

JaCarta PKI и EFSшифрование в Microsoft Windows

Руководство по настройке

Листов: 22 Автор: Dmitry Shuralev

Аннотация

Настоящий документ содержит сведения о настройке **EFS-шифрования**дляфайлов и директорийна рабочих местах под управлением **OC Windows** и доступа к зашифрованным данным по электронному ключу JaCartaPKI.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.

Настоящий 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.

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 компанией "Аладдин Р.Д." без предварительного уведомления. 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 компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация AppleInc. Владельцем товарного знака IOS является компания Cisco (CiscoSystems, Inc). Владельцем товарного знака WindowsVista и др. — корпорация Microsoft (MicrosoftCorporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев. Сведения, приведённые в данном документе, актуальны на дату его публикации.

Оглавление

O6 EFS	4
O JaCarta	4
Ход настройки	5
Выпуск сертификата шифрования	5
Настройка директорий шифрования	14
Проверка работоспособности	17
Контакты, техническая поддержка	20
Регистрация изменений	21

06 EFS

Во всех операционных системах Microsoft семействаNT, начиная с Windows 2000и выше (кроме домашних (home)версий), существует встроенная технология шифрования данных EFS (Encrypting File System).EFS-шифрование основано на возможностях файловой системы NTFS и архитектуре CryptoAPI и предназначено для быстрого шифрования файлов на жёстком диске компьютера.

Система EFS использует шифрование с открытым и закрытым ключами. Для шифрования в EFS используется личный и публичный ключи пользователя, которые генерируются при первом использовании пользователем функции шифрования. Данные ключи остаются неизменными всё время, пока существует его учётная запись. При шифровании файла EFS случайным образом генерирует уникальный номер, так называемый File Encryption Key (FEK) длиной 128 бит, с помощью которого и шифруются файлы. Ключи FEK зашифрованы мастер-ключом, который зашифрован ключом пользователей системы, имеющего доступ к файлу. Закрытый ключ пользователя защищается хэшем пароля этого самого пользователя.

Данные, зашифрованные с помощью **EFS**, могут быть расшифрованы только с помощью той же самой учётной записи Windows с тем же паролем, из-под которой было выполнено шифрование. А если хранить сертификат шифрования и закрытый ключ на USB-токене или смарт-карте, то для доступа к зашифрованным файлам потребуется ещё и этот USB-токен или смарт-карта, что решает проблему компрометации пароля, так как будет необходимо наличие и дополнительного устройства в виде электронного ключа.

Одной из важных отличительных особенностей **EFS**от других средств шифрования в Windows является возможность локальной (standalone) работы. То есть пользователь создаёт новый самозаверенный сертификат, записывает его на **JaCartaPKI**, настраивает **EFS**и в дальнейшем получает доступ к необходимым каталогам или файлам только при наличии электронного ключа и знания его PIN-кода.

O JaCarta

Для хранения закрытого ключа и сертификата шифрования**EFS** подойдёт вся линейка электронных ключей **JaCartaPKI**, в любом форм-факторе, включая и биометрические токены, и смарт-карты, где вместо ввода PIN-кода пользователь прикладывает к специальному считывателю свой палец.



JaCarta PKI — это линейка PKI-токенов для строгой аутентификации пользователей в корпоративных системах, безопасного хранения ключевых контейнеров программных СКЗИ и цифровых сертификатов.

Ход настройки

Ход настройки делится на 3 этапа:

- выпуск сертификата шифрования;
- настройка директорий шифрования;
- проверка работоспособности.

Выпуск сертификата шифрования

В начале необходимовыпустить и записать сертификат и закрытый ключ в память **JaCartaPKI**, для этого выполните следующие действия.

Для OC Windows 8 и выше - щёлкните правой кнопкой меню Пуск.



Выберите Панель управления.







Далее настройка идентична для всех версий ОС Windows. В открывшемся окне выберите **Учётные записи пользователей**.

к в пане.	
	ρ
т <mark>ров компьютера</mark> Просмотр: Мелкиезначки ▼	

В открывшемся окне выберите Управление сертификатами шифрования файлов.

