

Инструкция по первичной настройке использования ключей электронной подписи «УЦ Крымсвязь»

1. Термины и сокращения

Подлинник электронного документа - документ, подписанный электронной подписью, созданный изначально в формате электронного документа и не имеющий бумажного исходного подлинника;

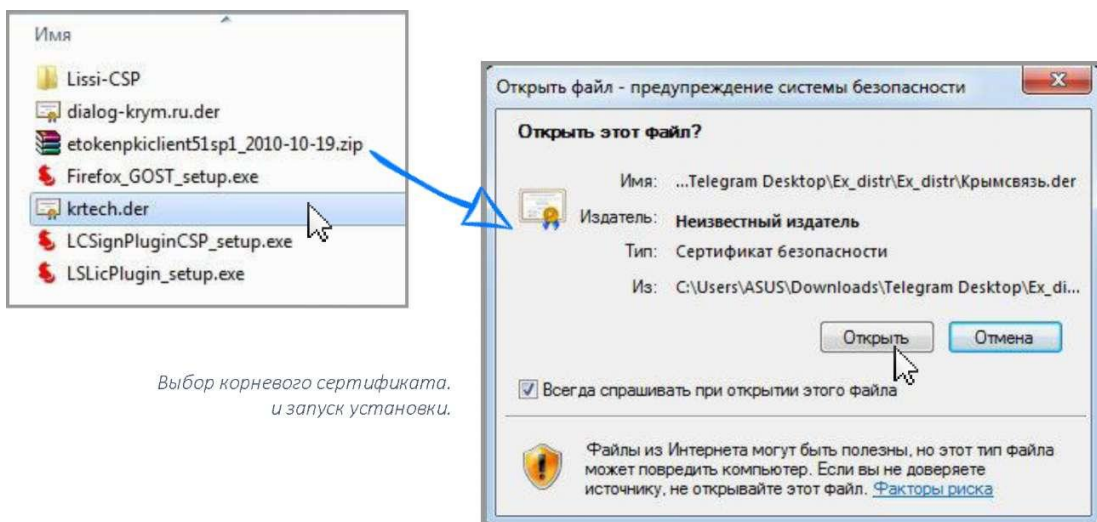
Реквизит документа - элемент оформления документа, придающий ему юридическую силу;

ЭП - электронная подпись, реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

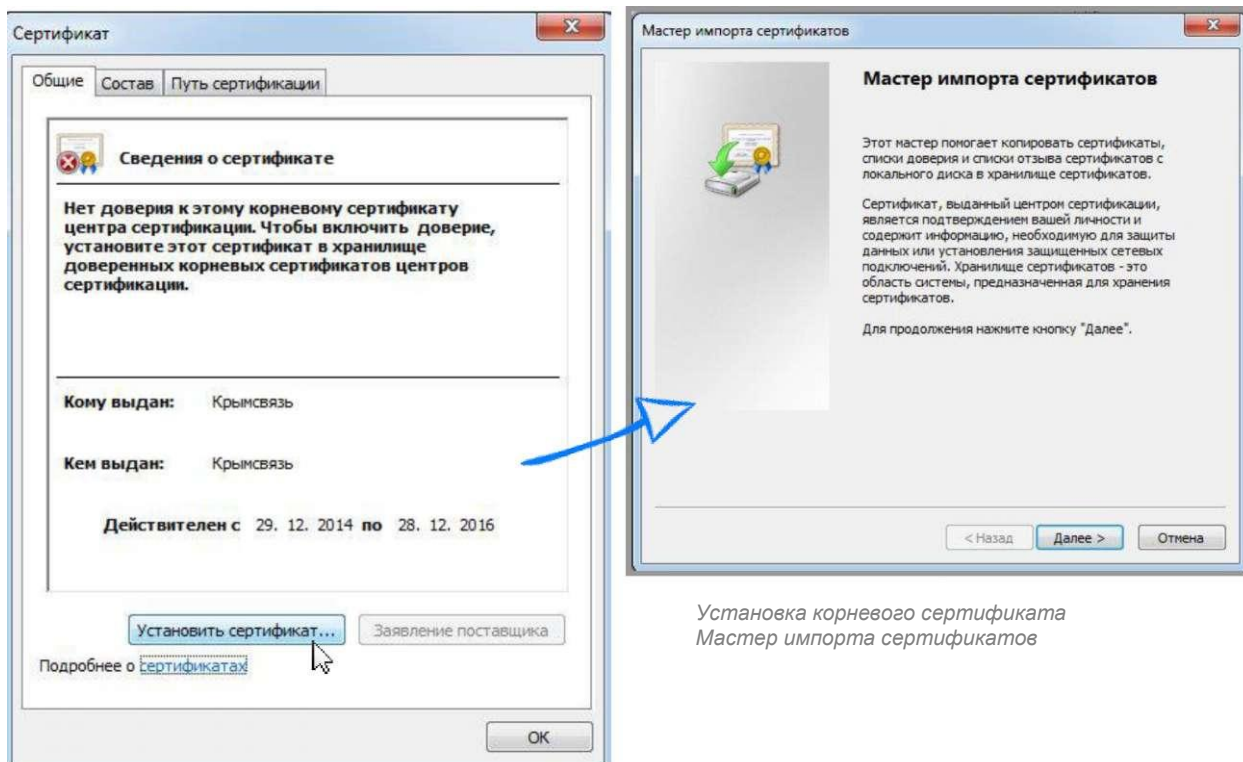
2. Добавление корневых сертификатов удостоверяющего центра

