eSMART®

ЭЦП и шифрование в Windows

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

Содержание

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*

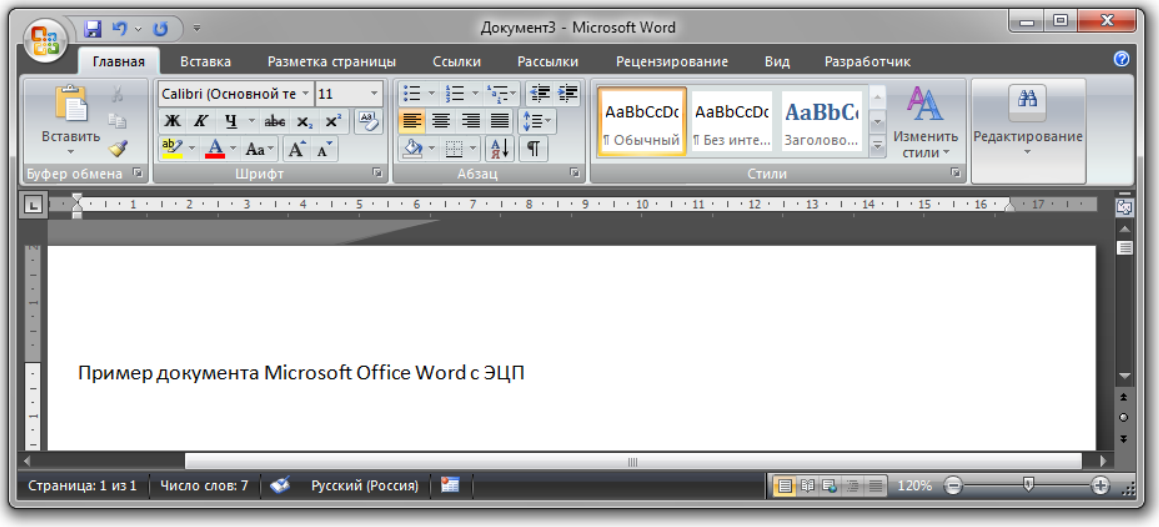
***требуется дополнительная настройка**. Поэтапно настройка указанных приложений приведена в руководстве для администраторов ESMART Token – Настройка пользовательских приложений.*

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.

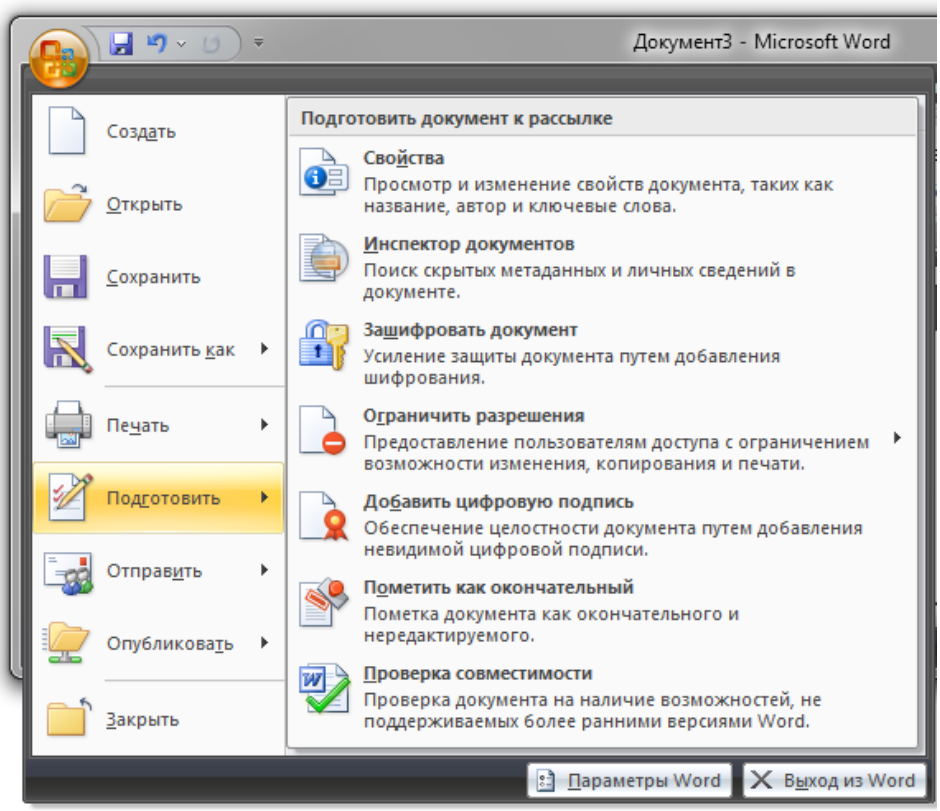
2. Офисные редакторы (на примере Microsoft Office Word 2007)

Откройте текстовый документ, или создайте новый:



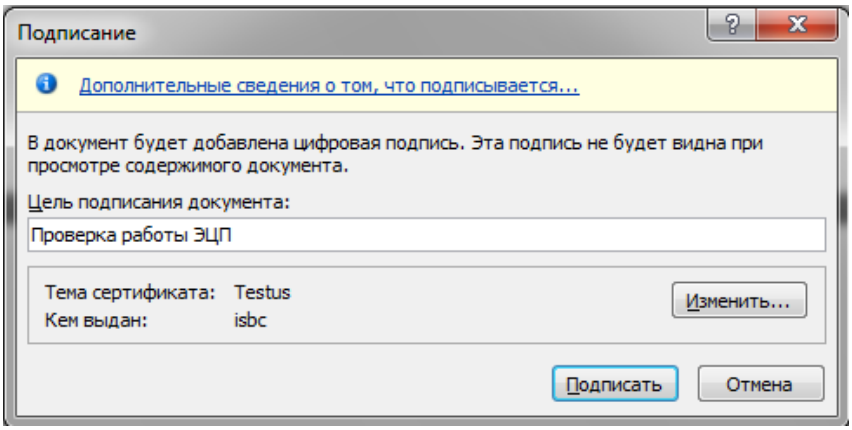
2.1 Настройки параметров ЭЦП и выбор сертификата

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

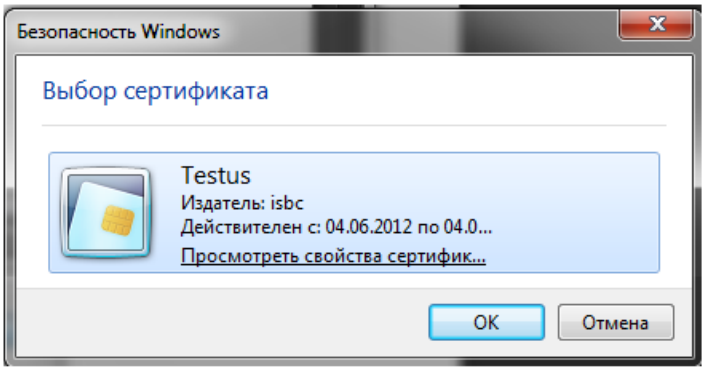


Во всплывающих окнах появится справочная информация об ЭЦП.

Появится окно:



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

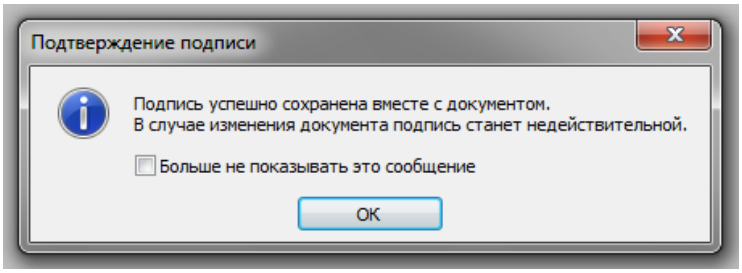


Выбрав сертификат, по желанию заполните поле ***Цель подписания*** *и нажмите* ***Подписать*** *(см. выше).*

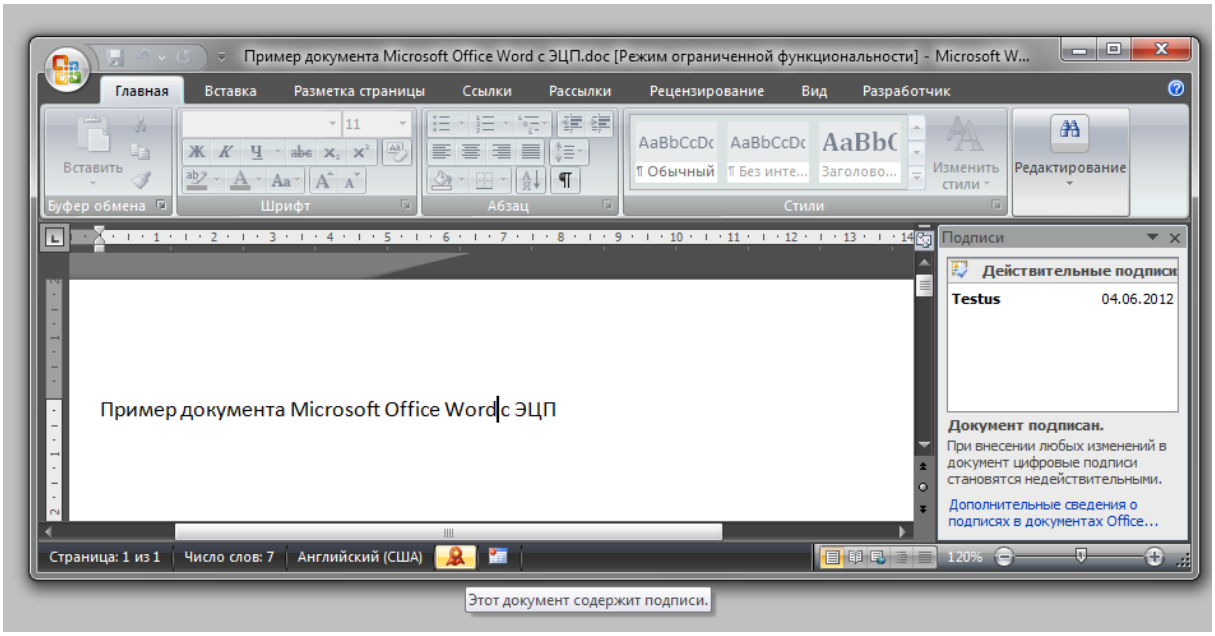
Введите в появившееся окно ПИН-код карты и нажмите ***Вход в систему****.*

Процесс подписи занимает некоторое время.

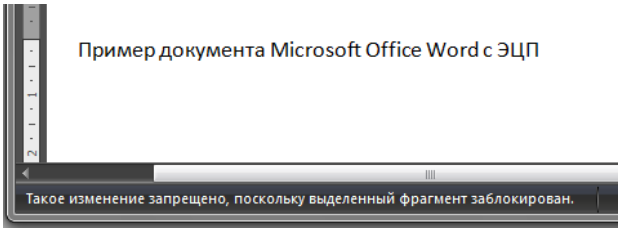
Появится информационное сообщение об успешном подписании документа. Появление этого окошка можно отключить.

