TRUSTED eSIGN

Руководство пользователя

Версия выпуска 1.2.0

ОГЛАВЛЕНИЕ

Общие сведения о программном продукте

Trusted eSign - это универсальное приложение с графическим пользовательским интерфейсом для выполнения операций по созданию и проверке электронной подписи файлов, шифрования и расшифрования, управления сертификатами, размещенных в хранилищах криптопровайдеров[1].

Приложение Trusted eSign является кроссплатформенным, и представлено различными установочными дистрибутивами под платформы: Microsoft Windows, Linux, OSX. На каждой из платформ реализована поддержка российских криптографических стандартов (в том числе ГОСТ Р 34.10-2012) посредством использования криптопровайдера КриптоПро CSP.

В приложении поддерживается работа с ключевыми носителями Рутокен и JaCarta через криптопровайдер КриптоПро CSP.

Приложение Trusted eSign включено в реестр отечественного ПО как прикладное программное обеспечение общего пользования и отнесено к категории «Средства обеспечения информационной безопасности».

ФУНКЦИОНАЛЬНОСТЬ ВЕРСИИ 1.2.0

Приложение текущей версии рассчитано на выполнение операций:

Электронная подпись	– электронная подпись произвольных файлов на поддерживаемых платформах; – добавление электронной подписи к уже существующим (функция установки соподписи); – создание как присоединенной, так и отделенной электронная подписи; – поддержка стандарта электронной подписи ГОСТ Р 34.10-2012.
Шифрование	– шифрование и расшифрование файлов на поддерживаемых платформах; – удаление исходного файла после шифрования; – шифрование данных по стандарту PKCS#7/CMS.
Управление сертификатами и ключами	– отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых криптопровайдеров; – проверка корректности выбранного сертификата с построением цепочки доверия и скачиванием актуального списка отзыва; – хранение закрытых ключей на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.) при условии использования криптопровайдера КриптоПро CSP.

[1] Криптопровайдер (Cryptography Service Provider, CSP) — это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах MS Windows, Linux, OSX, управление которым происходит с помощью функций CryptoAPI. В качестве примера, устанавливаемого криптопровайдера (помимо системных), служит криптопровайдер КриптоПро CSP.

Поддерживаемые криптопровайдеры

Приложение работает с системными криптопровайдерами на платформе MS Windows через Crypto API. На платформах Linux и OSX реализовано собственное хранилище криптографических объектов (сертификатов и ключей), работа с которым не отличается от аналогичных решений.

Для корректной работы с ГОСТ алгоритмами требуется установка криптопровайдера КриптоПро CSP. В приложении осуществляется поддержка КриптоПро CSP версий 3.9, 4.0 и 5.0.

Лицензия на программный продукт

Для полнофункциональной работы приложения требуется приобретение и установка лицензии. Без установки лицензии на операции: установления TLS соединения, доступа к закрытому ключу при операциях подписи и расшифрования, и т.д. будут наложены ограничения.

Для приобретения лицензии на программный продукт Trusted eSign v.1.2.0 можно обратиться в компанию разработчика приложения. Контактные данные компании представлены в разделе 8.

Доля использования OpenSource проектов

При разработке программного продукта были использованы OpenSource проекты:

- В качестве браузера для воспроизведения графического интерфейса пользователя был использован проект **Electron** (https://github.com/electron/electron), версии 1.6.6. В проект были внесены изменения для получения требуемой функциональности.
- Для работы с криптографическими объектами (в т.ч. с различными хранилищами) используется нативный модуль для Electron OpenSource проекта **Crypto** (https://github.com/TrustedPlus/crypto).
- Графический интерфейс реализован с помощью React.js и представлен OpenSource проектом **eSign** (https://github.com/TrustedPlus/esign).
- Расширения OpenSSL для тесной интеграции с провайдером КриптоПро CSP представляют коммерческий интерес и не распространяются как проект OpenSource.

Системные требования

Для приложения сформулированы минимальные системные требования к конфигурации оборудования под платформами:

Windows

- Процессор Intel Core 2 Duo, Core i3, Core i5, Core i7 или Xeon (64 - бита), поддержка CMPXCHG16b, PrefetchW, LAHF/SAHF и SSE2;
- 2Gb оперативной памяти;
- 150 Mb дискового пространства для установки и работы приложения;
- Видеоадаптер DirectX версии не ниже 9 с драйвером WDDM 1. Должно поддерживаться минимальное разрешение 800x600.

Mac

- Процессор Intel Core 2 Duo, Core i3, Core i5, Core i7 или Xeon (64 - бита);
- 2Gb оперативной памяти;
- 150 Mb дискового пространства для установки и работы приложения;
- требование к видеоадаптеру не критично. Должно поддерживаться минимальное разрешение 800x600.

Linux

- Двухъядерный процессор с частотой 1,6GHz и мощнее - Unity, Gnome, KDE.
- 2Gb оперативной памяти;
- 150 Mb дискового пространства для установки и работы приложения;
- требование к видеоадаптеру не критично. Должно поддерживаться минимальное разрешение 800x600.

Поддерживаемые операционные системы

Каждая выпускаемая версия программного продукта тестируется на работоспособность заявленного функционала на операционных системах:

- Microsoft Windows 7 64bit.
- Microsoft Windows 10 64bit/32bit.
- Ubuntu 14.04 64bit/32bit.
- Ubuntu 16.04 64bit/32bit.
- CentOS 7.0 64bit/32bit.
- Rosa Fresh R8 64bit/32bit.
- Rosa Fresh R9 64bit/32bit.
- Rosa Enterprise Desktop (RED) X3 64bit.
- Гослинукс 6.4 64bit.
- Astra Linux Common Edition 64bit.
- Astra Linux Special Edition 64bit.
- Ось 2.1 64bit.
- ALT Linux 7.0 Centaurus 64bit/32bit.
- Mac OS X 10.10, 10.11, 10.12 (64 bit).

Не исключается возможность работы приложения на других платформах, не входящих в представленный выше перечень. Но следует учесть, что для работы с ГОСТ алгоритмами необходима установка криптопровайдера КриптоПРО CSP на выбранную платформу. Тестирование корректности работы приложения на иных платформах возлагается на самого пользователя. Для этих целей можно обратиться в компанию разработчика приложения и запросить временный лицензионный ключ.

1. Установка программного продукта

1.1. Установка на платформу Microsoft Windows

Для установки приложения Trusted eSign на платформу Microsoft Windows предлагаются два дистрибутива – под 64-битную и 32-битную платформы. В зависимости от выбранной разрядности запустите на исполнение файл:

Trusted-eSign_vx.x.x_x64.exe (где x.x.x – номер версии) для 64-разрядной ОС;

Trusted-eSign_vx.x.x_x32.exe (где x.x.x – номер версии) для 32-разрядной ОС).

Откроется мастер установки приложения Trusted eSign, начальный шаг которого представлен на рис.1.1.1.

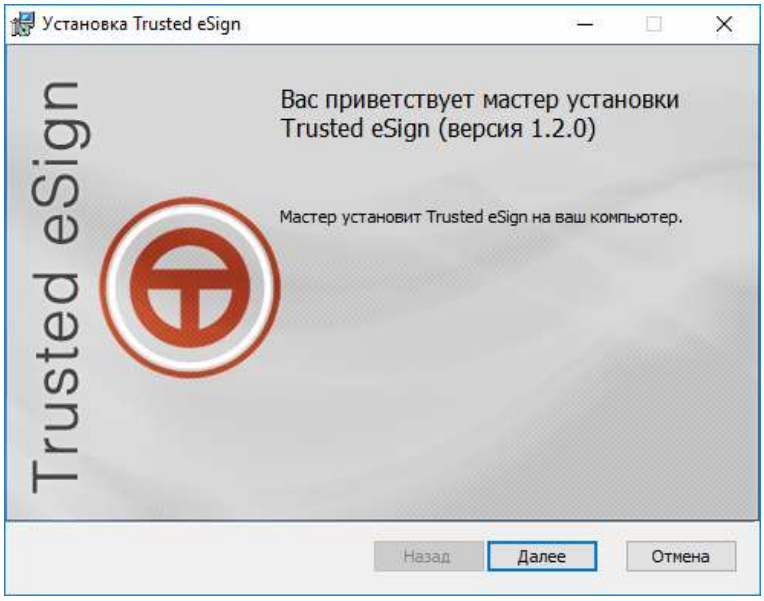


Рис.1.1.1. Начальный шаг мастера установки приложения

На следующем шаге мастера предлагается ознакомиться с условиями лицензионного соглашения (рис.1.1.2), и в случае согласия принять условия и перейти к следующему шагу мастера, нажав кнопку **Далее**.

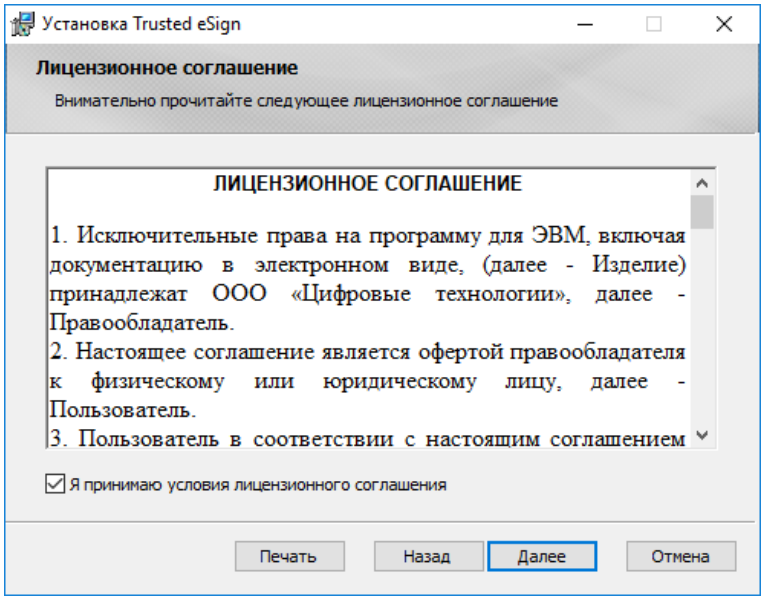


Рис.1.1.2. Условия лицензионного соглашения

На следующем шаге мастера выберете каталог для установки Trusted eSign (по умолчанию приложение устанавливается в каталог C:\Program Files\Trusted eSign\) и нажать **Далее** (рис.1.1.3). На шаге выборочной установки для текущей версии продукта не предлагается никаких дополнительных компонент.

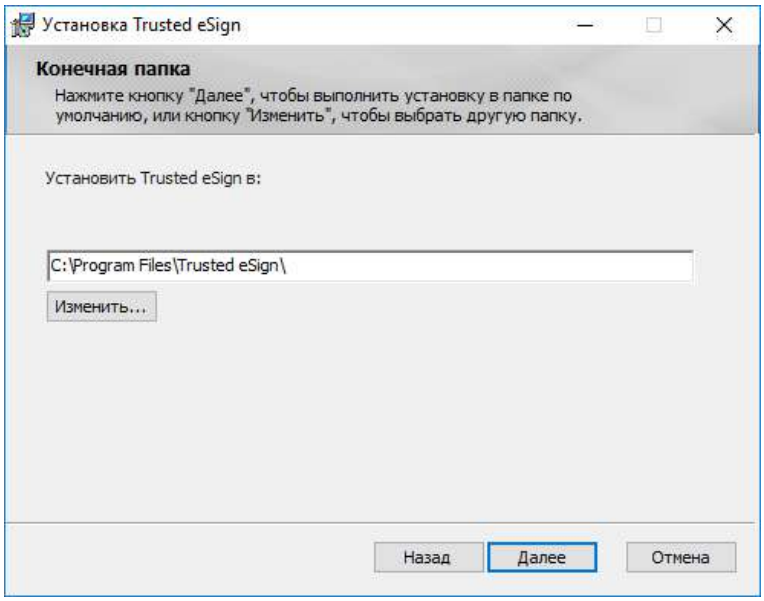


Рис.1.1.3. Выбор каталога установки приложения

На заключительном шаге мастера нажмите кнопку **Установить** (рис.1.1.4). Установка выполняется с правами администратора.

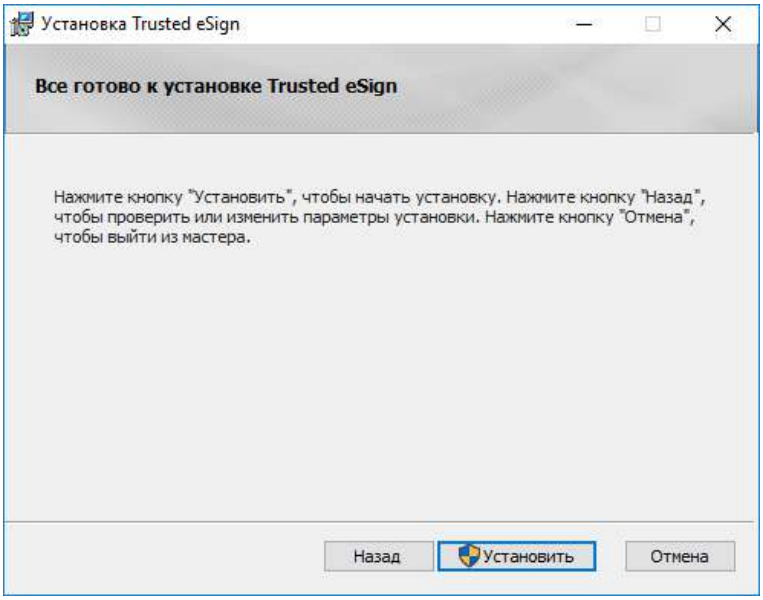


Рис.1.1.4. Выбор каталога установки приложения

После успешной установки приложения в главном меню появится новая группа Trusted eSign, которая содержит ярлык запуска приложения Trusted eSign и ярлык запуска мастера удаления программы. В указанном при установке каталоге (по умолчанию - каталог Program Files/Trusted eSign) будут размещаться файлы приложения Trusted eSign.

1.2. Установка на платформу Linux

Установка приложения Trusted eSign на операционную систему Linux может быть выполнена в графическом режиме (через мастер установки пакетов), через терминал в режиме командной строки и обычной распаковкой из архива. По умолчанию приложение устанавливается в каталог /opt/trustedesign/.

- В режиме графической установки приложения Trusted eSign запустите на исполнение файл: основанных на Debian (Debian/Ubuntu);

  Trusted-eSign_vx.x.x_x64.rpm (где x.x.x – номер версии) для 64-разрядных ОС, основанных на RPM;

  Trusted-eSign_vx.x.x_x32.rpm (где x.x.x – номер версии) для 32-разрядных ОС, основанных на RPM.

  Откроется пакетный менеджер, в котором нужно нажать Установить. Так как установка производится от имени администратора системы, то появится диалог ввода пароля администратора системы (Root).

- Второй способ установки приложения выполняется с помощью командной строки. Для этого нужно запустить терминал и ввести команду:

  sudo dpkg - i Trusted-eSign_vx.x.x_xYY.deb (YY - разрядность ОС) - для ОС, основанных на Debian (Debian/Ubuntu);

sudo rpm - i Trusted-eSign_vx.x.x_xYY.rpm (YY - разрядность ОС) - для ОС, основанных на RPM;

После установки приложения в меню появится ярлык Trusted eSign.

- В том случае, когда не поддерживается пакетный режим установки приложения, его можно установить из предоставленного архива, распаковав содержимое в каталог **/opt/trustedesign/**. Распаковку архива необходимо производить с правами администратора.

1.3. Установка на платформу OS X

Для установки программы «Trusted eSign» запустите на исполнение файл **Trusted-esign_vx.x.x_x64.pkg** (где x.x.x – номер версии). Откроется мастер установки «Trusted eSign». Нажмите кнопку **Продолжить** для продолжения установки. На каждом шаге можно вернуться на предыдущий шаг нажатием **Назад**.

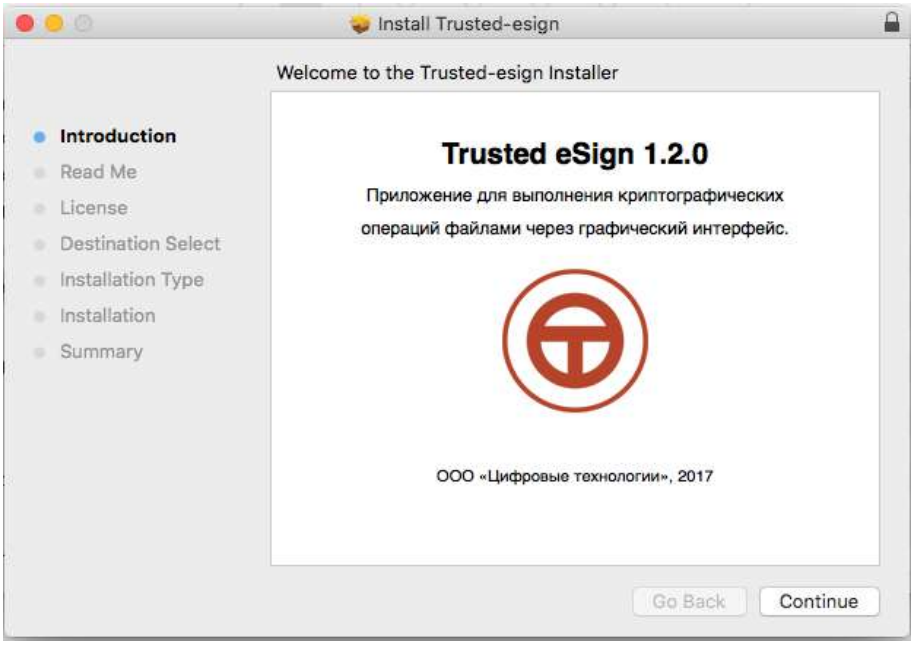


Рис.1.3.1. Начальный шаг мастера установки пакета приложения

Ознакомьтесь с описание программы и нажмите **Продолжить**. На данном этапе описание можно распечатать или сохранить в файл.

