

# ЭЦП и шифрование в Windows

Ha примере программ: MS Office 2007 Adobe Acrobat 9 MS Outlook 2007 Mozilla Thunderbird 16 Mozilla Firefox 16



## Содержание

1.	Общая информация	3
2.	Офисные редакторы (на примере Microsoft Office Word 2007)	4
2.1	Настройки параметров ЭЦП и выбор сертификата	4
2.2	Добавление поля для подписи	6
3.	PDF (на примере Adobe Acrobat 9)	9
3.1	Установка модуля защиты ESMART Token в Adobe Acrobat	9
3.2	Цифровая подпись PDF	
3.3	Шифрование документа PDF	
4.	Почтовый клиент Microsoft OUTLOOK 2007	
4.1	Настройка сертификатов	
4.2	Электронная подпись сообщения	
4.3	Шифрование	
4.4	Составление сообщения	
4.5	Получение зашифрованного электронного сообщения	
5.	Почтовый клиент Mozilla Thunderbird	
5.1	Настройка почтового клиента	
5.2	Настройка параметров учетной записи	
5.3	Электронное письмо с ЭЦП	
5.4	Шифрование электронной почты	
6.	Браузер Mozilla Firefox	
6.1	Авторизация по сертификату	



## 1. Общая информация

Электронно-цифровая подпись (ЭЦП) позволяет защитить документы от изменения, сделав документ недоступным для редактирования. Также ЭЦП позволяет установить подлинность авторства документа, т.е. владелец подписи не может отказаться от факта, что он на момент подписания имел доступ к данному документу или файлу.

В данном руководстве описана процедура использования ЭЦП и шифрования с использованием сертификата формата X.509 с ключевой парой, записанной на смарт-карту или USB-ключ ESMART Token. На ПК должен быть установлен ESMART PKI Client для соответствующей операционной системы. Для использования ESMART Token с пользовательскими программами:

- Adobe Acrobat
- Mozilla Firefox
- Mozilla Thunderbird

**требуется дополнительная настройка**. Поэтапно настройка указанных приложений приведена в руководстве для администраторов ESMART Token – Настройка пользовательских приложений.

Как правило, настройка приложений выполняется администратором. Опытные пользователи могут выполнить настройку программ самостоятельно, ознакомившись с руководством.

Дополнительная настройка для программ MS Windows из пакета Microsoft Office и браузера Internet Explorer не требуется.



## 2. Офисные редакторы (на примере Microsoft Office Word 2007)

Откройте текстовый документ, или создайте новый:

<b>[</b> ]	🥑 👻 Документ3 - Microsoft Word	
Главная	Вставка Разметка страницы Ссылки Рассылки Рецензирование Вид Разработчик	0
Вставить У Буфер обмена	Саlibri (Основной те • 11 • ) Ж К Ц • авь х, х • Э •	
на стример	рдокумента Microsoft Office Word с ЭЦП	
- - < Страница: 1 из 1	и Число слов: 7   🚿 Русский (Россия)   🔚   👘 💭 😌 😌	* 0 *

## 2.1 Настройки параметров ЭЦП и выбор сертификата

Нажмите на кнопку **Office** (в левом верхнем углу), выберите **Подготовить - Добавить цифровую подпись**:

- (U ~ (U) =	Документ3 - Microsoft Word
Создать	Подготовить документ к рассылке
<u>О</u> ткрыть	Сво <u>и</u> ства Просмотр и изменение свойств документа, таких как название, автор и ключевые слова.
Сохранить	Инспектор документов Поиск скрытых метаданных и личных сведений в документе.
Сохранить как •	Зашифровать документ Усиление защиты документа путем добавления шифрования.
Пе <u>ч</u> ать •	О <u>г</u> раничить разрешения Предоставление пользователям доступа с ограничением возможности изменения, копирования и печати.
Подготовить 🔸	До <u>б</u> авить цифровую подпись
	невидимой цифровой подписи.
	Пометить как окончательный
Опубликовать 🕨	нередактируемого.
Закрыть	Проверка совместимости Проверка документа на наличие возможностей, не поддерживаемых более ранними версиями Word.
	🗈 Параметры Word 🗙 В <u>ы</u> ход из Word

Во всплывающих окнах появится справочная информация об ЭЦП.

Появится окно:

	Тодписание						
	Дополнительные сведения о том, что подписывается						
į	В документ будет добавлена цифровая подпись. Эта подпись не будет видна при просмотре содержимого документа.						
l	Цель подписания доку	мента:				_	
	Проверка работы ЭЦГ	1				-1	
	Тема сертификата: Testus Кем выдан: isbc						
			0	Подписать	Отмена		

Если сертификат не отображается, или чтобы выбрать другой сертификат, нажмите Изменить:

Безопасность Wi	ndows		×
Выбор серт	гификата		
	Testus Издатель: isbc Действителен с: 04.06.2012 Просмотреть свойства сер	по 04.0 тифик	
		ОК	Отмена

Выбрав сертификат, по желанию заполните поле **Цель подписания** и нажмите **Подписать** (см. выше). Введите в появившееся окно ПИН-код карты и нажмите **Вход в систему**.

Процесс подписи занимает некоторое время.

Появится информационное сообщение об успешном подписании документа. Появление этого окошка можно отключить.