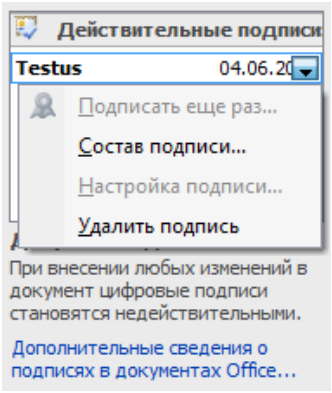


В строке состояния программы появится значок, показывающий, что данный документ содержит ЭЦП.



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.

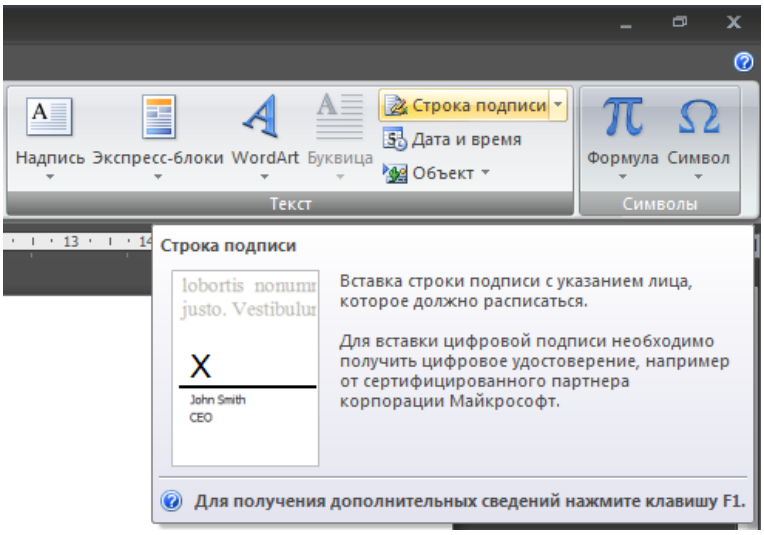




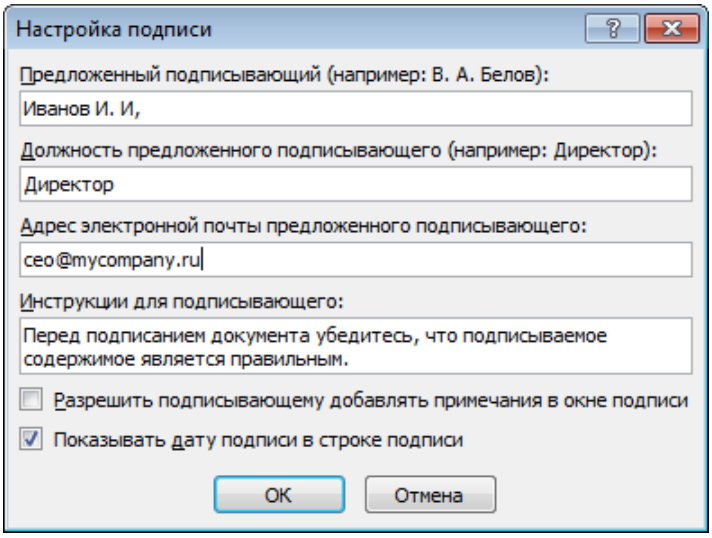
2.2 Добавление поля для подписи

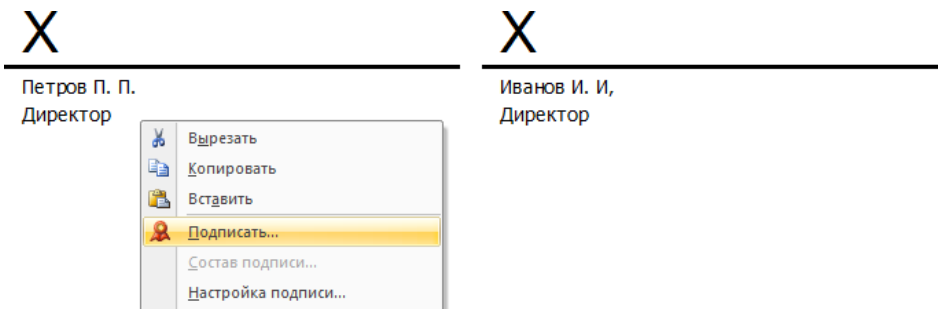
Microsoft Office, начиная с выпуска 2007, позволяет добавить в документ одно или несколько полей для подписи. Поля подписи позволяют в наглядном виде отобразить, чьи электронные подписи имеются в документе и когда документ был подписан каждой из сторон.

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



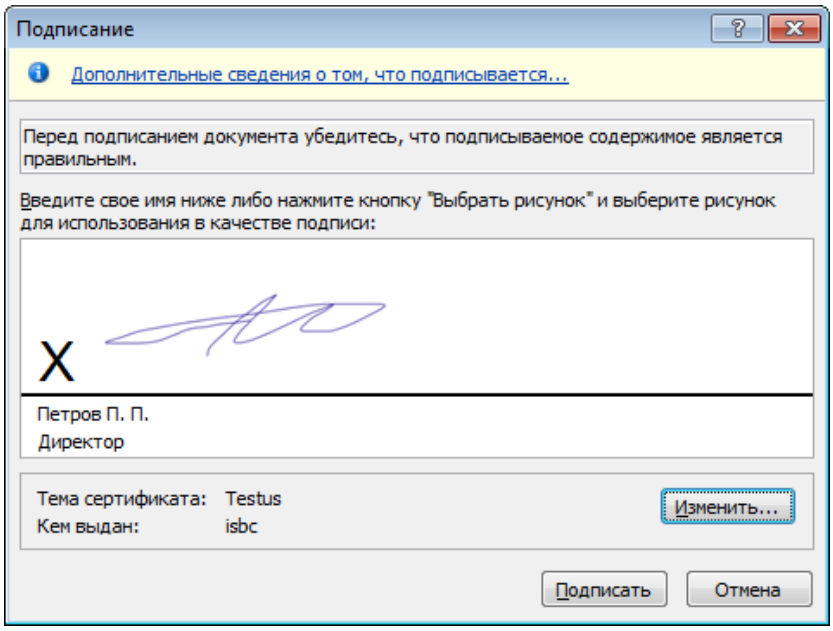
Заполните форму для каждого поля подписи.





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

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



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

30.07.2012

X

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

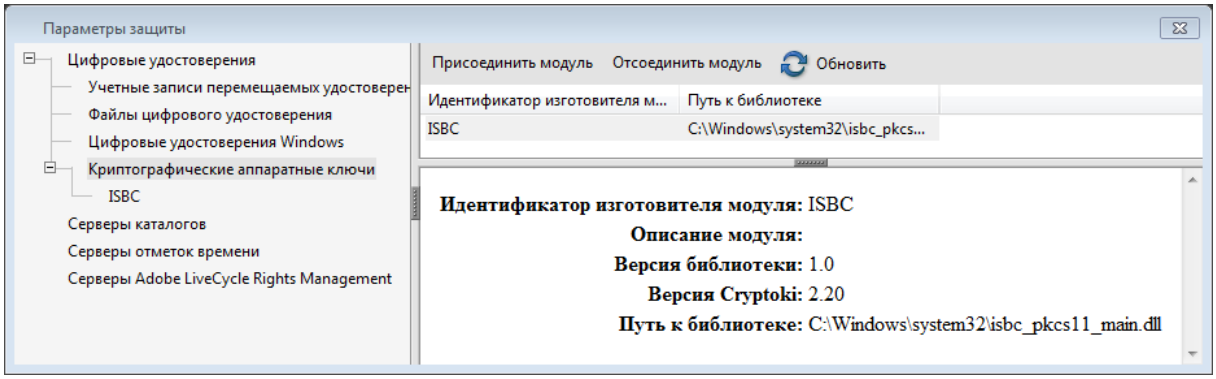
Adobe Acrobat 9 и Adobe Acrobat X имеют возможность импортировать модуль PKCS#11 для работы с сертификатами на смарт-картах.

Для установки модуля выберите меню: ***Дополнительно › Параметры защиты.***

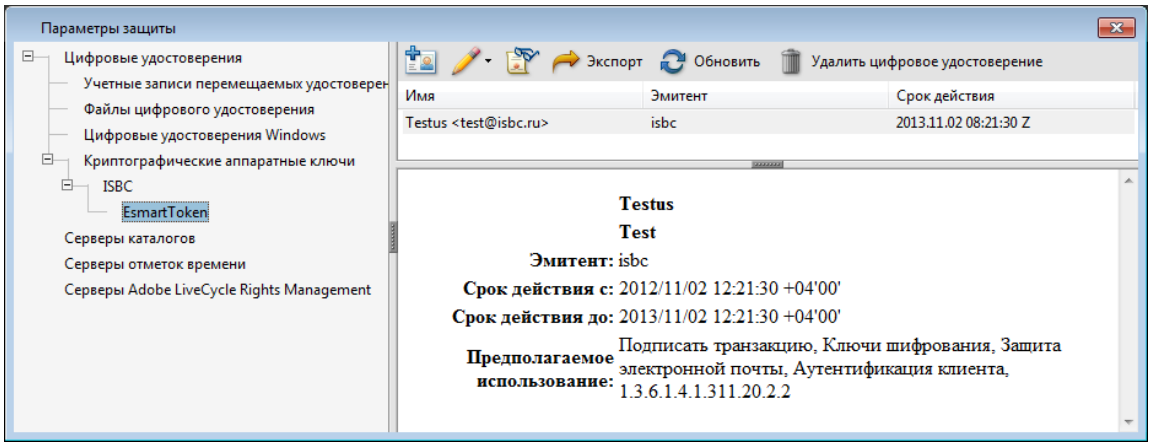
В открывшемся окне откройте в левой панели: ***Цифровые удостоверения › Криптографические аппаратные ключи****.*

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****.*

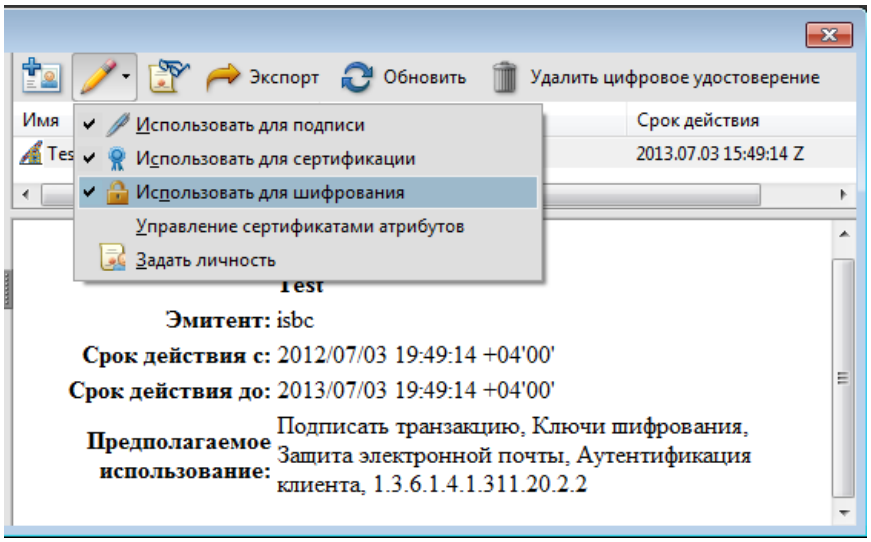
Установленный модуль появится в списке.



