

JaCarta PKI и Microsoft Outlook 2016

Шифрование и подпись электронных писем

Листов: 19 Автор: Dmitry Shuralev

Аннотация

Настоящий документ описывает настройку**MicrosoftOffice 2016** для реализации шифрования писем и добавления электронной подписи к письмам с использованием цифровых сертификатов, хранящихся на электронных ключах**JaCartaPKI.**

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.

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.

Оглавление

Введение	4
Требования к инфраструктуре	4
Принцип работы	5
Для чего нужно шифровать сообщения?	5
Что подтверждает цифровая подпись?	6
Поддерживаемые модели электронных ключей	6
Настройка и проверка шифрования и подписи	7
Настройка параметров безопасности	7
Отправка и получение подписанного сообщения	12
Отправка и получение зашифрованного сообщения	14
Контакты, техническая поддержка	17
Регистрация изменений	18

Введение

Программное обеспечение **Microsoft Outlook** на протяжении многих лет является наиболее популярным офисным и домашним инструментом в мире для работы с электронной почтой.По сути, ПО является полноценным органайзером, предоставляющим функции календаря, планировщика задач, записной книжки и менеджера контактов. Кроме того, **MS Outlook** позволяет отслеживать работу с документами пакета **Microsoft Office.**

ДВ настоящем документе показаны примеры на базе Outlook2016, но его можно использовать и для других более старых версий.

Используя цифровой сертификат, записанный на электронный ключ **JaCartaPKI**, пользователь может с лёгкостью подписать и зашифровать электронное сообщение, тем самым обеспечить защиту сообщения и вложения.

Требования к инфраструктуре

Серверная часть

WindowsServerсрольюконтроллера домена(ADDC)

WindowsServerсролью центра сертификации(ADCA)

WindowsServerсролью почтового сервераMicrosoftExchange

Д Указанные роли могут быть 4азвернуты в рамках одногофизического или виртуального сервера Windows. Настоящий документ не рассматривает настройку указанных серверных ролей.

Клиентская часть

Любая клиентская версия Windowsc установленным ПО MicrosoftOutlooku "Единый Клиент JaCarta".

Принцип работы

Шифрование электронных писем и выработка/проверкаэлектронной подписи играют важную роль при обеспечении информационной безопасности. У пользователей есть электронный ключ JaCartaPKI с цифровым сертификатом и ключевой парой (открытый и закрытый ключи). Третья сторона (Центр сертификации или Удостоверяющий центр) удостоверяет по цифровому сертификату его законного владельца.

Электронная подпись почтовых сообщений производится отправителем почтового сообщения с использованием своего закрытого ключа. При помощи открытого ключа можно проверить правильность цифровой подписи, а также посмотреть информацию об отправителе.

Для **шифрования почтовых сообщений** два пользователя сначала должны обменяться подписанными сообщениями. Почтовое сообщение шифруется отправителем при помощи открытого ключа получателя. Таким образом, любой может зашифровать сообщение для пользователя при помощи открытого ключа, но только владелец закрытого ключа может расшифровать сообщение.

Для надёжной сохранности сертификат и ключ необходимо хранить на **USB-токене**или **смарт**картеJaCartaPKI. При использовании JaCartaPKIтолько легальный пользователь сможет прочесть зашифрованное для него сообщение. Центр сертификации и почтовый сервер необходимы в инфраструктуре, но настройка электронной подписи и шифрования почтовых сообщений не зависит от них.Настройка ЭП и шифрования почтовых сообщений сводится к настройке программы почтового клиента.

Электронный ключ**JaCartaPKI**, в отличие от других известных способов хранения, обеспечивает неизвлекаемость ключевой информации на USB-токене или смарт-карте. Неизвлекаемое хранение подразумевает, что ключ из токена или карты не попадает никуда извне, например, на жёсткий диск компьютера или в оперативную память. А при обращении к информации на электронном ключе требуется знание PIN-кода, неправильный ввод которого приведёт к блокировке устройства. Это в свою очередь защищает от подбора комбинации PIN-кода, сводя количество попыток к определённому значению, например, 3.

