуется пароль		×
?	Введите мастер-пароль для доступа в JaCarta	
	ОК Отмена	

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

Отобразится следующее окно.

апросидентификации пользователя	×		
Сайту необходимо определить, с каким сертификатом вас ассоциировать: test.com:443			
организация: «test» Выдано: «»			
Выберите сертификат для идентификации:			
JaCarta:le-!041f!043e!043b!044c!0437!043e-14475 [61:3C:D1:36:00:00:00:00:00:02]			
Информация о выбранном сертификате:			
Кому выдано: E=a1@test.com,CN=a1,CN=Users,DC=test,DC=com Серийный номер: 61:3C:D1:36:00:00:00:00:00:02 Действителен с 30.06.2011 16:13:33 по 29.06.2012 16:13:33 Назначения: Клиент,Подпись,Шифрование Использование сертификата ключа: Подпись,Шифрование ключа Электронная почта: a1@test.com Кем выдано: CN=EntCA,DC=test,DC=com Место хранения: JaCarta			
☑ Запомнить это решение			
ОК Отмена			

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

После этого вы попадете на защищённый сайт.

### JaCarta для Microsoft Windows Руководство по внедрению

### Регистрация изменений

Версия	Изменения
2.0	Документ свёрстан 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 CC).

#### 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.Ко0082 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