В строке состояния программы появится значок, показывающий, что данный документ содержит ЭЦП.



При нажатии на него открывается панель работы с подписью, в которой можно увидеть данные сертификата, а также при необходимости удалить подпись. При попытке внести изменения внизу появится сообщение том, что подписанный документ нельзя редактировать.

	Пример документа Microsoft Office Word с ЭШП
-	примердокумента инстозотсоптсе мога с эцп
•	
-	
-	
<	



### 2.2 Добавление поля для подписи

Microsoft Office, начиная с выпуска 2007, позволяет добавить в документ одно или несколько полей для подписи. Поля подписи позволяют в наглядном виде отобразить, чьи электронные подписи имеются в документе и когда документ был подписан каждой из сторон.

Чтобы добавить в документ поле для подписи, откройте на ленте вкладку **Вставка**. В группе **Текст** выберите **Строка подписи**.



		_ 🕫 X
		0
А А А Надпись Экспресс-блоки WordArt Бун	Строка подписи •	πΩ Формула Символ
Текст		Символы
<ul> <li>· · · · 13 · · · · 14</li> <li>Строка подписи</li> <li>lobortis попшт justo. Vestibulur</li> <li>X</li> <li>John Smith CEO</li> <li>Ø Для получения</li> </ul>	Вставка строки подписи с ука которое должно расписаться Для вставки цифровой подп получить цифровое удостов от сертифицированного пар корпорации Майкрософт. дополнительных сведений на	азанием лица, я. иси необходимо ерение, например отнера ажмите клавишу F1.

Заполните форму для каждого поля подписи.

ſ	Наст	ройка подписи	? 💌		
	Предложенный подписывающий (например: В. А. Белов):				
	Иванов И. И,				
	Должность предложенного подписывающего (например: Директор):				
	Директор				
	Адрес электронной почты предложенного подписывающего:				
	ceo(	Dmycompany.ru			
	Инст	рукции для подписывающег	0:		
	Перед подписанием документа убедитесь, что подписываемое содержимое является правильным.				
	Разрешить подписывающему добавлять примечания в окне подписи				
	Показывать дату подписи в строке подписи				
	ОК ОТМЕНА				
Х			Х		
	1				
Директор	·		Директор		
	*	В <u>ы</u> резать			
		<u>К</u> опировать			
		Вст <u>а</u> вить			
	æ	<u>П</u> одписать			
		<u>С</u> остав подписи			
		Настройка полписи			

Чтобы добавить в поле подпись, вызовите контекстное меню и выберите Подписать.

Выберите изображение с подписью и сертификат, который будет использоваться для подписи документа.

Подписание	×				
Ополнительные сведения о том, что подписывается					
Перед подписанием документа убедитесь, что подписываемое содержимое является правильным.					
Введите свое имя ниже либо нажмите кнопку "Выбрать рисунок" и выберите рисуно для использования в качестве подписи:	ок				
x					
Петров П. П.					
Директор					
Тема сертификата: Testus Кем выдан: isbc					
Подписать Отме	на				

После успешного подписания в поле подписи появится изображение, указанное на предыдущем этапе, а также дата подписи.

30.07.2012

A

Иванов И. И, Директор

Список возможных проблем и методы их решения приведены в руководстве для администраторов ESMART Token – Настройка пользовательских приложений.

## 3. PDF (на примере Adobe Acrobat 9)

## 3.1 Установка модуля защиты ESMART Token в Adobe Acrobat

Adobe Acrobat 9 и Adobe Acrobat X имеют возможность импортировать модуль PKCS#11 для работы с сертификатами на смарт-картах.

Для установки модуля выберите меню: Дополнительно > Параметры защиты.

В открывшемся окне откройте в левой панели: **Цифровые удостоверения > Криптографические** аппаратные ключи.

В панели справа нажмите **Присоединить модуль**. В появившемся окне нажмите **Обзор** и перейдите к файлу *isbc\_pkcs11\_main.dll* в папке C:\Windows\System32 и нажмите **Открыть**.

Установленный модуль появится в списке.

Параметры защиты						
Параметры защиты Цифровые удостоверения Учетные записи перемещаемых удостоверен Файлы цифрового удостоверения Цифровые удостоверения Windows Криптографические аппаратные ключи ISBC Серверы каталогов Серверы отметок времени Серверы Adobe LiveCycle Rights Management	Присоединить модуль         Отсоединить модуль         Обновить           Идентификатор изготовителя м         Путь к библиотеке         ISBC         C:\Windows\system32\isbc_pkcs           Идентификатор изготовителя модуля:         ISBC         Описание модуля:         ISBC           Описание модуля:         Версия библиотеки:         1.0         Версия Стурtoki:         2.20           Путь к библиотеке:         C:\Windows\system32\isbc         pkcs11         main         dll					
	*					

В левой панели разверните список под подключенным модулем. Выберите профиль карты.