С переносного носителя переместите или скачайте по ссылке http://krtech.ru/work/certification_authority/ корневые сертификаты: GUC_root; GUC_cross; УЦ Крымсвязь.

Двойным кликом начните установку сертификата.

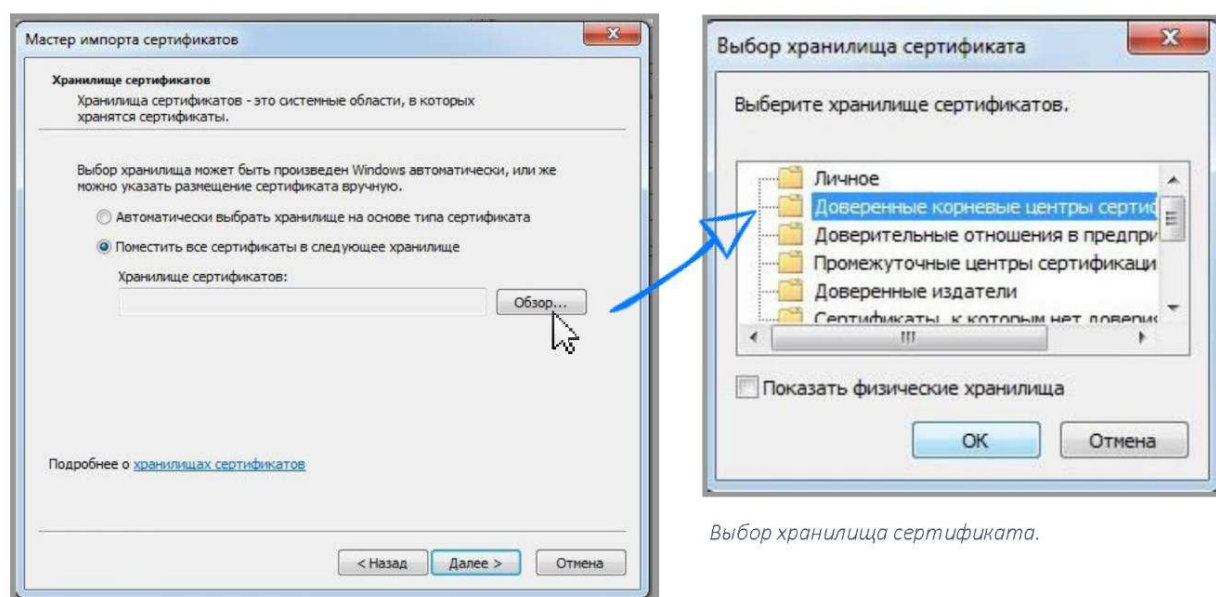


*Выбор корневого сертификата,
и запуск установки.*



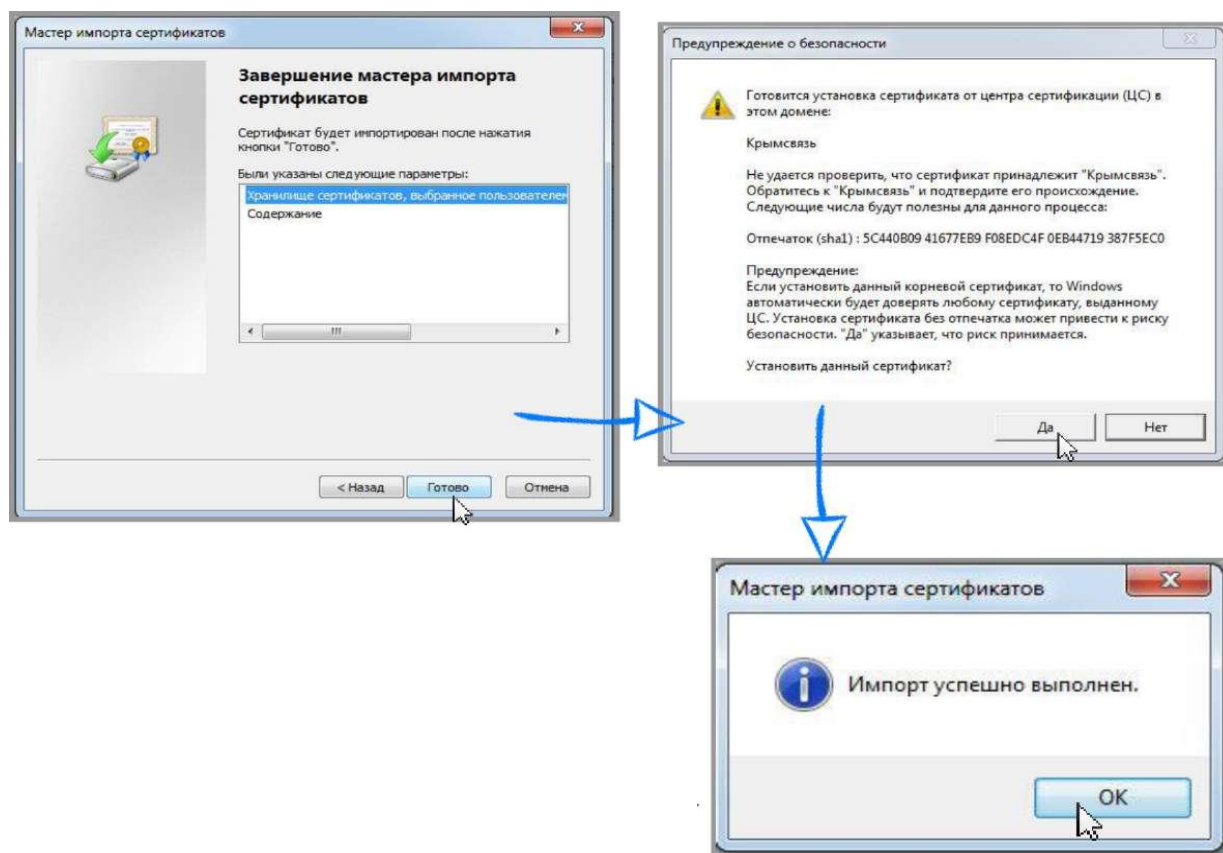
Установка корневого сертификата
Мастер импорта сертификатов

В модальном окне выберите «Установить сертификат». Для продолжения установки, в первом модальном окне ознакомьтесь с информацией и нажмите кнопку «Далее». Выберите маркер «Поместить все сертификаты в следующее хранилище» и выберите хранилище с помощью кнопки «Обзор». Выберите из списка «Доверенные корневые центры сертификации» и нажмите «Ок».