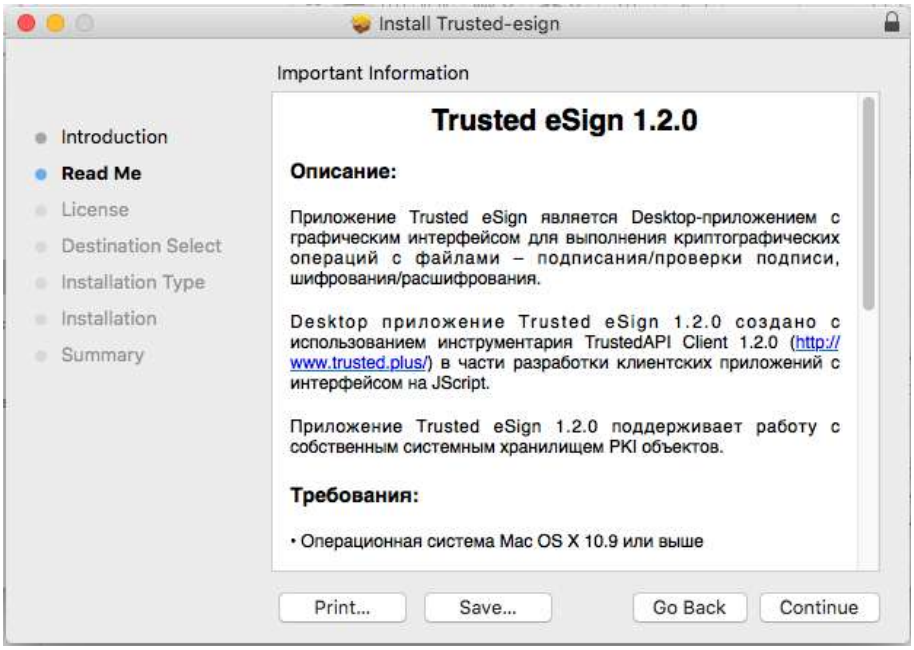


Рис.1.3.2. Просмотр информации о программном продукте

Ознакомьтесь с условиями лицензионного соглашения, нажмите **Продолжить**. На данном этапе лицензионное соглашение можно распечатать или сохранить в файл.

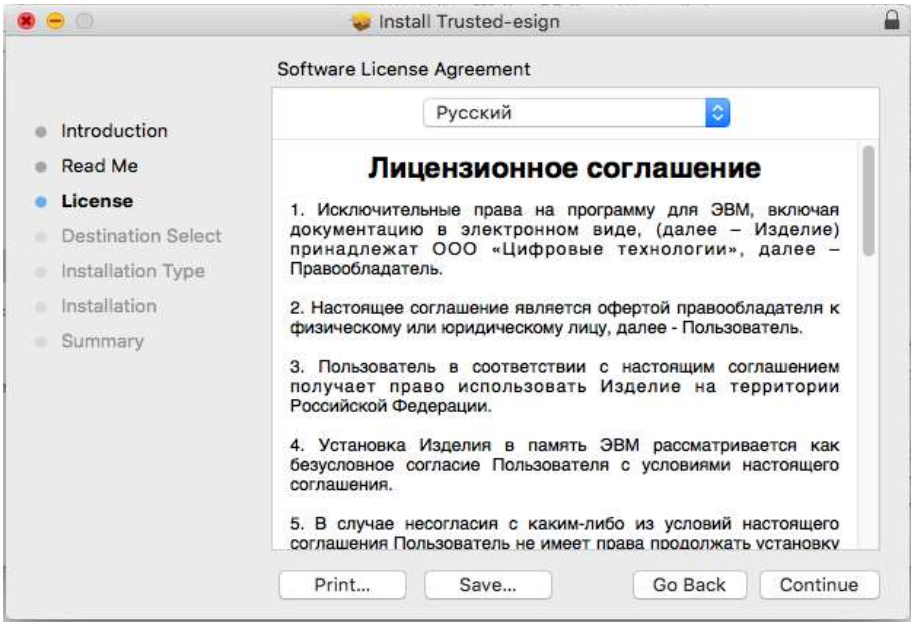


Рис.1.3.3. Просмотр информации о лицензии

Нажмите кнопку **Принимаю** для продолжения установки приложения или **Не принимаю** - для отмены установки.

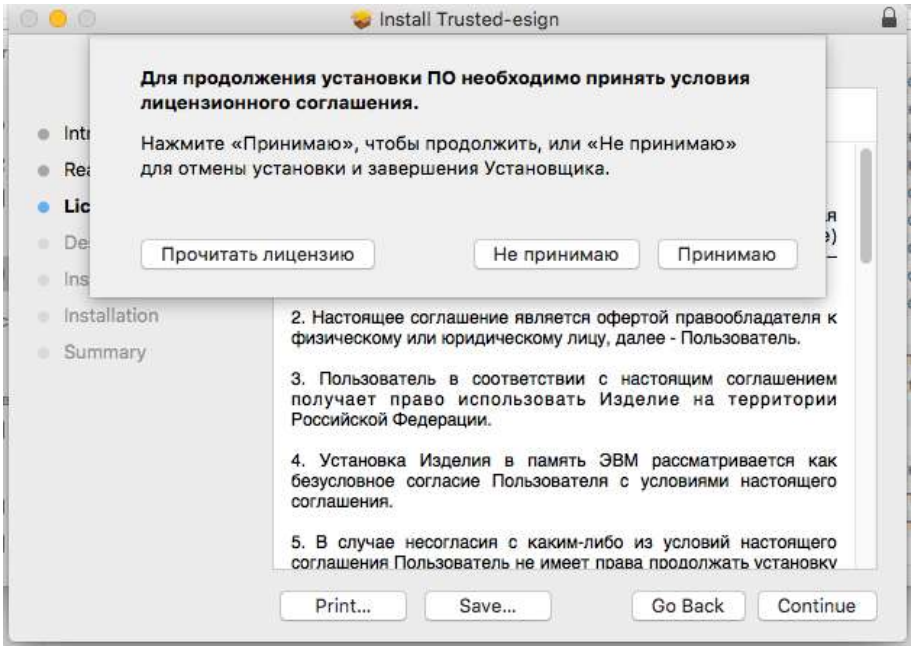


Рис.1.3.4. Соглашение с условиями лицензии

Выберете диск, на который будет установлено приложение (рис.1.3.5) и нажмите **Продолжить**.

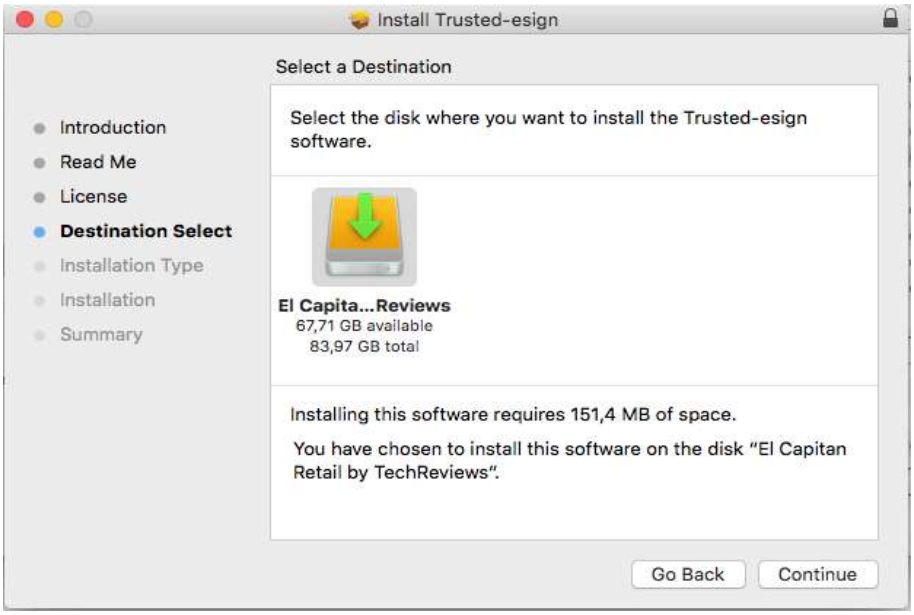


Рис.1.3.5. Информация о размещении приложения на жестком диске

На следующем шаге мастера нажмите кнопку **Установить** (рис.1.3.6).

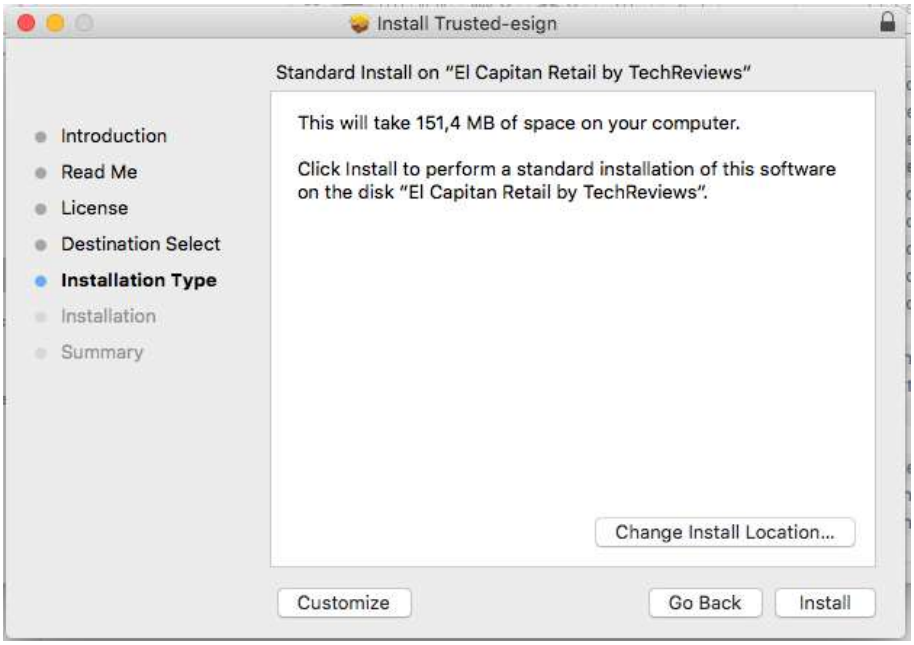


Рис.1.3.6. Подтверждение установки на физический носитель

Введите пароль администратора и нажмите **Установить** приложение**.**

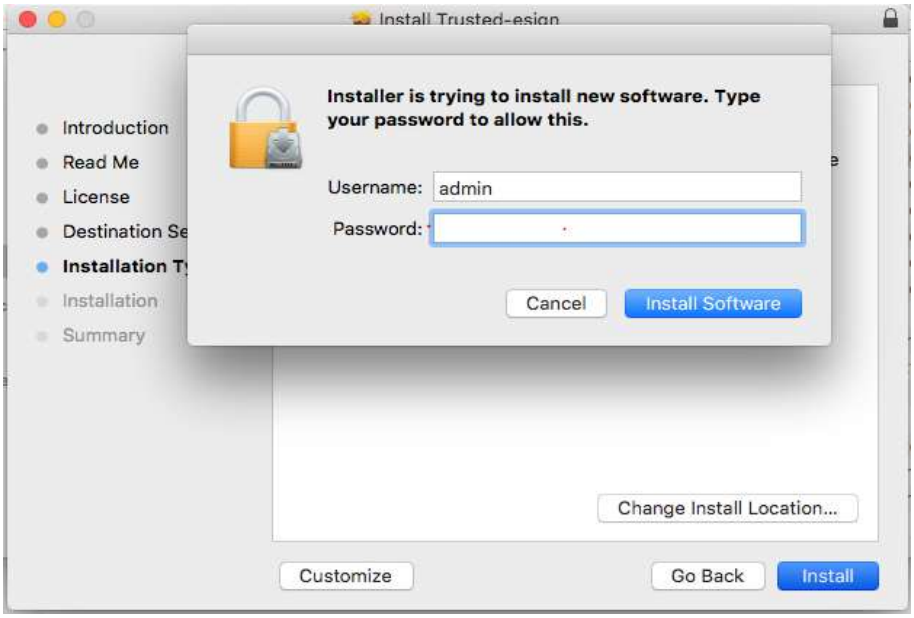


Рис.1.3.7. Информация о размещении приложения на жестком диске

Начнется установка программы на компьютер. По окончании установки нажмите кнопку **Закрыть**.

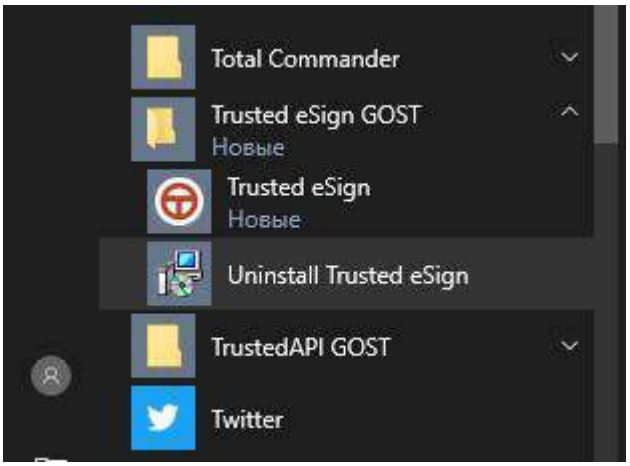
После установки программы в Launchpad появится ярлык приложения «Trusted eSign» и в каталоге Applications («Программы») будут созданы подкаталоги приложения.

2. Удаление программного продукта

2.1. Удаление приложения на платформе MS Windows

Удалить приложение Trusted eSign можно следующим образом:

- Воспользоваться стандартными средствами удаление программ в операционной системе Windows. Через кнопку **Пуск** откройте Панель управления. В окне **Настройка параметров** компьютера активизируйте ярлык **Программы и компоненты**. Откроется одноименное окно, в котором перечислены программы, установленные на компьютере. Выберите в списке программу «Trusted eSign», нажмите на кнопку **Удалить**, и подтвердите решение об удалении. Выполнение процесса удаления будет отображаться в виде индикатора прогресса в специальном окне. По завершении процесса программа «Trusted eSign» будет удалена с компьютера и из списка элементов **Установленные программы**.
- Второй способ удаления доступен через главное меню операционной системы. В главном меню найдите раздел с приложением - **Пуск, Все программы, Trusted eSign**. В списке найдите **Удалить Trusted eSign** (Uninstall Trusted eSign) (см. рисунок ниже) и активизируйте команду.



Начнется процесс удаления приложения Trusted eSign. Выполнение процесса отображается в виде индикатора прогресса. После завершения этого процесса приложение Trusted eSign будет удалено из операционной системы.

2.2. Удаление приложения на платформе Linux

Удаление приложения Trusted eSign на операционных системах Linux выполняется через графический интерфейс (пакетный менеджер), либо через терминал в режиме командной строки.

- Удаление приложения Trusted eSign через графический интерфейс выполняется следующим образом. Нужно открыть менеджер программ (пакетный менеджер) и найти приложение Trusted eSign. Найденное приложение следует пометить для удаления и нажать на кнопку **Удалить**. После этого программа «Trusted eSign» будет удалена с компьютера.
- Второй способ удаления основан на запуске команд в терминале:

  sudo dpkg - P trusted-esign - для ОС, основанных на Debian (Debian/Ubuntu);

  sudo rpm - e rusted-esign - для ОС, основанных на RPM;

После выполнения команды приложение будет удалено из операционной системы.

2.3. Удаление приложения на платформе OS X

Для удаления приложения Trusted eSign на операционной системе OS X можно воспользоваться менеджером Finder. В менеджере выберете вкладку Программы и найдите приложение Trusted eSign. Перетащите приложение Trusted eSign в Корзину. Таким образом приложение будет удалено из операционной системы.

3. Установка лицензии на программный продукт

Для полноценной работы приложения Trusted eSign необходима установка лицензионного ключа. Лицензионный ключ выдается пользователю после приобретения данного продукта и представляет собой файл, который необходимо расположить в специально созданном каталоге приложения.

Установка лицензионного ключа может производиться как через пользовательский интерфейс, так и с помощью консольных команд, выполняющих копирование файла лицензии в заданный каталог.

3.1. Установка лицензии через пользовательский интерфейс

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через главное меню приложения. На открывшейся странице, которая представлена на рис.3.1.1 нажать на кнопку **Ввести ключ**. В результате должно появиться всплывающее окно ввода лицензии, предполагающее выполнение действия одним из двух способов (рис. 3.1.2): выполнение ввода копированием содержимого файла лицензии в текстовое поле и выполнение ввода указанием файла лицензии.

Примечание. При установке лицензии будут запрошены права администратора (Root) на доступ к каталогу пользователя. После установки лицензии желательно перезагрузить приложение.