Параметры защиты 🖂 Цифровые удостоверения	📩 🥢 - 🔭 🤿 Экспор	г 🎅 Обновить 🏛 Уда	алить цифровое удостоверение	×
Учетные записи перемещаемых удостоверен Файлы цифрового удостоверения Цифровые удостоверения Windows	Имя Testus <test@isbc.ru></test@isbc.ru>	Эмитент isbc	Срок действия 2013.11.02 08:21:30 Z	
<ul> <li>Криптографические аппаратные ключи</li> <li>ISBC</li> <li>EsmartToken</li> </ul>	Te	stus		*
Серверы каталогов Серверы отметок времени Серверы Adobe LiveCycle Rights Management	а Эмитент: isb Срок действия с: 20	st c 12/11/02 12:21:30 +04'00	D,	
Срок действия до: 2013/11/02 12:21:30 +04'00' Предполагаемое использование: Подписать транзакцию, Ключи шифрования, Защита электронной почты, Аутентификация клиента, 1.3.6.1.4.1.311.20.2.2				
				Ŧ

Можно просмотреть существующие на карте сертификаты, выбрать их назначение по умолчанию, например, использовать один сертификат для подписи, а другой для шифрования.





## 3.2 Цифровая подпись PDF

В программе Adobe Acrobat предусмотрено 3 вида подписи:

- **Собственноручная подпись** позволяет «нарисовать» подпись в документе. Не является разновидностью ЭЦП. Не защищает документ. Далее не рассматривается.
- // Подпись Простых электронных подписей может быть в документе любое количество, например, договор может быть подписан двумя сторонами.
- *Сертифицирующая подпись* Может быть поставлена только первой. Если в документе уже есть подпись, сертифицирующую подпись поставить нельзя. В отличие от обычной подписи позволяет изменять возможности пользователей.
  - Невидимая поле для подписи не отображается в документе
  - Видимая в документ добавляется поле для подписи

## 🛣 Видимая сертифицирующая подписы



Прочитайте всплывающие окна с информацией и подсказками.





Удерживая нажатой левую кнопку мыши, обведите область, в которой будет отображаться видимая часть подписи.

В появившемся окне выберите сертификат, вариант оформления и действия, которые сможет выполнять пользователь, когда документ будет подписан.

Выбрав необходимые опции, нажмите Подпись:



В поле, которое было выделено на предыдущем этапе, появятся данные электронной подписи.





## 🥖 Подпись

Обычная (не сертифицирующая) подпись ставится таким же образом. В одном документе может быть несколько не сертифицирующих подписей. Но этот вид подписи не позволяет выбрать, какие возможности будут доступны пользователю для редактирования.

Для примера также показано альтернативное оформление с использованием изображения, например, отсканированная собственноручная подпись.

Подписать документ		×
Подписать как:	Testus	• 3
Эмитент сертифик	ата: isbc	Информация
	Оформление: Подписано циф подписью: Testu DN: dc=ru, dc=is ou=Test, cn=Tes email=testus@te	Создан 2011.07.2€ ▼ ровой Is bc, dc=corp, tus, Ist.test 1000000000000000000000000000000000000
	Дата: 2012.06.04 +04'00' Подпись	Отмена

Для изменения подписи, щелкните правой кнопкой мыши на поле подписи и выберите **Очистить подпись**. Там же можно подтвердить подпись или просмотреть информацию.



## 3.3 Шифрование документа PDF

Выберите на панели инструментов команду Защита или в меню Дополнительно – Защита – Encrypt with Certificate



Появится окно с запросом на выполнение операции, его можно отключить. Подтвердите операцию.

Выберите опции шифрования и нажмите Далее



Настройки защиты с помощью сертифик	ата			×
Шаги				
🔶 Основные настройки	Введите общие необходимо вве	сведения для стратегии Защита с помощью сертификата. ссти по крайней мере название.	Чтобы продолжить,	
Выбрать получателей				
Содержание отчета	🔘 Сохранить эти			
	Орименить и у Орименить и Орименить и С Орименить и С Орименить и С О	/далить эти настройки		
	Имя стратегии:	Encrypt with Certificate	не более 50 символов	
	Описание:	This policy will allow you to require access to a specific private key when opening a document.	не более 250 символов	
	Выбрать части	] документа, которые будут зашифрованы все содержимое документа		
	Шифровате	все содержимое документа кроме метаданных (совместимо	с Acrobat б и выше)	
	Шифровате	отолько вложенные файлы (совместимо с Acrobat 7 и выше)		
	Все сод поиско	ержимое документа будет зашифровано, при этом вые программы не будут иметь доступа к метаданным		
	При примене	нии этой стратегии запрашивать получателей		
	Алгоритм шифр	ования: 128-битный AES (совместим с Acrobat 7.0 и выше)	•	
	Отмена			< Назад Далее >

Выберите сертификаты предполагаемых получателей. В этом же окне можно задать определенные ограничения на работу с файлом, например, запретить определенным пользователям печать и изменение документа.

Шаги			
Основные настройки	Обновление списка предполагаем ограничения на документ для пол	ных получателей документов, защищенных данной стратеги учателя, выбрав его и нажав "Права доступа".	ей. Вы можете наложить
Содержание отчета	Имя	F-mail	Поиск
	Testus	testus@test.test	Полека
			Обзор
			Удалить
			Полобно
			Подросно
			Разрешения
	Права доступа		
	Изменить параметры защиты:	Разрешено	
	Изменения:	Все, кроме извлечения страниц	
	Печать:	С высоким разрешением	
	Копирование:	Разрешено	
	Лоступ	Разрешено	
	доступ		

Нажмите Далее, а в последнем окошке подтвердите шифрование, нажав Готово.