26	Учетные записи пользователей		-	Ц	x
÷	- 🔶 👻 🛧 🍇 > Панель упра	вления > Все элементы панели управления > Учетные записи пользователей 🗸 🗸	Поиски	в пане	Q
	Панель управления — домашняя страница	Внесение изменений в учетную запись пользователя			?
	Администрирование учетных записей	Изменение учетной записи в окне "Параметры компьютера"			
~	<u>Управление сертификатами</u> <u>шифрования файлов</u>	Изменить параметры контроля учетных записей Изменить параметры контроля учетных записей Дадрій само само само само само само само само			
V	Управление профилями пользователей	Управление учетными записями пользователей			
	Изменение переменных среды	Чтобы изменить пароль, нажмите клавиши CTRL+ALT+DELETE и выберите "Сменить пароль".			

		×
~	₇ Шифрующая файловая система (EFS)	
	Управление сертификатами шифрования файлов	
	Шифрованная файловая система (EFS) позволяет хранить информацию на жестком диске в зашифрованном формате и выбирать, какие пользователи смогут получать к ней доступ. Шифрование защищает файлы от несанкционированного доступа.	
	Чтобы получить доступ к зашифрованным файлам, требуется сертификат шифрования и ключ расшифровки на компьютере или смарт-карте. Этот инструмент можно использовать для обновления файлов, уже зашифрованных с помощью другого сертификата и ключа.	
	Далее Отмен	la

Перед продолжением убедитесь в том, что JaCartaPKIподсоединена к компьютеру, а на компьютере установлено ПО "Единый Клиент JaCarta".

		×
←	剜 Шифрующая файловая система (EFS)	
	Создать сертификат	
	О Создать новый самозаверяющий сертификат и сохранить его на моем <u>к</u> омпьютере	
	Создать сертификат, чтобы защитить файлы в случае потери компьютера	
	Создать новый самозаверяющий сертификат и сохранить его на моей смарт-карте	
	Создайте сертификат, чтобы защитить файлы в случае потери компьютера. При доступе к файлам, зашифрованным с помощью этого сертификата, необходимо использовать смарт-карту. Вставьте смарт-карту, если применяется этот вариант.	
	Получить сертификат, выданный центром сертификации моего домена Сертификат этого типа использует параметры шифрования, выбранные системным администратором. Подключитесь к домену и в случае использования смарт-карты вставьте ее.	
	Далее Отми	ена

Ввелите	PIN-кол	вставленной	карты
оведине	т ты код	BCTUB/ICTITION	карты

Корзина Сорзина		×
	😋 💀 Шифрующая файловая система (EFS)	
Google	Какой тип сертификата вы хотите создать?	pted
Chrome	Выберите подходящий вариант для автоматического (сертификата шифрования файлов.	создания и хранения
	 Самозаверяющий сертификат на этом компьютере Использу сертифик 	a
	Самозаве Вставьте: Подождите, пока будет созда самозаверяющий сертификат шифрования файдов.	ан новый т для
	О Сертифик Убедитеся хранится н	кат
	V	Введите пароль пользователя
	<u>какои тип сертификата следует использовать?</u>	
		Сменить после проверки
		Отмена Подтвердить
🙆 🧭 🔚 🕻		RU 🔺 隆 🛱 🌒 15:08 29.06.2017

На следующем шаге укажите директории, которые будут связаны с новым сертификатом, при необходимости можно указать все логические диски.

	x
🚽 📶 Шифрующая файловая система (EFS)	
Обновить ранее зашифрованные файлы	
Выберите папки, содержащие зашифрованные файлы, которые следует связать с новым сертификатом и ключом. Немедленное обновление позволяет избежать потери доступа к зашифрованным файлам в случае утраты прежнего сертификата или ключа.	
Папки:	
Все логические диски	
Отло <u>ж</u> ить перешифрование файлов	
Обновление файлов может занять значительное время, которое зависит от количества обновляемых файлов. Если выполнить выход или извлечь смарт-карту в процессе обновления, файлы не будут обновлены.	
Далее Отмен	Ia