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



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

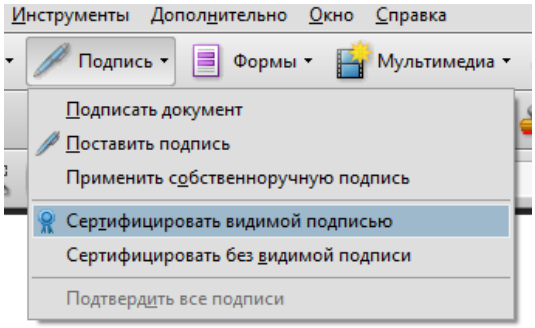


3.2 Цифровая подпись PDF

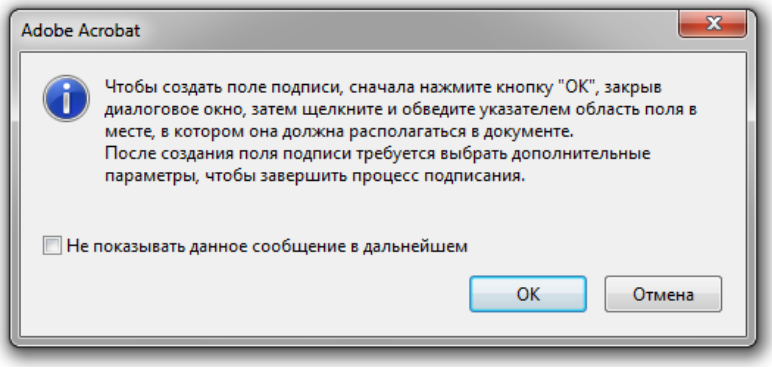
В программе Adobe Acrobat предусмотрено 3 вида подписи:

- ***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 подпись



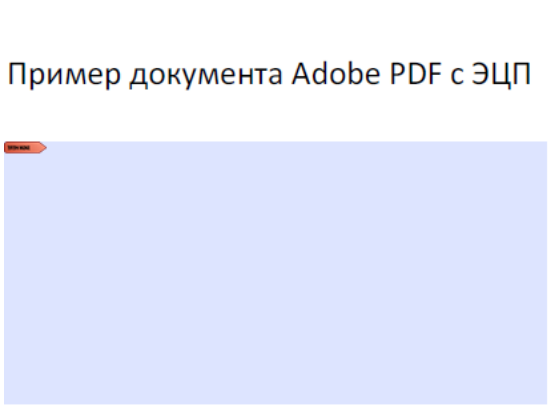
Прочитайте всплывающие окна с информацией и подсказками.

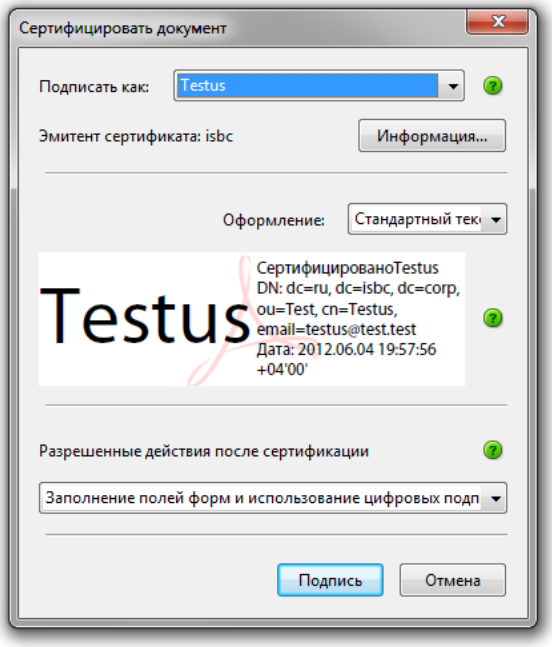


Удерживая нажатой левую кнопку мыши, обведите область, в которой будет отображаться видимая часть подписи.

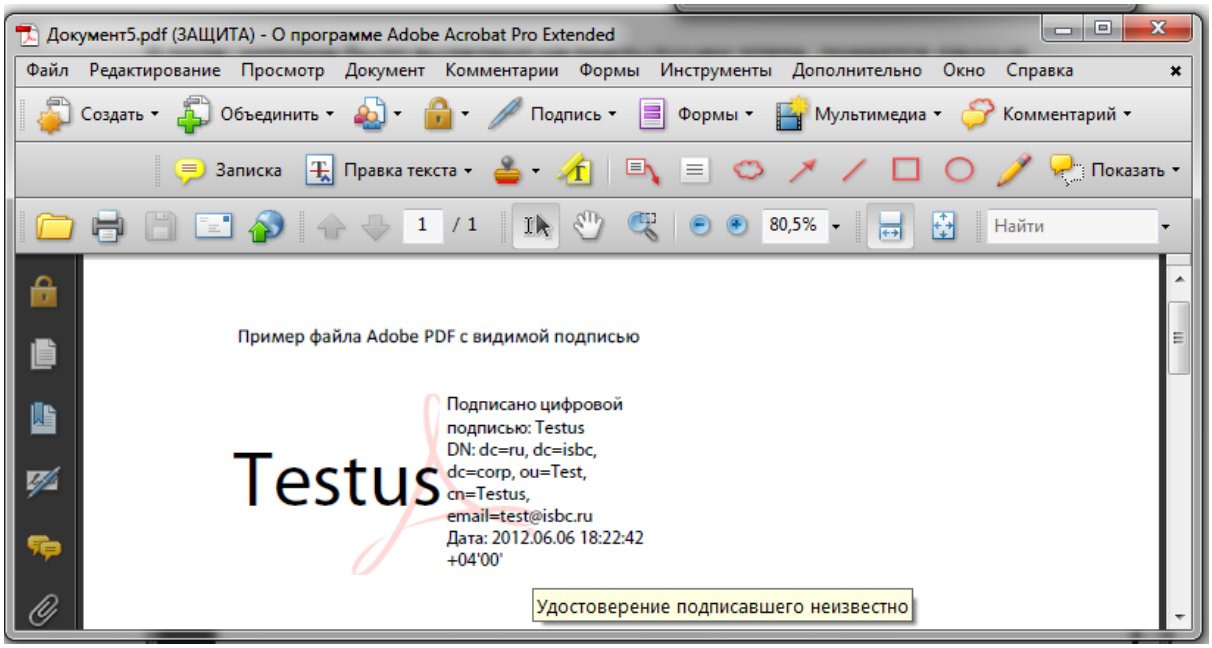
В появившемся окне выберите сертификат, вариант оформления и действия, которые сможет выполнять пользователь, когда документ будет подписан.

Выбрав необходимые опции, нажмите ***Подпись****:*





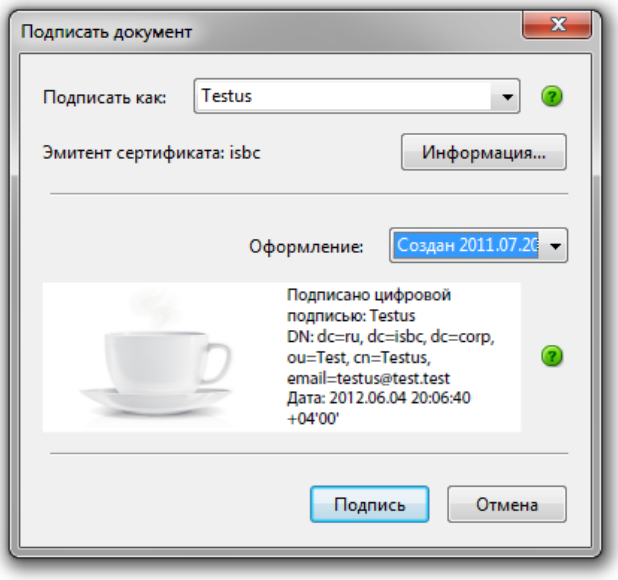
В поле, которое было выделено на предыдущем этапе, появятся данные электронной подписи.



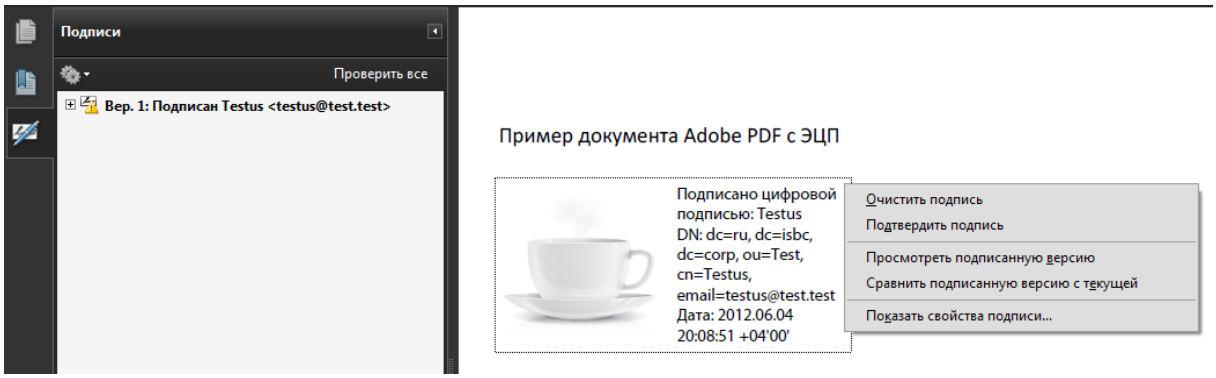
Подпись

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.