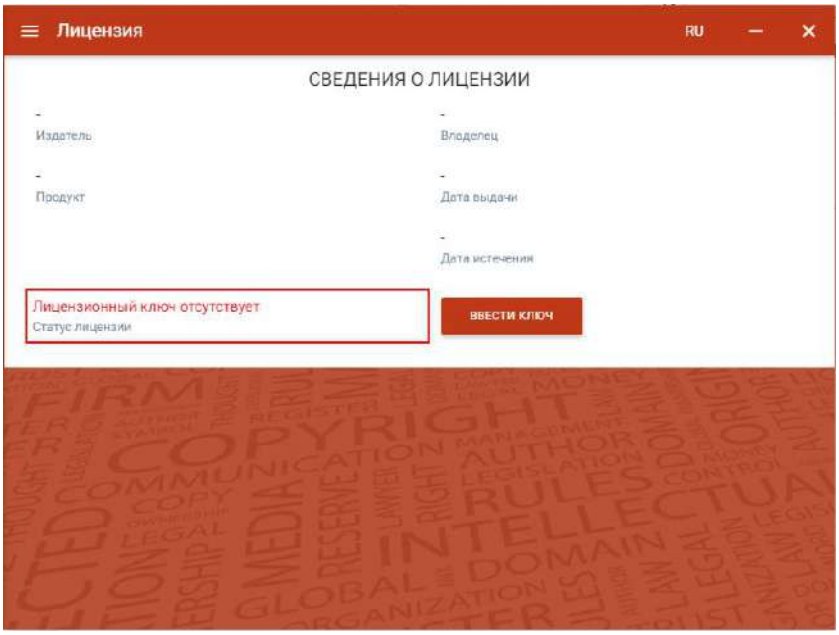


Рис.3.1.1. Страница ввода лицензионного ключа на программный продукт

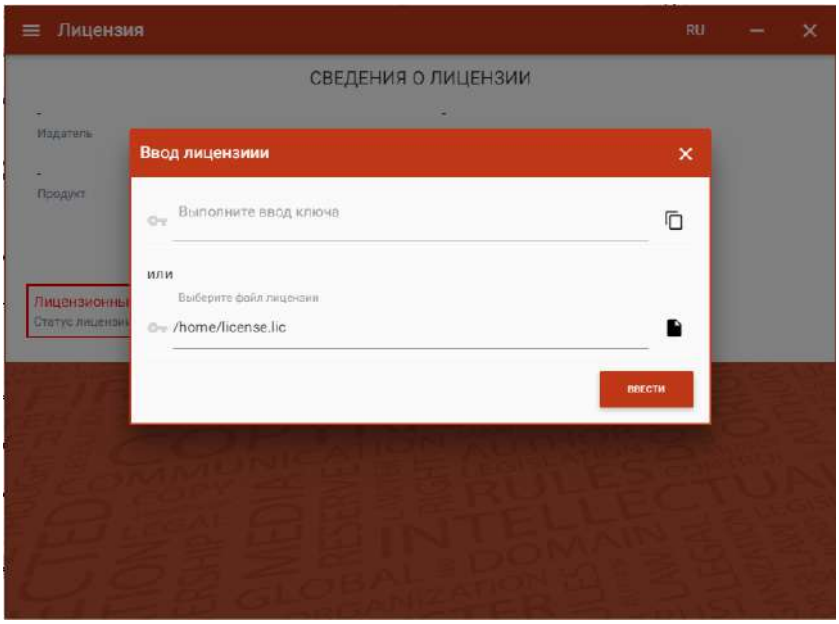


Рис.3.1.2. Диалоговое окно с выбором варианта ввода лицензионного ключа

Если установка лицензионного ключа прошла успешно, то появляется всплывающее сообщение с информацией об этом. На странице **Лицензия** отображается информация о введенном лицензионном ключе на приложение с данными об издателе программного продукта, продукте, владельце лицензии, дате выдачи лицензии, дате истечения лицензии, статусе лицензии.

В том случае, если лицензия на продукт не введена или не действительна при каждом запуске приложения будет появляться всплывающее сообщение с информацией об этом.

3.2. Установка лицензии через командную строку

Для целей развертывания приложения на множестве рабочих мест использование диалога ввода лицензии не подходит. Наилучшим вариантом здесь является установка лицензии с помощью командного скрипта, выполняющим копирование файла лицензии license.lic в каталог установки:

- Под платформой Windows – каталог C:\Users\<имя пользователя>\AppData\Local\Trusted \Trusted eSign.
- Под платформой Linux – каталог ./etc/Trusted/Trusted eSign/.

Примечание. Для последующей установки лицензии пользователями каталог Trusted eSign должен иметь права на запись, а минимально необходимые права – права на чтение для пользователей на рабочем месте.

4. Установка криптопровайдера КриптоПро CSP

Для выполнения операций с использованием российских криптографических алгоритмов на рабочее место нужно установить СКЗИ «КриптоПро CSP» версии 3.9, 4.0 или 5.0.

4.1. Установка криптопровайдера на платформу MS Windows

Для установки КриптоПро CSP (версии 3.0 или 4.0) на платформу Windows можно воспользоваться инструкцией, доступной по адресу https://cryptostore.ru/article/instruktsii/kak_ustanovit_criptopro_csp/ .

Приложение Trusted eSign совместимо с криптопровайдером КриптоПро Cloud CSP (КриптоПро CSP 5.0), который доступен для скачивания по ссылке https://www.cryptopro.ru/sites/default/files/private/csp/cloudcsp.zip. Помимо дистрибутива в архиве будет также краткая инструкция по использованию. Установка дистрибутива не вызовет сложностей. Но есть одно условие, перед установкой КриптоПро Cloud CSP нужно предварительно удалить все другие криптопровайдеры.

4.2. Установка криптопровайдера на платформу Linux

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo. Пакеты зависят друг от друга, поэтому должны устанавливаться по порядку с учётом этих зависимостей.

Для установки пакета используется команда:

rpm -i <файл_пакета>
Например, **rpm -i ./lsb-cprocsp-base-3.6.1-4.noarch.rpm**

На ОС, основанных на Debian (Debian/Ubuntu), для установки пакетов используется команда:

alien -kci <файл_пакета>
Например, **alien -kci ./lsb-cprocsp-base-3.6.1-4.noarch.deb**

На ОС, основанных на Debian (Debian/Ubuntu), для установки 32-битных пакетов на 64битную ОС используется команда:

dpkg-architecture -ai386 -c alien -kci <файл_пакета>

Порядок установки пакетов приведен ниже. Возможно, потребуется предварительно установить пакеты **lsb-base**, **alien**, **lsb-core** из стандартного репозитория ОС:

sudo apt-get install lsb-base alien lsb-core
sudo alien -kci lsb-cprocsp-base-<...>.noarch.deb
sudo alien -kci lsb-cprocsp-rdr-64-<...>.deb
sudo alien -kci lsb-cprocsp-capilite-<...>.deb
sudo alien -kci lsb-cprocsp-kc1-<...>.deb

Установку провайдера можно осуществить, запустив файл из дистрибутива **install.sh**. Файлы из пакетов устанавливаются в **/opt/cprocsp**.

Для работы с контейнерами закрытых ключей требуется ввод пароля. Графический интерфейс диалога ввода пароля содержится в пакете **cprocsp-rdr-gui**, который можно установить командой:

sudo alien -kci cprocsp-rdr-gui-<>.deb

Для работы электронных идентификаторов Рутокен в deb-based системе должны быть установлены: библиотека libccid не ниже 1.3.11, пакеты pcscd и libpcsclite1.

Для работы в RPM-based системе должны быть установлены: пакеты ccid, pcscd и pcsc-lite с помощью команд:

sudo alien -kci cprocsp-rdr-pcsc-<...>.deb
sudo alien -kci cprocsp-rdr-rutoken-<...>.deb
sudo alien -kci ifd-rutokens_1.0.4_1.x86_64.deb

Примечание. Директория расположения утилит КриптоПро CSP /opt/cprocsp/bin/<arch>/, где под <arch> подразумеваться один из следующих идентификаторов платформы: ia32 - для 32-разрядных систем; amd64 - для 64-разрядных систем.

Установка программного обеспечения «КриптоПро CSP» без ввода лицензии подразумевает использование временной лицензии с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).

Просмотр информации о лицензии осуществляется командой:

 # cpconfig -license -view

Ввод лицензии производится командой (серийный номер следует вводить с соблюдением регистра символов):

 # cpconfig -license -set <серийный_номер>

4.3. Установка криптопровайдера на платформу OS X

Для установки КриптоПро CSP на платформу OS X можно воспользоваться инструкцией, доступной по адресу https://cryptoarm.ru/How-to-install-cryptopro-csp-4-on-mac-os-x .

5. Перенос контейнера закрытого ключа под требуемую операционную систему

Для примера рассмотрим наиболее часто встречающуюся задачу переноса контейнера закрытого ключа из операционной системы Windows под Linux или OS X. Если в операционной системе Windows сертификат и закрытый ключ могут находится в локальном хранилище Crypto API, то для работы под операционными системами Linux или OS X его нужно импортировать в специальное системное хранилище. Важно, чтобы у закрытого ключа должен быть установлен флаг «Экспортируемый».

Перенос выполняется в два шага – экспорт контейнера и сертификата, импорт контейнера и установка сертификата в личное хранилище:

- В операционной системе Windows скопировать контейнер закрытого ключа можно следующим образом. Откройте приложение КриптоПро CSP и перейдите на вкладку **Сервис**. На вкладке выберите команду **Скопировать контейнер закрытого ключа**. Введите пароль для ключевого контейнера и задайте имя ключевого контейнера (например, test). Сохраните контейнер на диск или флешку. После этого откройте диалог Сертификаты (должна запуститься консоль MMC), перейдите в раздел **Личное, Реестр, Сертификаты** и экспортируйте сертификат без закрытого ключа с помощью мастера. Сохраните его в файл (например, test.cer).
- Для импорта импортировать сертификата под операционными системами Linux (OS X) выполните следующие действия. Скопируйте контейнер закрытого ключа (директорию /test/ в формате 8.3) и файл сертификата (test.cer) из корня дискеты или флешки в директорию /var/opt/cprocsp/keys/имя_пользователя. При этом необходимо проследить чтобы: владельцем файлов был пользователь, в директории с именем которого расположен контейнер (от его имени будет осуществляться работа с ключами); на директорию с ключами были выставлены права, разрешающие владельцу всё, остальным ничего; на файлы были выставлены права, разрешающие владельцу по крайней мере чтение и запись, остальным ничего.

  Проверить, отображается ли контейнер можно командой

  /opt/cprocsp/bin/<arch>/csptest -keyset -enum_cont -fqcn -verifycontext

  Привязать сертификат к закрытому ключу можно командой

  /opt/cprocsp/bin/<arch>/certmgr -inst -store uMy

  -file /var/opt/cprocsp/keys/<сертификат>.cer -cont '\\.\HDIMAGE\test' –pin ***

  Выполнить проверку привязки сертификата к закрытому ключу можно через команду

  /opt/cprocsp/bin/<arch>/certmgr -list -store uMy

  в результате выполнения предыдущей команды должно быть выведено сообщение **PrivateKey Link: Yes. Container: HDIMAGE\\test.000\.**

  В приведенных выше командах под **<arch>** подразумеваться один из следующих идентификаторов платформы: **ia32** - для 32-разрядных систем Linux; **amd64** - для 64-разрядных систем Linux; **не указывается** - для OS X.

6. Установка сертификата с токена с сохранением привязки к закрытому ключу

Если сертификат и закрытый ключ находятся на токене, то для работы с таким сертификатом его надо установить в локальное хранилище. Установка отличается в операционных системах Windows, Linux и OS X.

– Установка на операционной системе Windows выполняется следующим образом. Нужно подключить токен (например, Рутокен) и открыть программу КритоПро CSP. В появившемся диалоге перейти на вкладку **Сервис**, как показано на рис.6.1.1.

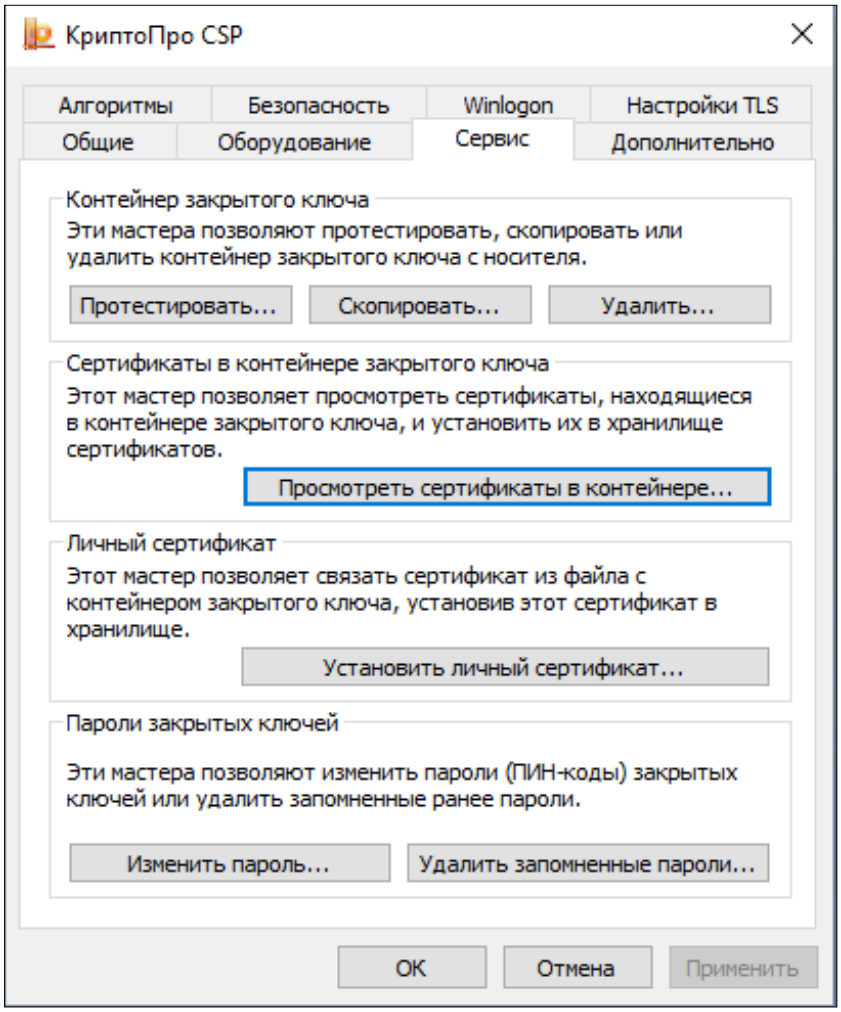


Рис.6.1.1. Диалог настроек криптопровайдера. Вкладка Сервис

После нажатия на кнопку **Просмотреть сертификаты в контейнере** должен открыться диалог поиска контейнера (рис. 6.1.2) в котором требуется нажать кнопку **Обзор**.

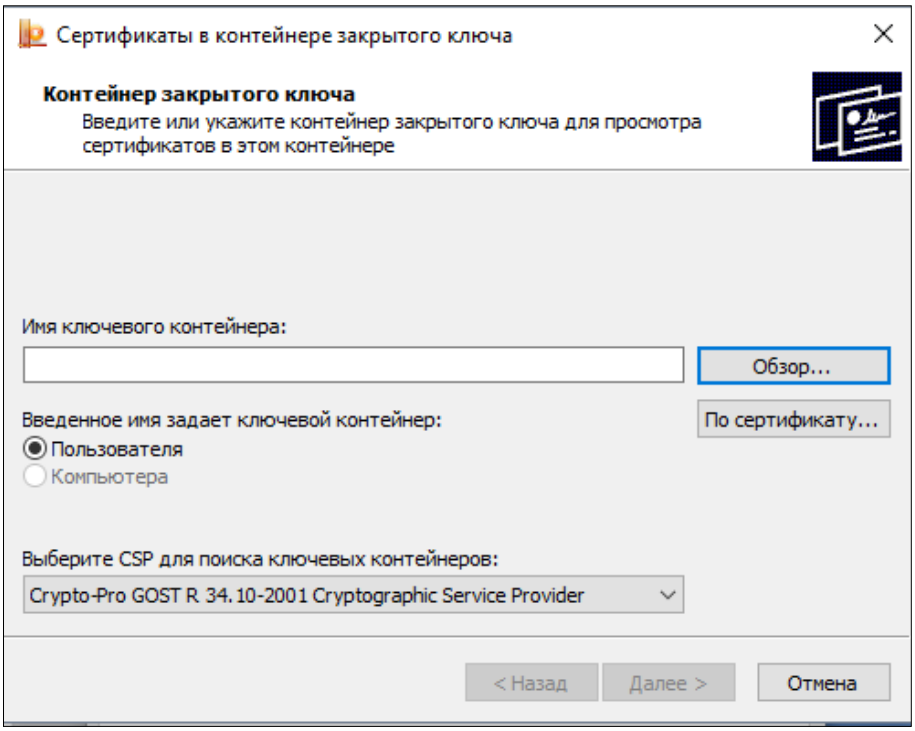


Рис.6.1.2. Диалог поиска ключевого контейнера

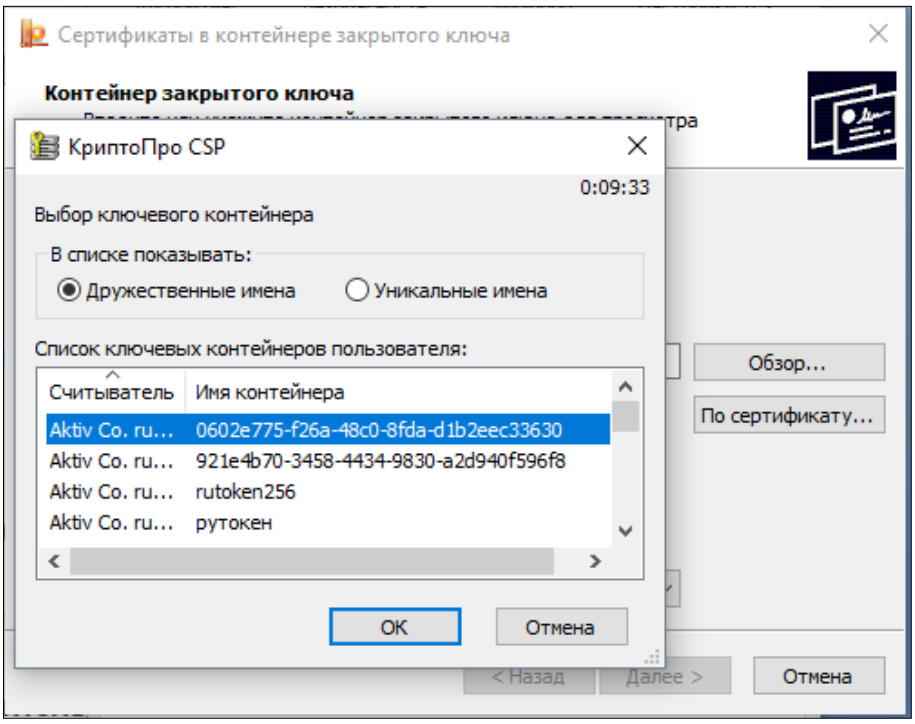


Рис.6.1.3. Выбор ключевого контейнера

Затем нужно выбрать нужный контейнер и нажать на кнопку **Далее** (см. рис. 6.1.4).