Программа предложит сохранить документ, чтобы изменения вступили в силу. Сохраните файл, чтобы применить шифрование.

Слева появится замочек, который означает, что шифрование прошло успешно. В панели будет отображаться общая информация о параметрах защиты.



Список возможных проблем и методы их решения приведены в руководстве для администраторов **ESMART Token – Настройка пользовательских приложений**.



Обращаем внимание, что отправка электронной почты с использованием шифрования и цифровой подписи возможна только от имени отправителя, указанного в сертификате. Иначе почтовый клиент выдаст получателю соответствующее предупреждение. В данном руководстве рассмотрено шифрование и подпись электронной почты сертификатом X.509 со смарт-карты ESMART Token.

## 4. Почтовый клиент Microsoft OUTLOOK 2007

## 4.1 Настройка сертификатов

Выберите в меню Сервис > Центр управления безопасностью > Защита электронной почты:



Установите соответствующие галочки в разделе **Шифрованная электронная почта**, если хотите шифровать сообщения и использовать цифровую подпись по умолчанию для всех писем.

Устанавливать шифрование и добавлять цифровую подпись можно для каждого индивидуального сообщения. В данной вкладке задаются настройки, которые будут применяться по умолчанию.

Для выбора сертификата, который будет использоваться для ЭЦП и шифрования, необходимо создать конфигурацию. Как правило, конфигурация создается автоматически. Если этого не произошло, нажмите **Параметры**.



Изменение настройки безопасности							
Настройка безопасности							
Имя конфигурации:							
Установки S/MIME (test@isbc.ru) ▼							
Формат криптографии: S/MIME							
📝 Настройка безопасности по умолчанию для этого формата							
Настройка по умолчанию для всех сообщений							
Метки безопасности Создать Удалить Пароль							
Сертификаты и алгоритмы	_						
Сертификат подписи: Testus Выбрать							
Алгоритм хеширования: SHA1 🔻							
Сертификат шифрования: Testus Выбрать							
Алгоритм шифрования: 3DES 💌							
Передавать сертификаты с сообщением							
ОК Отмена							

В разделе **Сертификаты и алгоритмы** должны быть выбраны сертификаты, которые будут использоваться для подписи и шифрования. Нажмите **Выбрать** и укажите в появившемся окне нужный сертификат:



При необходимости измените используемые алгоритмы хэширования и шифрования. Предварительные настройки для использования шифрования и ЭЦП завершены.



## 4.2 Электронная подпись сообщения

Создайте сообщение. Кнопка с иконкой сертификата должна быть активна. (Если на этапе настройки было выбрано **Добавлять цифровую подпись к исходящим сообщениям**, при создании каждого письма кнопка будет активна по умолчанию).

ſ		1 1 4 4	) =	Без	имени - Сообщение	(HTML)			
	Cooe	бщение В	ставка Пар	раметры	Формат текста			۲	
	Буфер об 🕞	Саlibri (Осно Ж. К. Ц а <u>b</u> 2 т. <u>А</u> т. Осно	о т 11 т Е т і Ξ т В Ξ Ξ Ξ овной текст		Адресная Проверить книга имена Имена	<ul> <li>●     <li>●     <li>●     <li>■     </li> <li>■      </li> <li>■      </li> <li>■     </li> <li>■     </li> <li>■     </li> <li>■      </li> <li>■      </li> <li>■     </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <li>■      </li> <lp>■      </lp></li> <lp>■</lp></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></li></ul>	К исполнению т Параметры	<ul> <li>АВС</li> <li>Орфография</li> <li>Правописание</li> </ul>	
	Отправит <u>ь</u>	Кому <u>.</u> Копи <u>я</u> Т <u>е</u> ма:	test <test@isbc< th=""><th><u>ru&gt;;</u></th><th></th><th></th><th></th><th>Сообщение с цифров Добавление к данно цифровой подписи, другим пользовател именно вы являетес сообщения.</th><th>юй подписью му сообщению которая позволит ям убедиться, что ь адресатом</th></test@isbc<>	<u>ru&gt;;</u>				Сообщение с цифров Добавление к данно цифровой подписи, другим пользовател именно вы являетес сообщения.	юй подписью му сообщению которая позволит ям убедиться, что ь адресатом
	Пример со	общения с З	эцп						

Нажмите Отправить и введите ПИН-код карты в появившееся окно.



В правом верхнем углу будет отображаться иконка с печатью, показывающая, что письмо подписано электронно-цифровой подписью. При нажатии на иконку можно посмотреть данные сертификата. Нажмите **Сведения...** для просмотра подробной информации.