Для чего нужно шифровать сообщения?

Если Вам нужно обеспечить конфиденциальность сообщения электронной почты, защитить сам текст письма и все вложения, то можно зашифровать это письмо. Шифрование сообщения в Outlook означает, что читаемый обычный текст преобразуется в зашифрованные данные. Расшифровать сообщение для прочтения может только получатель, у которого есть закрытый ключ, соответствующий открытому ключу, использованному для его шифрования. Для получателей, которые не имеют соответствующего закрытого ключа, будет отображаться искажённый текст.

Что подтверждает цифровая подпись?

• Подлинность.

Цифровая подпись подтверждает личность подписавшего.

• Целостность.

Цифровая подпись подтверждает, что содержимое документа не было изменено или подделано после заверения.

• Неотказуемость.

Цифровая подпись подтверждает происхождение заверенного содержимого. Подписавший не может отрицать свою связь с подписанным содержимым.

А Независимо от времени получения сертификата подписи и состояния его отзыва считается, что подписанные документы с действующей отметкой времени содержат действительные подписи.

Поддерживаемые модели электронных ключей



USB-токены:

- JaCarta PKI;
- JaCarta PKI/Flash;
- JaCarta PKI/FOCT;
- JaCarta PKI/FOCT/Flash.

Смарт-карты:

- JaCarta PKI;
- JaCarta PKI/FOCT.

Для смарт-карт требуется считыватель ASEDriveIIIUSB.

Настройка и проверка шифрования и подписи

Настройка параметровбезопасности



В главном окне Outlook 2016 выберите Файл -> Параметры.

В отобразившемся окне в левом меню выберите **Центр управления безопасностью** и справа нажмите **Параметры центра управления безопасностью.**

Параметры Outlook		?	×
Общие Почта	Обеспечение безопасности документов, а также защиты и работоспособности компьютера.		
Календарь	Безопасность и другие сведения		
Люди	Дополнительные сведения о защите конфиденциальности и безопасности приведены на сайте Office.com.		
Задачи	<u>Создание защищенных информационных систем</u>		
Поиск	Центр управления безопасностью Microsoft Outlook		
Язык	Центр управления безопасностью содержит параметры		-1
Дополнительно	безопасности и конфиденциальности. Эти параметры помогают обеспечить безопасность компьютера. Изменать их не	ностью.	
Настроить ленту	рекомендуется.		_
Панель быстрого доступа			
Надстройки			
Центр управления безопасностью			
	ОК	Отме	на

В окне **Центр управления безопасностью** выберите **Защита электронных писем**, отметьте пункт **Добавлять цифровую подпись к исходящим сообщениям.**

Центр управления безопасностью		?	×
Надежные издатели Шиф	рованная электронная почта		
Параметры конфиденциальности	П Шифповать содержиное и вложения исхоляции сообщений		
Защита электронных писем 🏹	 Шифровать содержимое и вложения исходящих сообщения Добавлять цифровую подпись к исходящим сообщениям 		
Обработка вложений	Отправлять подписанные сообщения открытым текстом		
Автоматическое скачивание	☐ <u>З</u> апрашивать уведомление S/MIME для всех подписанных сообщений S/MIME		
Параметры макросов	По у <u>м</u> олчанию: Установки S/MIME (D.Shuralev@aladdin-rd.ru) V Параметр <u>ы</u>		
Программный доступ Циф	ровые удостоверения (сертификаты)		
	Цифровые удостоверения или сертификаты являются документами, которые обеспечивают безопась ваших электронных транзакций.	ность	
	Опуб <u>л</u> иковать в глобальном списке адресов Импорт/ <u>э</u> кспорт <u>П</u> олучить удостоверение	è	
Чита	ть как обычный текст		
	Цитать обычные письма как обычный текст		
	Цитат <u>ь</u> письма с цифровой подписью как обычный текст		
Сцен	арии в папках		
	2азрешить сценарии в общих папках		
	Разрешить сценарии в общедоступных папках		
,	ОК	Отм	ена

Нажмите Параметры.