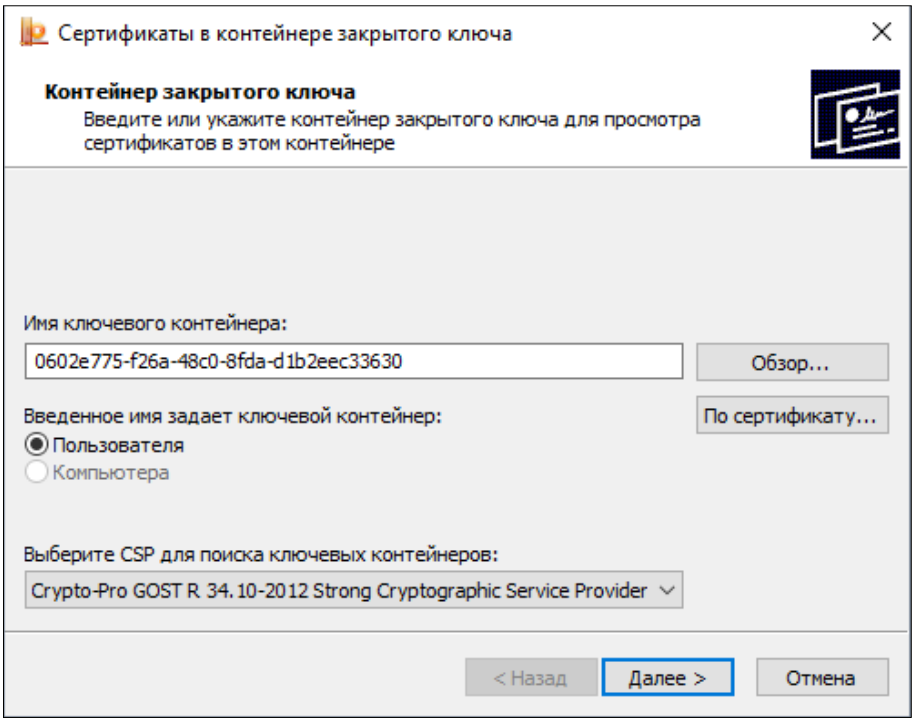


Рис.6.1.4. Просмотр содержимого контейнера

В контейнере содержится сертификат, сведения о котором будут отображены на последнем шаге мастера (рис.6.1.5). Этот сертификат можно установить в систему, нажав на кнопку **Установить**.

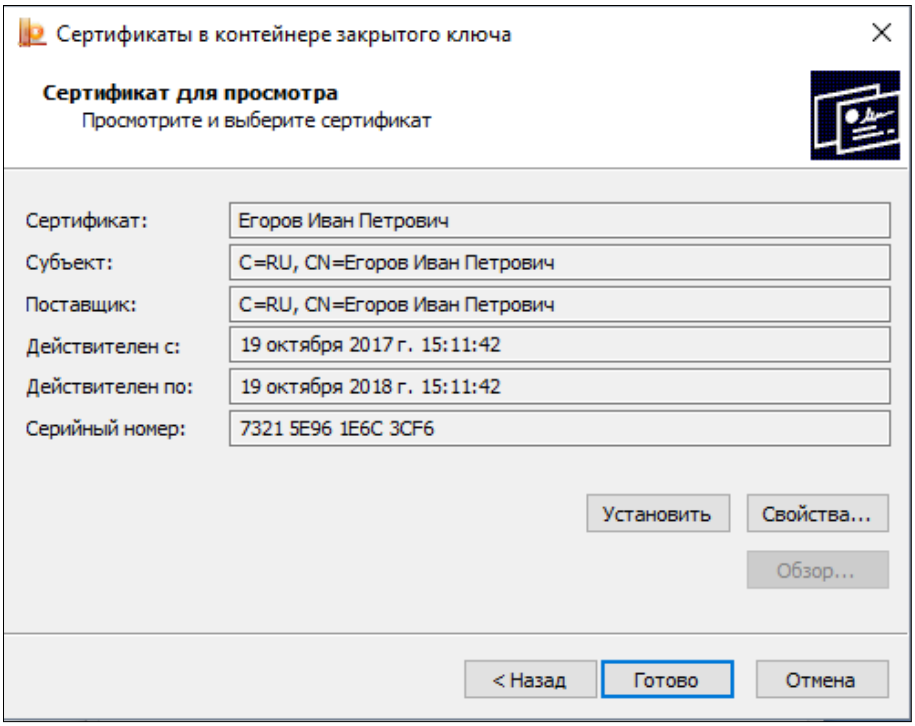


Рис.6.1.5. Сведения о сертификате внутри контейнера

После успешной установки сертификата можно открыть приложение Trusted eSign и перейти на вкладку **Сертификаты**. Установленный сертификат должен отображаться в списке **Личные сертификаты**.

– Для установки сертификата под операционной системой Linux нужно подключить токен (например, Рутокен) и открыть Терминал (Terminal). Далее следует ввести команду:

/opt/cprocsp/bin/<arch>/list_pcsc

В результате получаем имя устройства, например,

Aktiv Rutoken ECP 00 00
Total: SYS: 0.010 sec USR: 0.000 sec UTC: 0.430 sec
ErrorCode: 0x00000000]

В команде под **<arch>** подразумеваться один из следующих идентификаторов платформы:

ia32 - для 32-разрядных систем;

amd64 - для 64-разрядных систем.

Далее нужно ввести команду:

sudo /opt/cprocsp/sbin/<arch>/cpconfig -hardware reader -add "имя_устройства", где в кавычках указывается имя устройства. Например, **sudo /opt/cprocsp/sbin/amd64/cpconfig -hardware reader -add "Aktiv Rutoken ECP"**

Затем потребуется ввести пароль администратора (пользователя root), после чего должно появиться сообщение вида

Adding new reader:
Nick name: Aktiv Rutoken ECP
Succeeded, code:0x0

Для просмотра контейнеров на токене можно ввести команду

/opt/cprocsp/bin/<arch>/csptest -keys -verifyc -enu –fq -u

В результате получаем имя устройства и имя контейнера и после символа | - имя устройства и уникальное имя:

\\.\Aktiv Rutoken ECP\имя_контейнера | \\.\Aktiv Rutoken ECP\уникальное_имя

Затем требуется ввести для копирования сертификата с токена

/opt/cprocsp/bin/<arch>/certmgr -inst -cont '\\.\Aktiv Rutoken ECP\уникальное_имя'

В кавычках должно быть указано имя Вашего устройства и уникальное имя контейнера (справа от символа |). В терминале должна вывестись информация об установленном Вами сертификате.

После завершения установки можно открыть программу Trusted eSign и перейти на вкладку **Сертификаты**. Установленный сертификат должен отображаться в списке Личные сертификаты. Если сертификат отображается как действительный (зеленый индикатор), то с ним можно работать. Если сертификат отображается как недействительный (красный индикатор), то надо устанавливать корневой и промежуточные сертификаты. Для получения корневых и промежуточных сертификатов лучше обратиться в удостоверяющий центр.

– Для установки сертификата по операционной системой OS X требуется подключить токен (например, Рутокен) и открыть Терминал (Terminal). В терминале следует ввести команду:

/opt/cprocsp/bin/csptest -card -enum

В результате получаем имя устройства, например,

Aktiv Rutoken ECP 00 00
Total: SYS: 0.010 sec USR: 0.000 sec UTC: 0.430 sec
ErrorCode: 0x00000000]

Затем требуется ввести команду

sudo /opt/cprocsp/sbin/cpconfig -hardware reader -add "имя_устройства", где в кавычках указывается имя устройства. Например**, sudo /opt/cprocsp/sbin/cpconfig -hardware reader -add "Aktiv Rutoken ECP"**

Далее требуется ввести пароль администратора (пользователя root). В результате должно быть выведено сообщение вида:

Adding new reader:
Nick name: Aktiv Rutoken ECP
Succeeded, code:0x0

Для просмотра контейнеров на токене ввести команду:

/opt/cprocsp/bin/csptest -keys -verifyc -enu –fq -u

В итоге получаем имя устройства и имя контейнера и после символа | - имя устройства и уникальное имя:

\\.\Aktiv Rutoken ECP\имя_контейнера | \\.\Aktiv Rutoken ECP\уникальное_имя

Ввести или вставить команду для копирования сертификата с токена

/opt/cprocsp/bin/certmgr -inst -cont '\\.\Aktiv Rutoken ECP\уникальное_имя'

В кавычках должно быть имя Вашего устройства и уникальное имя контейнера (справа от символа |). В терминале должна вывестись информация об установленном Вами сертификате. После установки требуется открыть программу Trusted eSign, перейти на вкладку **Сертификаты**. Установленный сертификат должен отображаться в списке **Личные сертификаты**. Если сертификат отображается как действительный (зеленый индикатор), то с ним можно работать. Если сертификат отображается как недействительный (красный индикатор), то надо устанавливать корневой и промежуточные сертификаты. Для получения корневых и промежуточных сертификатов лучше обратиться в удостоверяющий центр.

7. Установка доверенных коневых, промежуточных сертификатов и списка отзыва сертификата

Для работы с сертификатами нужно установить сертификат удостоверяющего центра (обычно файл с расширением .cer или .p7b), при необходимости, цепочку сертификатов (обычно файл с расширением .cer или .p7b), а также список отозванных сертификатов (обычно файл с расширением .crl). Чаще всего расширение .cer соответствует сертификату, а .p7b - контейнеру, в котором может содержаться один или больше сертификатов (например, их цепочка).

Для получения корневых и промежуточных сертификатов нужно обратиться в удостоверяющий центр.

Установка корневого, промежуточных и списка отозванных сертификатов осуществляется командами:

- Установка корневого сертификата удостоверяющего центра

  /opt/cprocsp/bin/<arch>/certmgr -inst -cert -file <название файла корневого сертификата>.cer -store uRoot

- Установка цепочки промежуточных сертификатов

  /opt/cprocsp/bin/<arch>/certmgr -inst -cert -file <название файла промежуточных сертификатов>.p7b -store CA

- Установка списка отозванных сертификатов

  /opt/cprocsp/bin/<arch>/certmgr -inst -crl -file <название файла списка отозванных сертификатов>.crl

В приведенных выше командах под <arch> подразумеваться один из следующих идентификаторов платформы:

ia32 - для 32-разрядных систем Linux;

amd64 - для 64-разрядных систем Linux;

для OS X разрядность не указывается.

8. Графический пользовательский интерфейс приложения

8.1. Главное окно приложения

Работа с приложением Trusted eSign ГОСТ начинается со стартовой страницы (рис.8.1.1), на которой расположены кнопки перехода к мастерам приложения.

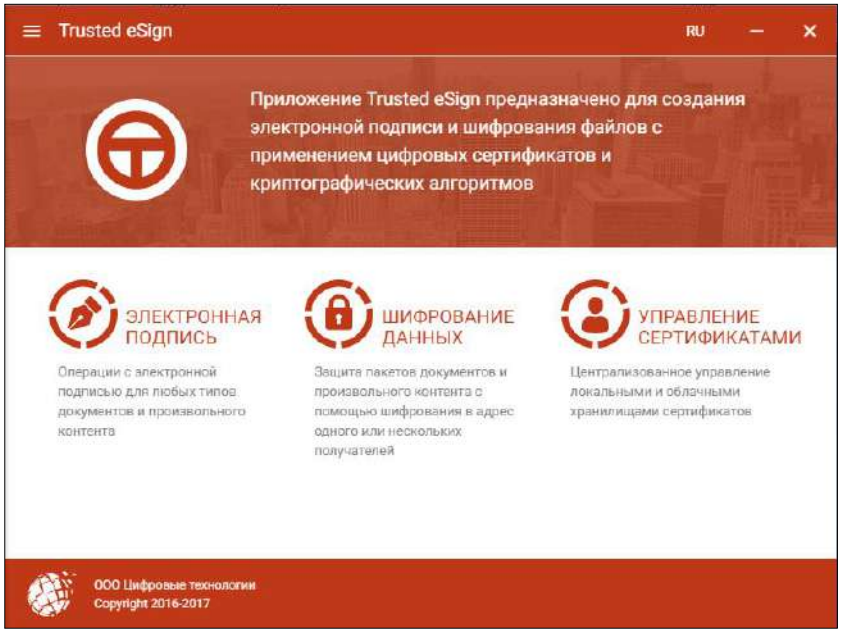


Рис.8.1.1. Главное окно приложения

В верхней левой части окна расположена кнопка вызова главного меню приложения ☰, через которое можно выполнить переход ко всем представлениям (рис.7.1.2).

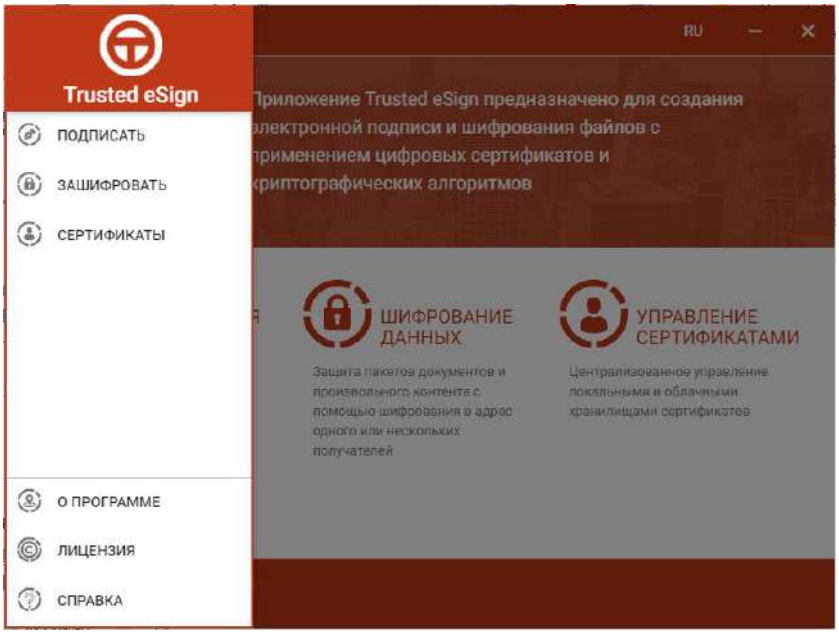


Рис.7.1.2. Основное меню приложения

При первом запуске приложения в домашней папке пользователя создается подкаталог с наименованием **.Trusted**. Данный подкаталог содержит файловые объекты, необходимые для корректного функционирования приложения. В частности, в подкаталоге размещаются импортированные в приложение цифровые сертификаты пользователей, ключи и списки отзыва. В файле **settings.json** сохраняются пользовательские настройки.

Запуск приложения на рабочем месте сразу дает возможность проверить его функциональность - в хранилище сертификатов присутствует тестовый сертификат, с помощью которого можно выполнить операции подписи и шифрования файлов.

8.2. Создание электронной подписи

Представление мастера подписания/проверки подписи (рис. 8.2.1) имеет три функциональных элемента: слева располагаются области выбора сертификата подписчика и настройки подписи, справа - область формирования списка файлов для выполнения операций.

Выставленные настройки сохраняются при переходе по вкладкам, а также при закрытии приложения.

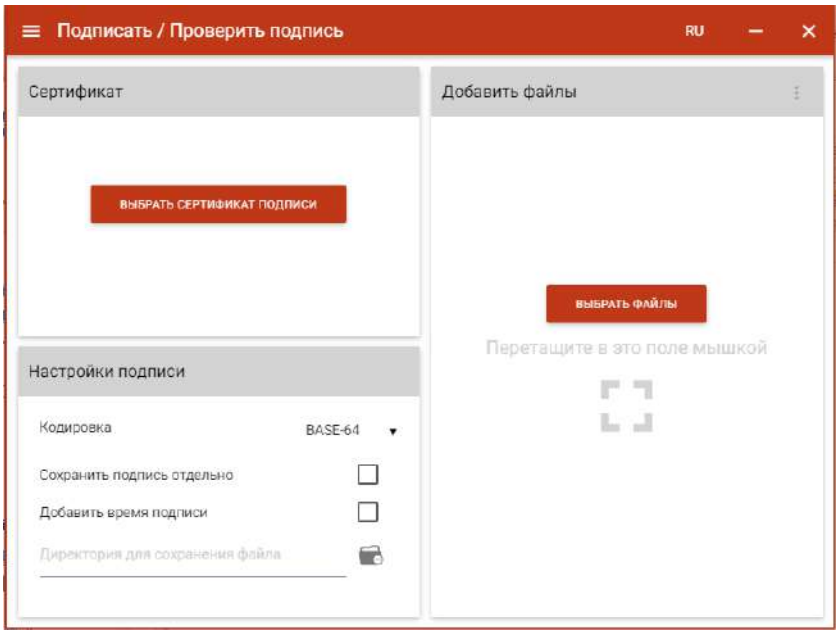


Рис.8.2.1. Страница создания/проверки электронной подписи файлов

В представленном мастере можно выполнить действия по:

- Настройке подписи;
- Выбора сертификата подписчика;
- Подписи одного или нескольких файлов.

Настройки подписи. В виде настроек подписи передаются следующие параметры:

- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER;

- **Сохранить подпись отдельно** - при установленном флажке подпись сохраняется отдельно от исходного файла;
- **Добавить время подписи** - при установленном флажке в подпись сохраняется время (системное) подписи;
- **Директория для сохранения файла** - при выбранной директории подпись сохраняется в данной директории. Если директория не указано, то подпись размещается рядом с исходным файлом.

Выбор сертификата подписчика. Для того, чтобы выполнить подпись необходимо выбрать цифровой сертификат, к которому привязан закрытый ключ. Эта операция производится нажатием кнопки **Выбрать сертификат подписи**. В появившемся диалоговом окне (рис.8.2.2) отображается вкладка **Личные сертификаты**, содержащая сертификаты, которые могут использоваться для подписи. У отображаемых в списке сертификатов присутствует закрытый ключ. Выбор сертификата подписчика осуществляется его выделением и нажатием на кнопку **Выбрать**. При этом в правой части отображается информация о сертификате. Допускается смена выбранного сертификата с помощью кнопки в верхней части элемента.