ить всем 🙈 Пересдать   🔡 🚩 📑 Отправить и полу <u>ч</u> ить 👻 🔛 поиск в	задресной книге 🔹 🛞 🖕
Пример письма с ЭЦП	
test [test@isbc.ru] Отправлено: Вт 05.06.2012 20:48 Кому: test@isbc.ru Подписано: test@isbc.ru	8
Это электронное письмо с ЭЦП	Свойства безопасности сообщения
Цифровая подпись: правильная	Тена: Пример письма с ЭЦП Сообщения могут шифроваться и содержать слои цифровых подписей. Каждый слой
Тема:         Пример письма с ЭЦП           От:         test           Подписано:         test@lisbc.ru           Ост:         test@lisbc.ru           Ост:         сертификате, применяемом в цифровой подписи сообщения, нажните кнопку "Сведения".           Предупреждать об ошибках в подписанных сообщениях до открытия.           Закрыть	допускает наличие нескольких подписей. Слоя безопасности Выберите слой для проснотра его описания. ✓ Тема: Пример письма с ЭЦП ✓ Уровень цифровых подписей ✓ Подписано: test@isbc.ru
	Описание:
	ОК: подписанное сообщение. Следующие кнопки позволяют проснотреть дополнительные сведения или внести изменения в выбранный слой: Изменить доверие Подробности Доверие к центру сертификации Предупреждать об ошибках в подписанных сообщениях. Закрыть

## 4.3 Шифрование

В отличие от цифровой подписи, которая может быть отправлена в одностороннем порядке, для использования шифрования необходимо, чтобы оба адресата предварительно обменялись сертификатами. Чтобы обменяться частями сертификатов с открытыми ключами, стороны отправляют друг другу электронные письма с ЭЦП, а затем добавляют друг друга в адресную книгу.

Другие способы обмена сертификатами описаны на сайте Microsoft:

http://office.microsoft.com/ru-ru/outlook-help/HP001230536.aspx

В карточке контакта в разделе Сертификаты будут перечислены доступные сертификаты.

1	<b>(</b> ) 🖬 🔊 U	4 7	) =	test - Контакт			- • <b>×</b>
	Контакт	Вставк	а Формат текста				۲
	Сохранить Х		<ul> <li>Электронная почта</li> <li>Электронная почта</li> <li>Собрание</li> <li>Собрание</li> <li>Вызов *</li> </ul>	<ul> <li>Рисунок *</li> <li>Выбрать категорию т карточка *</li> <li>К исполнению *</li> </ul>	2 11 8/	АВС Орфография	
	деиствия	ПОКАЗАТЬ	Связь	Параметры		правописание	
	При отправке шиф из этих сертификат данного контакта, л Сертификаты (циф) Testus(По умолчан	рова Серт ов. С либо От кон ровы УДС отг кон	тификаты ображение страницы "Сертиф нтакта, которая содержит циф остоверения, используемые для правки зашифрованных писем нтакту.	эзоваться один общения с цифровой общения с цифровой этому	подпи	ісью от	Свойства
							По умолчанию Импорт Экспорт Удалить



### 4.4 Составление сообщения

	ា ថ 🖂 🤊	<ul> <li>Пример сообщения с шифрованием - Сообщение (HTML)</li> </ul>	
Cool	бщение	Вставка Параметры Формат текста	
Вставить	Calibri XXX 2	(Осно × 11 × А́ х́) У Ц І = × № Ф́ Ф́ Ф́ № ена А × ■ ≡ ≡ ⊕ Основной текст Б Включить Б Параметры	АВС Орфография Правописание
 Отправит <u>ь</u>	Кому <u>.</u> Копи <u>я</u>	<u>test ≺test@isbc.ru&gt;;</u>	Шифровать Шифрование данного сообщения с целью затруднить его прочтение несанкционированными пользователями.
Это приме	т <u>е</u> ма: ер электрог	пример сообщения с шифрованием	

### 4.5 Получение зашифрованного электронного сообщения

При получении письма программа Outlook не показывает его содержимое во всплывающих уведомлениях. Тест сообщения нельзя прочитать в боковой панели, как в случае с незашифрованными сообщениями. Прочитать зашифрованное сообщение можно, только открыв его в новом окне. При попытке открыть письмо запрашивается ПИН-код карты, на которой хранится сертификат с закрытым ключом.



Нажав на иконку с замочком можно просмотреть свойства безопасности и данные сертификата.

<b>Ca</b> ) 🖬 " U 🍲 🕈 Ŧ	Тестовое письмо с ши	ифрованием - Сообщение (HTML)		
Сообщение				
Стветить Ответить Переслать всем Ответить Тереслать	Удалить Удалить В папку * Эдалить Эругие действия * Действия	<ul> <li>Заблокировать отправителя</li> <li>Надежные списки *</li> <li>Не является нежелательным Нежелательная почта</li> </ul>	<ul> <li>Выбрать категорию *</li> <li>К исполнению *</li> <li>Пометить как непрочтенн Параметры</li> </ul>	ные
От: test [test@isbc.ru]			Отправлено: Ср	06.06.2012 18
Тема: Тестовое письмо с ш Пример письма с шифрова	ифрованием Свойства безопа	сности сообщения		
	Сообщения могут	т шифроваться и содержать слои циф	ровых подписей. Каждый слой	
	допускает наличи Слои безопасно	ие нескольких подписей. ости		
	допускает наличи Слон безопасно Выберите слой дл У Тема: Тестов	ие нескольких подписей. ости ля просмотра его описания. зое письмо с шифрованием		
	допускает налич Слои безопасни Выберите слой дл Тема: Тестой С. Уровень	ие нескольких подписей. эсти ля просмотра его описания. вое письмо с шифрованием шифрования		
	допускает налич Слои безопасни Выберите слой дл Тема: Тесто Уровень	ие нескольких подписей. эсти ля просмотра его описания. вое письмо с шифрованием шифрования	· · · · ·	
	допускает налич Слоя безопасни Выберите слой дл Гена: Тесто У Уровень	ие нескольких подписей. эсти ля просмотра его описания. вое письмо с шифрованием шифрования		
	допускает налич Слои безопасин Выберите слой дл Тема: Тесто Уровень Описание: ОК: шифрованно	ие нескольких подписей. <b>эсти</b> пя просмотра его описания. вое письмо с шифрованием шифрования не сообщение.		
	допускает налич Слоя безопасни Выберите слой дл Гена: Тесто Гена: Тесто Описание: ОК: шифрованно	ие нескольких подписей. <b>эсти</b> пя просмотра его описания. вое письмо с шифрованием шифрования не сообщение.		
	допускает налич Слоя безопасни Выберите слой ди Гена Тестоя Слисание: Описание: ОК: шифрованно След ующие кноп изменения в выбр	ие нескольких подписей. <b>эсти</b> ля просмотра его описания. <b>вое письмо с шифрованием</b> шифрования не сообщение. ки позволяют просмотреть дополнит занный слой:	ельные сведения или внести	
	Допускает налич Слов безопасни Выберите слой д Гена: Тесто Гена: Тесто Уровень Описание: ОК: шифрованно След ующие кноп изменения в выбр Изменить дове	ие нескольких подписей. <b>pcти</b> ля просмотра его описания. вое писано с шифрованием шифрования е сообщение. ки позволяют просмотреть дополнит ранный слой: рие Подробности Доп	гельные сведения или внести верие к центру сертификации	