Центр управления безопасностью		? >	K
Надежные издатели	Шифрованная электронная почта		
Параметры конфиденциальности Защита электронных писем Обработка вложений Автоматическое скачивание Параметры макросов	 ☐ Щифровать содержимое и вложения исходящих сообщений ☐ Добавлять цифровую подпись к исходящим сообщениям ☐ Отправлять подписанные сообщения открытым текстом ☐ Запрашивать уведомление S/MIME для всех подписанных сообщений S/MIME По умолчанию: 		
Программный доступ	Цифровые удостоверения (сертификаты)		
	Щифровые удостоверения или сертификаты являются документами, которые обеспечивают безопасноващих электронных транзакций. Опубдиковать в глобальном списке адресов Импорт/ <u>э</u> кспорт Получить удостоверение Читать как обычный текст		
L L	ОК	Отмена	

В отобразившемся окне выберите **сертификат подписии алгоритм хэширования.** В случае если необходимо выполнить ещё и шифрование, то укажите **сертификат шифрования** и **алгоритм шифрования.**В настоящем примере для подписи и шифрования используется один сертификат пользователя, находящийся на **USB-токенеJaCartaPKI.**

Изменение настройки безопа	сности		×
Настройка безопасности —— <u>И</u> мя конфигурации:			
Установки S/MIME (D.Shura	lev@aladdin-rd.ru)		~
Ф <u>о</u> рмат криптографии:	S/MIME		\sim
✓ <u>Н</u> астройка безопасности	по умолчанию для	этого формат	a
✓ Настро <u>й</u> ка по умолчанию	о для всех сообщен	ий	
<u>М</u> етки безопасности	<u>С</u> оздать	Удалит <u>ь</u>	
Сертификаты и алгоритмы			
Сертификат подписи:	Dmitry Shuralev		<u>В</u> ыбрать
<u>А</u> лгоритм хеширования:	SHA1	~	
Сертификат шифрования:	Dmitry Shuralev		В <u>ы</u> брать
А <u>л</u> горитм шифрования:	AES (256-bit)	~	
Передавать сертификать	с сообщением		
		ОК	Отмена

В открывшемся окне можно выбрать нужный сертификат и посмотреть его свойства. Нажмите ОК.



Отправка и получение подписанного сообщения

Перейдите в главное меню Outlook 2016 и создайте новое письмо для произвольного получателя.

Заполните необходимые поля для отправки, выберите Параметры -> Подпись.

Нажмите Подпись.

И Кнопки Подписать и Шифровать доступны только после настроек параметров электронной подписи и шифрования почтовых сообщений. При нажатии кнопки Подписать или Шифровать не происходит подписи или шифрования сообщения, подпись и шифрование происходят непосредственно перед отправкой сообщения, после ввода PIN-кода.

🗄 🕏 🖉 🛧 🤚 =пример подписи - Сообщение (НТМL)	5	-	×
Файл Сообщение Вставка Параметры Форматтекста Рецензирование 🖗 Что вы хотите сделать?			
В цвета * С Отраницато * С Отраницато * Отраниц			~
Кому Dmity Стправить Гена пример подписи			
Пример подписи			
С уважением, 3АО "Аладдин Р.Д." <u>www.aladdin-rof.ru</u>			

В предыдущем окне нажмите **Отправить**, отобразится окно ввода PIN-кода.

Введите PIN-код и нажмите **ОК.**



Полученное письмо с подписью будет иметь специальную пометку в виде печати и дополнительное поле Подписано.