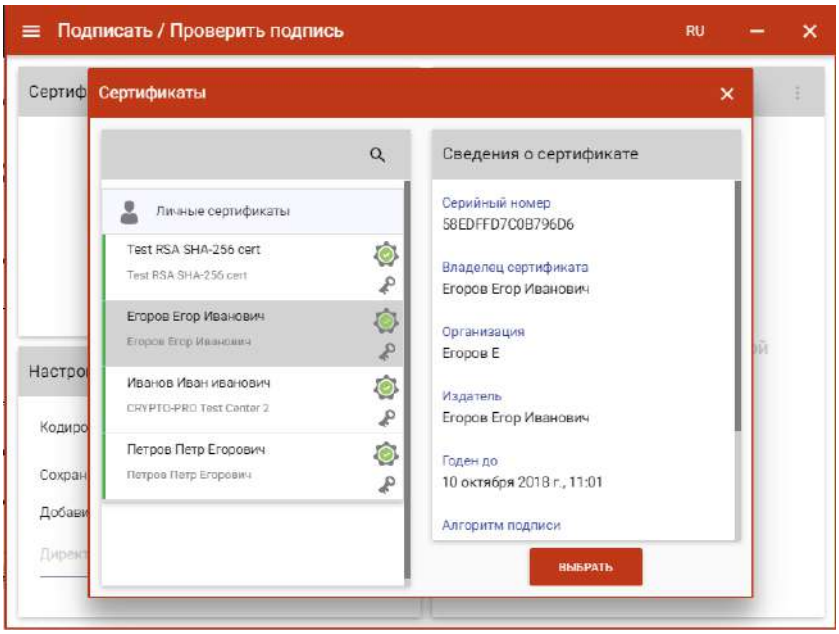


Рис.8.2.2. Диалоговое окно выбора сертификата подписчика

Выбор подписываемых файлов. В приложении доступно создание подписи для одного или группы выбранных файлов. Файлы для подписи можно добавить двумя способами: через кнопку **Выбрать файлы** или перетащив файлы мышкой в область формирования списка файлов для подписи.

Выбранные файлы заносятся в правую область и представляют собой одноуровневый список. Для данного списка доступно контекстное меню (рис. 8.2.3) в заголовке функционального элемента, состоящее из пунктов:

- **Выделить все** - выделяются все добавленные в список файлы;
- **Сбросить выделение** - отменяется выделение всех выбранных в списке файлов;

– **Удалить все из списка** - список очищается. При очистке списке файлы из файловой системы не удаляются.

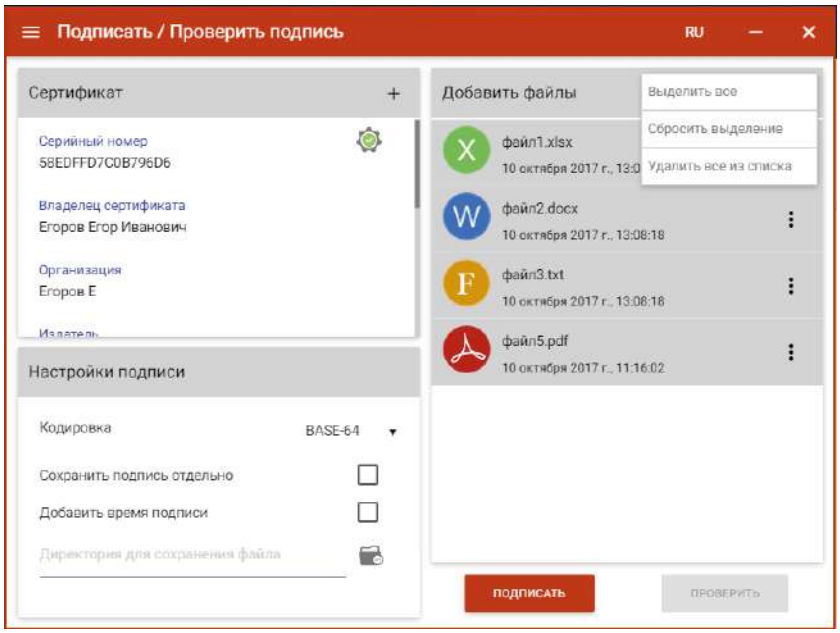


Рис. 8.2.3. Контекстное меню управления списком файлов

В списке отображается наименование файла с расширением и дата его создания. Для каждого элемента списка доступно контекстное меню (рис. 8.2.4), состоящее из пунктов:

– **Открыть файл** - выполняется открытие файла через приложение, которое ассоциировано с его расширением;
– **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл;
– **Удалить из списка** - файл удаляется из текущего списка выбранных файлов для подписания. При выполнении этой операции файл остается в файловой системе в неизменном виде.

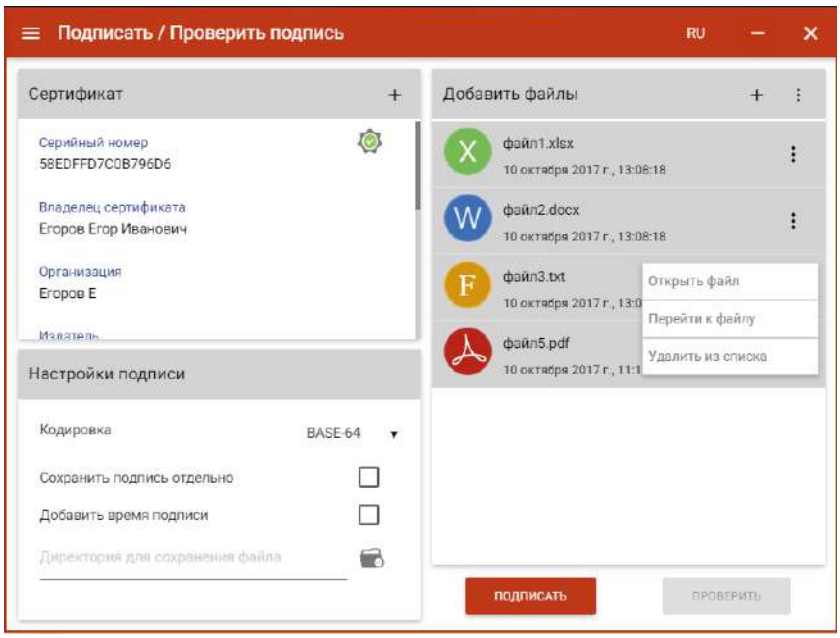


Рис. 8.2.4. Контекстное меню элемента списка (файла)

Подпись файлов. При условии выбора сертификата подписчика и подписываемых файлов в мастере становится доступной кнопка **Подписать** (рис.8.2.5).

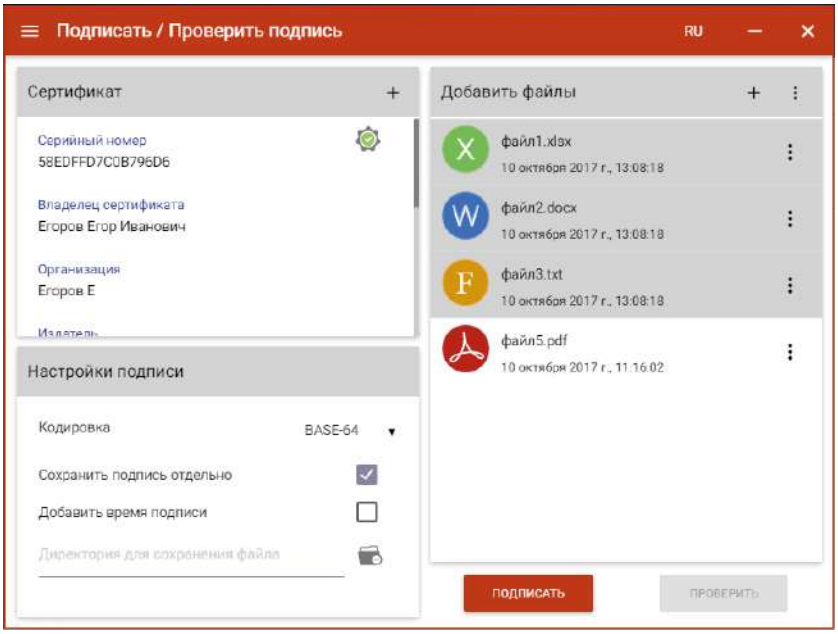


Рис.8.2.5. Подпись файлов

Нажатие на кнопку **Подписать** запускает процесс подписи. Выбранные файлы подписываются по очереди. Для подписанных файлов меняется иконка, наименование, дата создания. Если в настройках подписи не задан каталог для сохранения подписанных файлов, они сохраняются в тех же каталогах, где размещаются исходные подписываемые файлы. Для подписанных файлов становятся доступны кнопки **Проверить** и **Снять** для проверки и снятия подписи (рис. 8.2.6).

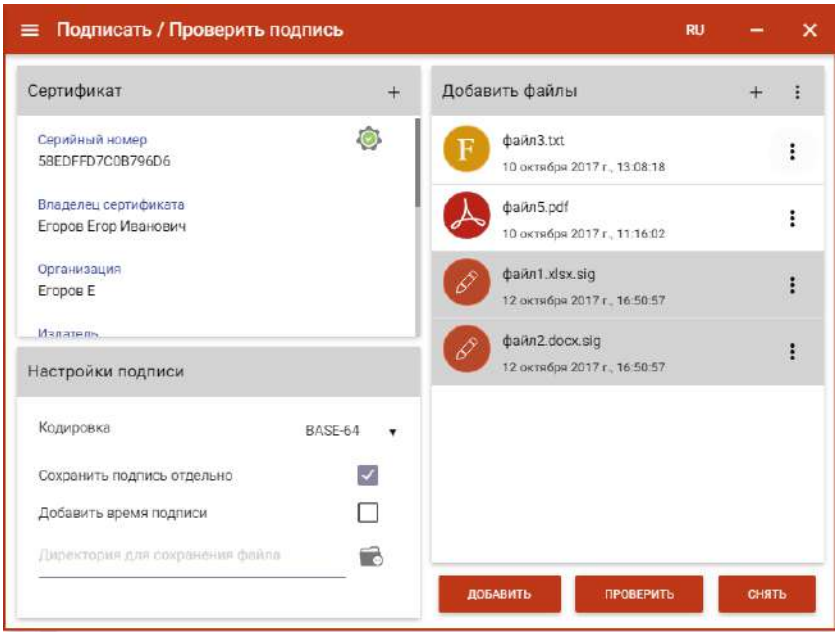


Рис.8.2.6. Проверка подписи файлов

8.3. Проверка электронной подписи

Для проверки подписи достаточно выбрать проверяемые файлы - файлы с расширением **.sig**, которые содержат электронную подпись и нажать на кнопку “Проверить”. Никаких дополнительных манипуляций при проверке подписи производить не нужно.

Если при проверке, отделенной от подписываемого файла подписи, исходный файл не будет найден автоматически, будет предложен его выбор.

Результат проверки подписей отображается в виде общего сообщения и цветового индикатора для каждого файла (рис. 8.3.1): зеленый - подпись действительна; красный - подпись недействительна.

При наведении мыши на индикатор появляется сообщение, соответствующее цвету индикатора.

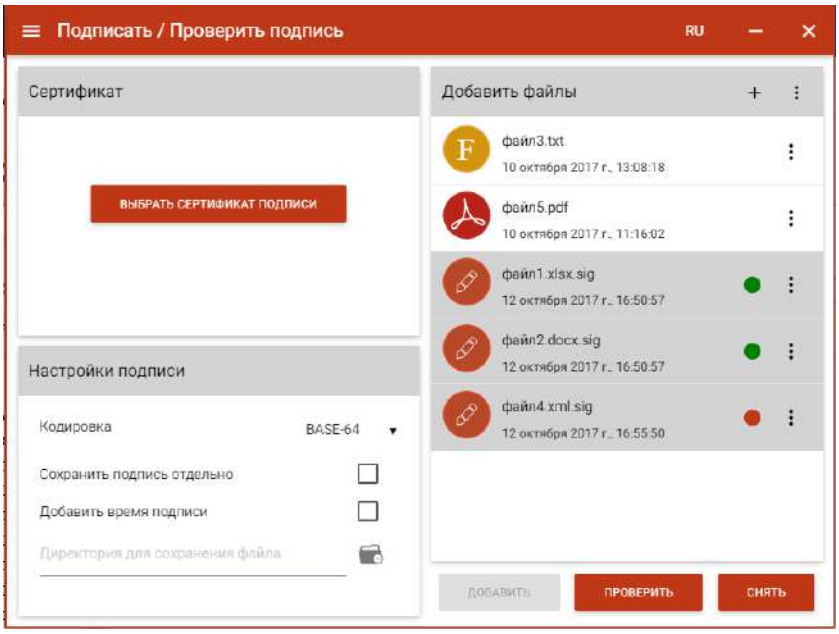


Рис. 8.3.1. Результат проверки подписи файлов

При выделении одного подписанного файла в левой области отображается информация о подписи, как показано на рис. 8.3.2.

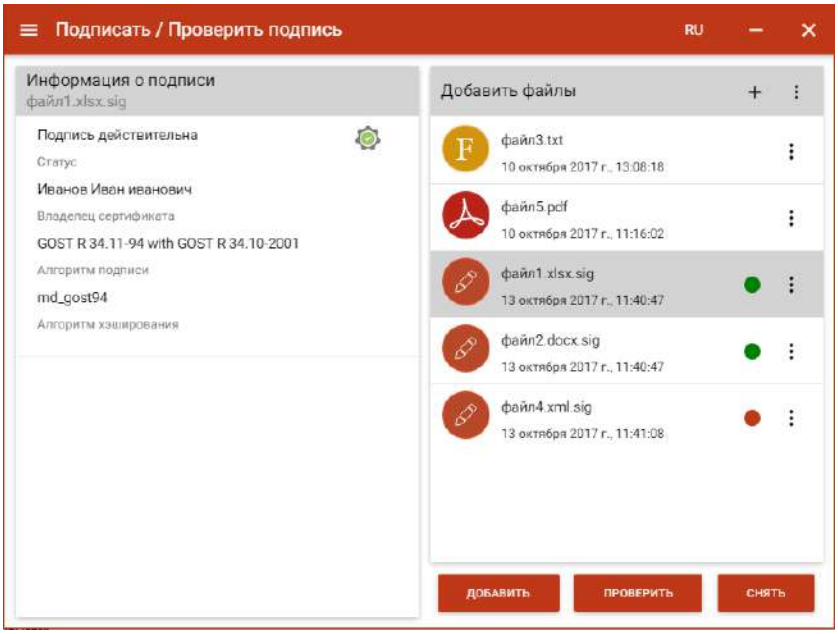


Рис. 8.3.2. Отображение информации о подписи

При нажатии на область с информацией о подписи открывается информация о цепочке сертификации (цепочке доверия) и сведения о выбранном сертификате в этой цепочке (рис.8.3.3).

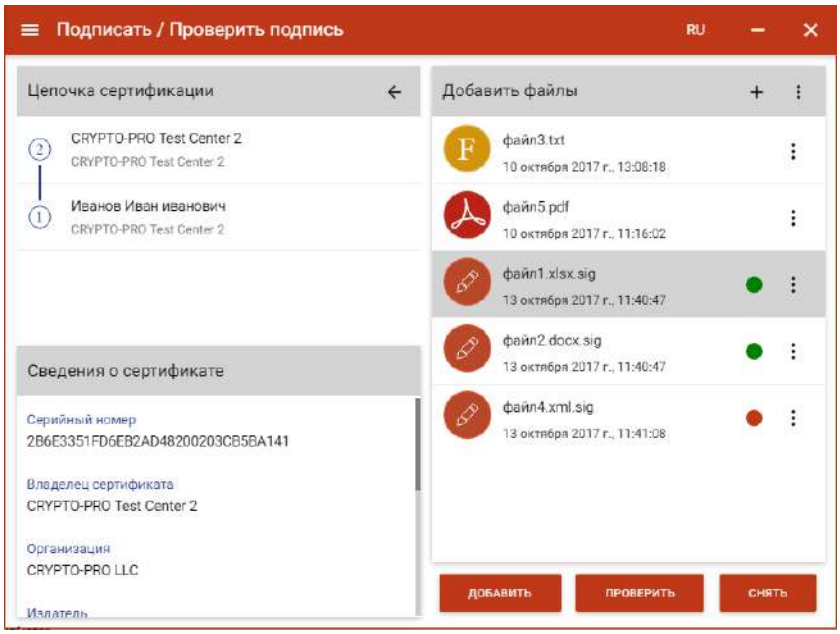


Рис. 8.3.3. Отображение цепочки сертификации подписанного файла

8.4. Снятие электронной подписи

Для снятия подписи достаточно выбрать подписанные файлы - файлы с расширением **.sig**, которые содержат электронную подпись и нажать на кнопку **Снять** (рис. 8.4.1).

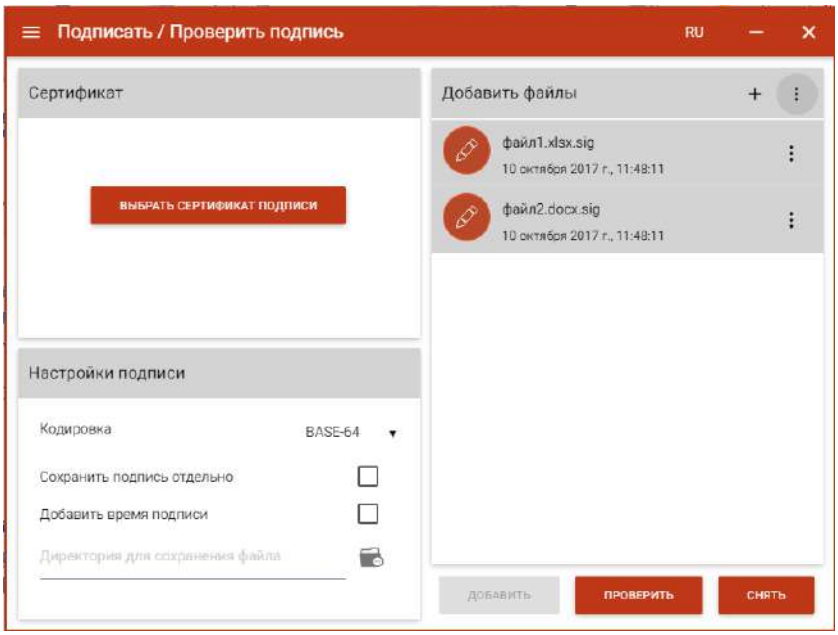


Рис. 8.4.1. Выделенные файлы для снятия подписи

При снятии подписи у файлов меняется иконка, наименование, дата создания. Если в настройках подписи не задан каталог для сохранения файлов, они сохраняются в тех же каталогах, где размещаются исходные подписанные файлы (рис. 8.4.2).