Список возможных проблем и методы их решения приведены в руководстве для администраторов ESMART Token – Настройка пользовательских приложений.



## 5. Почтовый клиент Mozilla Thunderbird

## 5.1 Настройка почтового клиента

Для подписи и шифрования сообщений электронной почты требуется предварительная настройка почтового клиента. Настройка может быть выполнена администратором или самим пользователем в соответствии с документом **ESMART Token – Настройка пользовательских приложений**.

### 5.2 Настройка параметров учетной записи

После выполнения подготовительной настройки почтового клиента Mozilla Thunderbird необходимо настроить правила использования сертификатов для каждой учетной записи.

Для каждой учетной записи можно настроить индивидуальные параметры защиты и выбрать определенный сертификат (если их несколько). Это расширяет возможности применения ЭЦП и шифрования. Например, добавление ЭЦП можно назначить по умолчанию для учетной записи корпоративной почты, но не применять защиту к учетной записи для личной почты.

Параметры сервера Копии и палки Составление и адресация Анти-спам фильтр Дисковое пространство Уведомления о прочтен Защита • Блоги и ленты новостей Дисковое пространство • SMTP Параметры с Копии и ланк Составление Анти-спам ф Дисковое пространство • SMTP Параметры с Копии и ланк Составление Анти-спам ф Дисковое пространство • SMTP Параметры с Копу выдано: E=test@isbc.ru_CN=Testus,OU=Test_DC=corp,DC=isbc,DC=ru Серийрикат: EsmantToken:45d23al1-3d04-475e-8475-599al7b65fa7 [39:0C:07:E0:00:01:00:00:01:7f] • Информация о выбранном сертификате: Колу выдано: E=test@isbc.ru_CN=Testus,OU=Test_DC=corp,DC=isbc,DC=ru Серийрикат: EsmantToken:45d23al1-3d04-475e-8475-599al7b65fa7 [39:0C:07:E0:00:01:00:00:01:7f] • Информация о выбранном сертификате: Колу выдано: E=test@isbc.ru_CN=Testus,OU=Test_DC=corp,DC=isbc,DC=ru Серийриката почта: E=test@isbc.ru_CN=Testus,OU=Test_DC=corp,DC=isbc,DC=ru Серийриката почта: test@isbc.ru Параметры с Копии и ланк Составление Анти-спам ф Дисковое про Уведомления о прочтен Защита а Test@isbc.ru Параметры с Копии и ланк Составление Анти-спам ф Дисковое про Уведомления о прочтен Защита а Локальные палки а Локальное палки а Локальное палки а Локальное палки а Локальное палки а Локальное палки а Л	Параметры учётной записи	
Ансковое пространство Соотщения цифровой подписы (по умолчанию)       А SMTP     Параметры с     Копии и папс     Составление     Анти-спам ф     Дисковое про     Уведомления о прочтен     Защита     Дисковое про     Уведомления о прочтен     Защита     Докальные папки     Ф	Параметры сервера Копии и папки Составление и адресс Анти-спам фильтр Дисковое пространст Уведомления о прочт Защита 4 Блоги и ленты новосте	Защита Чтобы получать и отправлять зашифрованные сообщения или сообщения с цифровой подписью, вам нужно указать сертификат ключа шифрования и сертификат ключа подписи. Цифровая подпись Личный сертификат для подписи: Выбрать Очистить
Параметры с Копии и папк Составление Анти-спам ф Дисковое пре Уведомления Защита 4 test@isbc.ru Параметры с Копии и папк Составление Анти-спам ф Дисковое пре Уведомления Серийный номер: 39:0C:D7:E0:00:01:00:00:01:7F Действителен с 02:11:2012 12:21:30 по 02:11:2013 12:21:30 Использование сертификате: Копии и папк Составление Анти-спам ф Дисковое пре Уведомления о прочтен Защита 4 Локальные папки Серийный номер: 39:0C:D7:E0:00:01:00:00:01:7F Действия и папк Составление Анти-спам ф	▲ SMTP	Подписывать сообщения цифровой подписью (по умолчанию)
Копии и папк Составление Анти-спам ф Дисковое про Уведомления Защита 4 test@isbc.ru Параметры с Копии и папк Составление Анти-спам ф Дисковое про Уведомления Защита 4 test@isbc.ru Параметры с Копии и папк Составление Анти-спам ф Дисковое про Уведомления о прочтен Защита 4 test@isbc.ru Параметры с Копии и папк Составление Анти-спам ф Дисковое про Уведомления о прочтен Защита 4 действия для учётной записи	Параметры с	о сертификата