🗄 S	J 🗘	÷	🗧 пример подписанного сообщения Сообщение (HTML) 🛛 🗖 🗕	□ ×
Файл С	ообщение 🛛 🖓	Что вы хоті	те сделать?	
Г Т Удалить Удалить	Ответить Ответить все Ответить все Переслать Ответить		Переместить в: ? Э Руководителю Сообщение гр Т Быстрые действия Б Переместить	~
	Dmitry	писанно	о сообщения.	
Кому @aladd	in-rd.ru			
Копия @aladd	in-rd.ru			_
Подписано	@aladdin-	rd.ru		8
Пример по С уважении	дписанного соо(ем,	бщения.		
			ЗАО "Аладдин Р.Д." <u>www.aladdin-rd.ru</u>	
Для просмо	тра свойств п	одписи і	цёлкните значок 🕄.	
Цифровая	подпись: пра	вильная	×	
Тема:	c			

От:	1
Подписано:	D.Shuralev@aladdin.ru
8	Цифровая подпись сообщения является действительной и доверенной.
	Для просмотра сведений о сертификате, применяемом в цифровой подписи сообщения, нажмите кнопку "Сведения".
	Сведения
<u>Предупре</u>	ждать об ошибках в подписанных сообщениях до открытия.
	<u>З</u> акрыть

Перейдите в главное меню Outlook 2016 и создайте новое письмо для произвольного получателя.

Заполните необходимые поля для отправки, выберите Параметры -> Подпись.

Нажмите Подпись, нажмите Шифрование.

В письмо вложите произвольный документ, например, .txt файл.

⊟ 5 0 ↑ ↓ =	•	0	пример подписанного и зашифр	ованного письма - Сообщен
Сообщение вставка параметры Щвета * А Щрифты * Темы Эффекты * страницы * Темы Темы Темы Ворона СК От Показать поля	Форматтекста Рецензирование Шифровать Разрешение Разрешение	учно выхоните сделать: Уведомить о доставке Уведомить о прочтении Отслеживание	ранить отправленный Задержка Н элемент ч доставки Дополнительные параметры	4аправлять ответы в
тема пример подписанного и заи Вложение 111.btt	ифрованного письма			
Это пример подписанного и зашифрованного пис С вложением. С уважением,	ома.	- T X		
Файл Правка Формат Вид Справка это простой текст		^		
<				

Кнопки Подписать и Шифровать доступны только после настроек параметров электронной подписи и шифрования почтовых сообщений. При нажатии кнопки Подписатьили Шифровать не происходит подписи или шифрования сообщения, подпись и шифрование происходят непосредственно перед отправкой сообщения, после ввода PIN-кода.

🚍 🐬 🤫 Работа с вложениями	пример п	одписанного и зашифрованного письма - Сообщение (HTML)	∞ – □ ×	
Файл Сообщение Вложения	9 Что вы хотите сделать?			[
	🗙 🖻 🚱			
Открыть Быстрая Отправить Сохранить Сохранит	ть Удалить Копировать Показать			
Действия	Выделение Сообщение			~
Cp 05.07.2017 16:04				
Dmitry Shuralev				
пример подписанного и зац	шифрованного письма			
Подписано D.Shuralev			🗎 R .	~
1111.txt 0 5				
Это пример подлисанного и зашифрованноп С вложением. С уважением, Длитрий Шуралев d.shuralev@aladdin.nd.ru 3A0 *	то письма.	2		

Полученное зашифрованное письмо будет иметь специальную пометку в виде замка который можно посмотреть свойства безопасности сообщения, в том числе алгоритм шифрования.

Свойства безопасности сообщения	×
К Тема: пример подписанного и зашифрованного письма	
Сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой допускает наличие нескольких подписей.	
Слои безопасности	
<u>В</u> ыберите слой для просмотра его описания.	
Уровень шифрования Уровень цифровых подписей Подписано: D.Shuralev	
Описани <u>е</u> :	
ОК: защищено 168-разрядным шифрованием 3DES.	
Следующие кнопки позволяют просмотреть дополнительные сведения или внест изменения в выбранный слой:	и
Из <u>м</u> енить доверие Подро <u>б</u> ности Доверие к центру сертификации	
Предупреждать об ошибках в подписанных сообщениях <u>З</u> акрыть	,

Если это письмо будет перехвачено злоумышленником или даже сам легитимный пользователь откроет его из стороннего места, без сертификата, то ничего, кроме темы, ему доступно не будет, так как письмо надёжно зашифровано алгоритмом 3DES.



smime.p7m

На этом настройка и проверка шифрования и подписи электронных писем в **MicrosoftOutlook 2016**завершена.

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>