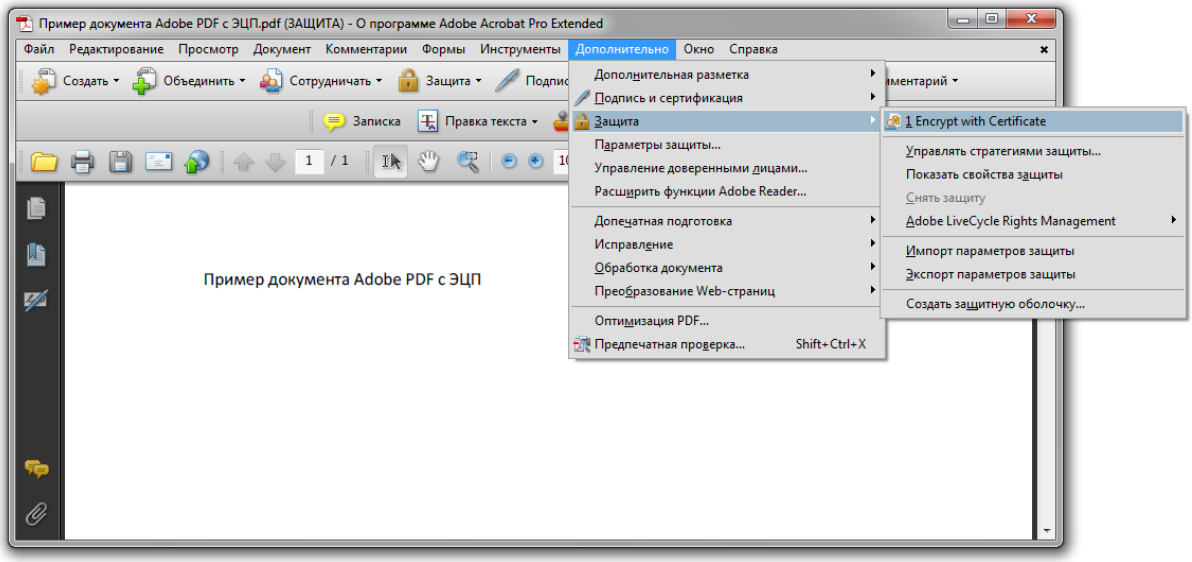


*Для изменения подписи, щелкните правой кнопкой мыши на поле подписи и выберите **Очистить подпись**. Там же можно подтвердить подпись или просмотреть информацию.*



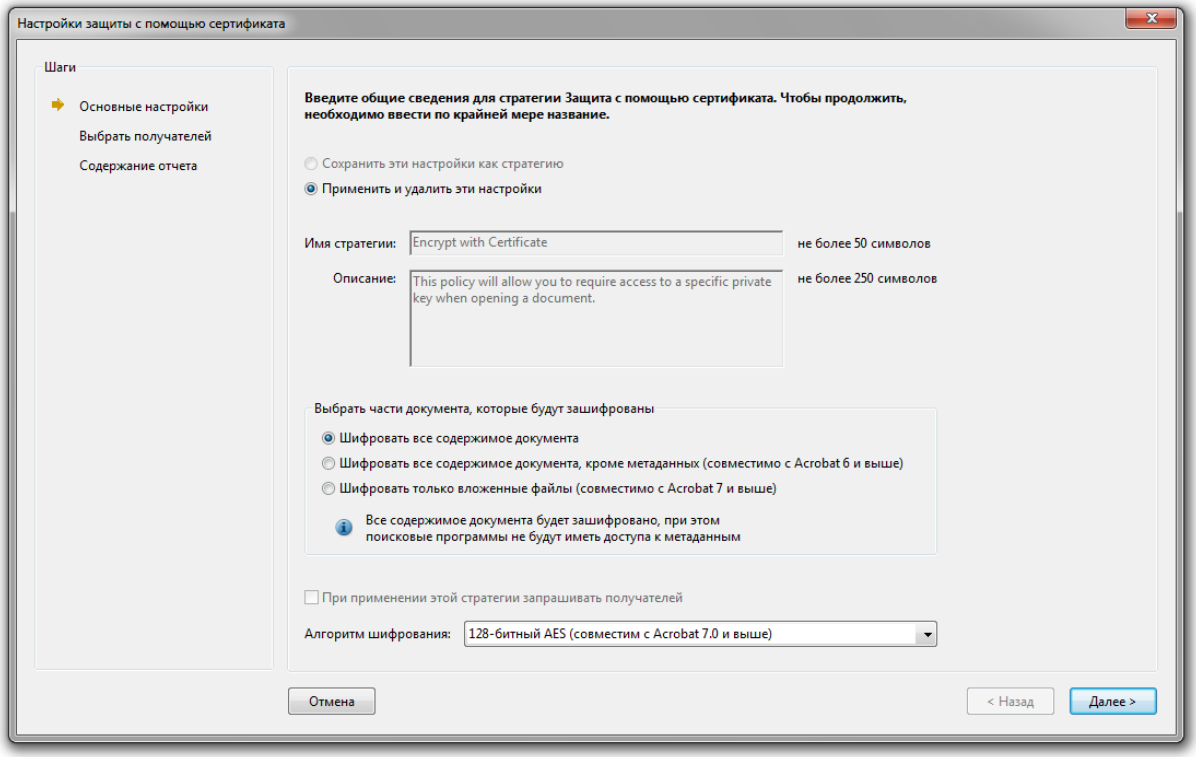
3.3 Шифрование документа PDF

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

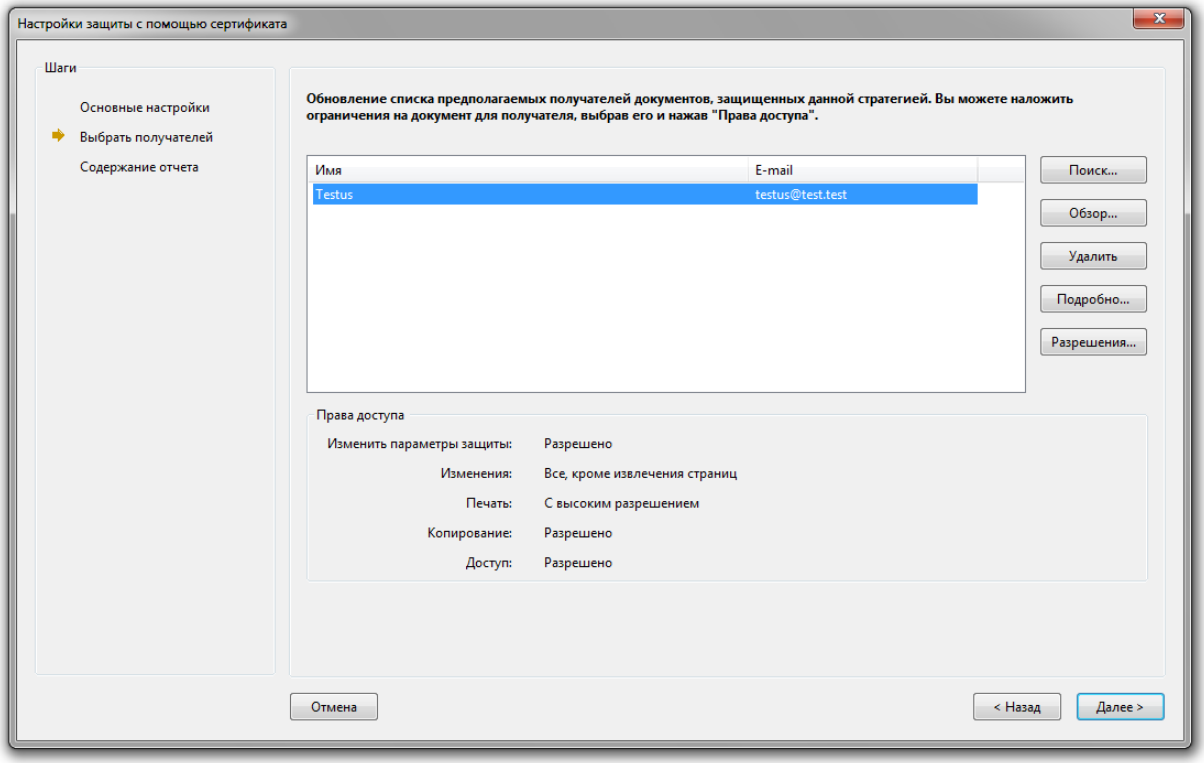


Появится окно с запросом на выполнение операции, его можно отключить. Подтвердите операцию.

*Выберите опции шифрования и нажмите **Далее***



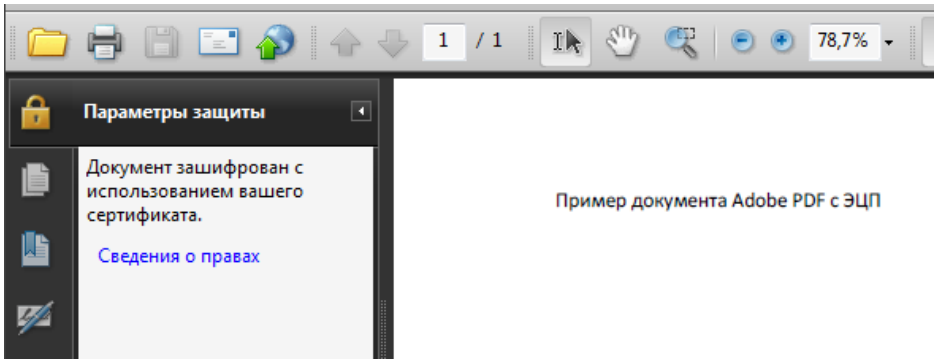
Выберите сертификаты предполагаемых получателей. В этом же окне можно задать определенные ограничения на работу с файлом, например, запретить определенным пользователям печать и изменение документа.



*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.



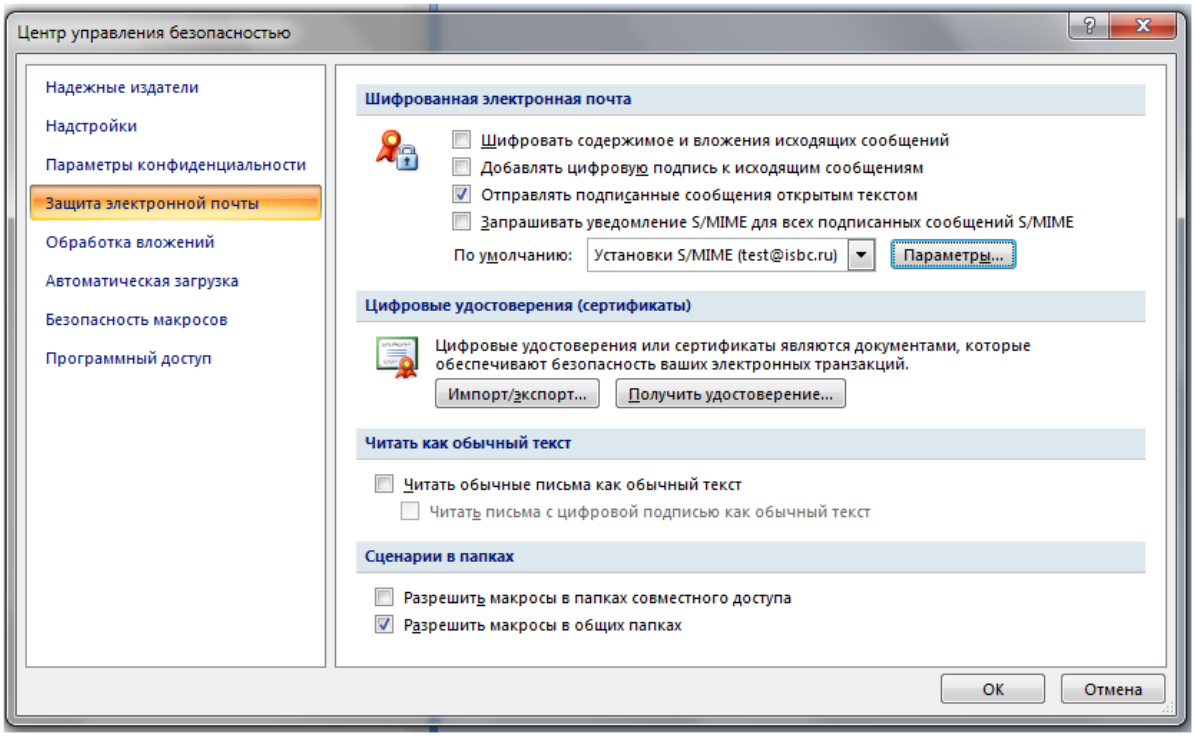
Список возможных проблем и методы их решения приведены в руководстве для администраторов ***ESMART Token – Настройка пользовательских приложений****.*