Выбор хранилища сертификата.

В следующем модальном окне нажмите «Готово», после чего подтвердите установку сертификата и закройте окно мастера импорта сертификата, нажав на кнопку «Ок».



Завершение импорта сертификатов

Описанную процедуру проделайте со всеми корневыми сертификатами.

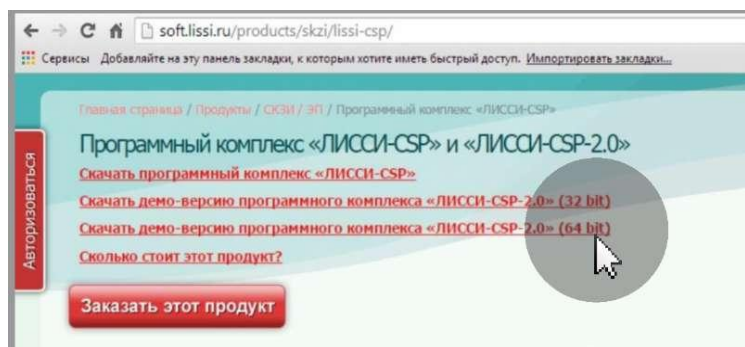
3. Установка браузера Firefox Gost

Для установки браузера Firefox Gost запустите предоставленный вам файл «Firefox_GOST_setup.exe», и выполните установку с параметрами по умолчанию.

При запуске браузера на запрос программного токена введите мастер пароль для доступа 01234567.