Составление Анти-спам ф Дисковое пре Уведомления Защита 4 test@isbc.ru Параметры с Копии и папк Составление Анти-спам ф Дисковое пре Уведомления о прочтен Защита 4 test@isbc.ru Параметры с Анти-спам ф Дисковое пре	Копии и папк Серт	ификат: EsmartToken:45d23a11-3d04-475e-8475-599a17b65f87 [39:0C:D7:E0:00:01:00:00:01:7F] 💌
Анти-спам ф Дисковое про Уведомления Защита а test@isbc.ru Параметры с Кому выдано: E=test@isbc.ru, CN=Testus, OU=Test, DC=corp, DC=isbc, DC=ru Серийный номер: 39:0C:D7:E0:00:01:00:00:01:7F Действителен с 02:11:2012 12:21:30 по 02:11:2013 12:21:30 Использование сертификата ключа: Подпись, Шифрование ключа Электронная почта: test@isbc.ru Кем выдано: CN=isbc, DC=corp, DC=isbc, DC=ru Место хранения: EsmartToken ОК Отмена ОК Отмена Анти-спам ф Дисковое про Уведомления о прочтен Защита а Локальные папки Действия для учётной записи •	Составление	
Анти-спам ф Дисковое про Уведомления о прочтен Защита и Локальные папки СДействия для учётной записи т	Анти-спам фі Дисковое про Уведомления Деі Защита Эле ▲ test@isbc.ru Кем Параметры с Мес Копии и папк	ормация о выбранном сертификате: у выдано: E=test@isbc.ru, CN=Testus, OU=Test, DC=corp, DC=isbc, DC=ru рийный номер: 39:0C:D7:E0:00:01:00:00:01:7F йствителен с 02.11.2012 12:21:30 по 02.11.2013 12:21:30 пользование сертификата ключа: Подпись, Шифрование ключа ектронная почта: test@isbc.ru выдано: CN=isbc, DC=corp, DC=isbc, DC=ru то хранения: EsmartToken
ОК Отмена Дисковое про Уведомления о прочтен Защита а Локальные папки Сействия для учётной записи *	Составление	
Уведомления о прочтен Защита и Локальные папки Действия для учётной записи *	Лисковое про	ОК Отмена
Защита <i>а</i> Локальные папки Действия для учётной записи т	Уведомления о проч	тен
ОК Отмена	Защита Локальные папки Действия для учётной за	тиси т

Откройте Инструменты > Параметры учетной записи > Защита:

Выберите сертификаты, которые будут использоваться, а также отметьте (по желанию) опции Подписывать сообщения цифровой подписью (по умолчанию) и Использовать шифрование при отправке сообщений.

Ставить цифровую подпись и применять шифрование можно к каждому письму индивидуально. В данном окне задаются только значения по умолчанию.

Нажмите Выбрать и укажите нужный сертификат (может быть доступно несколько сертификатов).

Параметры учётной записи	×				
Дисковое пространство 🛛	Защита				
Уведомления о прочтен					
Защита	Чтобы получать и отправлять зашифрованные сообщения или сообщения с				
4 Блоги и ленты новостей	сертификат ключа подписи.				
Дисковое пространство	Шифровая подпись				
▲ SMTP	Личный сертификат для подписи:				
Параметры сервера	Ermattakan/5/22-11.2/04.475-08/75.500-17/65/97 Buinatt				
Копии и папки					
Составление и адресация	📃 Подписывать сообщения цифровой подписью (по умолчанию)				
Анти-спам фильтр					
Дисковое пространство	Шифрование				
Уведомления о прочтен	Личный сертификат для шифрования:				
Защита	EsmartToken:45d23a11-3d04-475e-8475-599a17b65f87 Вы <u>б</u> рать Оч <u>и</u> стить				
⊿ test@isbc.ru	Использовать шифрование при отправке сообщений:				
Параметры сервера 🗧	Никогла (не использовать цимфрование)				
Копии и папки					
Составление и адресация	Всегда (сообщение не будет отправлено, если не у всех адресатов есть сертификаты)				
Анти-спам фильтр	cep in writer by				
Дисковое пространство	Сертификаты				
Уведомления о прочтен	Просмотр сертификатов Устройства защиты				
Защита					
Локальные папки					
Анти-спам фильтр					
Дисковое пространство					
Сервер исходящей почты					
Дейст <u>в</u> ия для учётной записи •					
	ОК Отмена				

Настройки учетной записи завершены. Повторите процедуру для каждой учетной записи.



#### 5.3 Электронное письмо с ЭЦП

ЭЦП можно добавить в любое сообщение электронной почты. Отметьте опцию Цифровая подпись в панели инструментов письма.