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

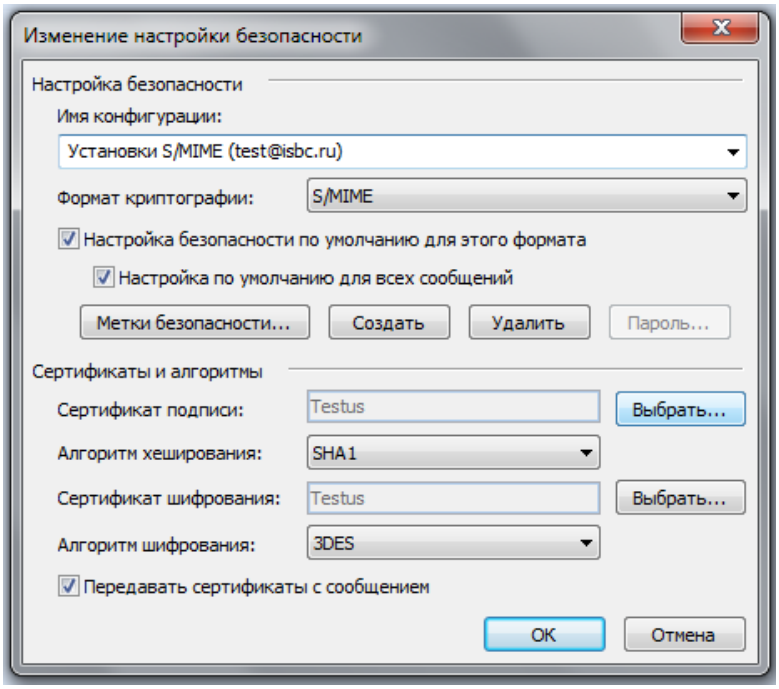
*Выберите в меню **Сервис › Центр управления безопасностью › Защита электронной почты**:*



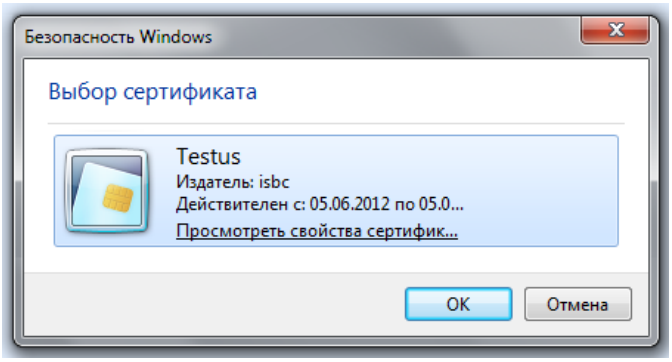
*Установите соответствующие галочки в разделе **Шифрованная электронная почта**, если хотите шифровать сообщения и использовать цифровую подпись по умолчанию для всех писем.*

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**.*



*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:*

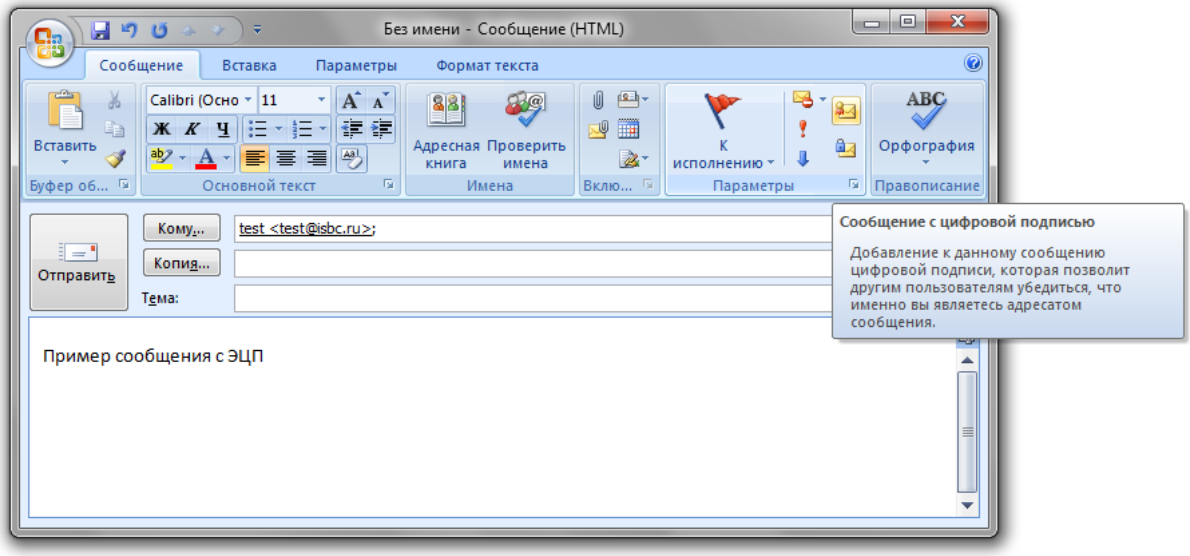


При необходимости измените используемые алгоритмы хэширования и шифрования.

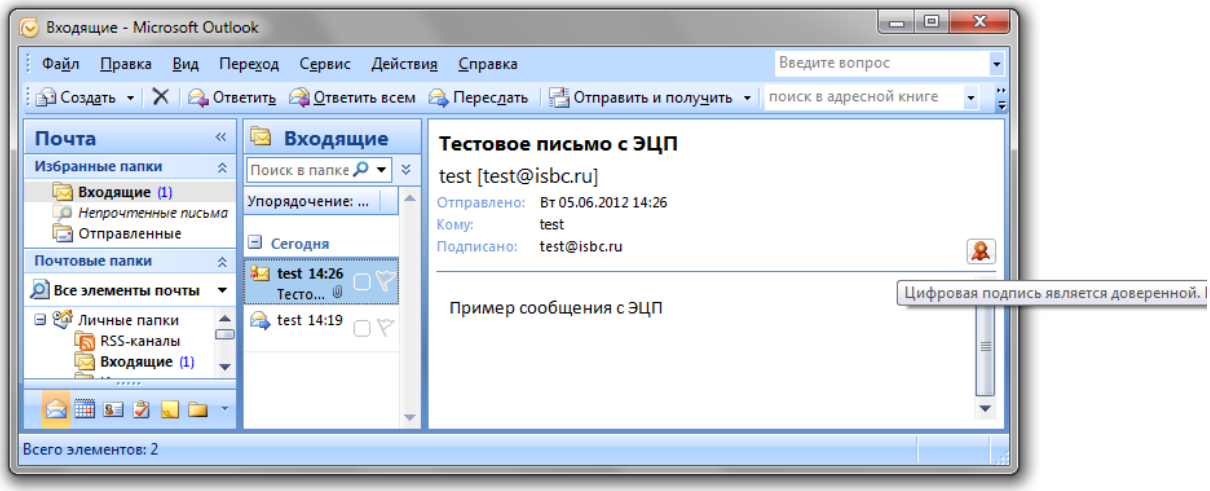
Предварительные настройки для использования шифрования и ЭЦП завершены.

4.2 Электронная подпись сообщения

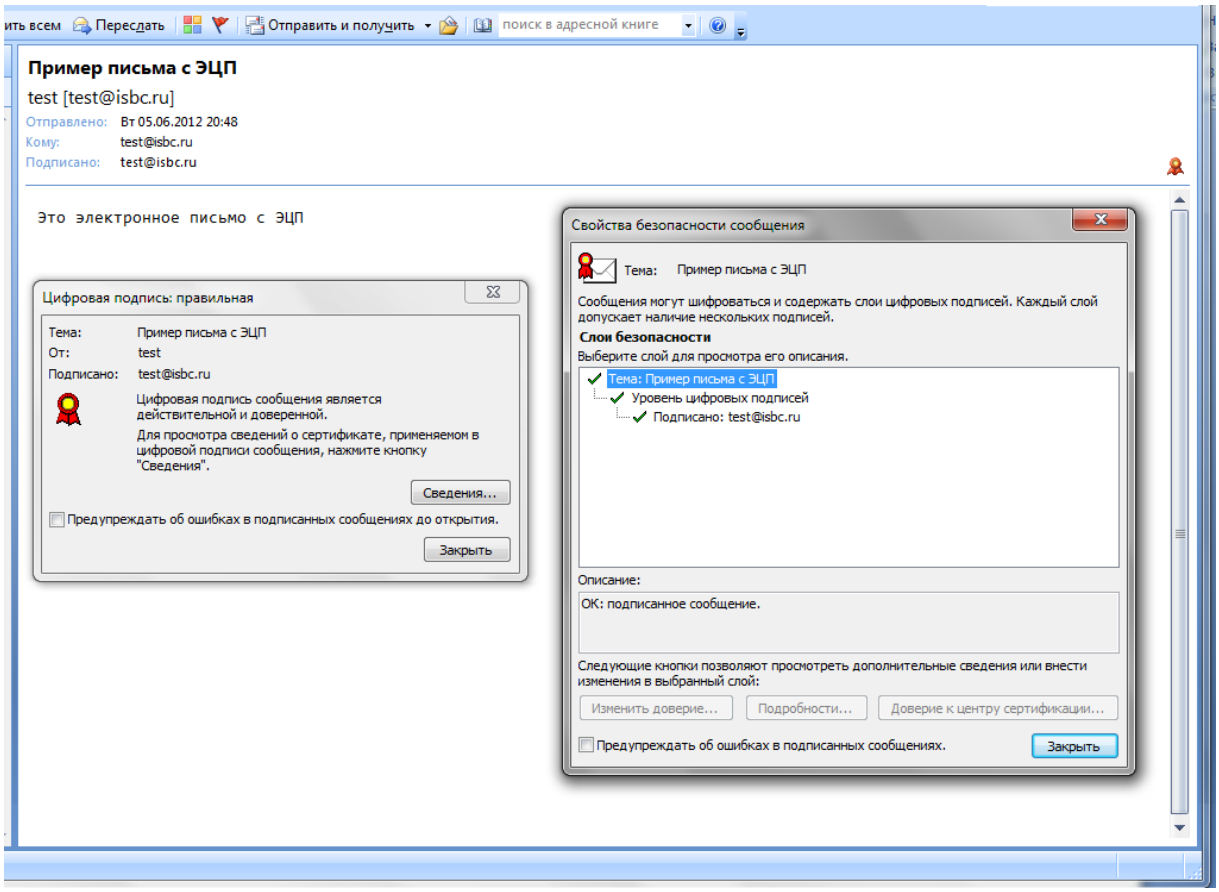
*Создайте сообщение. Кнопка с иконкой сертификата должна быть активна. (Если на этапе настройки было выбрано **Добавлять цифровую подпись к исходящим сообщениям**, при создании каждого письма кнопка будет активна по умолчанию).*