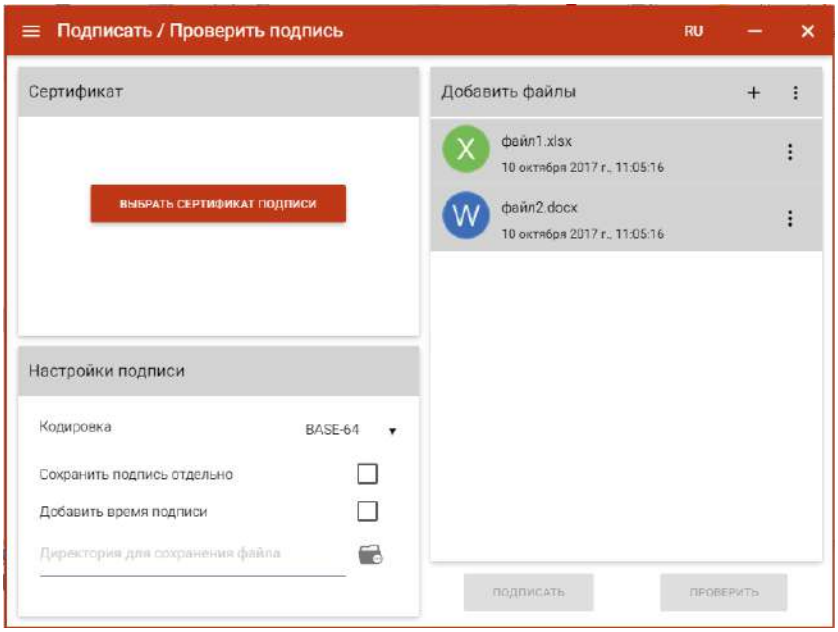


Рис. 8.4.2. Результат снятия подписи с файлов

У отделенной подписи при выполнении операции снятия подписи возникает сообщение об ошибке.

8.5. Добавление подписи

Приложение «Trusted eSign» позволяет добавлять электронные подписи к уже подписанному файлу. Добавление подписи осуществляется по нажатию на кнопку **Добавить** (рис. 8.5.1), при условии, что выбран сертификат подписчика и файлы, содержащие электронную подпись - файлы с расширением **.sig**.

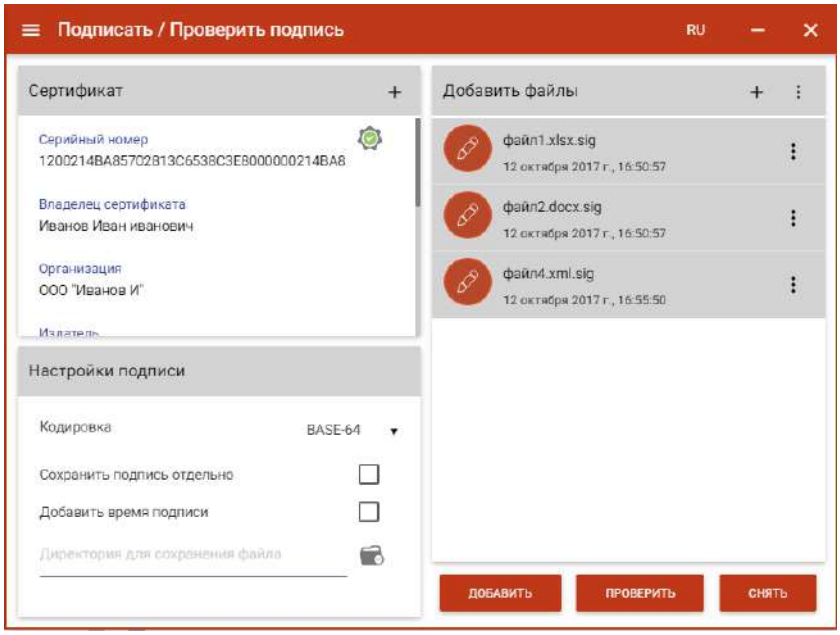


Рис. 8.5.1. Добавление электронной подписи к уже подписанным файлам

Для всех добавленных подписей настройки подписи используются по-умолчанию, как для первой подписи (рис. 8.5.2).

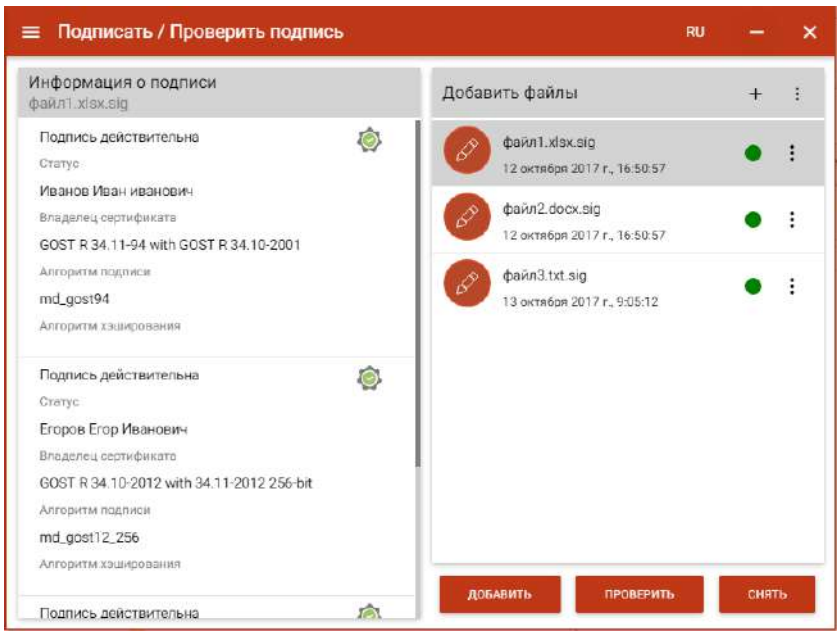


Рис. 8.5.2. Отображение информации о нескольких подписях файла

8.6. Шифрование файлов

Представление мастера шифрования/расшифрования (рис. 8.6.1) имеет три функциональных элемента: слева располагаются области выбора сертификатов получателей, настройки шифрования, справа - область формирования списка файлов для выполнения операций.

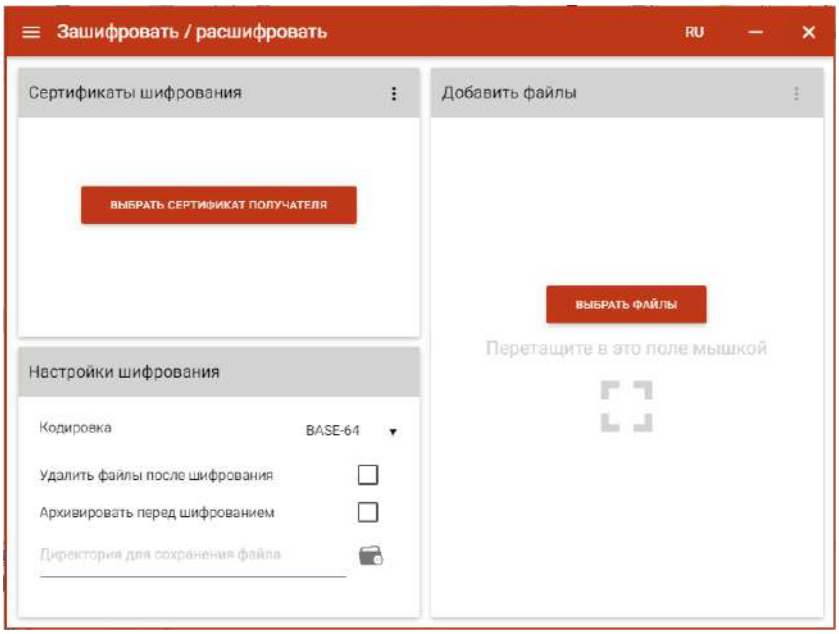


Рис. 8.6.1. Страница шифрования / расшифрования файлов

Выбор шифруемых файлов. В приложении доступно шифрование для одного или группы выбранных файлов. Файлы для шифрования можно добавить двумя способами: через диалог выбора файлов, который откроется после нажатия на кнопку **Выбрать файлы** или перетащив файлы мышкой в область формирования списка файлов для шифрования.

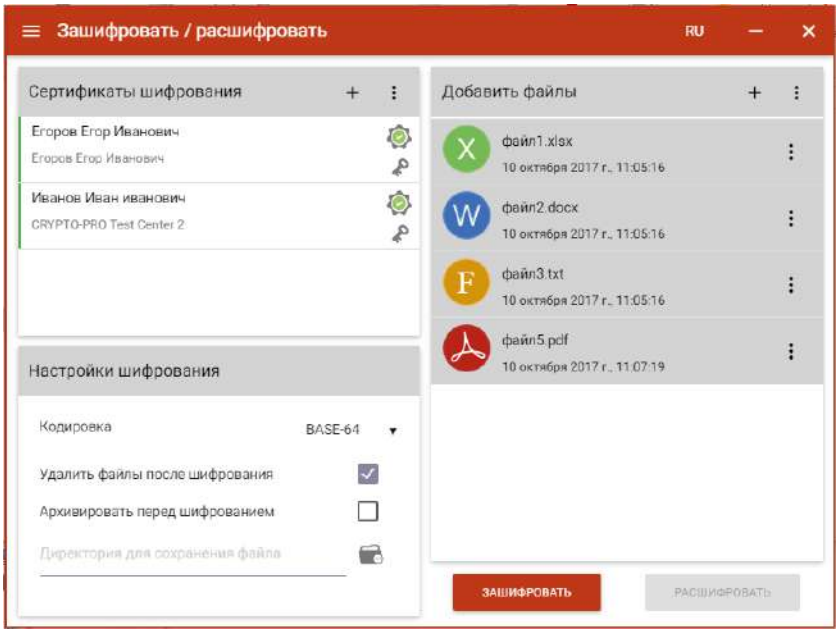


Рис. 8.6.2. Выбор файлов для шифрования

Выбранные файлы заносятся в правую область и представляют собой одноуровневый список. Для данного списка доступно контекстное меню в заголовке функционального элемента (рис. 8.6.3), состоящее из пунктов:

- **Выделить все** - выделяются все добавленные в список файлы;
- **Сбросить выделение** - отменяется выделение всех выбранных в списке файлов;
- **Удалить все из списка** - список очищается. При очистке списке файлы из файловой системы не удаляются.

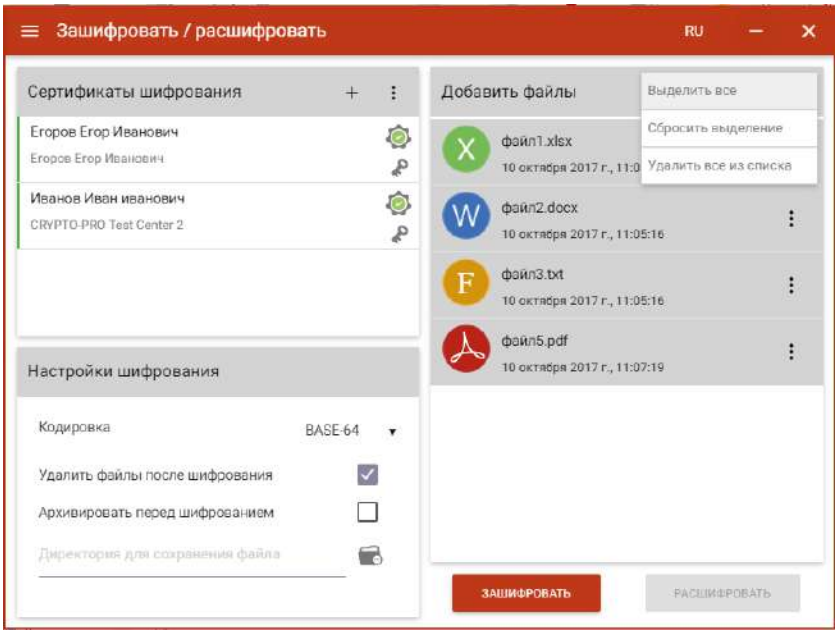


Рис. 8.6.3. Общее меню для выделенной группы файлов

В списке отображается наименование файла с расширением и дата его создания. Для каждого элемента списка доступно контекстное меню (рис. 8.6.4), состоящее из пунктов:

- **Открыть файл** - выполняется открытие файла через приложение, которое ассоциировано с его расширением;
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл;
- **Удалить из списка** - файл удаляется из текущего списка выбранных файлов для шифрования. При выполнении этой операции файл остается в файловой системе в неизменном виде.

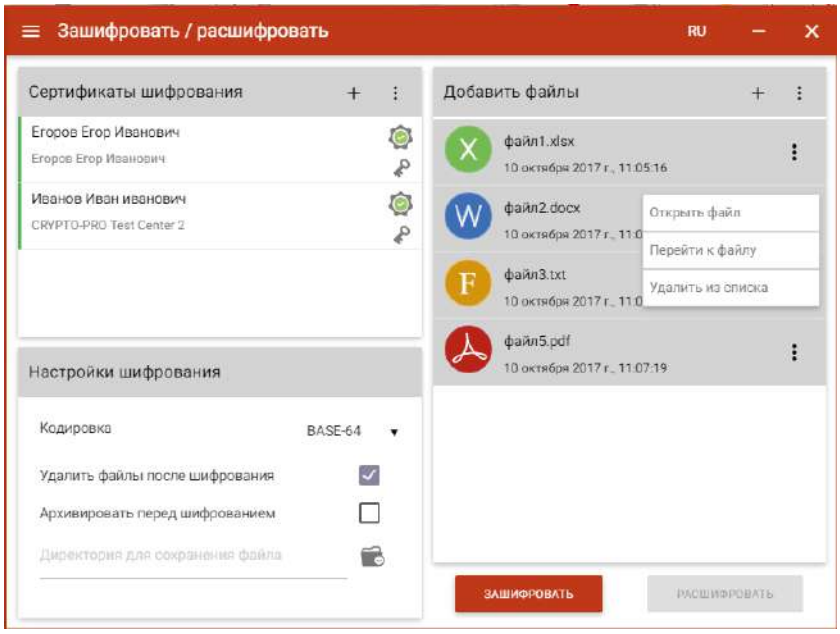


Рис. 8.6.4. Контекстное меню отдельного файла

ВЫБОР СЕРТИФИКАТОВ ПОЛУЧАТЕЛЕЙ. Для того, чтобы выполнить шифрование необходимо выбрать цифровые сертификаты получателей шифрованных файлов (рис. 8.6.5). Выбранные получатели смогут расшифровать файлы, если у них имеется закрытый ключ.

Операция выбора осуществляется нажатием кнопки **Выбрать сертификаты получателей**. В появившемся диалоговом окне отображаются категории, содержащие сертификаты, которые могут использоваться для шифрования. В списке сертификатов допускается выбор нескольких сертификатов, так как число получателей может быть различным.

Выбранные сертификаты получателей перемещаются в правый список и по ним можно посмотреть детальную информацию, выбрав интересующий сертификат в правой области (рис. 8.6.6).

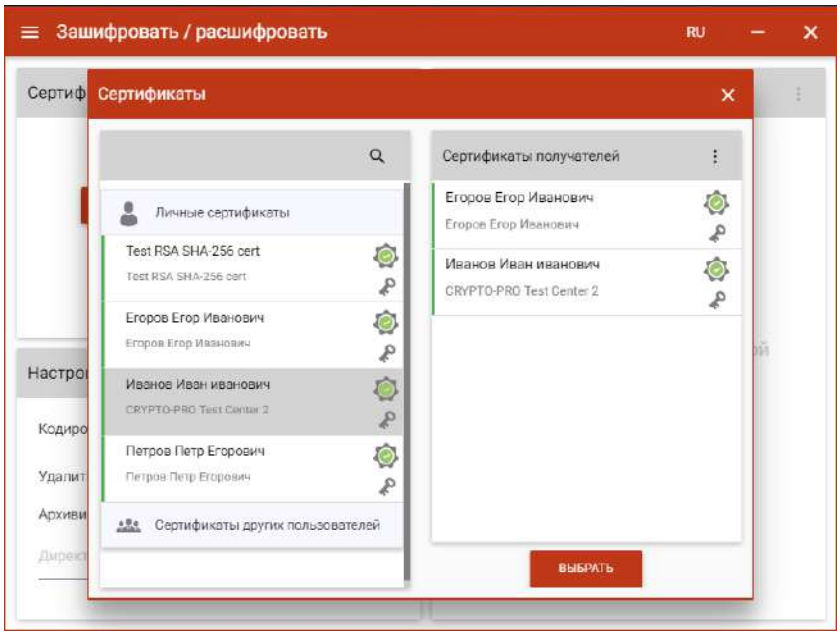


Рис. 8.6.5. Выбор сертификатов получателей

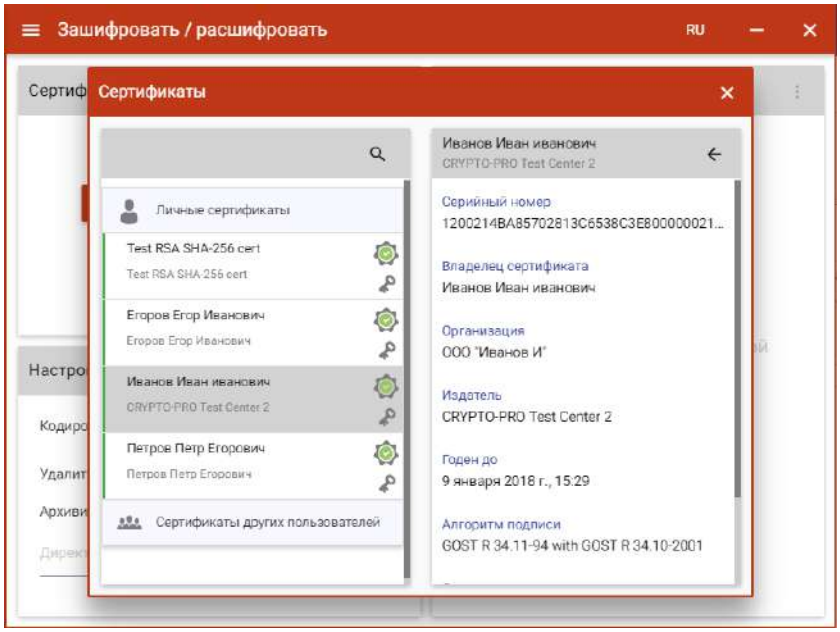


Рис.8.6.6. Детальная информация о сертификате получателя

Удалить сертификаты из списка получателей можно по одному, убирая выделение с сертификата в левом списке, или очистить весь список с помощью контекстного меню в правом списке (рис. 8.6.7).