🕞 Создание сообщения: Пример письма с ЭЦП	
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид В <u>с</u> тавить <u>Ф</u> ормат Настро <u>й</u> ки	и <u>И</u> нструменты <u>С</u> правка
🛄 Отправить 🔤 Орфография 🔹 🖖 Вложить 🔹	• 🚰 Защита • 📊 Сохранить •
O <u>r</u> : test <test@isbc.ru> test@isbc.ru</test@isbc.ru>	<u>Требова</u> Просмотр или изменение параметров защиты
• Кому: 🔒 test@isbc.ru	✓ Цифровая подпись
	Защита <u>с</u> ообщения
<u>Тема:</u> Пример письма с ЭЦП	
Обычный текст 👻 Пропорциональный	<mark>··</mark> ▲ ▲ ▲ ▲ ⊨ ≟ 표 표 Ξ · ■ · ◎ ·
Это электронное письмо с ЭЦП	



Принятое письмо с ЭЦП будет выглядеть следующим образом (для просмотра информации о подписи нажмите на значок конверта):





### 5.4 Шифрование электронной почты

Для отправки зашифрованного сообщения отметьте опцию Требовать шифрования.

Создание сообщения: Письмо с шифрованием	
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид В <u>с</u> тавить <u>Ф</u> ормат Настро <u>й</u> ки	Инструменты Справка
📗 Отправить 🛛 abc Орфография 🔹 🖖 Вложить ୟ	Защита • 🕞 Сохранить •
O <u>r</u> : [test <test@isbc.ru> test@isbc.ru</test@isbc.ru>	✓ <u>Т</u> ребовать шифрования
• Кому: 🔒 test@isbc.ru	Цифровая подпись
	Защита сообщения
<u>Тема:</u> Письмо с шифрованием	
Обычный текст 🗸 Пропорциональный	- ■ A A A A A ⊟ ≟ ☲ ☲ ☲ = = •
Это пример письма с шифрованием	
	<b>≙</b>

Чтобы получатель зашифрованного сообщения смог его открыть и прочесть, необходимо предварительно обменяться сертификатами с открытыми ключами.

Самым простым способом обмена сертификатами является обмен сообщениями с ЭЦП. При получении сообщения с ЭЦП программа Thunderbird получает ключи из принятого сертификата. Добавьте пользователя в адресную книгу.

Теперь, открыв **Менеджер сертификатов**, можно увидеть, с кем происходил обмен сертификатов. Менеджер сертификатов можно открыть с вкладки **Сертификаты** в окне настроек или вкладки **Защита** в окне редактирования параметров учетной записи.

ши сертификаты   Люди   Сеј У вас хранатса сертификаты	оверы Центры сертификации Д		
Увас хранятся сертификаты, Имя сертификата	Срок действия	Адрес электронной почты	Ę
⊿isbc Tectus	05.06.2013	tert@icbc.ru	
Про <u>с</u> мотреть И <u>з</u> менит	њ И <u>м</u> портировать Эк <u>с</u> и	портировать Удалить	

Полученное сообщение с шифрованием (при наличии у обеих сторон ключей после обмена сертификатами) будет отображаться следующим образом (для просмотра информации о шифровании нажмите на иконку с замочком):



Список возможных проблем и методы их решения приведены в руководстве для администраторов **ESMART Token – Настройка пользовательских приложений**.



## 6. Браузер Mozilla Firefox

Браузер Mozilla Firefox может использоваться для организации доступа к корпоративным сайтам и отдельным разделам сайта по сертификату, т.е. чтобы получить возможность доступа на сайт пользователь должен предъявить сертификат на ESMART Token и ввести верный ПИН-код.

С помощью авторизации по сертификату могут быть дополнительно защищены административные разделы сайта или разделы, где есть сведения, относящиеся к коммерческой тайне.

Для работы Mozilla Firefox с сертификатами требуется выполнить предварительную настройку программы в соответствии с руководством для администраторов ESMART Token – Настройка пользовательских приложений.

### 6.1 Авторизация по сертификату

Для авторизации по сертификату наберите или скопируйте в адресную строку браузера адрес защищенного сайта или защищенного раздела сайта, или перейдите по ссылке. В появившееся окошко введите ПИН-код пользователя. Если на карте записано несколько сертификатов, выберите нужный. При необходимости отметьте опцию **Запомнить это решение**.

прос идентификации пользователя	
Сайту необходимо определить, с каким сертификатом вас ассоциироват	ь
Организация:	
Выдано: «Thawte, Inc.»	
Выберите сертификат для идентификации:	
EsmartToken:7db7209a-f3f2-18e4-58aa-fc1ae5623a07(Import) [03]	•
Информация о выбранном сертификате:	
Кому выдано: CN=User ID Alexander,OU=ISBC Certification Center,O=ISBC Серийный номер: 03 Действителен с 02.03.2012 17:24:38 по 02.03.2013 17:24:38 Использование сертификата ключа: Подпись. Неоспоримость. Шифрование ключа. Шифрование данных	
Кем выдано: OU=ISBC Certification Center,CN=ISBC Root Authority,O=ISBC	•
Запомнить это решение	
ОК Отмена	

Список возможных проблем и методы их решения приведены в руководстве для администраторов **ESMART Token – Настройка пользовательских приложений**.