*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.*



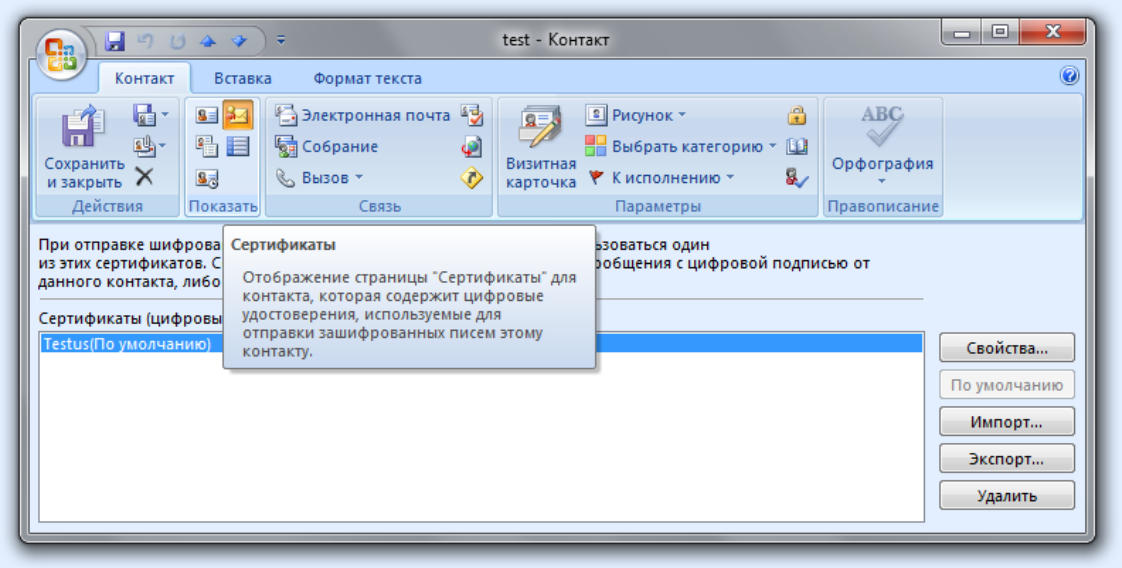
4.3 Шифрование

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.

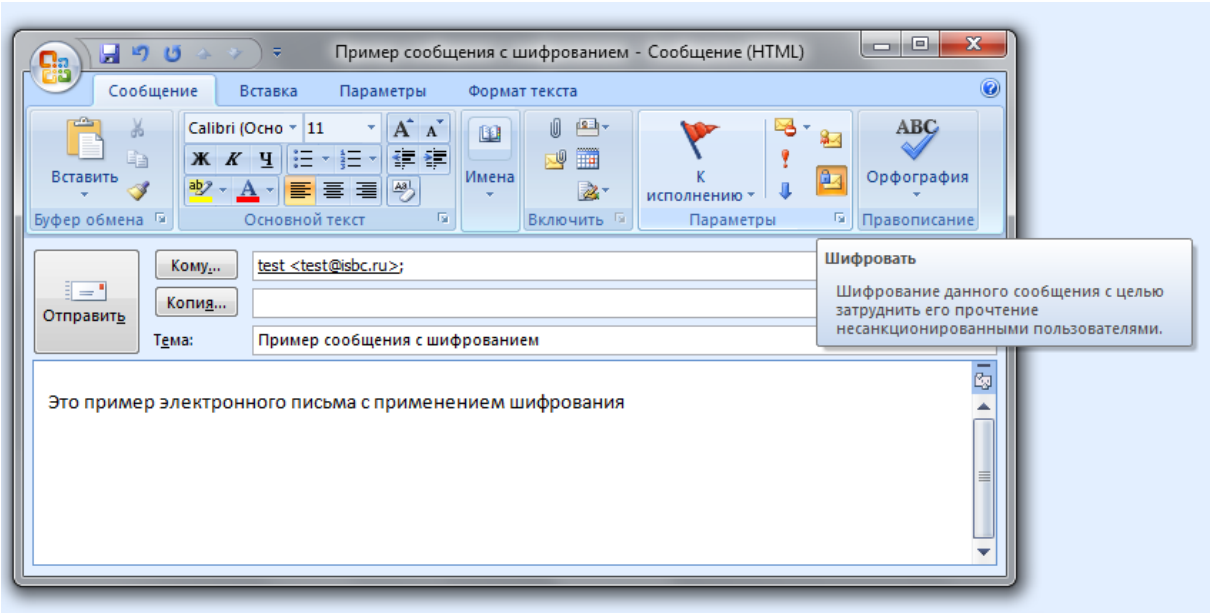
Другие способы обмена сертификатами описаны на сайте Microsoft:

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

В карточке контакта в разделе ***Сертификаты*** *будут перечислены доступные сертификаты.*



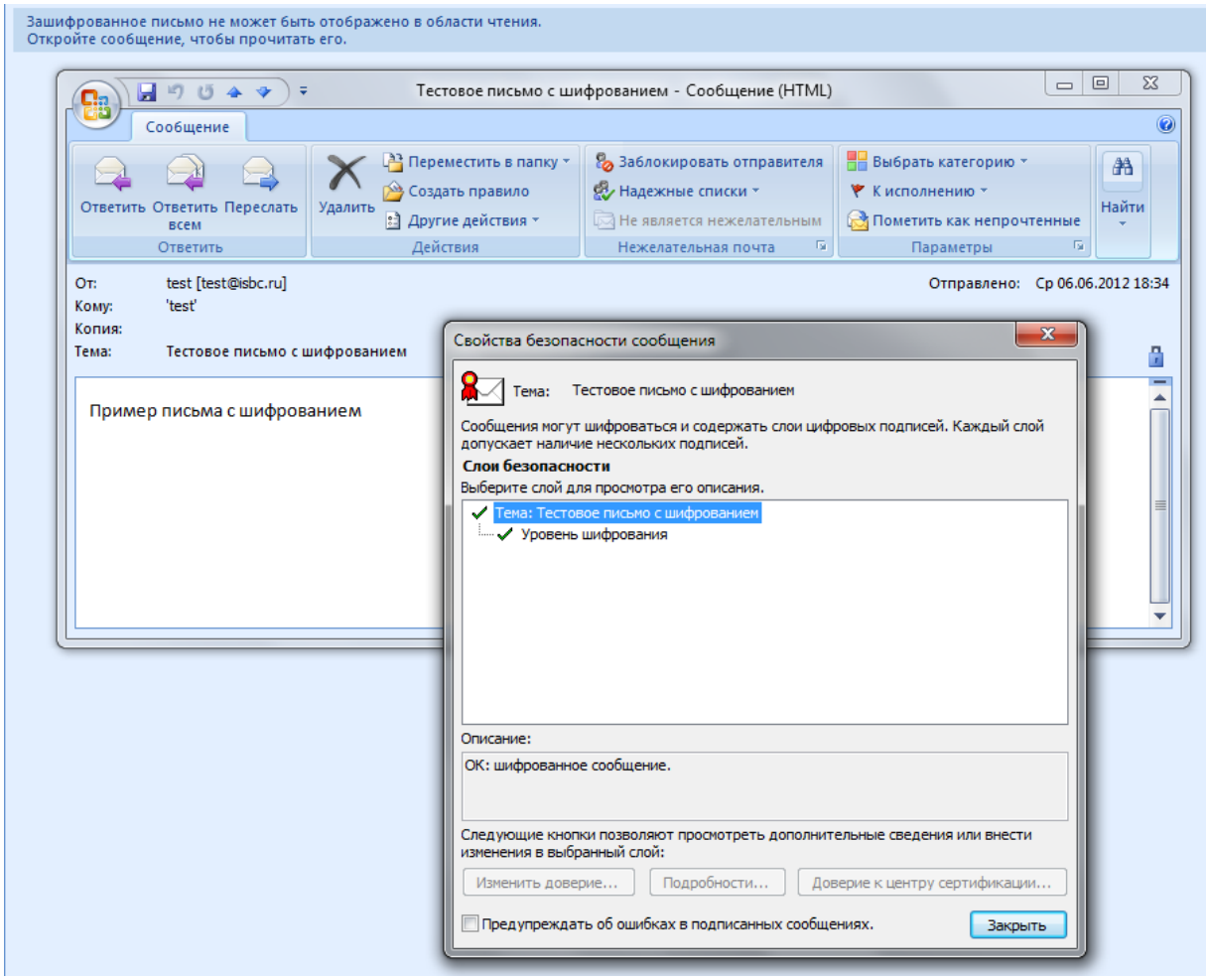
4.4 Составление сообщения



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.



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**.*

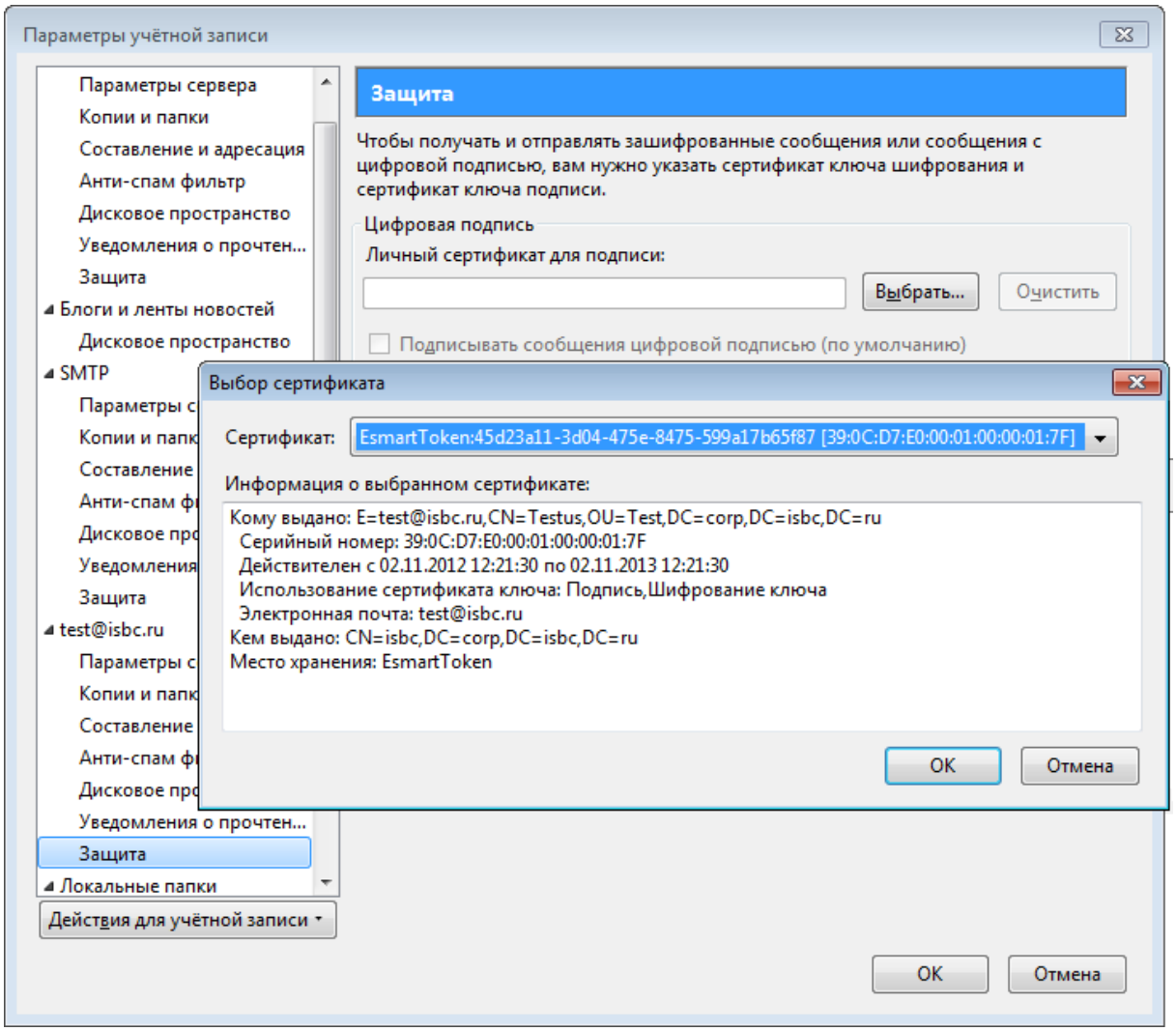
5.2 Настройка параметров учетной записи

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.