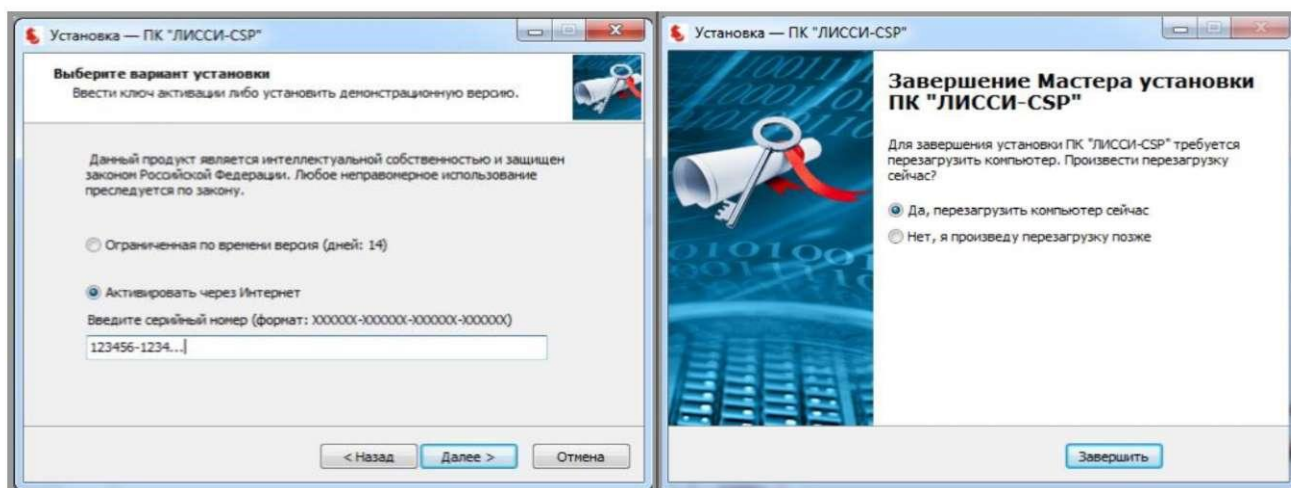
4. Программное обеспечение шифрования данных

Для работы в системе требуется установка программного комплекса «ЛИССИ- CSP-2.0» для обеспечения криптографической защиты информации при работе с данными через web-интерфейсы.



Для установки программы запустите предоставленный «LISSI-CSP-2.0-Setup-win32.exe» или «LISSI-CSP-2.0-Setup-x64.exe» (в зависимости от разрядности вашей операционной системы), при его отсутствии в адресной строке браузера наберите адрес <http://soft.lissi.ru/products/skzi/ligsi-csp/>, перейдите на указанную страницу и скачайте необходимый продукт, в соответствии с типом вашей операционной системы.

Запустите программу установки. В открывшемся окне выберите вариант установки «Активировать через интернет» и введите серийный номер, полученный от администратора системы и нажмите «Далее». В процессе установки, программа запрашивает подтверждение действий. Отвечайте утвердительно на все запросы.



Завершение установки программы.

Последним окном программы установки является предупреждение о необходимости перезагрузки компьютера. Ответьте утвердительно и нажмите кнопку «завершить». Компьютер будет перезагружен и после этого готов к работе.

Так же установите плагины «LCSignPluginCSP_setup.exe», и «LSLicPlugin_setup.exe».

После установки необходимо включить плагины в настройках браузера. Запустите Firefox Gost 35, нажмите кнопку «Открыть меню», в правом верхнем углу выберите пункт меню «Дополнения» и перейдите на вкладку «Плагины». Найдите в списке плагины «LCSignCSPPlugin» и «LSLicPlugin» и присвойте им статус «Всегда включать».

5. Работа с защищенным носителем

Для осуществления работы с защищенным носителем eToken необходимо установить «eToken PKI Client», подходящий для Вашей системы. Дистрибутивы для установки расположены в архиве etokenpkiclient51sp1.zip на предоставленном вам носителе.

6. Устранение неисправностей

6.1. Блокировка программного токена

Если при запуске Mozilla_Firefox_GOST после ввода PIN-кода для программного токена LS11SW2012 модальное окно «Требуется пароль» не закрывается, значит была произведена блокировка программного токена LS11SW2012. Блокировка происходит в случае четырех (4) попыток ввода неправильного PIN- кода токена. Для устранения неисправности удалите из системы программный токен LS11SW2012, содержащий ошибку.



Для удаления токена, найдите каталог (папку) с названием LS11SW. Для этого используйте поиск по файловой системе вашего компьютера. Поиск можно произвести в соответствующей строке меню «Пуск» или использовать поле поиска проводника.



Когда соответствующие папки будут найдены на вашем компьютере, удалите их с помощью комбинации клавиш Shift+Delete.

Для завершения процесса необходимо осуществить повторную установку Mozilla_Firefox_GOST и перезагрузить компьютер.

6.2. Блокировка программно-аппаратного носителя eToken

В случае если при попытке доступа к eToken система выдает сообщение о блокировке носителя Вам необходимо обратиться в техническую поддержку удостоверяющего центра «УЦ Крымсвязь» для осуществления разблокировки ключевого носителя.

6.3. Иные сообщения об ошибках

В случае других сообщений об ошибках, не описанных в данной инструкции, обращайтесь в техническую поддержку «УЦ Крымсвязь» по контактному телефону +79780000474 или по адресу эл. почты: uc@krtech.ru.