Введите PIN-код ещё	раз.
---------------------	------



Сертификат выдан и записан на JaCartaPKI. Нажмите Закрыт	ь.
От технорующая фаиловая система (сго)	
Ваши зашифрованные файлы были обновлены	
Сведения о сертификате:	
<u>сосрении с сортнрикато.</u> Кому вылан: dshuraley	Просмотр сертификата
Конувыдан: dshuralev	
Действителен до: 05.06.2117	Пр <u>о</u> смотр журнала
	_
	Закрыть

Настройка директорий шифрования

Далее необходимо указать директорию, которая будет зашифрована со всем содержимым, можно зашифровать весь диск со всеми вложенными директориями. В настоящем примере используется директория **encrypted**, находящаяся на **диске С.**Щёлкните правой кнопкой по директории и выберите **Свойства**.



1		h
т	•	υ

	ypied	
Предыду	щие версии	Настройка
Общие	Доступ	Безопасность
) . e	encrypted	
Тип:	Папка с файлами	
расположение:	C:\	
Размер:	109 ME (115 269 351	байт)
На диске:	109 ME (115 281 920) байт)
Содержит:	Файлов: 7; папок: 0	
Создан:	29 июня 2017 г., 15:	06:51
Атрибуты:	Только для чтени (применимо толь)	1я ко к файлам в папке)
	Скр <u>ы</u> тый	Другие

(Отметьте	флаг	Шиф	ровать	соде	ржимое	для	защити	ы дан	ных.
r										

Дополнительные атрибуты					
Установите подходящие параметры для этой папки. При изменении этих параметров будет задан вопрос, следует ли затрагивать вложенные папки и файлы.					
Атрибуты индексирования и архивации					
Папка готова для архивирования					
Разрешить индексировать содержимое файлов в этой папке в дополнение к свойствам файла					
Атрибуты сжатия и шифрования					
🔲 Сжимать содержимое для экономии места на диске					
Шифровать содержимое для защиты данных Подробно					
ОК Отмена					

Нажмите ОК, нажмите Применить.

В отобразившемся окне выберите К данной папке и ко всем вложенным папкам и файлам.И нажмите ОК.

выбор пункта Применение только к этой папке не зашифрует все вложенные ниже директории и файлы в них.

Подтверждение изменения атрибутов					
Выбраны следующие изменения атрибутов:					
зашифровать					
Применить эти изменения только к данной папке или также ко всем вложенным папкам и файлам?					
Применение изменений только к этой папке					
К данной папке и ко всем вложенным папкам и файлам					
ОК Отмена					

Нажмите ОК.

По завершении процесса шифрования зашифрованная директория будет подсвечена другим цветом.



Проверка работоспособности

Сразу после завершения настройки **отключитеJaCartaPKI**, выполните выход из системы или перезагрузку ПК, далее снова войдите в систему**без JaCartaPKI**. Перейдите в папку encryptedu попробуйте открыть какой-либо файл из неё.Если все настройки сделаны верно, отобразится предложение вставить смарт-карту.





Вставьте смарт-карту, щёлкните по документу ещё раз и введите PIN-код.



На этом настройка EFS-шифрования закончена, доступ к файлам теперь возможен только при наличии JaCartaPKI и PIN-кода.

Контакты, техническая поддержка

Офис (общие вопросы)

Адрес:129226, Москва, ул. Докукина, д. 16, стр. 1, 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:www.aladdin-rd.ru

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

Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

www.aladdin-rd.ru/support/index.php

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

Регистрация изменений

Версия	Изменения			
1.0	Исходная версия документа			



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12 Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14 Лицензия Министерства обороны РФ № 1384 от 22.08.16 Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011 Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15 Аррle Developer

© ЗАО "АладдинР.Д.", 1995–2017. Все права защищены.

Тел. +7 (495) 223-00-01 Email: <u>aladdin@aladdin-rd.ru</u>Web: <u>www.aladdin-rd.ru</u>