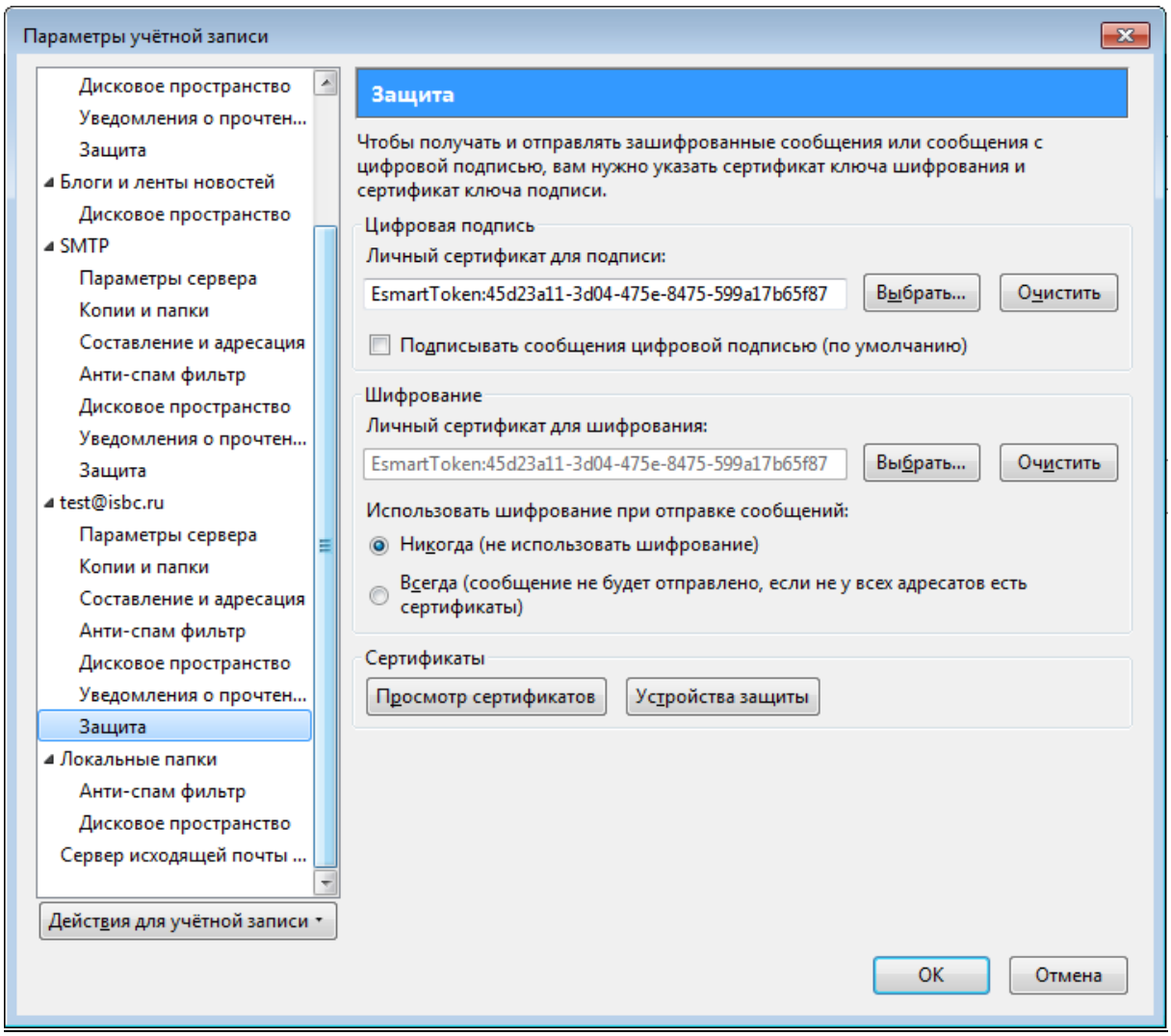
*Откройте **Инструменты › Параметры учетной записи › Защита**:*



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.

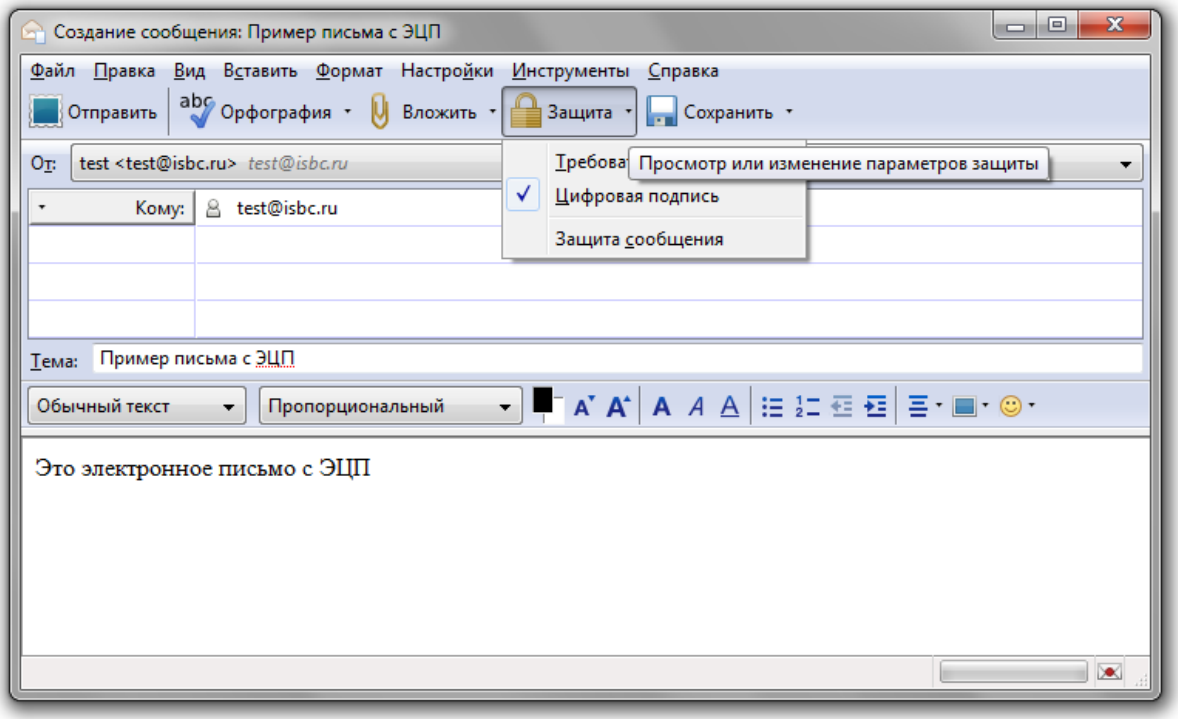
Нажмите ***Выбрать*** *и укажите нужный сертификат (может быть доступно несколько сертификатов).*



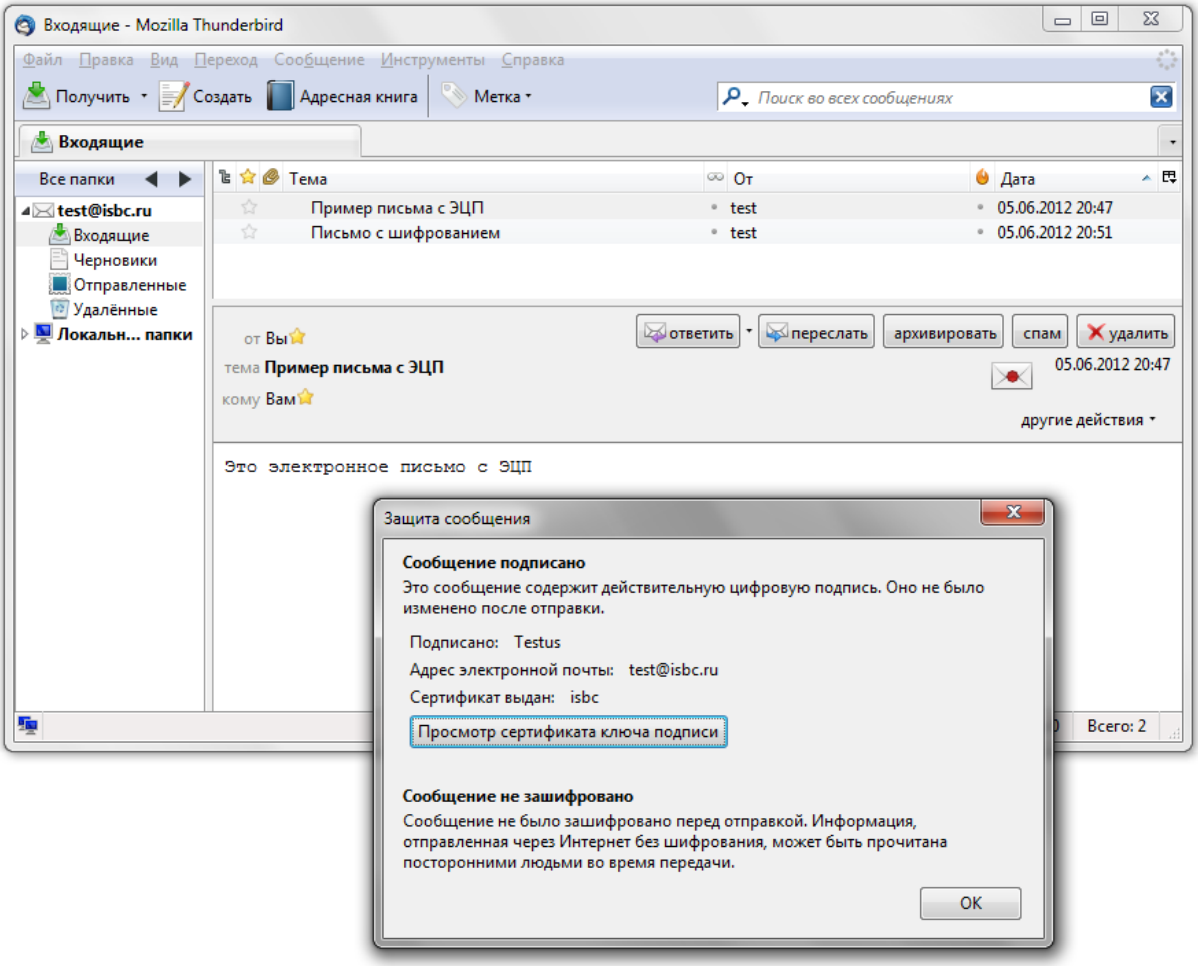
Настройки учетной записи завершены. Повторите процедуру для каждой учетной записи.