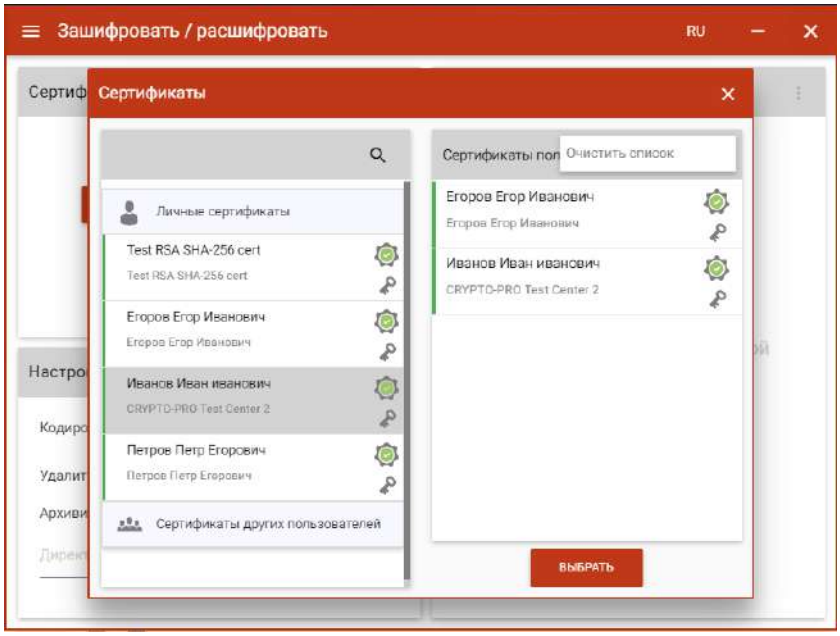


Рис. 8.6.7. Очистка списка сертификатов получателей

Если список сертификатов получателей заполнен, то его можно зафиксировать нажатием на кнопку **Выбрать** (рис. 8.6.8). Допускается изменение списка сертификатов получателей с помощью кнопки и контекстного меню в верхней части элемента.

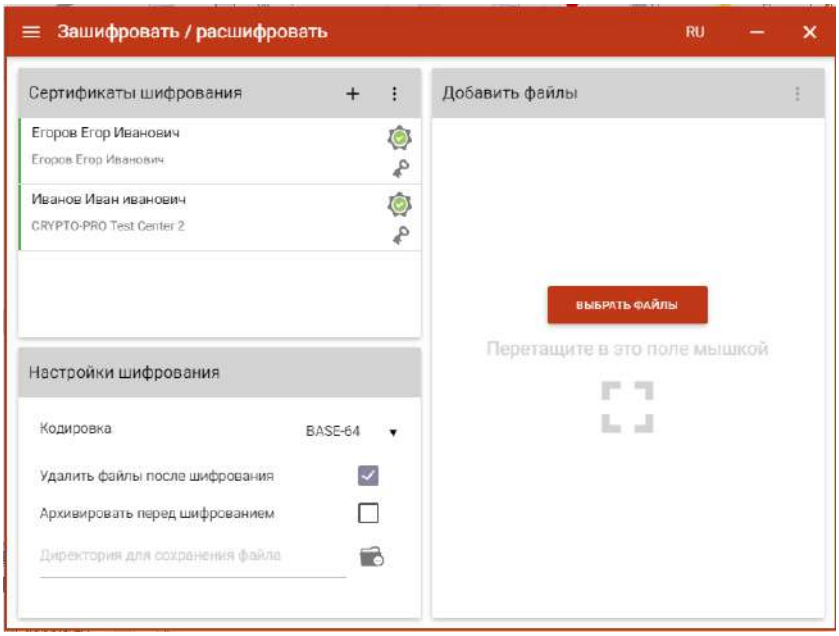


Рис. 8.6.8. Сформированный список получателей

НАСТРОЙКИ ШИФРОВАНИЯ. Настройки шифрования выставляются и сохраняются для последующих аналогичных операций. В области настроек выставляются следующие параметры:

- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования удаляются из файловой системы в случае успешного завершения операции.
- **Архивировать перед шифрованием** - файлы архивируются (ZIP) перед выполнением операции шифрования. Шифруется созданный ZIP-архив.
- **Директория для сохранения файла** - при выбранной директории зашифрованный файл сохраняется в данной директории. В противном случае зашифрованный файл размещается рядом с исходным файлом.

ШИФРОВАНИЕ ФАЙЛОВ. При условии выбора сертификатов получателей и шифруемых файлов в мастере становится доступной кнопка **Зашифровать** (рис. 8.6.9). Нажатие на эту кнопку запускает процесс шифрования. Выбранные файлы шифруются по очереди, если не выбрана опция предварительной архивации. Для шифрованных файлов меняется иконка, наименование, дата создания. Если в настройках подписи не задан каталог для сохранения шифрованных файлов, они сохраняются в тех же каталогах, где размещаются исходные файлы.

Для зашифрованных файлов становится доступна кнопка **Расшифровать**.

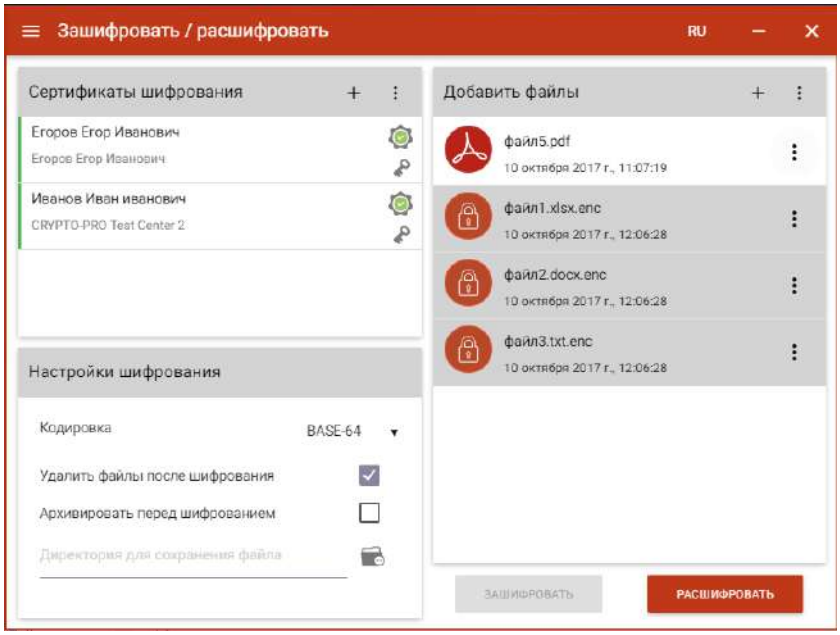


Рис. 8.6.9. Мастер расшифрования файлов

8.7. РАСШИФРОВАНИЕ ФАЙЛОВ

Для расшифрования достаточно выбрать файлы - файлы с расширением **.enc**, и нажать на кнопку **Расшифровать**. Если в хранилище сертификатов не окажется сертификата с закрытым ключом, который был выбран в качестве сертификата получателя при шифровании, расшифрование не будет выполнено.

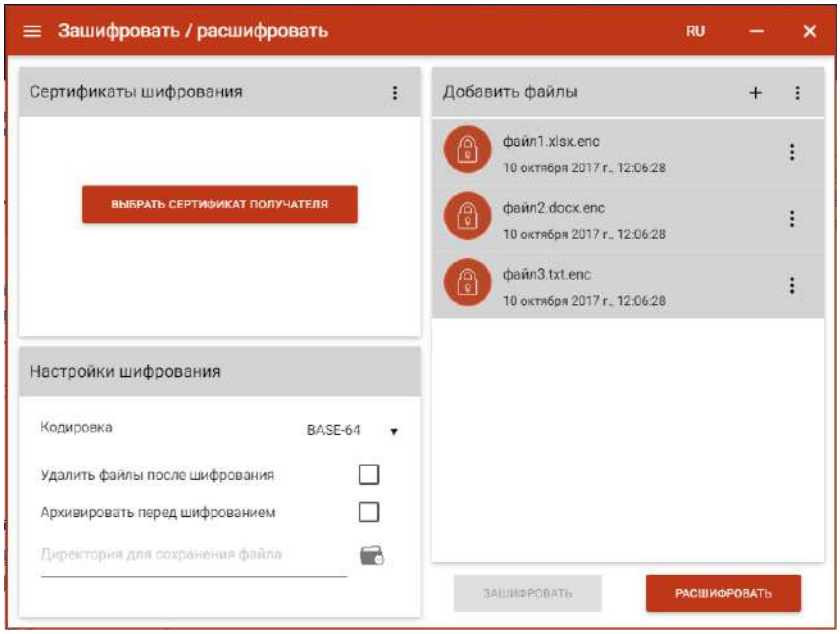


Рис. 8.7.1. Мастер расшифрования файлов

При расшифровании у файлов меняется иконка, наименование, дата создания. Если в настройках шифрования не задан каталог для сохранения файлов, они сохраняются в тех же каталогах, где размещаются исходные зашифрованные файлы.

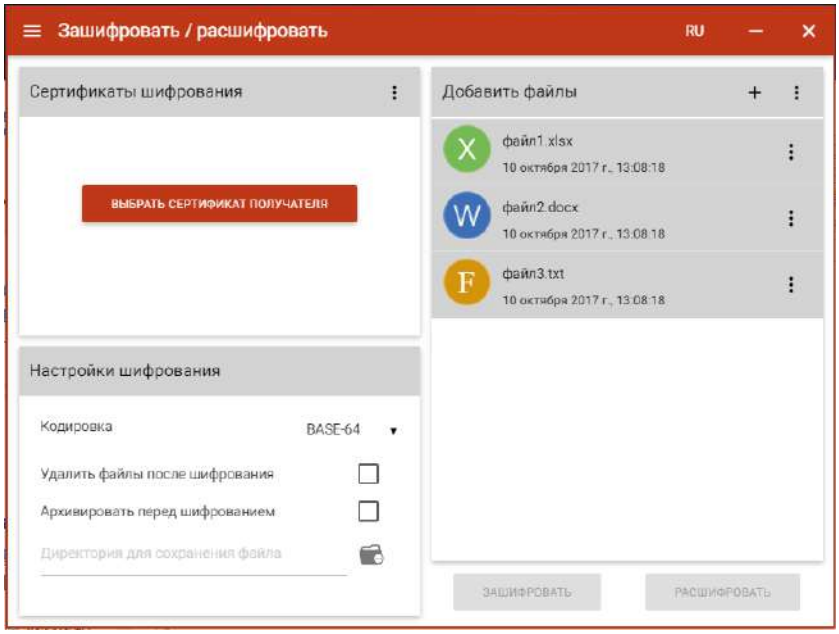


Рис. 8.7.2. Результат операции расшифрования

8.8. Управление сертификатами и ключами

Для управления сертификатами и ключами в приложении добавлено отдельное представление списка сертификатов, которое связано с локальным системным хранилищем. В левой области представления отображаются разделы, соответствующие категориям сертификатов (рис. 8.8.1). В правой области отображается информация о выделенном сертификате.

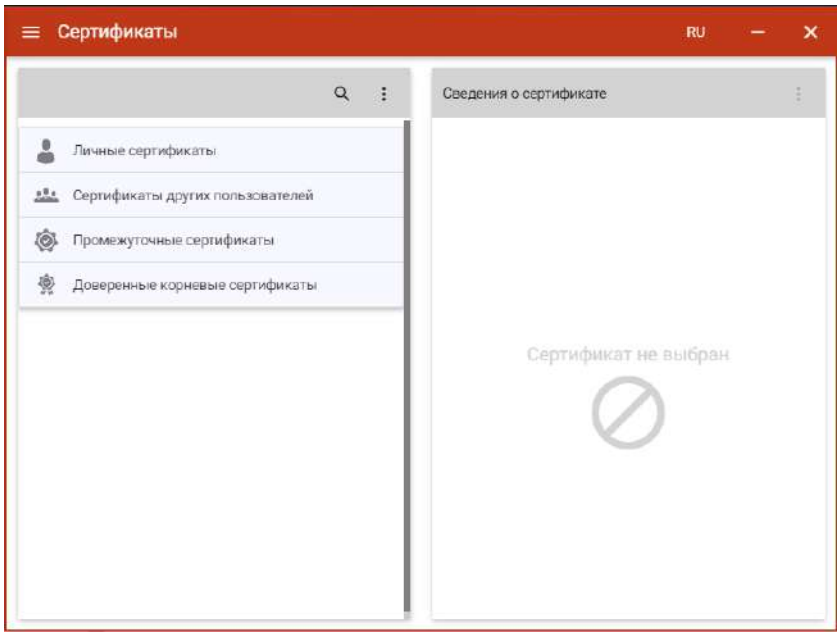


Рис. 8.8.1. Категории сертификатов

В каждой из категорий представления списка сертификатов отображаются сертификаты со всех подключённых хранилищ криптопровайдеров. В случае отсутствия сертификатов по отдельным категориям, они могут быть скрыты как пустые. При отображении списка

сертификатов, они проверяются на корректность (математическая корректность и построение цепочки доверия). Если к сертификату привязан закрытый ключ, то отображается знак ключа. Возможно появление одного из двух статусов проверки сертификата: сертификат корректный, сертификат не корректный.

После выбора сертификата в списке отображается информация о нем (рис. 8.8.2). Информация о сертификате представлена на двух вкладках: **Сведения о сертификате** и **Цепочка сертификации**.

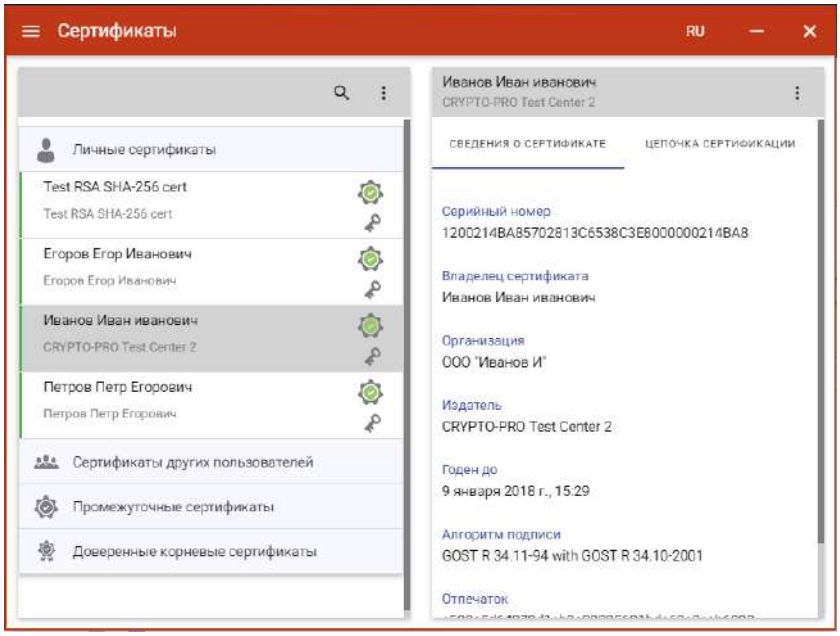


Рис. 8.8.2. Отображение сведений о выбранном сертификате

На вкладке **Цепочка сертификации** отображается общий статус построения цепочки доверия и приводится «дерево» сертификации, как показано на рис. 8.8.3.

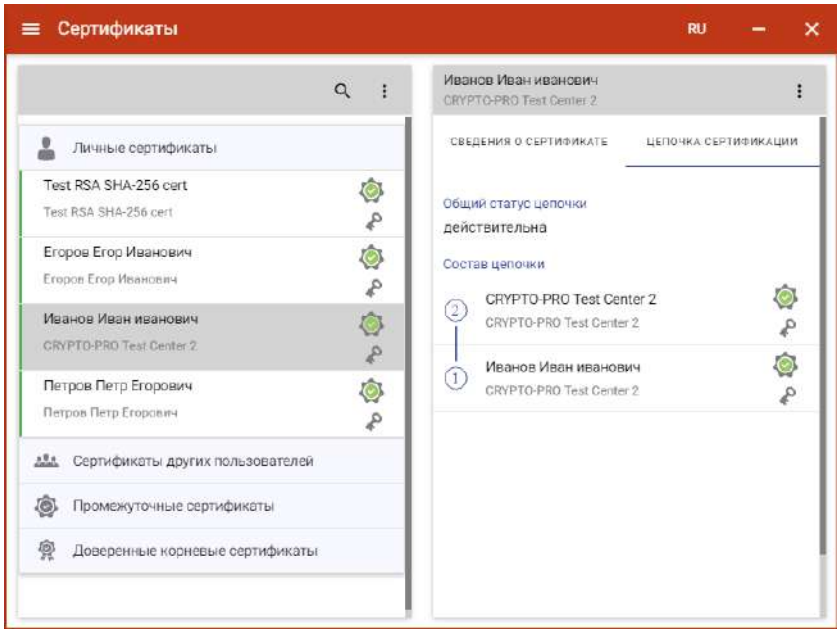


Рис. 8.8.3. Представление цепочки сертификации (цепочки доверия)

ИМПОРТ СЕРТИФИКАТА. Для выполнения импорта нового сертификата в хранилище можно воспользоваться контекстным меню - выбрать операцию **Импортировать сертификат** (рис. 8.8.4). В появившемся диалоговом окне нужно выбрать файл сертификата (поддерживаются кодировки BASE64 и DER).