5.3 Электронное письмо с ЭЦП

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

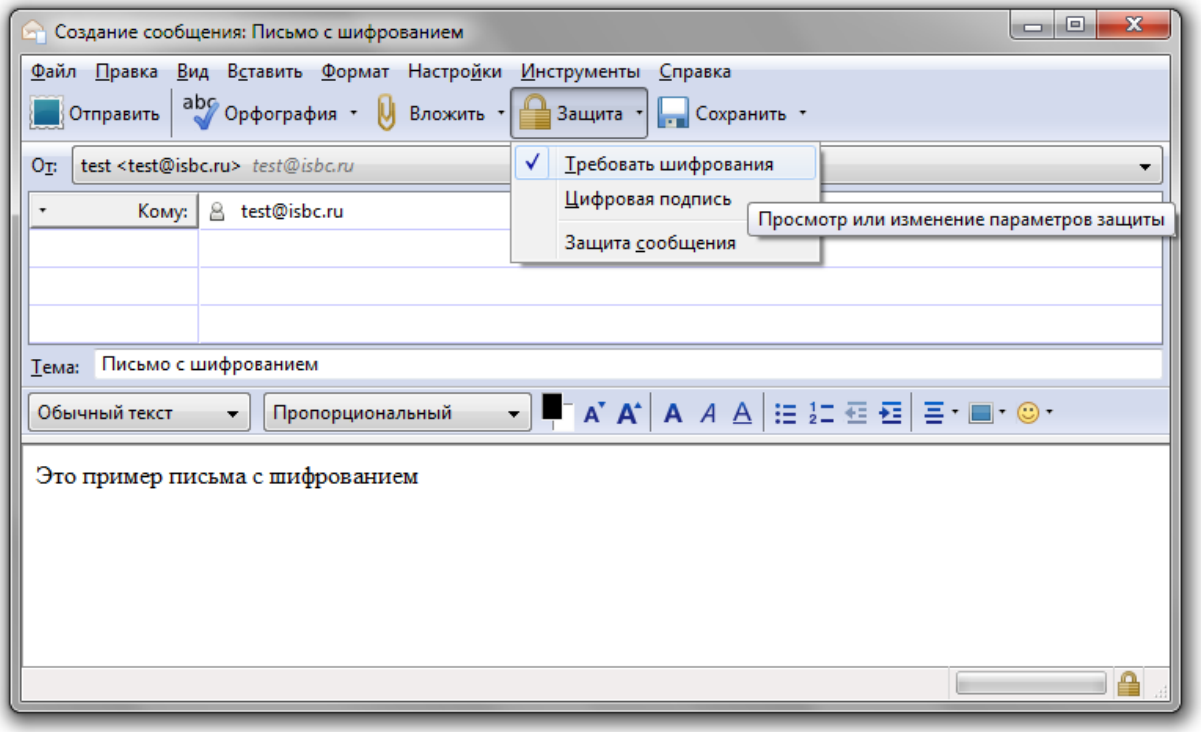


Принятое письмо с ЭЦП будет выглядеть следующим образом (для просмотра информации о подписи нажмите на значок конверта):



5.4 Шифрование электронной почты

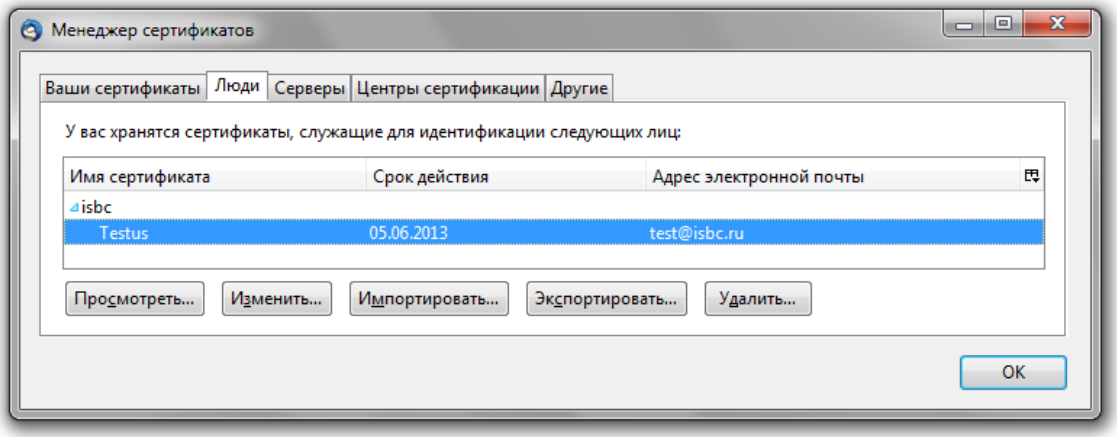
*Для отправки зашифрованного сообщения отметьте опцию **Требовать шифрования**.*



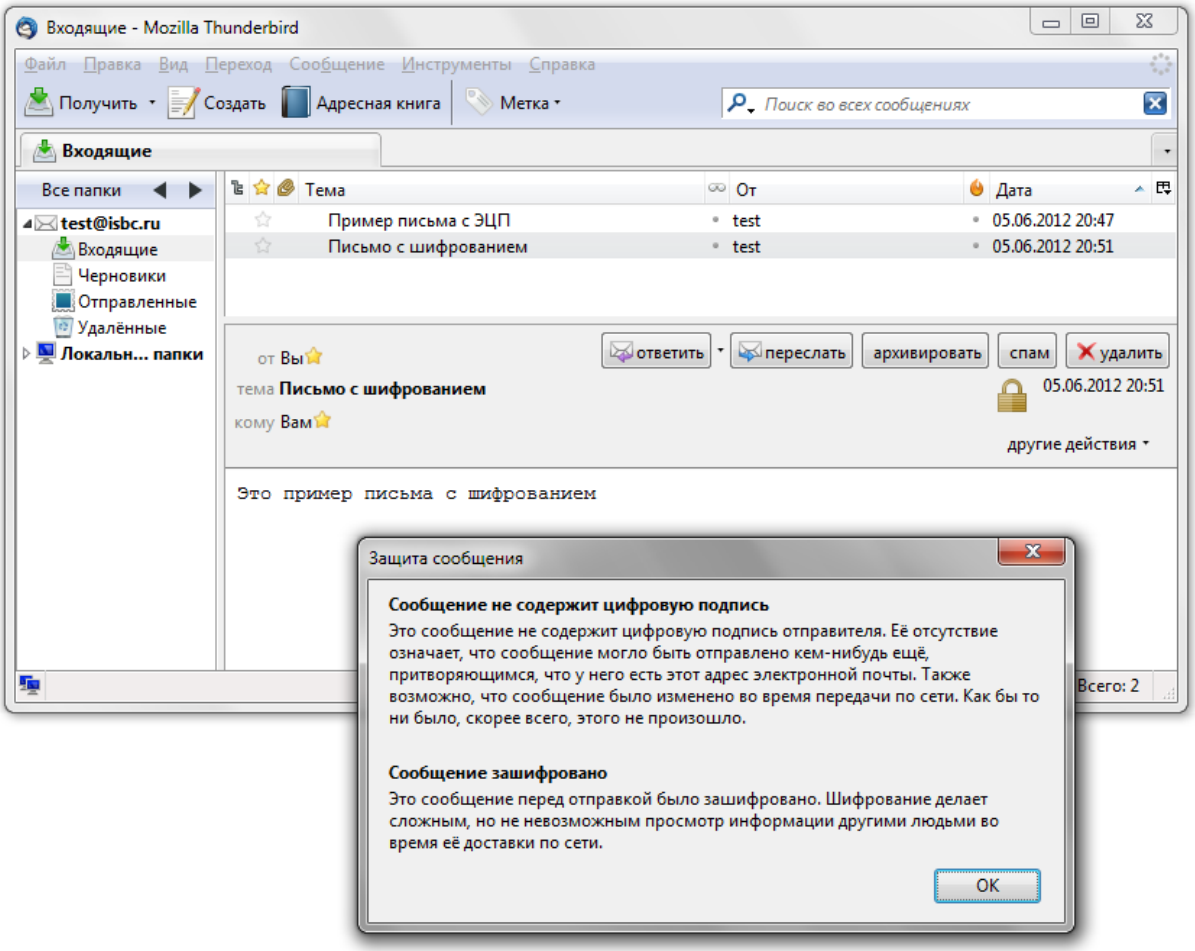
Чтобы получатель зашифрованного сообщения смог его открыть и прочесть, необходимо предварительно обменяться сертификатами с открытыми ключами.

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.*



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

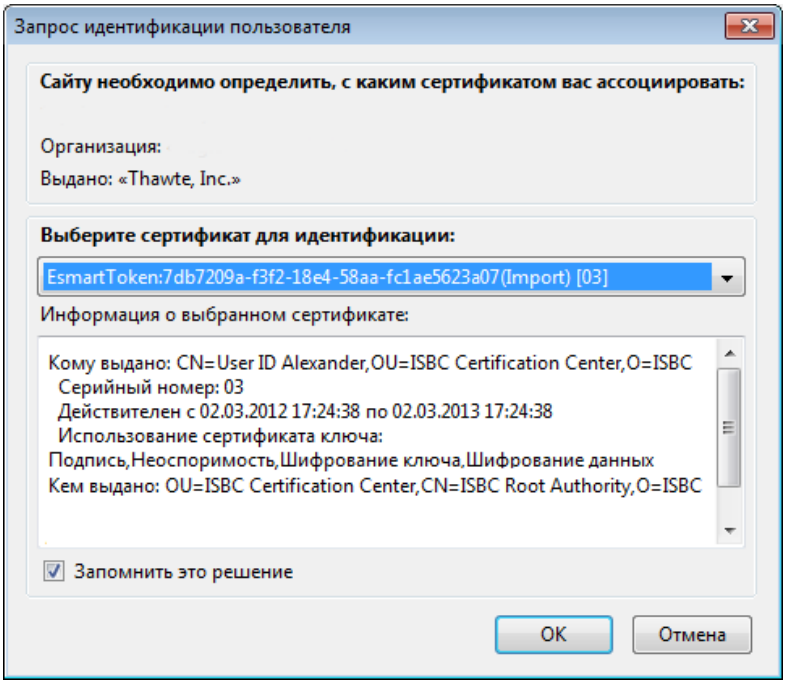
Браузер Mozilla Firefox может использоваться для организации доступа к корпоративным сайтам и отдельным разделам сайта по сертификату, т.е. чтобы получить возможность доступа на сайт пользователь должен предъявить сертификат на ESMART Token и ввести верный ПИН-код.

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****.*



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