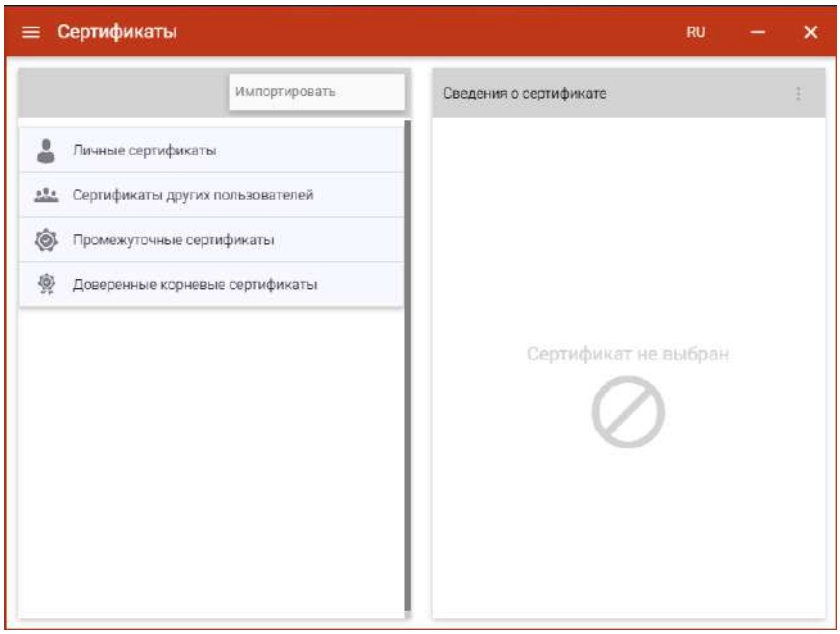


Рис.8.8.4. Меню импорта сертификата

Сертификат при импорте автоматически помещается в соответствующую категорию:

- **Личные сертификаты** – сертификаты, используемые пользователем и связанные с закрытыми ключами;
- **Сертификаты других пользователей** – сертификаты пользователей для обмена шифрованными или подписанными данными;
- **Промежуточные сертификаты** - сертификаты промежуточных центров сертификации;
- **Доверенные корневые сертификаты** - автоматически подписанные сертификаты от центра сертификации, которые неявным образом являются доверенными. Здесь хранятся сертификаты, изданные сторонними удостоверяющими центрами, Microsoft.

Импортированные таким образом сертификаты помещаются в системное хранилище приложения Trusted eSign (рис. 8.8.5).

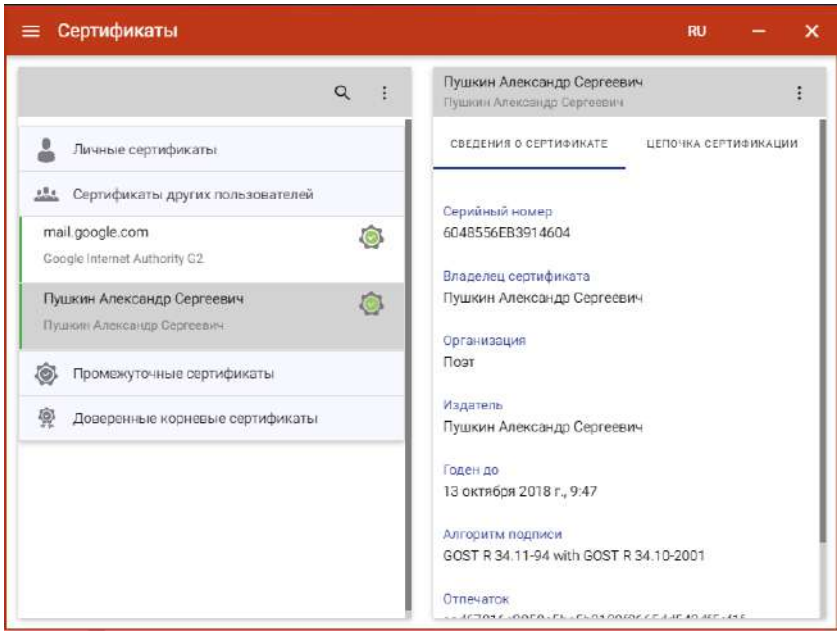


Рис. 8.8.5. Отображение импортированного сертификата

ЭКСПОРТ СЕРТИФИКАТА В ФАЙЛ. Для экспорта сертификата в файл в контекстном меню сертификата нужно выбрать пункт **Экспортировать** (рис. 8.8.6). В появившемся диалогом окне указать путь и имя файла, куда будет сохранен сертификат (по-умолчанию, файл сертификат.pfx).

Примечание. В текущей версии приложения экспорт сертификата с закрытым ключом реализован только для RSA сертификатов.

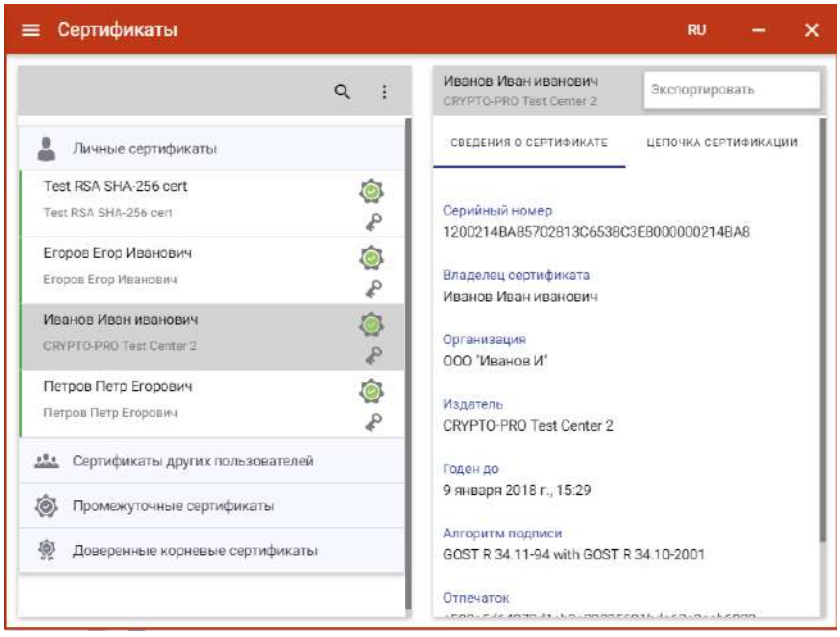


Рис. 8.8.6. Меню экспорта сертификата

Для обеспечения безопасности следует защитить контейнер закрытого ключа паролем, как показано на рис. 8.8.7. По окончании операции возникнет сообщение об успешном экспорте

сертификата. Формат созданного и сохраненного файла - файл обмена личной информацией - PKCS#12 (.PFX).

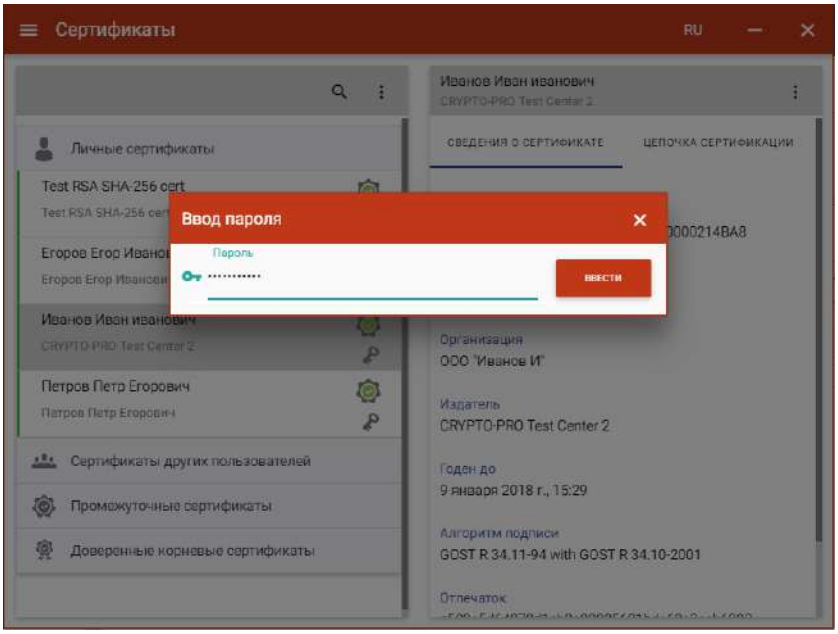


Рис. 8.8.7. Ввод пароля защиты контейнера закрытого ключа

8.9. Поиск сертификата

В элементах пользовательского интерфейса, где процесс выполнения операции учитывает выбор сертификата из списка, реализована функция поиска сертификатов (рис. 8.9.1). Для включения режима поиска нужно нажать на кнопку **Поиск** и в строке поиска ввести ключевую фразу.

Поиск сертификатов реализован на основе совпадения ключевой фразы с любым текстовым свойством сертификата. В результате вместо полного списка в окне остаются только сертификаты, удовлетворяющие критерию поиска.

Чтобы отменить фильтр поиска требуется удалить ключевую фразу или нажать на кнопку Отмена.

Примечание. В случае неправильно указанного критерия поиска список сертификатов может оказаться пусты, о чем будет свидетельствовать надпись - «Сертификаты отсутствуют».

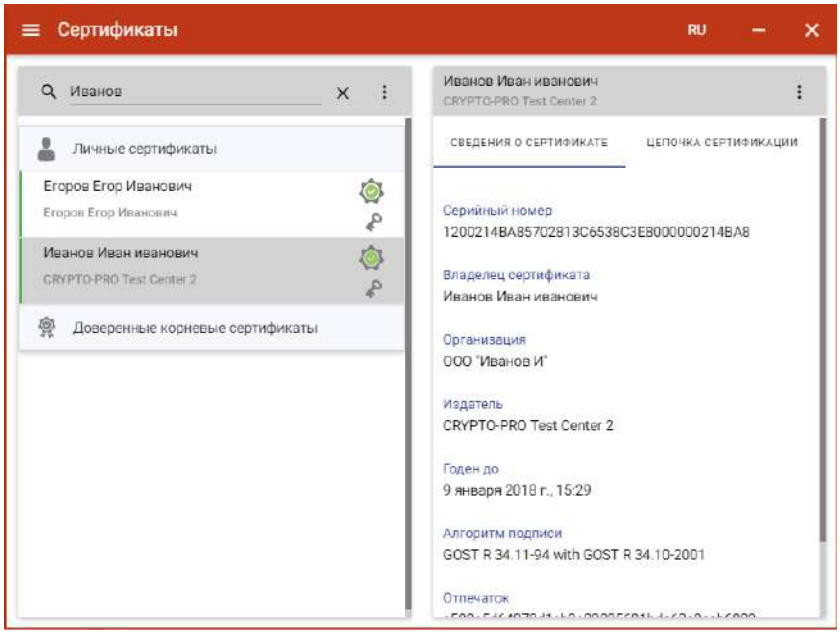


Рис. 8.9.1. Поиск сертификата

8.10. Обратная связь

Для удобства организации обратной связи пользователей приложения и разработчиков в пользовательском интерфейсе имеется пункт **О программе** (рис. 8.10.1). Воспользовавшись формой обратной связи можно задать вопрос или написать сообщение в службу технической поддержки.

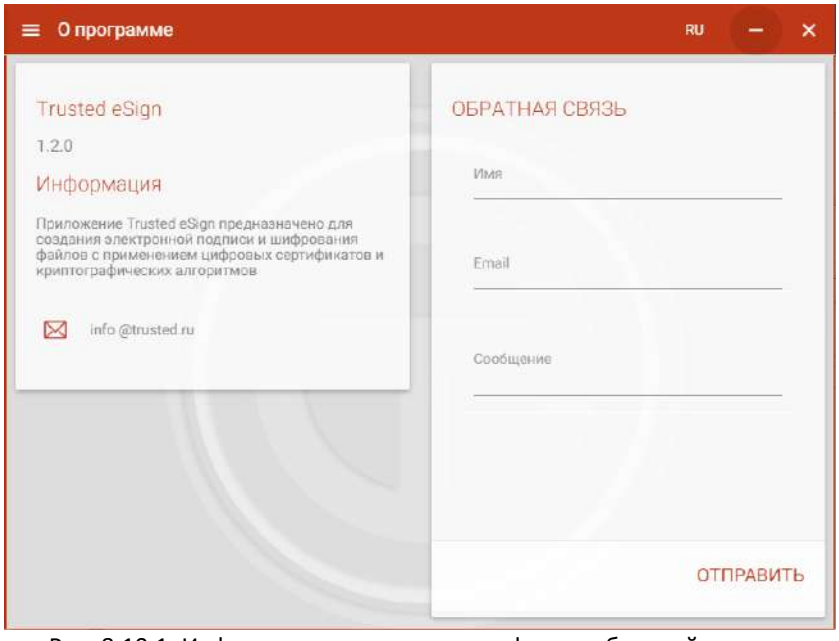


Рис. 8.10.1. Информация о программе и форма обратной связи

8.11. КРАТКАЯ СПРАВОЧНАЯ ПОМОЩЬ

В разделе меню **Справка** пользовательского интерфейса представлено краткое описание возможностей приложения Trusted eSign (рис. 8.11.1).

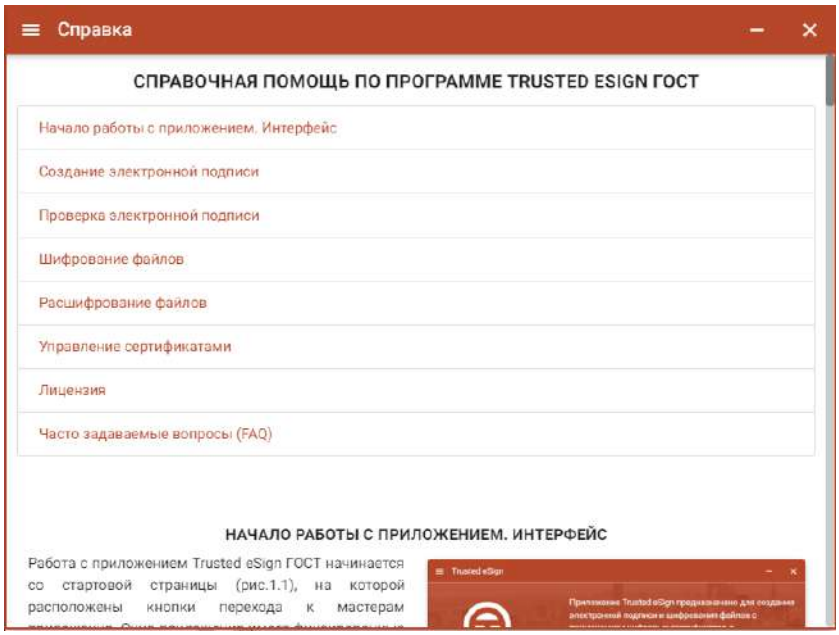


Рис. 8.11.1. Отображение справки по работе с приложением

Команда разработки и сопровождения продукта

Селедкин Андрей Евгеньевич

Менеджер по маркетингу, andrey.selyodkin@digt.ru

Компетенции в рамках проекта: изучение узкого сегмента рынка программных продуктов, формирование стратегии развития продукта, организация испытаний на совместимость продукта, вывод продукта на рынок, презентация продукта.

Чесноков Сергей Евгеньевич

Инженер-программист, shesnokov@gmail.com

Компетенции в рамках проекта: планирование процесса разработки продукта. разработка графического пользовательского интерфейса продукта, разработка ядра продукта, сборка продукта для различных платформ, создание технической и пользовательской документации, техническая поддержка продукта

Гаврилов Александр Владимирович

Инженер-программист, alg@digt.ru

Компетенции в рамках проекта: разработка графического пользовательского интерфейса, разработка внешних модулей для криптографических преобразований, интеграция с криптопропровайдерами, сопровождение репозиториев OpenSource-частей проекта, техническая поддержка продукта.

Шалагина Наталья Владимировна

Специалист по тестированию, nsh@digt.ru

Компетенции в рамках проекта: разработка методик тестирования продукта под различными платформами, создание технической и пользовательской документации, техническая поддержка продукта.

Контактная информация

Компания «Цифровые технологии» – российский разработчик и поставщик программного обеспечения в области защиты информации, телекоммуникаций и Интернет-сервисов.

Направление исследований и создания программных продуктов:

- разработка кроссплатформенных решений в области защиты данных, как в виде отдельных собственных продуктов, так и технологических стеков.
- встраивание российских сертифицированных криптографических алгоритмов в информационные системы, независимо от их бизнес-задачи.
- создание систем авторизации и аутентификации пользователей.
- консалтинг в области использования средств криптографической защиты информации (СКЗИ) в государственной и коммерческой среде.

Особое внимание разработчики компании уделяют внедрению и поддержки отечественных стандартов защиты информации, в том числе сертифицированных продуктов.

В случае необходимости получения дополнительной информации по продукту «Trusted eSign», можно обратиться непосредственно к разработчикам продукта или в службу технической поддержки компании – support@trusted.ru.

Контактная информация:

info@trusted.ru

8 (8362) 33-70-50, 8 (499) 705-91-10, 8 (800) 555-65-81

424033, РМЭ, г. Йошкар-Ола, ул. Петрова, д.1, а/я 67